[+] (IN)SECUREMagazine

07 | 2022

ISSUE 72

Moving forward

7 threat detection challenges CISOs face and what they can do about it

How to set up a powerful insider threat program

An offensive mindset is crucial for effective cyber defense

CUSTOMERS' CHOICE THREE YEARS RUNNING

"Implementing the IT VRM solution was a breeze in OneTrust."

Get The Report

Gartner
Licensed for Distribution
IS THIS CONTENT HELPFUL TO YOU?
YES
NO
Learn how Gartner can help you succeed
Become a Client

Gartner Peer Insights 'Voice of the Customer': IT Vendor Risk Management Tools

Published 2 March 2022 - ID G00763741 - 10 min read

By Peer Contributors

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process in an effort to ensure they are authentic.

What Are IT Vendor Risk Management Tools?

IT vendor risk management (VRM) is the process of ensuring that the use of external IT service providers and other IT vendors (third parties) does not create unacceptable potential for business disruption or have a negative impact on business performance. IT VRM solutions support enterprises that have to assess, monitor and manage their exposure to risks arising from their use of third parties that provide IT products and services or that have access to their information. Some solutions' capabilities extend to fourth parties and subcontractors — a feature increasingly important to customers.

What Is Gartner Peer Insights "Voice of the Customer"?

The "Voice of the Customer" is a document that synthesizes Gartner Peer Insights' reviews into insights for IT decision makers. This aggregated peer perspective, along with the individual detailed reviews, is complementary to Gartner expert research and can play a key role in your buying process, as it focuses on direct peer experiences of implementing and operating a solution. In this document, only vendors with 20 or more eligible published reviews during the specified 18-month submission period are included. Reviews from end users of companies with less than $50M in revenue are excluded from this methodology. See the full "Voice of the Customer" methodology here.

Along with the historical peer-based perspective represented in this document, Gartner has a related expert-led Magic Quadrant for the IT VRM market. For related research in this market, please visit the Magic Quadrant for IT Vendor Risk Management Tools.

In the IT VRM market, Gartner Peer Insights has published 835 reviews and ratings in the 18-month period ending 30 November 2021. Figure 1 shows all eligible vendors categorized into four quadrants based on User Interest and Adoption (X-axis) and Overall Rating (Y-axis). Within each quadrant, vendors are listed in alphabetical order.

Vendors' User Interest and Adoption scores incorporate three factors, each given one-third weight: review volume, user willingness to recommend, and review market coverage across industry, company size, and deployment region. A vendor must meet or exceed the market average User Interest and Adoption Score to qualify for the right-hand quadrants.

The market average Overall Rating is the mean of all eligible vendors' average Overall Ratings. Vendors must meet or exceed the market average Overall Rating to be positioned in the upper quadrants.

For ease of understanding, each quadrant is labeled as described below. **For information on how to evaluate vendors in each quadrant of the "Voice of the Customer" graphic, see the full methodology** here.

Vendors placed in the upper-right quadrant of the "Voice of the Customer" quadrants are
Peer Insights Customers' Choice distinction, denoted with a Customers' Cho
or exceed both the market average Overall Rating and the mark

Vendors placed in the lower-right "Est
average User Interest

OneTrust

PRIVACY, SECURITY & GOVERNANCE

Table of contents

Featured experts

A.N. ANANTH, President, Netsurion

JOHN DeSIMONE, President of Cybersecurity, Intelligence and Services, Raytheon Intelligence & Space

JUAN JONES, Security Engineer, LogDNA

JORDAN LaROSE, Director of Consulting and IR, Americas, WithSecure

HRVOJE MARTINCIC, Senior IT Consultant

SANJAY RAJA, VP of Products, Gurucul

YONI SHOHET, CEO, Valence Security

SIMON WHITBURN, GM and Senior VP of International Business, Exterro

Visit the magazine website and subscribe at www.insecuremag.com

Zeljka Zorz
Editor-In-Chief
press@helpnetsecurity.com

Mirko Zorz
Director of Content
press@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

Review: Hornetsecurity 365 Total Protection Enterprise Backup

Hrvoje Martincic

Senior IT Consultant

Hornetsecurity 365 Total Protection Enterprise Backup is a cloud-based security solution that provides protection against spam, malware, and other advanced threats, combined with backup and recovery features.

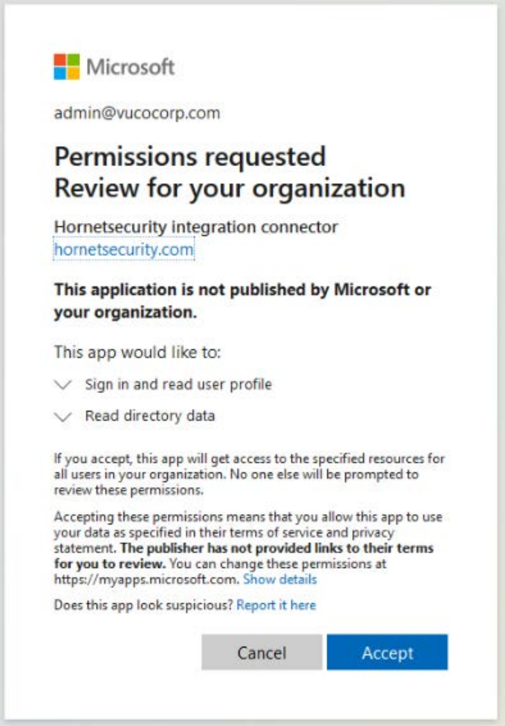
The solution is specifically designed for and fully integrated with Microsoft 365, offering email and data protection to customers. Its main objective is to create a simple, secure, and hassle-free environment.

Installation

It all starts with the onboarding wizard, where you, as the IT admin, must enter the primary domain for your tenants and your global admin credentials to access the Microsoft tenants. The only “manual” part of the process is the transfer of the DNS record. The solution is activated once you finish onboarding and switch the appropriate MX records over to Hornetsecurity.

Hornetsecurity Outlook Add-in

After finishing the initial setup, you can install the Hornetsecurity Outlook Add-in on your users’ Outlook applications. The add-in can be used as a quick tool for classifying information related to “Allow” and “Deny” lists, by reporting messages to



Microsoft

admin@vucocorp.com

Permissions requested
Review for your organization

Hornetsecurity integration connector
hornetsecurity.com

This application is not published by Microsoft or your organization.

This app would like to:

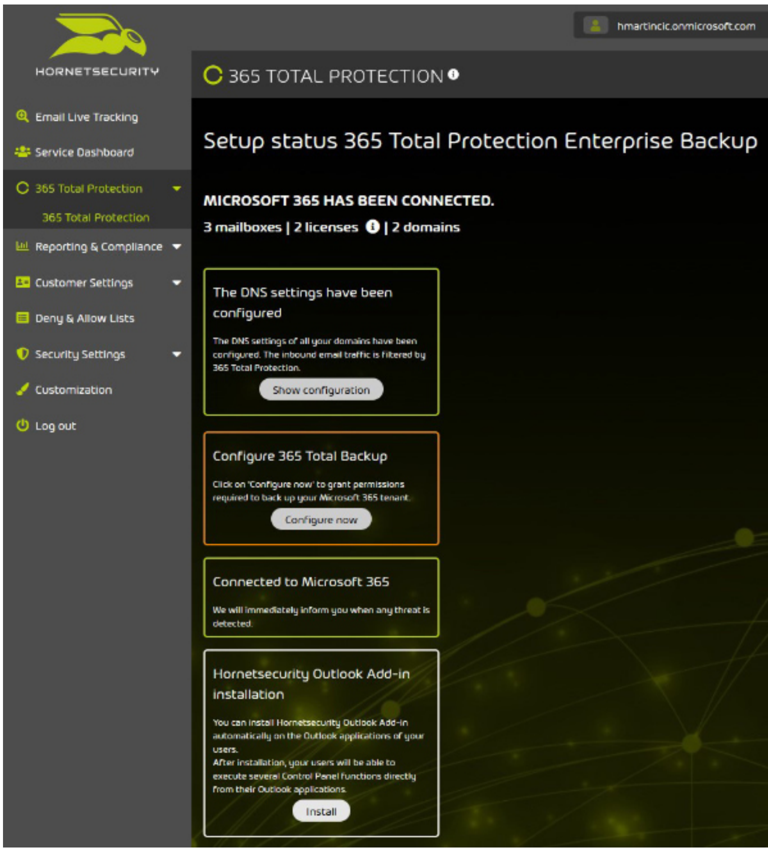
- Sign in and read user profile
- Read directory data

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Figure 1 – Permissions required for the solution to work



Setup status 365 Total Protection Enterprise Backup

MICROSOFT 365 HAS BEEN CONNECTED.

3 mailboxes | 2 licenses | 2 domains

The DNS settings have been configured

The DNS settings of all your domains have been configured. The inbound email traffic is filtered by 365 Total Protection.

Configure 365 Total Backup

Click on 'Configure now' to grant permissions required to back up your Microsoft 365 tenant.

Connected to Microsoft 365

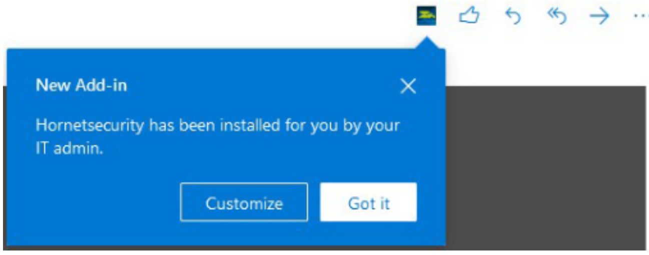
We will immediately inform you when any threat is detected.

Hornetsecurity Outlook Add-in installation

You can install Hornetsecurity Outlook Add-in automatically on the Outlook applications of your users.
After installation, your users will be able to execute several Control Panel functions directly from their Outlook applications.

Figure 2 – Options after finishing the installation

the Control Panel directly. Additionally, it allows administrators to review “Allow” and “Deny” list entries created by each (user) account. Unfortunately, the archive interface (i.e., logging in to the Control Panel) from within Outlook is only available on Windows Outlook clients – it is not supported on Mac or the Outlook web interface.


New Add-in

Hornetsecurity has been installed for you by your IT admin.

Figure 3 – Users get notified of the add-in installation

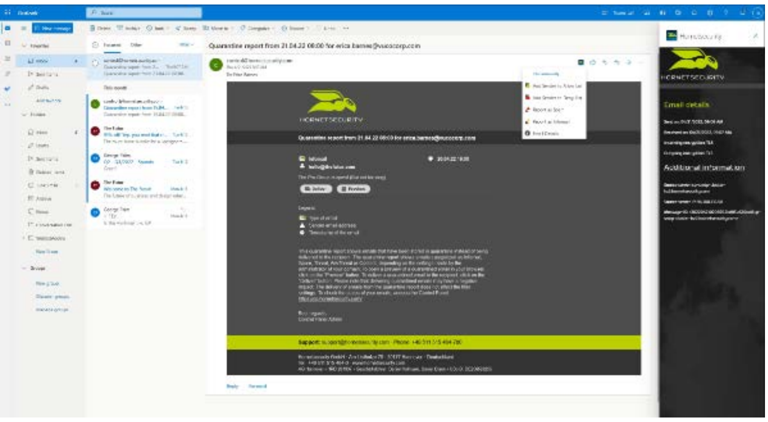
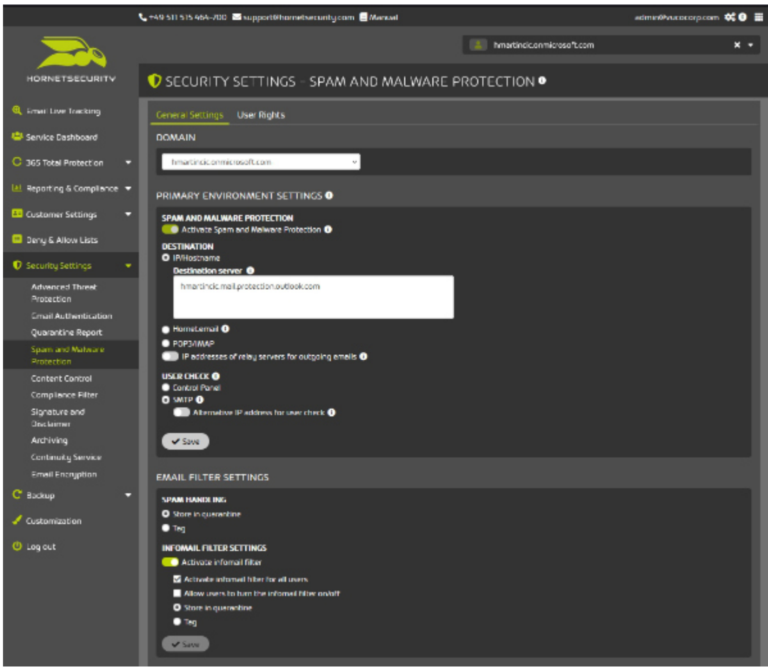


Figure 4 – Add-in options for a quarantine report delivered to a user

Security Settings

This is where all email protection modules are listed and additional services are activated. I will summarize the options that can be fine-tuned.

Though I found the default settings suitable, **Spam and Malware Protection** – the solution’s main service – can be customized. As admin, you may want to look up the available options under “User rights” and give access to (or limit) the options available to your users via the Outlook add-in.



SECURITY SETTINGS - SPAM AND MALWARE PROTECTION

General Settings | User Rights

DOMAIN

hmartincic.onmicrosoft.com

PRIMARY ENVIRONMENT SETTINGS

SPAM AND MALWARE PROTECTION
Activate Spam and Malware Protection

DESTINATION
◉ IP/Hostname
Destination server
hmartincic.mail.protection.outlook.com
○ Hornetemail
○ POP3/IMAP
IP addresses of relay servers for outgoing emails

USER CHECK
○ Control Panel
◉ SMTP
Alternative IP address for user check

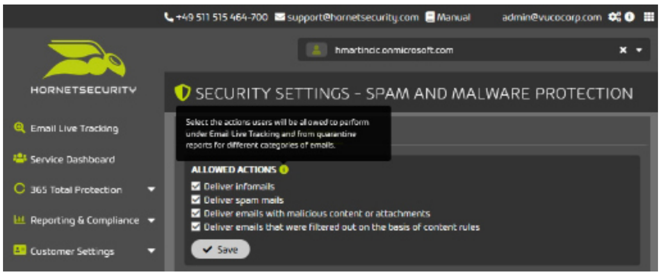
✓ Save

EMAIL FILTER SETTINGS

SPAM HANDLING
◉ Store in quarantine
○ Tag

INFOMAIL FILTER SETTINGS
Activate infomail filter
☑ Activate infomail filter for all users
☐ Allow users to turn the infomail filter on/off
◉ Store in quarantine
○ Tag

✓ Save



SECURITY SETTINGS - SPAM AND MALWARE PROTECTION

Select the actions users will be allowed to perform under Email Live Tracking and from quarantine reports for different categories of emails.

ALLOWED ACTIONS
☑ Deliver infomails
☑ Deliver spam mails
☑ Deliver emails with malicious content or attachments
☑ Deliver emails that were filtered out on the basis of content rules

✓ Save

Figure 5 and 6 – Spam and Malware Protection options

Hornetsecurity recommends activating **Advanced Threat Protection** because it will add multiple elements to help combat the more sophisticated attacks coming via email:

• Real-Time Alert sends notifications to the personnel in charge if emails that were received by users of the domain later turn out to be dangerous

• URL Rewriting will create “click protection” for any links within emails, by replacing them with custom links that will redirect users through the solution’s Web Filter. Any email that went through this process is clean. If it has a link that is weaponized later and the user clicks on it, a rescan of the link is initiated and the user is still protected by the Web Filter

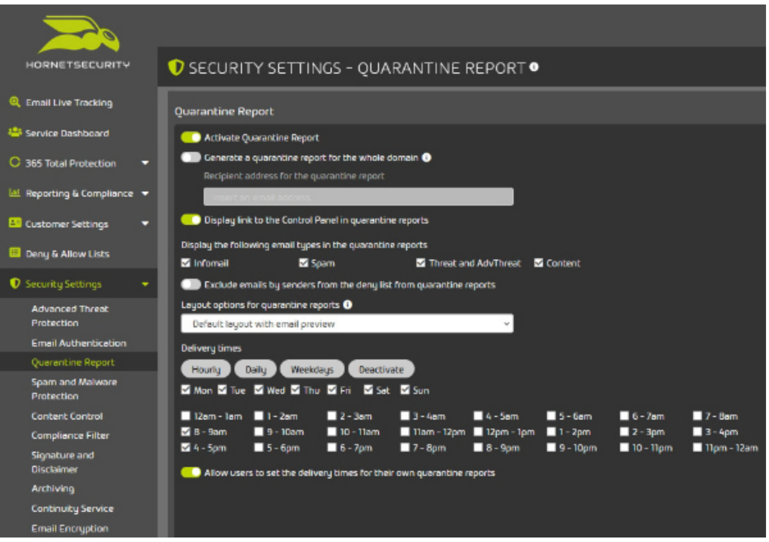
- Targeted Fraud Forensics Filter blocks targeted (personalized) malicious emails without malware or links

Another option you might want to switch on is the Quarantine Report, which can be activated for an entire customer or for specific users.

When **Quarantine Report** is configured for the customer's domain, one of these two options can be selected: either the users will receive and can access the quarantine reports intended for them, or a quarantine report that contains quarantined emails of the whole domain will be sent to an email address specified by the administrator.

After quarantine criteria is configured by the admin, quarantine reports will be created for potentially malicious emails that have been stored in quarantine instead of being delivered to the recipient.

Depending on the settings made by admin, the quarantine report can show emails categorized as Infomail, Spam, Threat, AdvThreat or Content. Users can "release" some categories of emails to themselves without logging in to the Control Panel. Emails classified as Spam and Infomail can be "released" by the users to their own mailbox, while those falling into the Threat, AdvThreat or Content categories cannot, because additional admin review is needed for further action.



SECURITY SETTINGS - QUARANTINE REPORT

Quarantine Report

● Activate Quarantine Report
○ Generate a quarantine report for the whole domain
Recipient address for the quarantine report
Insert an email address
● Display link to the Control Panel in quarantine reports

Display the following email types in the quarantine reports
☑ Infomail ☑ Spam ☑ Threat and AdvThreat ☑ Content

○ Exclude emails by senders from the deny list from quarantine reports

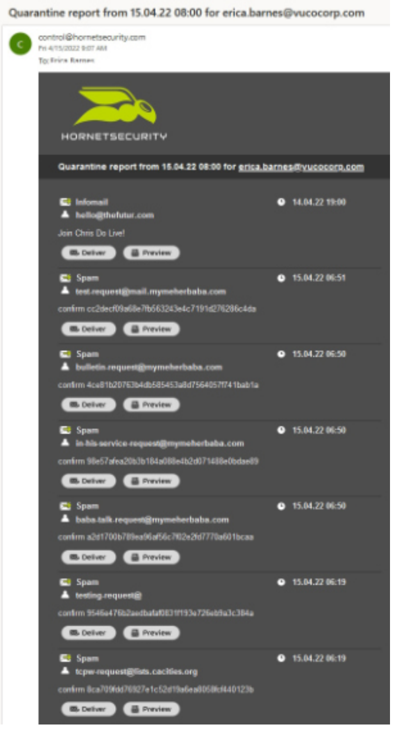
Layout options for quarantine reports
Default layout with email preview

Delivery times
Hourly | Daily | Weekdays | Deactivate
☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

☐ 12am - 1am ☐ 1 - 2am ☐ 2 - 3am ☐ 3 - 4am ☐ 4 - 5am ☐ 5 - 6am ☐ 6 - 7am ☐ 7 - 8am
☑ 8 - 9am ☐ 9 - 10am ☐ 10 - 11am ☐ 11am - 12pm ☐ 12pm - 1pm ☐ 1 - 2pm ☐ 2 - 3pm ☐ 3 - 4pm
☑ 4 - 5pm ☐ 5 - 6pm ☐ 6 - 7pm ☐ 7 - 8pm ☐ 8 - 9pm ☐ 9 - 10pm ☐ 10 - 11pm ☐ 11pm - 12am

● Allow users to set the delivery times for their own quarantine reports

Figure 7 – IT admins' choices for the Quarantine Report option


Quarantine report from 15.04.22 08:00 for erica.barnes@vucocorp.com

control@hornetsecurity.com
Fri 4/15/2022 9:07 AM
To: Erica Barnes

Quarantine report from 15.04.22 08:00 for erica.barnes@vucocorp.com

Infomail 14.04.22 19:00
hello@thefutur.com
Join Chris Do Live!
Deliver | Preview

Spam 15.04.22 06:51
test.request@mail.mymeherbaba.com
confirm cc2decf09a68e7fb563243e4c7191d276286c4da
Deliver | Preview

Spam 15.04.22 06:50
bulletin.request@mymeherbaba.com
confirm 4ca81b20763b4db585453a8d7564057f741bab1a
Deliver | Preview

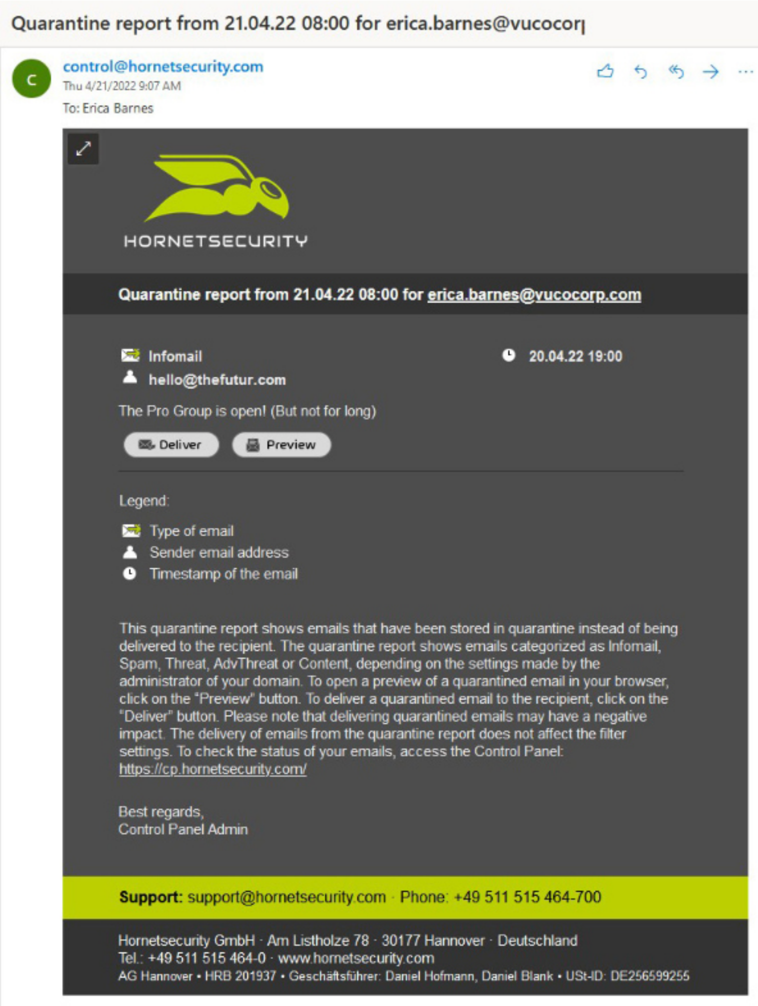
Spam 15.04.22 06:50
in-his-service-request@mymeherbaba.com
confirm 98e57afea20b3b184a088e4b2d071488e0bdae89
Deliver | Preview

Spam 15.04.22 06:50
baba.talk.request@mymeherbaba.com
confirm a2d1700b789ea96af56c7f02e2fd7770a601bcaa
Deliver | Preview

Spam 15.04.22 06:19
testing.request@
confirm 9546e476b2aedbafaf0831f193a726ab9a3c384a
Deliver | Preview

Spam 15.04.22 06:19
tcpw-request@lists.cacities.org
confirm 8ca709fdd76927e1c52d19a6ea8058fd440123b
Deliver | Preview

Figure 8 – A general quarantine report delivered to a user


Quarantine report from 21.04.22 08:00 for erica.barnes@vucocor|

control@hornetsecurity.com
Thu 4/21/2022 9:07 AM
To: Erica Barnes

Quarantine report from 21.04.22 08:00 for erica.barnes@vucocorp.com

Infomail 20.04.22 19:00
hello@thefutur.com
The Pro Group is open! (But not for long)
Deliver | Preview

Legend:
Type of email
Sender email address
Timestamp of the email

This quarantine report shows emails that have been stored in quarantine instead of being delivered to the recipient. The quarantine report shows emails categorized as Infomail, Spam, Threat, AdvThreat or Content, depending on the settings made by the administrator of your domain. To open a preview of a quarantined email in your browser, click on the "Preview" button. To deliver a quarantined email to the recipient, click on the "Deliver" button. Please note that delivering quarantined emails may have a negative impact. The delivery of emails from the quarantine report does not affect the filter settings. To check the status of your emails, access the Control Panel: https://cp.hornetsecurity.com/

Best regards,
Control Panel Admin

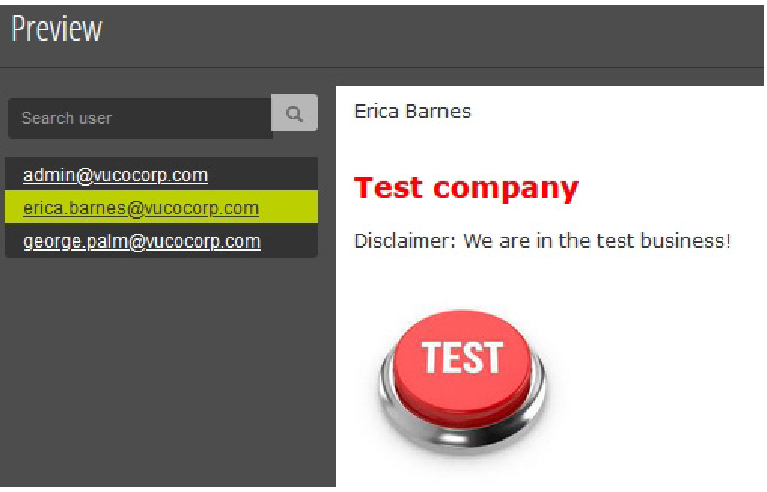
Support: support@hornetsecurity.com · Phone: +49 511 515 464-700

Hornetsecurity GmbH · Am Listholze 78 · 30177 Hannover · Deutschland
Tel.: +49 511 515 464-0 · www.hornetsecurity.com
AG Hannover • HRB 201937 • Geschäftsführer: Daniel Hofmann, Daniel Blank • USt-ID: DE256599255

Figure 9 – A specific quarantine report delivered to a user

The **Signature and Disclaimer** feature enables the admin to set up email signatures and disclaimers across the domain for all users. Different signatures and disclaimers can be set up for various inter-organizational groups (e.g., different departments, regional offices, and so on).

New signature/disclaimer entries can be created via the embedded HTML editor and data can be pulled from Azure AD. Admins can also embed banners, links, images, social media icons, etc. Once a signature/ disclaimer entry is created, admins can preview how it's going to look like before applying it to domains, users or a specific group.



Preview

Search user

admin@vucocorp.com
erica.barnes@vucocorp.com
george.palm@vucocorp.com

Erica Barnes

Test company

Disclaimer: We are in the test business!

Figure 10 – A preview of a custom signature and disclaimer

Several methods for **Email Encryption** are offered:

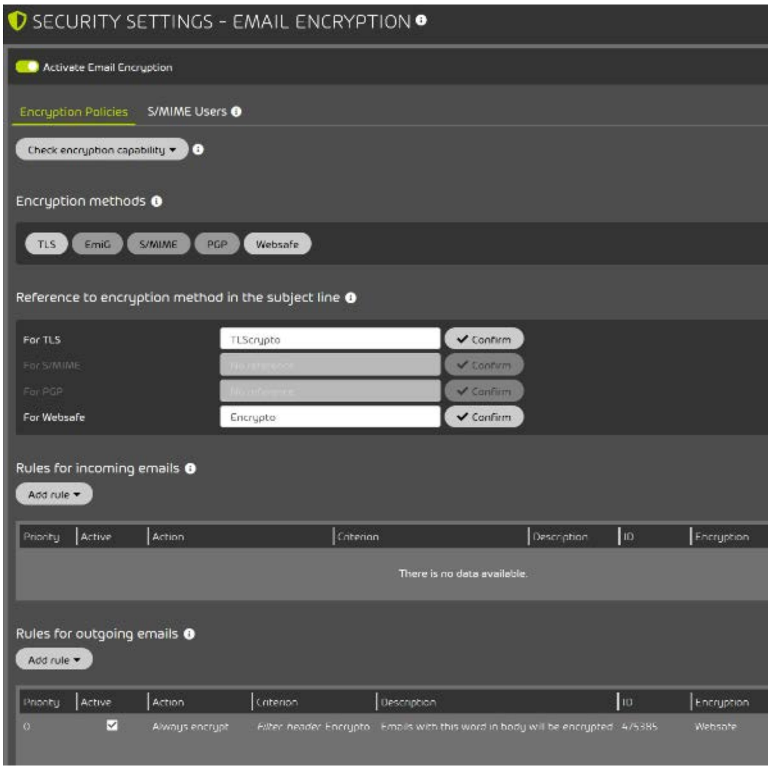
- TLS (Transport Layer Security) – Encrypts emails between the outgoing and incoming mail server **(always activated)**

- EmiG (E-Mail made in Germany) – A form of TLS encryption with requirements for the TÜV-certified communication partners, their server security and the certificates used for encryption

- S/MIME – A standard for encrypting and signing MIME emails. The certificate authority (CA) assures the validity of the email address and sender's name

- PGP (Pretty Good Privacy) – An asymmetric encryption standard using public and private keys

- Websafe – Allows users to send encrypted emails to recipients who do not support any other supported encryption methods



SECURITY SETTINGS - EMAIL ENCRYPTION

Activate Email Encryption

Encryption Policies | S/MIME Users

Check encryption capability ▾

Encryption methods

TLS | EmiG | S/MIME | PGP | Websafe

Reference to encryption method in the subject line

For TLS	TLScrypto	✓ Confirm
For S/MIME	No reference	✓ Confirm
For PGP	No reference	✓ Confirm
For Websafe	Encrypto	✓ Confirm

Rules for incoming emails

Add rule ▾

Priority	Active	Action	Criterion	Description	ID	Encryption
There is no data available.						

Rules for outgoing emails

Add rule ▾

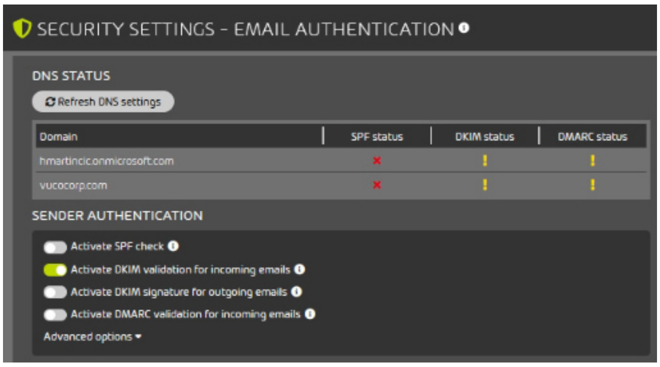
Priority	Active	Action	Criterion	Description	ID	Encryption
0	☑	Always encrypt	Filter header: Encrypto	Emails with this word in body will be encrypted	475385	Websafe

Figure 11 – Email Encryption options

Hornetsecurity says that, in their experience, customers mainly use the TLS and Websafe options.

When using Websafe, the emails are sent to a portal (and stored there for 3 months). The recipients receive an email with credentials to access the portal. Registration is completed after the recipients enter a PIN (delivered via phone), a password and the answer to a security question. Once created, the account is valid for all future emails received through the Websafe portal.

Depending on your preferred email setup, additional **Email Authentication** methods (SPF, DKIM, DMARC) can be enabled:



SECURITY SETTINGS - EMAIL AUTHENTICATION

DNS STATUS

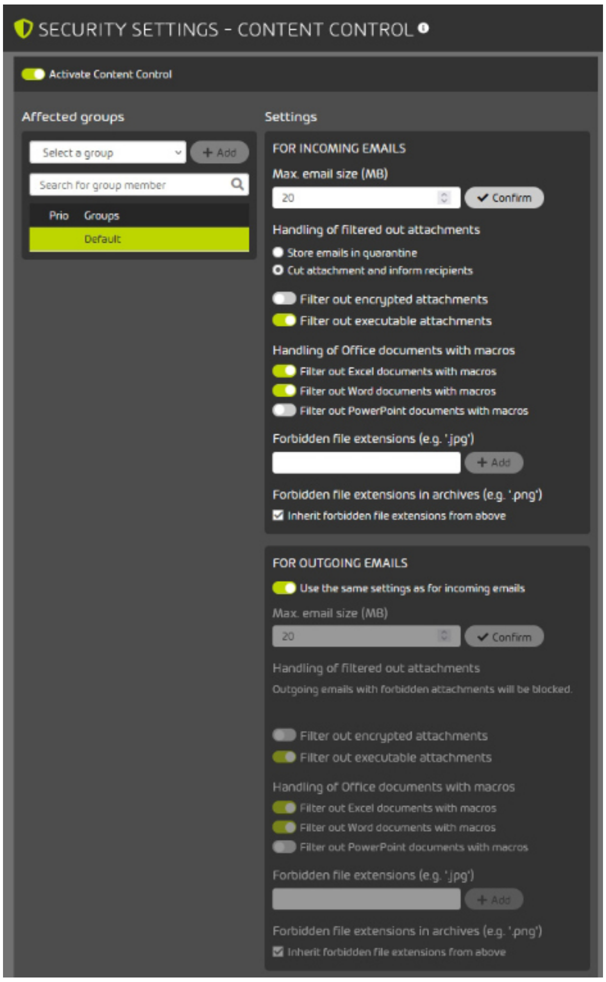
Domain	SPF status	DKIM status	DMARC status
hmartincic.onmicrosoft.com	✗	!	!
vucocorp.com	✗	!	!

SENDER AUTHENTICATION

- ☐ Activate SPF check
- ☑ Activate DKIM validation for incoming emails
- ☐ Activate DKIM signature for outgoing emails
- ☐ Activate DMARC validation for incoming emails

Figure 12 – Email Authentication options

The Security Settings also include options for **Content Control** for incoming and outgoing emails. Admins can set email size limits, filter out executable or encrypted attachments, Office documents with macros, etc.



SECURITY SETTINGS - CONTENT CONTROL

☑ Activate Content Control

Affected groups

Prio	Groups
	Default

Settings

FOR INCOMING EMAILS

Max. email size (MB): 20

Handling of filtered out attachments

- ● Store emails in quarantine
- ○ Cut attachment and inform recipients

- ☐ Filter out encrypted attachments
- ☑ Filter out executable attachments

Handling of Office documents with macros

- ☑ Filter out Excel documents with macros
- ☑ Filter out Word documents with macros
- ☐ Filter out PowerPoint documents with macros

Forbidden file extensions (e.g. '.jpg')

Forbidden file extensions in archives (e.g. '.png')

☑ Inherit forbidden file extensions from above

FOR OUTGOING EMAILS

☑ Use the same settings as for incoming emails

Max. email size (MB): 20

Handling of filtered out attachments

Outgoing emails with forbidden attachments will be blocked.

- ☐ Filter out encrypted attachments
- ☑ Filter out executable attachments

Handling of Office documents with macros

- ☑ Filter out Excel documents with macros
- ☑ Filter out Word documents with macros
- ☐ Filter out PowerPoint documents with macros

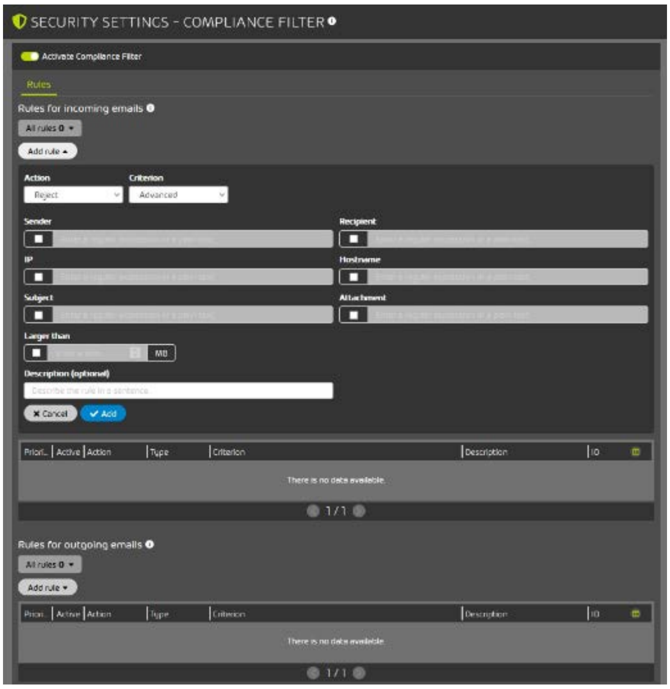
Forbidden file extensions (e.g. '.jpg')

Forbidden file extensions in archives (e.g. '.png')

☑ Inherit forbidden file extensions from above

Figure 13 – Content Control options

Additional filtering rules can be created via the **Compliance Filter** to classify incoming emails as Clean, Spam or Threat. Admins can also make it so that specific emails are rejected, redirected through a different server, or forwarded to other recipients.



SECURITY SETTINGS - COMPLIANCE FILTER

☑ Activate Compliance Filter

Rules for incoming emails

Action: Reject

Criterion: Advanced

Sender ☐

Recipient ☐

IP ☐

Hostname ☐

Subject ☐

Attachment ☐

Larger than ☐ MB

Description (optional): Describe the rule in a sentence.

Priori...	Active	Action	Type	Criterion	Description	ID
There is no data available.						

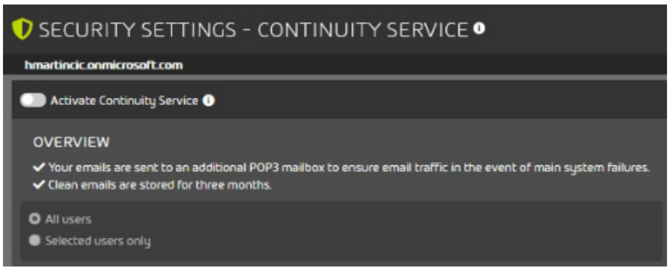
Rules for outgoing emails

Priori...	Active	Action	Type	Criterion	Description	ID
There is no data available.						

Figure 14 - Compliance Filter options

Archiving: After the service is activated, from that point on all received and sent emails on the connected domain are archived for 10 years. The option can be deactivated for individual domains, groups and/or users. By adding an exception, the archiving period can also be changed, or archiving entirely deactivated.

Continuity Service allows users to continue to receive and send emails even if the email server fails. This could come in handy during disaster recovery.



SECURITY SETTINGS - CONTINUITY SERVICE

hmartincic.onmicrosoft.com

☐ Activate Continuity Service

OVERVIEW

✓ Your emails are sent to an additional POP3 mailbox to ensure email traffic in the event of main system failures.
✓ Clean emails are stored for three months.

- ○ All users
- ● Selected users only

Figure 15 – Continuity Service options

Reporting and Compliance

In this tab, admins can view and generate **Email Statistics** according to specified criteria, see a report of attempted attacks during a specified time frame via **Threat Live Report**, and track user activities in the Control Panel via **Auditing 2.0.**

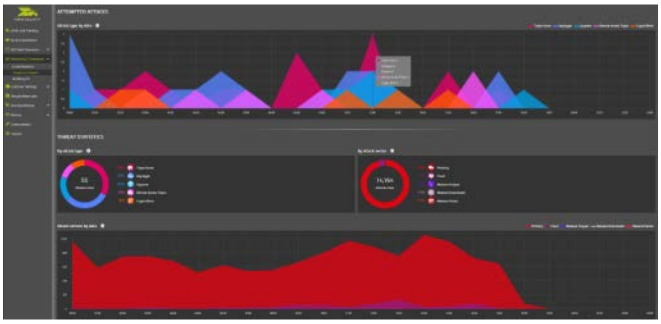


Figure 16 - Threat Live Report

365 Total Backup

This solution provides backup and recovery for Microsoft 365 mailboxes, OneDrive accounts, SharePoint document libraries, Teams chats, and Windows-based endpoints. Storage is provided and maintained by Hornetsecurity and is unlimited in size with a “forever” retention period (i.e., until deleted by the user). Due to the possible sensitive nature of the backed-up data, Hornetsecurity offers full GDPR compliance, with an additional layer of security: the data stored on the company’s servers is encrypted using AES-256 encryption.

The following data is backed up:

• Mailbox: Emails, calendar entries, contact addresses

• OneDrive: All files stored in the user’s OneDrive for Business account

• Teams Chats: Teams chats for users and groups within your organization, including any files that are shared during the conversations

• SharePoint: Files and communication in SharePoint document libraries, along with access permissions

The Data Restore function supports the following scenarios:

• Data can be restored to the original mailbox/ OneDrive account/SharePoint site

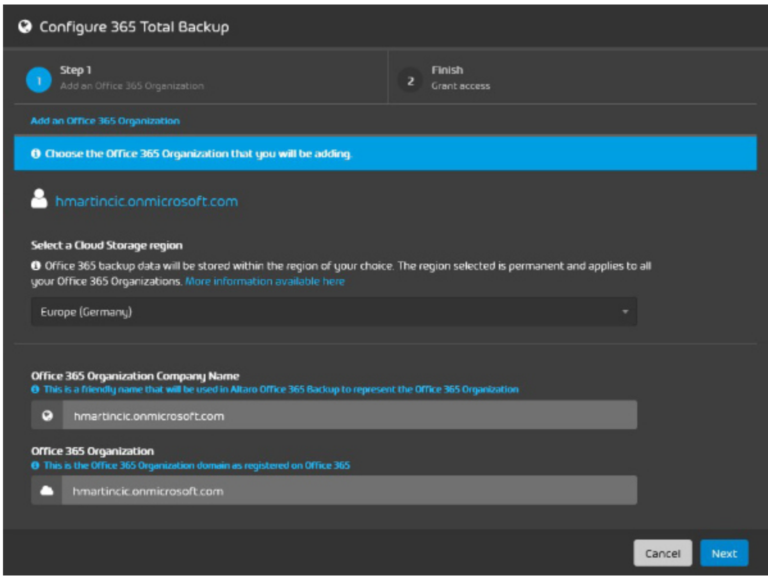
• Data can be restored to a different mailbox/ OneDrive account/SharePoint site within the same or in a different organization belonging to the same customer

• Data can be restored to a ZIP archive, which can then be downloaded

• Data can be restored as a **PST file** (this option is available only for mailboxes)

• Microsoft 365 Teams chats can be restored to a new team within Microsoft Teams or restored to HTML files, which can then be downloaded

• By using **Granular Restore**, the admin can select specific elements inside a specific backup snapshot to be restored or downloaded (a download link to the password-protected restored content will be sent via email)



Configure 365 Total Backup

1 Step 1
Add an Office 365 Organization

2 Finish
Grant access

Add an Office 365 Organization

Choose the Office 365 Organization that you will be adding.

hmartincic.onmicrosoft.com

Select a Cloud Storage region

Office 365 backup data will be stored within the region of your choice. The region selected is permanent and applies to all your Office 365 Organizations. More information available here

Europe (Germany)

Office 365 Organization Company Name

This is a friendly name that will be used in Altaro Office 365 Backup to represent the Office 365 Organization

hmartincic.onmicrosoft.com

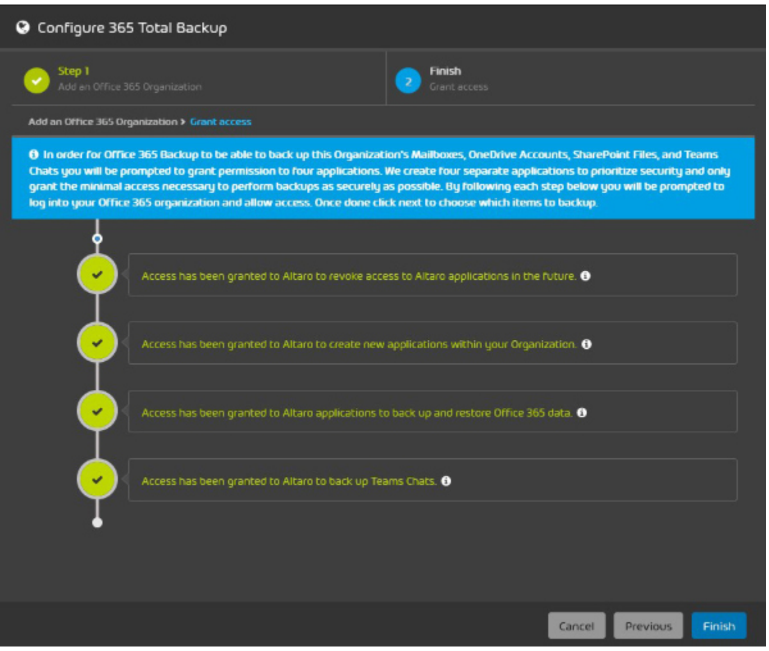
Office 365 Organization

This is the Office 365 Organization domain as registered on Office 365

hmartincic.onmicrosoft.com

Figure 17 – The information required for configuring 365 Total Backup

In my test, the activation of 365 Total Backup went without a hitch. The information you must provide is minimal and you must grant access and permissions to Altaro Office 365 Backup (Hornetsecurity acquired Altaro, a company that specialises in backup and recovery software, in 2021.)


Configure 365 Total Backup

Step 1 – Add an Office 365 Organization
2 Finish – Grant access

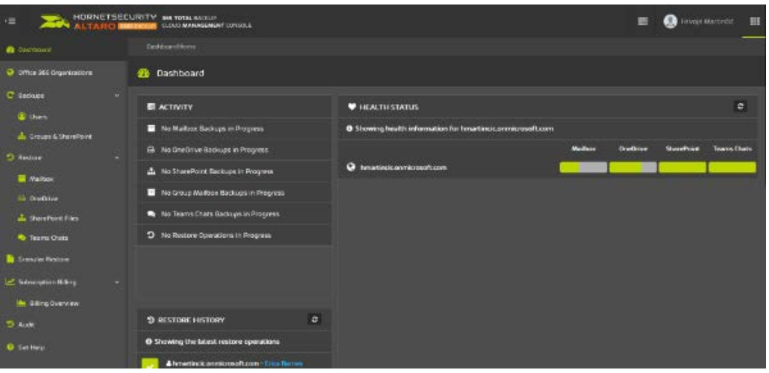
Add an Office 365 Organization > Grant access

In order for Office 365 Backup to be able to back up this Organization's Mailboxes, OneDrive Accounts, SharePoint Files, and Teams Chats you will be prompted to grant permission to four applications. We create four separate applications to prioritize security and only grant the minimal access necessary to perform backups as securely as possible. By following each step below you will be prompted to log into your Office 365 organization and allow access. Once done click next to choose which items to backup.

- Access has been granted to Altaro to revoke access to Altaro applications in the future.
- Access has been granted to Altaro to create new applications within your Organization.
- Access has been granted to Altaro applications to back up and restore Office 365 data.
- Access has been granted to Altaro to back up Teams Chats.

Figure 18 – Granting permissions to Altaro applications

After being presented with a user-friendly dashboard, the discovery of new users and mailboxes, groups and SharePoint document libraries starts automatically. It can also be triggered via a button later.



Dashboard

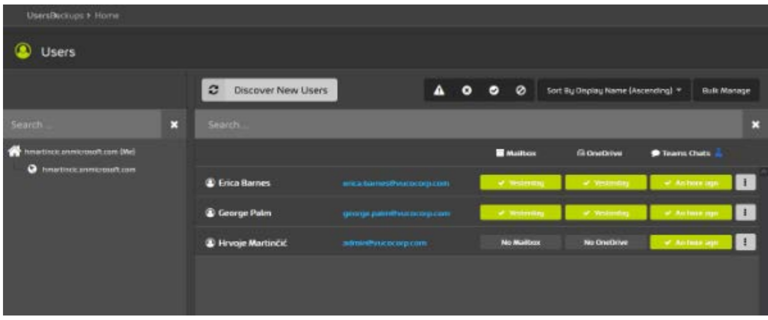
ACTIVITY
- No Mailbox Backups in Progress
- No OneDrive Backups in Progress
- No SharePoint Backups in Progress
- No Group Mailbox Backups in Progress
- No Teams Chats Backups in Progress
- No Restore Operations in Progress

HEALTH STATUS
Showing health information for hmartincic.onmicrosoft.com

	Mailbox	OneDrive	SharePoint	Teams Chats
hmartincic.onmicrosoft.com				

RESTORE HISTORY
Showing the latest restore operations
hmartincic.onmicrosoft.com - Erica Barnes

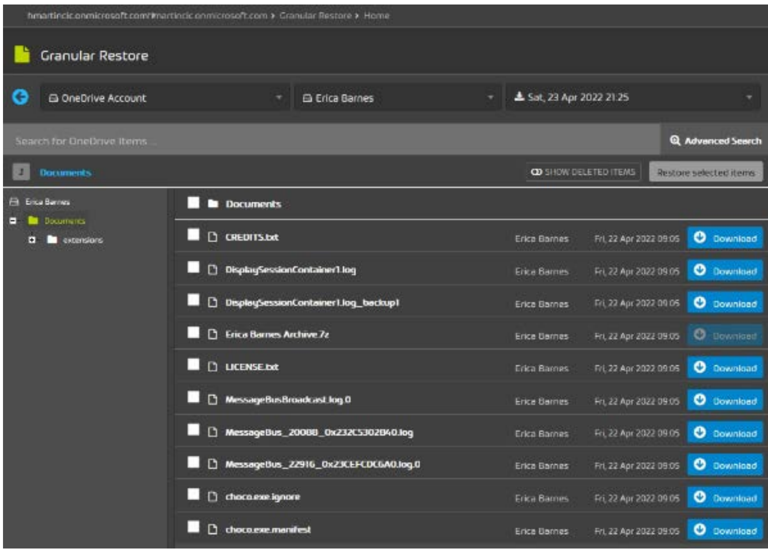
Figure 19 – The 365 Total Backup dashboard


UsersBackups > Home
Users
Discover New Users
Sort By Display Name (Ascending)
Bulk Manage
Search ...
hmartincic.onmicrosoft.com (Me)
hmartincic.onmicrosoft.com

		Mailbox	OneDrive	Teams Chats
Erica Barnes	erica.barnes@vucocorp.com	✓ Yesterday	✓ Yesterday	✓ An hour ago
George Palm	george.palm@vucocorp.com	✓ Yesterday	✓ Yesterday	✓ An hour ago
Hrvoje Martinčić	admin@vucocorp.com	No Mailbox	No OneDrive	✓ An hour ago

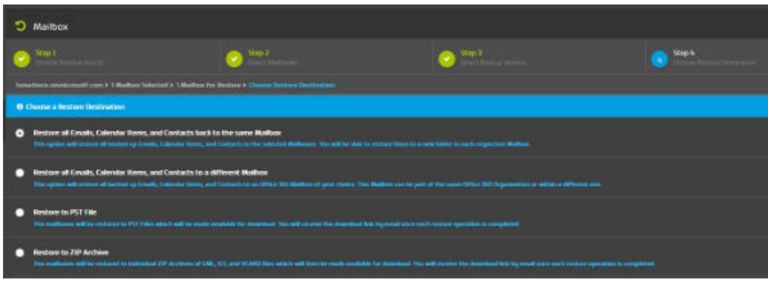
Figure 20 – Users and backups

Restore actions are done through wizards or Granular Restore, enabling admins to restore a whole account or a single file from a backup snapshot.



Documents			
CREDITS.txt	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
DisplaySessionContainer1.log	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
DisplaySessionContainer1.log_backup1	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
Erica Barnes Archive.7z	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
LICENSE.txt	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
MessageBusBroadcast.log.0	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
MessageBus_20088_0x232C5302B40.log	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
MessageBus_22916_0x23CEFCDC6A0.log.0	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
choco.exe.ignore	Erica Barnes	Fri, 22 Apr 2022 09:05	Download
choco.exe.manifest	Erica Barnes	Fri, 22 Apr 2022 09:05	Download

Figure 21 – Granular Restore


Mailbox

Step 1 – Choose Restore Source
Step 2 – Select Mailboxes
Step 3 – Select Backup Version
Step 4 – Choose Restore Destination

hmartincic.onmicrosoft.com > 1 Mailbox Selected > 1 Mailbox For Restore > Choose Restore Destination

Choose a Restore Destination

● Restore all Emails, Calendar Items, and Contacts back to the same Mailbox
This option will restore all backed up Emails, Calendar Items, and Contacts to the selected Mailboxes. You will be able to restore them to a new folder in each respective Mailbox.

○ Restore all Emails, Calendar Items, and Contacts to a different Mailbox
This option will restore all backed up Emails, Calendar Items, and Contacts to an Office 365 Mailbox of your choice. This Mailbox can be part of the same Office 365 Organization or within a different one.

○ Restore to PST File
The mailboxes will be restored to PST Files which will be made available for download. You will receive the download link by email once each restore operation is completed.

○ Restore to ZIP Archive
The mailboxes will be restored to individual ZIP Archives of EML, ICS, and VCARD files which will then be made available for download. You will receive the download link by email once each restore operation is completed.

Figure 22 – The options for restoring mailboxes

During my testing, I haven't had any issues while backing up or restoring mailbox and OneDrive data – it all went smoothly and quickly. Of course, the recovery speed depends on the size of the dataset that needs to be restored. The download of the data needed for backup integrity verification went as fast as my ISP allowed.

One last thing to mention is that Hornetsecurity 365 Total Protection Enterprise Backup includes support for (Windows) endpoint backup.

The Endpoint Backup Manager must be installed on a Windows server. This EBM server doesn't have to be on the same network as the workstations, but a connection between them is required.

After installing the EBM, it can be linked to the Cloud Management Console, from which the admin can setup backup policies and deploy the endpoint agents to the workstations. The EBM is used to configure and coordinate the backups and set the storage configuration. The storage needs to be Azure Cloud Storage, provisioned and managed by an MSP or the customer company. This is different from 365 Total Backup, for which Hornetsecurity provides and manages the storage.

Verdict

In my opinion, Hornetsecurity 365 Total Protection offers a level of email, OneDrive and SharePoint protection that should be enough for most Microsoft 365 users.

During my testing of the email protection features I have encountered no false positives. Emails were correctly categorized and user categorization from the email client or quarantine report worked flawlessly. I loved the user-friendly interface and appreciated how simple it is to handle the solution.

Customers should assess for themselves whether they need some of the additional mail services such as Email Encryption or Continuity Service.

The Enterprise Backup side of the solution covers all enterprise backup needs for the most common user-generated type of data inside a Microsoft 365 environment. It delivers a simple solution that can be set up in under 15 minutes (if you already defined organizational backup policies).

If you are running a Microsoft 365 environment and you care about email protection and backup, I can recommend this solution. It provides a centralized backup solution, adds extra security layers over Microsoft 365 services, and offers value for both users and IT administrators.

7 threat detection challenges CISOs face and what they can do about it

Sanjay Raja

VP of Products, Gurucul

Security operations (SecOps) teams continue to be under a constant deluge of new attacks and malware variants. In fact, according to recent research, there were over 170 million new malware variants in 2021 alone. As a result, the burden on CISOs and their teams to identify and stop these new threats has never been higher. But in doing so, they're faced with a variety of challenges: skills shortages, manual data correlation, chasing false positives, lengthy investigations, and more. In this article, I'd like to explore some of the threat detection program challenges CISOs are facing and provide some tips on how they can improve their security operations.

CISOs ensure the security operations program for threat detection, investigation and response (TDIR) is executing at peak performance. Let's look at seven key issues that can affect TDIR programs and some questions CISOs should consider asking their organization, security operations team, and the vendors providing solutions to resolve them.

1. There are too many indicators of compromise (IoCs) or security events happening across a network to properly identify malicious activity. As a result, CISOs are looking for advanced tools that can correlate and analyze this data effectively to eliminate false positives. The last thing any CISO wants is for his/her team to waste time on an event that might simply be a failed login associated with a user incorrectly typing their password multiple times.

> *The last thing any CISO wants is for his/her team to waste time on an event that might simply be a failed login associated with a user incorrectly typing their password multiple times.*

Questions to ask: Can I correlate data from any source (such as logs, cloud, applications, network, endpoints, etc.), no matter what it is? Can I fully monitor all these systems, ingest all the telemetry needed, and perform correlation automatically? And what is it costing me to correlate all that data (i.e., what is my solution provider charging)?

2. Correlating data over time is hard. It's like putting puzzle pieces together from a box filled with multiple puzzles. An attack that occurs once can be difficult enough to identify. But once threat actors are inside an environment, they'll often do a little activity spread over a longer period (sometimes days, weeks or months later). This makes is almost impossible for a human analyst to take these seemingly disparate events across time and connect them to complete the puzzle.

Most tools also struggle to correlate those seemingly independent events as part of the same attack because they seem unrelated over time. CISOs are responsible for making sure the team has everything it needs (based on constrained budgets) to put that puzzle together before damage is done.

Questions to ask: Do I have a wide variety of data sources and analytics that can process events and correlate them across time effectively? Is out-of-the-box threat content included for real-time attack detection?

3. When piecing together an attack campaign, manual correlation and investigation of disparate security sources drastically extends the time and resources required from a CISO and his/her team. Pulling data from several systems at once is necessary to get the contextual information needed to find out what's wrong (and how to respond). But in the time this takes, the damage could already be done. This challenge can easily frustrate CISOs that have invested so much time and money in building up the security operations program.

Questions to ask: Does your current team have to do a lot of manual correlation, and how are they able to accomplish that with events that span weeks or even months? Does your team have to search through multiple tools and put together context on their own to see patterns that will help formulate a better response when working with other IT teams?

4. The skills gap remains a problem. However, as more seasoned practitioners who were fundamentally trained across networking, servers, and other aspects of IT are aging out of the workforce, CISOs are being forced to hire more security focused analysts, but with less broad practitioner experience. This is impacting the amount of on-the-job training and experience required (and offered) for them to be effective. There are just not enough skilled cybersecurity professionals in the market today.

Questions to ask: How can my TDIR platform automate certain tasks and bring the right context to the forefront? How can it provide the necessary context that can help a less experienced analyst learn over time and increasingly add value?

5. Vendors are overpromising and underdelivering. When it comes to threat detection, too many vendors falsely claim or exaggerate that they have machine learning (ML), artificial intelligence (AI), multicloud support, and/or apply risk metrics. CISOs are barraged with vendors claiming to offer a silver bullet at worst or using questionable marketing claims at best. Neither delivers what's promised.

Questions to ask: Does the solution use rule-based ML/AI (which is important to understand considering it's static in nature, requires updating, and is ineffective at identifying new attacks and variants)? Does multicloud just do correlation (leaving it up to the analyst to determine if an attack is occurring across multi-cloud)? Is risk scoring just aggregated scores from public sources (not leveraging an enterprise-class risk engine powered by analytics)?

6. The tradeoff of cost and budget versus better security visibility can be a painful choice. CISOs often are presented with platforms (like a SIEM) that charge organizations based on volume of data ingested. As an organization grows, charging by data ingested is unpredictable and can quickly lead to rapidly escalating costs in licensing and storage. As a result, CISOs should be looking for solutions that reduce this cost burden, while still allowing the organization to pull in and ingest as much data as possible. The result is better SOC visibility and more effective TDIR.

Questions to ask: For a solution that employs true machine learning, the more data that can be pulled in the better. Does my solution penalize me for bringing in more data? Or does it embrace more data ingestion to offer better visibility and do so by providing flexible licensing? How can my provider help reduce storage costs?

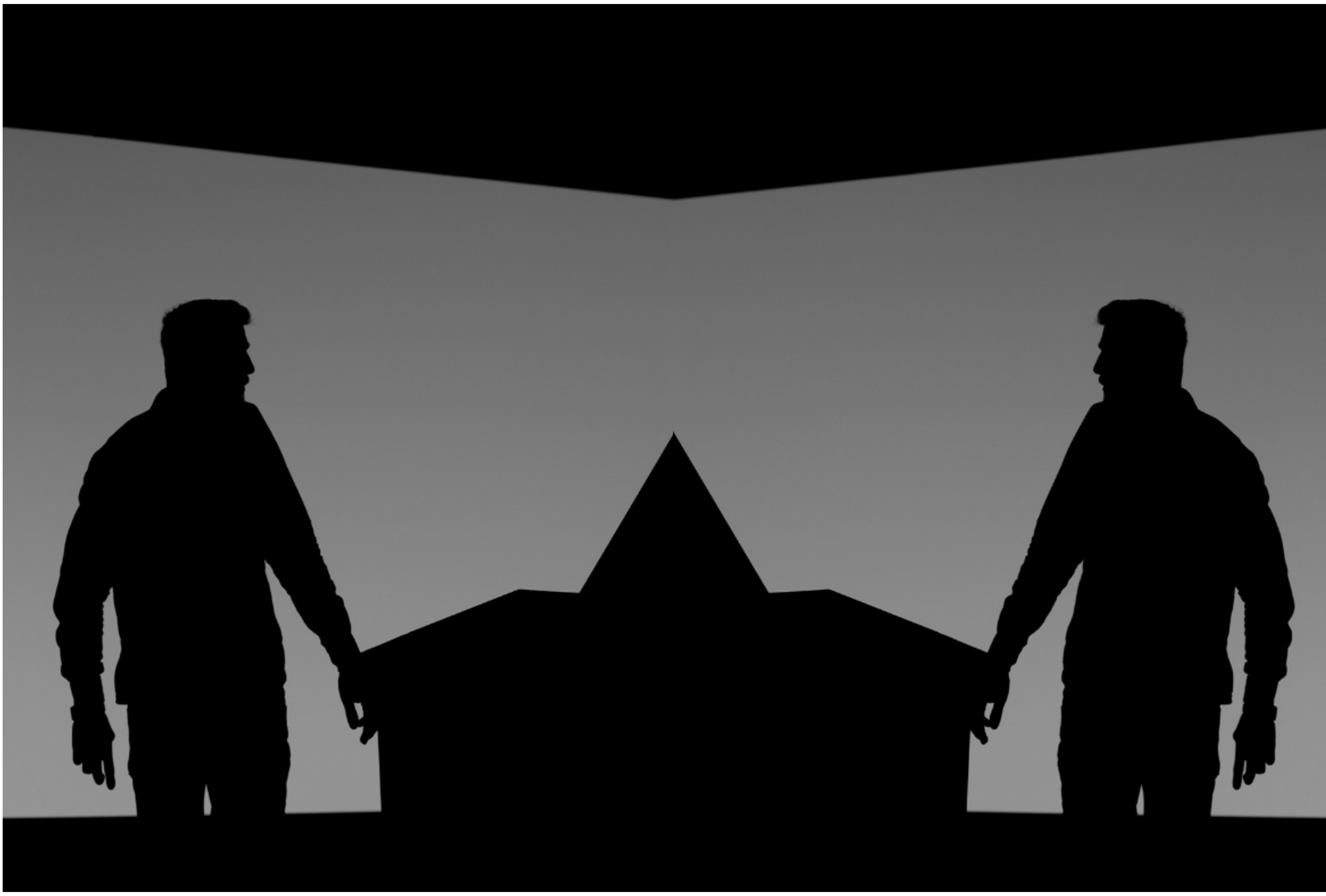
7. Automation can drive efficiency and speed threat detection. This can free up security team members to focus their attention on more intensive tasks. When done effectively, this provides OPEX savings – which means less time and resources spent on simple and manual tasks of low value, while also shrinking the time for high-value tasks. It can also provide better experience for junior analysts, especially when your analytics and automation are transparent, allowing them to learn and improve.

But not all automation is created equal. Solutions that produce too much noise and too many false positives make it difficult to prioritize investigation and automate responses. The more accurate the threat detection is, the more targeted the automated response can be.

> *Solutions that produce too much noise and too many false positives make it difficult to prioritize investigation and automate responses.*

Questions to ask: Is automation in the solution inherent across my entire SOC lifecycle? If so, how do I know it's working and how can I trust that it's optimizing my operations (for example, can it show that I'm stopping threats earlier in the kill chain)?

As CISOs and their security operations teams look to improve threat detection they'll face a variety of issues around visibility, cost, flexibility (especially into cloud environments), analytics, prioritization, contextual data and much more. But by working together to understand these challenges – and by arming ourselves with knowledge and the right questions – our industry can continue to evolve and deliver better security operations for our organizations.



How to set up a powerful insider threat program

Simon Whitburn

GM and Senior VP of International Business, Exterro

Security spend continues to focus on external threats despite threats often coming from within the organization. A recent Imperva report (by Forrester Research) found only 18 percent prioritized spend on a dedicated insider threat program (ITP) compared to 25 percent focused on external threat intelligence.

And it's not just the employee with a grudge you need to worry – most insider incidents are non-malicious in nature. In its 2022 Cost of Insider Threats Global Report, Proofpoint and the Ponemon Institute found careless or negligent behavior accounted for 56 percent of all incidents and these also tend to be the most costly, with the average clean-up operation costing $6.6m.

Failed fixes

Part of the problem lies in perception: The Forrester report found almost a third of those questioned didn't regard employees as a threat. But it's also notoriously difficult to prevent these types of incidents because you're essentially seeking to control legitimate access to data. Mitigating these threats is not just about increasing security but about detecting potential indicators of compromise (IoC) in user behavior and, for this reason, most businesses rely on staff training to address the issue. Yet as the figures above reveal, training alone is often insufficient.

The same Forrester report found that while 65 percent use staff training to ensure compliance with data protection policies, 55 percent said their users have found ways to circumvent those same policies. Others said they rely on point solutions to prevent incidents, with 43 percent using data loss prevention (DLP) to block actions and 29 percent monitoring via the SIEM (although data can still be exfiltrated without detection by these systems). The problem is that network security and employee monitoring both fail to take into account the stress factors that can push resourceful employees resort to use workarounds.

While prevention is always better than cure, the current approach to insider threats is too heavily weighted in its approach. Consequently, there's insufficient focus on what to do if an insider threat, malicious or not, is realized. So, while training and network security controls do have their part to play, both need to be part of something much more wide ranging: the ITP.

An ITP aligns policies, procedures, and processes across different business departments to address insider threats. It's widely regarded as critical to the mitigation of insider threats, but only 28 percent of those surveyed by Forrester claim to have one in place. The reason for this is that many organizations find it daunting to set one up.

In addition to getting people onboard and policies in place, the business will need to inventory its data and locate data sources, determine how it will monitor behaviors, adapt the training program, and carry out investigations as well as how the ITP itself will be assessed on a regular basis.

> *The problem is that network security and employee monitoring both fail to take into account the stress factors that can push resourceful employees resort to use workarounds.*

Getting started

To begin with, a manager and dedicated working party are required to help steer the ITP. The members will need to have clear roles and responsibilities and to agree to a set code of ethics and/or sign an NDA. This is because there are many laws related to employee privacy and monitoring, as well as legal considerations and concerns that must be factored into the writing and execution of policy. The first job of the working group will be to create an operations plan and put together a high-level version of the insider threat policy.

They'll then need to consider how to inventory and access internal and external data sources and to do this the working group will need to familiar with record handling and use procedures specific to certain data sets. Once the processes and procedures needed to collect, integrate, and analyze the data have been created, the data should be marked according to its use and so may be related to a privacy investigation. (Interestingly, nearly 58 percent of incidents that impact sensitive data are caused by insider threats, according to Forrester.)

Consider whether you'll use technology to monitor end user devices, logins, etc. and document this through signed information systems security acknowledgement agreements. Potential indicators of compromise (IoCs) could include database tampering, inappropriate sharing of confidential company information, deletion of files or viewing of inappropriate content. When such behaviors come to light, discretion is critical, and any investigation needs to be watertight and defensible as it may result in a legal case.

Digital forensics for defensibility

How the business responds to and investigates incidents should also be detailed in the ITP. Consider whether the investigation will be internal and at what point you'll need to involve external agents and who will need to be notified. Where will the data for the investigation be held? How long will the information be held for? While it's important to retain relevant information, you don't want to fall into the trap of keeping more than necessary, as this elevates risk, which means ITP should also overlap with a data minimization policy.

How the business responds to and investigates incidents should also be detailed in the ITP.

Digital forensics tools should be used to enforce the ITP. You'll need to decide how you proactively manage insider threats and whether these tools will only be used post-analysis or covertly. For example, some businesses with high value assets will carry out a sweep to establish if data has been exfiltrated when an employee leaves the organization. You should also ensure these tools are able to remotely target endpoints and cloud sources even when they're not connected and should be OS-agnostic so you can capture data on Macs as well as PCs.

Digital forensics ensure the business can quickly capture and investigate any incidence of wrongdoing. For example, it can determine the date, time and pathway used to exfiltrate data from the corporate information estate to any device, endpoint, online storage service such as Google Drive or Dropbox, or even publication over a social media platform. Once the data has been traced, it's then possible to narrow down likely suspects until the team have indisputable proof.

Both the way the investigation is done and the evidence itself must be beyond reproach and legally defensible because such incidents may lead to dismissal or even prosecution. If challenged in a legal tribunal, the business would then need to prove due diligence so there must be a forensically sound and repeatable process and a proper chain of custody when it comes to safeguarding the handling of the evidence.

Keeping employees onside

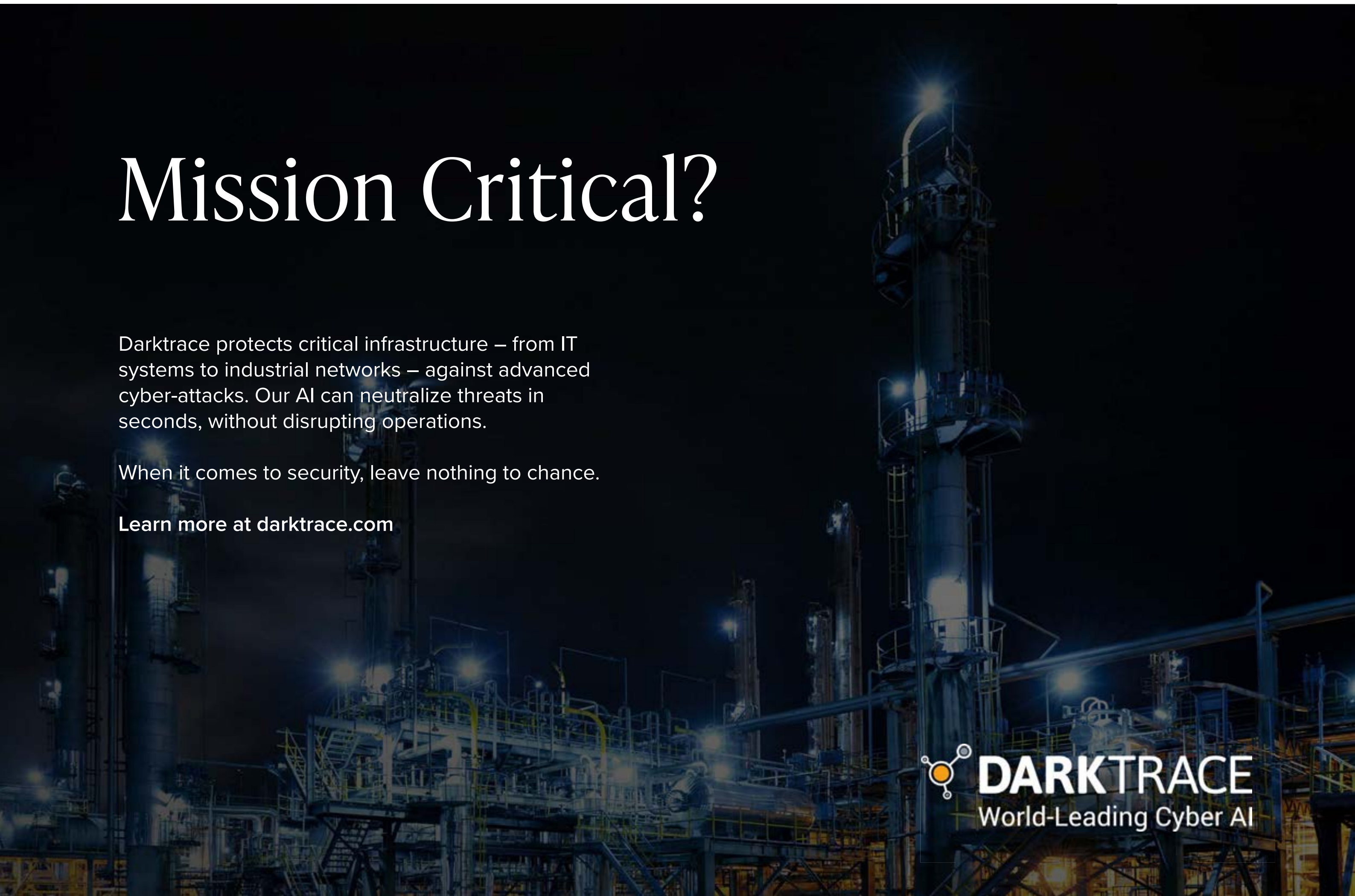
Employee buy-in is also essential to success. The policy should communicate the risks of compromise in terms of the privacy, financial and even physical repercussions of a breach so that the workforce are aware of the risks involved. But there should also be processes in place to enable users to report behavioral IoCs. Guidelines should stipulate how and when IoCs should be reported via specific channels, i.e., via a tip phone line, email, DropBox, etc. The completion of the awareness training should also be documented.

The ITP will need to be put to the test but preferably not with an actual incident. Instead, an insider threat risk assessment should be executed to identify gaps in security controls and business processes or to assess the ease with which data can be exfiltrated and how well digital forensics processes performed. Consider how you can bring in insider threat management to other security policies, such as those covering BYOD, and ensure that trusted business partners and sub-contractors are subjected to insider threat risk assessments too.

The aim of implementing an insider threat program is to ensure that not just the business, its data or its processes are protected from harm, but also its employees.

Finally, bear in mind that the strategy will need to adapt and change as new processes are brought online and data sources are added. Key to this is maintaining an accurate data inventory and ensuring that your digital forensics tools offer you sufficient range to deal with new technologies and/or exfiltration pathways but you can also benchmark your program against other businesses within your sector.

The aim of implementing an insider threat program is to ensure that not just the business, its data or its processes are protected from harm, but also its employees. Covertly monitoring workflows can enable IoCs to be flagged more accurately, helping to prevent the escalation of incidents. But when the unthinkable happens, and an unsuspecting employee does expose sensitive data, having robust defensible processes in place that have already documented the incident make it much easier to carry out a digital forensics investigation and to bring any legal case that results to a swift conclusion.



Security world

69% of employees need to deal with more security measures in a hybrid work environment

Ivanti worked with global digital transformation experts and surveyed 10,000 office workers, IT professionals, and the C-Suite to evaluate the level of prioritization and adoption of DEX in organizations and how it shapes the daily working experiences for employees. The report revealed that 49% of employees are frustrated by the tech and tools their organization provides and 64% believe that the way they interact with technology directly impacts morale.

Conflicting views remain between C-Suite, IT, and employees when it comes to the future of work and technology's role in enabling the culture of hybrid work. Just 13% of knowledge workers prefer to work exclusively from the office, yet 56% of CXOs still feel that employees need to be in the office to be productive, although 74% of the C-Suite report they are more productive since the start of the pandemic – showing a disconnect between what they have experienced and what they believe employees need to do to be productive.

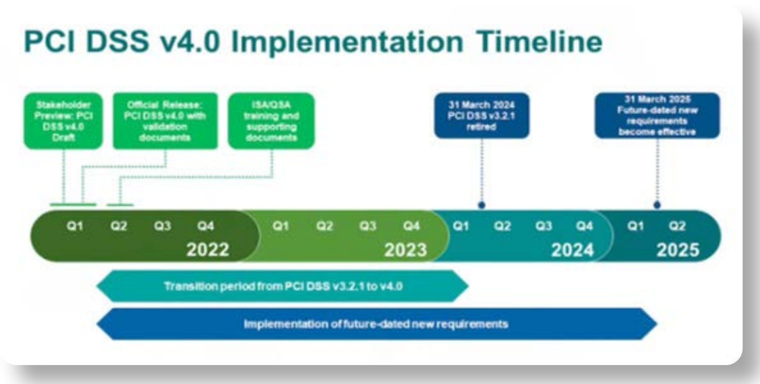
EMEA continues to be a hotspot for malware threats

Ransomware detections in the first quarter of this year doubled the total volume reported for 2021, according to the latest quarterly Internet Security Report from the WatchGuard Threat Lab. Researchers also found that the Emotet botnet came back in a big way, the infamous Log4Shell vulnerability tripled its attack efforts and malicious cryptomining activity increased.

The report also shows that EMEA continues to be a hotspot for malware threats. Overall regional detections of basic and evasive malware show WatchGuard Fireboxes in EMEA were hit harder than those in North, Central and South America (AMER) at 57% and 22%, respectively, followed by Asia-Pacific (APAC) at 21%.

"Based on the early spike in ransomware this year and data from previous quarters, we predict 2022 will break our record for annual ransomware detections," said Corey Nachreiner, chief security officer at WatchGuard. *"We continue to urge companies to not only commit to implementing simple but critically important measures but also to adopt a true unified security approach that can adapt quickly and efficiently to growing and evolving threats."*

PCI DSS 4.0 released, addresses emerging threats and technologies


PCI DSS v4.0 Implementation Timeline
Stakeholder Preview: PCI DSS v4.0 Draft
Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025 Future-dated new requirements become effective
Q1 Q2 Q3 Q4 2022
Q1 Q2 Q3 Q4 2023
Q1 Q2 Q3 Q4 2024
Q1 Q2 2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

The PCI Security Standards Council (PCI SSC) published version 4.0 of the PCI Data Security Standard (PCI DSS). PCI DSS is a global standard that provides a baseline of technical and operational requirements designed to protect account data.

To provide organizations time to understand the changes in the new version and implement any updates needed, the current version of PCI DSS, 3.2.1, will remain active for two years until it is retired on 31 March 2024. Once assessors have completed training in PCI DSS 4.0, organizations may assess to either PCI DSS 4.0 or PCI DSS 3.2.1. The standard also provides additional time for organizations to implement many of the new requirements.

Examples of the changes include:

- Updated firewall terminology to network security controls to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.
- Expansion of Requirement 8 to implement multi-factor authentication (MFA) for all access into the cardholder data environment.
- Increased flexibility for organizations to demonstrate how they are using different methods to achieve security objectives.
- Addition of targeted risk analyses to allow entities the flexibility to define how frequently they perform certain activities, as best suited for their business needs and risk exposure.

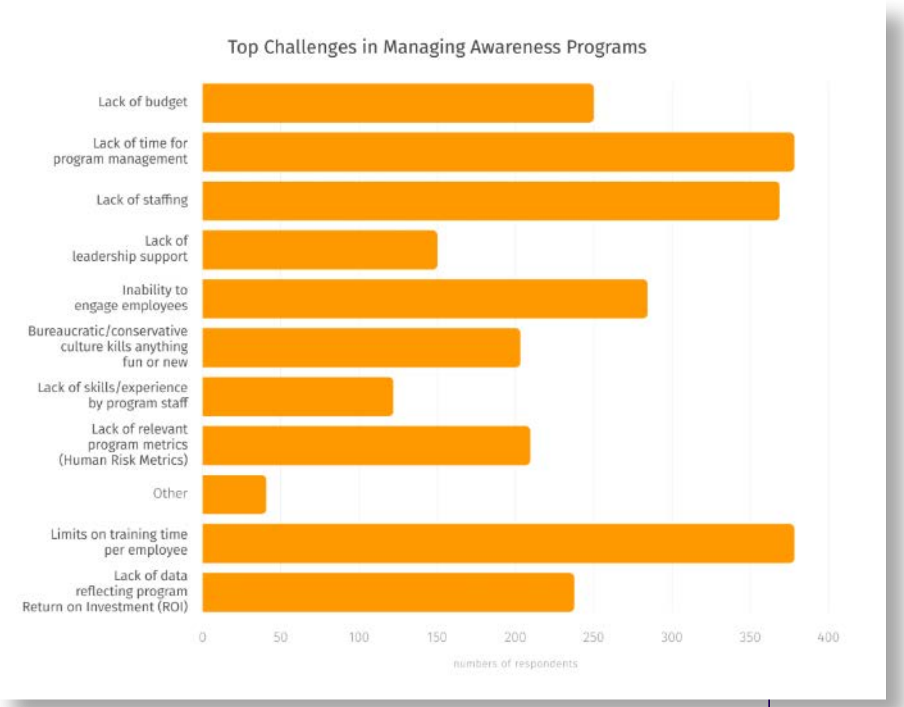
Cybersecurity is driving digital transformation in alternative investment institutions

As the alternative investment industry tackles a rapidly changing threat landscape, increased regulation, and a continuous need to innovate, most firms are increasing their DX and security budgets and cite security as critically important to their DX initiatives, according to IDC.

Senior leaders from 400 global alternative investment institutions in U.S., Canada, France, U.K., and Germany were surveyed to understand the current state of digital transformation and cybersecurity, identify key barriers and benefits of an aligned strategy, and explore the growing role of consulting services as strategic partners.

89% of surveyed institutions are increasing their digital transformation and security budget in 2022 over 2021, and nearly half (48%) are increasing spending by at least 10 percent. Survey findings also indicate that institutions are increasingly leveraging consulting services and managed services providers to support initiative execution and management.

People are the primary attack vector around the world



With an unprecedented number of employees now working in hybrid or fully remote environments, compounded by an increase in cyber threats and a more overwhelmed, COVID-19 information fatigued workforce, there has never been a more critical time to effectively create and maintain a cyber-secure workforce and an engaged security culture.

"People have become the primary attack vector for cyber-attackers around the world," said Lance Spitzner, SANS Security Awareness Director. *"Humans rather than technology represent the greatest risk to organizations and the professionals who oversee security awareness programs are the key to effectively managing that risk."*

"Awareness programs enable security teams to effectively manage their human risk by changing how people think about cybersecurity and help them exhibit secure behaviors, from the Board of Directors on down," said Spitzner.

Properly securing APIs is becoming increasingly urgent

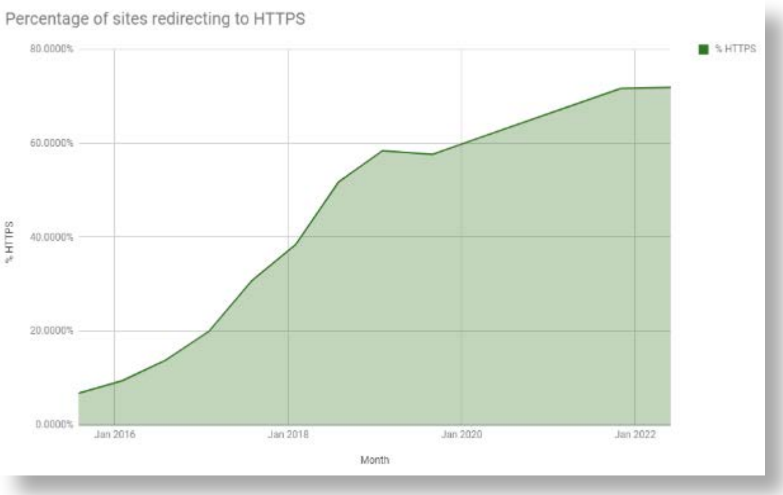
Imperva released a new study that uncovers the rising global costs of vulnerable or insecure APIs. The analysis of nearly 117,000 unique cybersecurity incidents estimates that API insecurity results in $41-$75 billion of losses annually.

The study, conducted by the Marsh McLennan Cyber Risk Analytics Center, found that larger organizations were statistically more likely to have a higher percentage of API-related incidents. In fact, enterprises with revenues of at least $100 billion were 3-4x more likely to experience API insecurity than small or midsize businesses. The data suggests that large companies are particularly vulnerable to the security risks associated with exposed or unprotected APIs as these mature organizations accelerate digital transformation.

An API is the invisible connective tissue that enables applications to share data to improve end-user experiences and outcomes. The volume of APIs used by businesses is growing rapidly; nearly half of all businesses have between 50-500 deployed, either internally or publicly, while some have over a thousand active APIs.

Many APIs connect directly to backend databases where sensitive data is stored. As a result, hackers are increasingly targeting APIs as a pathway to the underlying infrastructure to exfiltrate sensitive information. Today, as many as 1 in every 13 cyber incidents can be attributed to API insecurity. As the number of APIs in production multiplies, this figure is expected to grow in the coming years.

Evaluating the use of encryption across the world's top one million sites



A new report from security researcher and TLS expert Scott Helme, evaluates the use of encryption across the world's top one million sites over the last six months and reveals the need for a control plane to automate the management of machine identities in increasingly complex cloud environments.

The research suggests that while progress has been made in some areas, more education is needed to ensure that machine identities are used in the most effective way to protect our online world:

- Use of TLSv1.2 has declined by 13% over the last six months, with v1.3 in use by almost 50% of sites — more than twice as many sites as v1.2. The adoption of v1.3 is being driven by widespread digital transformation. initiatives, cloud migration and new cloud native stacks that default to v1.3.
- Even though organizations are adopting stronger TLS protocols, they are failing to couple this with a move to stronger keys for TLS machine identities.
- Industry-standard ECDSA keys are now used by just 17% of websites — up from 14% six months ago. Slower, less secure RSA keys are still used by 39% of the top one million websites.
- Growth in the adoption of HTTPS has plateaued at 72% — the same level as in December.

Security pros increasingly plan to adopt MDR services in the next 12 months

The managed cybersecurity services market is undergoing a significant shift, according to a new survey conducted by Osterman Research. As organizations struggle with too many alerts, too few security analysts, and increasingly complex security stacks, they are rapidly upgrading from Managed Security Service Providers (MSSPs) and legacy security tools such as SIEMs that aggregate alerts, to action-oriented MDR services.

Although detection remains a core capability, MDRs add automated response capabilities and access to cybersecurity professionals, enabling organizations to address alert overload, talent shortages and budget constraints.

"This study has found a significant change in how organizations plan to address today's security challenges," said Michael Sampson, senior analyst at Osterman Research. *"The perfect storm of too many security tools creating too many alerts for overstretched security teams has created an urgent need for many organizations to move to more advanced managed security services."*

Teams that shift security left and focus on attackability ship more secure code

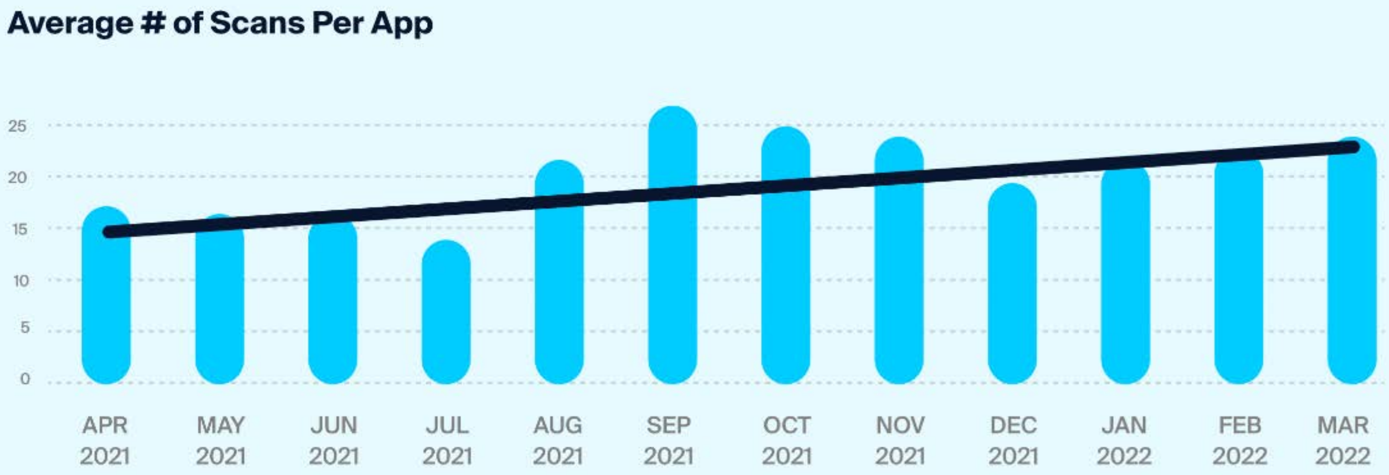
ShiftLeft released its second annual AppSec Progress Report documenting critical trends in application security and how organizations are shifting security left to deal with the ever-rising volume of attacks and disclosed vulnerabilities.

97% reduction in open source software (OSS) vulnerabilities – By identifying and prioritizing OSS vulns that are actually attackable, AppSec teams and developers fix what matters, ship code faster and actually improve security with fewer, better fixes.

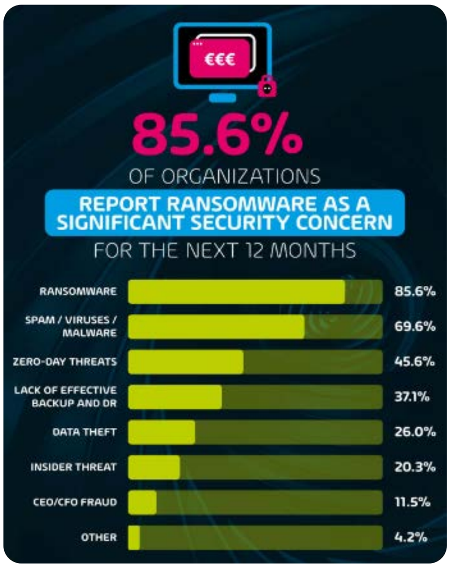
37% YoY reduction in Mean-Time-to-Remediate (MTTR) – Laser focus on attackability and reduced false positives allows developers to make fixes faster and reduce MTTR. This improves security posture and reduces the likelihood of attacks by reducing the time that vulnerabilities are exposed. In fact, ShiftLeft found that development teams were fixing 76% of attackable vulnerabilities within two sprints (12 days).

90 second median scan time – Rapid scans enable teams to scan more frequently, improving security coverage for fast iterating applications and enabling better coverage of very large applications that previously required hours or days to scan.

Significant increase in scan frequency – Faster scans, automated insertion in CI pipelines, and greater scan coverage across more languages, also enabled AppSec teams to shift from scanning for vulnerabilities monthly or weekly to daily scans. The report tracked 68% increase year-over-year in daily scans.



Rate of IT security incidents grows with company size



The rate of IT security incidents increases the more Microsoft 365 security features are used, according to Hornetsecurity. Organizations using Microsoft 365 and that use 1 or 2 of its stock security features reported attacks 24.4% and 28.2% of the time respectively, while those that use 6 or 7 features reported attacks 55.6% and 40.8% of the time respectively.

Overall, it was found that 3 in 10 organizations (29.2%) using Microsoft 365 reported a known security incident in the last 12 months.

Experts at Hornetsecurity say that these finding could be due to a number of factors. They point to the likelihood that organizations with a high number of implemented security features have done so as a result of sustained cyber-attacks over a period of time, in an attempt to mitigate security threats.

They also suggest that the more security features that IT teams attempt to implement, the more complex the security system becomes. Features may be misconfigured, leaving vulnerabilities. This is corroborated by the fact that 62.6% of respondents indicated that the main roadblock to implementing security features within their organization is 'not enough time or resources'.

Despite known security issues, VPN usage continues to thrive

VPN usage is still prevalent among 90% of security teams who have highlighted cost, time, and difficulty as reasons to not move forward with ZTNA adoption, according to a new survey conducted by Sapio Research. Furthermore, 97% say that adopting a zero trust model is a priority, with 93% of organizations having committed a budget to enhance their VPN or move toward ZTNA within the next year or two.

The last two years have shifted how we work, producing a new remote workforce that was essentially created overnight. As highlighted in this study, this has resulted in most workers – in this case 51% of respondents – using a combination of corporate and personal devices to connect to business applications and resources.

Personal devices often used by less security-conscious family members. This creates a very risky environment as personal devices are easy targets for threat actors especially since IT teams cannot fully monitor activity on these devices. Additionally, personal devices are often used by other family members – particularly children – which make them even more susceptible to malware and other viruses.

Despite known security issues, VPN usage continues to thrive, with 90% of respondents currently using a VPN in some capacity for secure remote access. When access is permitted on a personal device, it creates a risky situation for not only the user, but the entire organization. VPNs lack many of the application-level access controls and integrated security that are common in ZTNA solutions. As a result, cybercriminals will often target VPNs because a single set of compromised credentials can provide all of the access needed to carry out a data breach, ransomware incident, or other attacks.

Top 5 security analytics to measure

Juan Jones

Security Engineer, LogDNA

You don't need a Ph.D. in cybersecurity to recognize the importance of security analytics. Security analytics uses data analysis – often aided by machine learning – to detect security threats and measure the effectiveness of security operations.

But what may be challenging to determine, especially if you're not a cybersecurity expert, is what to analyze to improve security outcomes for your organization. This article discusses five of the most crucial security analytics to track.

As you'll see, some of these analytics assist with threat detection, which is one component of effective security operations. Others deal with assessing the effectiveness of your security operations processes to help you detect inefficiencies or risks within your approach to security management.

Mean time to detect

Mean time to detect, also known as MTTD, is a standard metric for IT operations teams, who use it to assess how quickly, on average, they can identify specific issues.

MTTD is particularly necessary for security analytics. Indeed, it's arguably even more critical in this context, given that many organizations struggle to detect cybersecurity breaches. Threat actors use increasingly stealthy tactics to hide their malicious intents. They orchestrate several "normal" actions to hide in plain sight.

> *Mean time to detect, also known as MTTD, is a standard metric for IT operations teams, who use it to assess how quickly, on average, they can identify specific issues.*

Plus, the longer it takes you to find out if there's a breach in your environment, the more damage the attack will likely cause. The episode is likely to escalate to affect more applications and data if you don't detect it and isolate affected resources.

You should comprehensively assess how long it takes your team to detect cybersecurity incidents and aim to improve that metric continuously for all these reasons.

> *MTTD is particularly necessary for security analytics. Indeed, it's arguably even more critical in this context, given that many organizations struggle to detect cybersecurity breaches.*

Mean time to resolve

Detection is only the first step in resolving security incidents. That's why the mean time to resolve (MTTR) is an equally important security analytics metric to measure.

MTTR reflects how efficiently and effectively your security operations team works when a breach occurs. By tracking this metric, you can assess how much efficiency you gain when you implement changes to your security operations strategy, such as adopting a new tool or making organizational changes to your security response team. MTTR is also useful for assessing how rapidly your team can resolve different security incidents, like DDoS attacks, ransomware attacks, and data leaks.

> *MTTR reflects how efficiently and effectively your security operations team works when a breach occurs.*

Mean time to contain

In between security incident detection and resolution comes containment. Containment is the process of isolating compromised resources once you've detected a breach to prevent further damage.

In some respects, mean time to contain, or MTTC, is even more important than MTTR. The overall cost of an incident depends partly on how quickly you can contain it.

For that reason, you should track MTTC alongside MTTD and MTTR. If you find that you detect incidents quickly but take a long time to contain them after that, it's a sign that you need to invest a bit more in containment strategies.

Unidentified devices on internal networks

Today's networks are very fluid. Endpoints come and go continuously, and most networks lack firm perimeters because they constantly connect to remote cloud infrastructure, off-site devices connected via VPNs, etc. Ultimately, this means that it's impossible to draw black-and-white distinctions between which devices should and shouldn't exist on your network.

In many cases, unidentified devices are benign. They could be new VMs that an engineer spun up or a mobile device that a worker brought on-site as part of a BYOD policy.

However, you can and should systematically track how many unidentified devices exist on your network. Unidentified devices are devices whose origins and purposes are unknown.

In many cases, unidentified devices are benign. They could be new VMs that an engineer spun up or a mobile device that a worker brought on-site as part of a BYOD policy.

Still, the number of unidentified devices on your network should generally follow a consistent pattern. Suppose you detect a sudden spike in unknown devices. In that case, it could be a sign of risk, like the unauthorized creation of new endpoints by employees who are not adhering to your company's IT governance rules, or (worse yet) efforts by attackers to bring malicious devices into the environment to escalate a breach.

Access control metrics

Access control roles and policies for modern IT environments are complex. Different parts of your environment (like a public cloud on the one hand and on-premises servers and workstations on the other) typically use different access control systems and require different types of settings.

There is no simple way to track access control configurations or positively identify a risk. For that, you'll need comprehensive and detailed access control management techniques, like cloud security posture management (CSPM) and cloud infrastructure entitlements management (CIEM).

There is no simple way to track access control configurations or positively identify a risk.

Nonetheless, even the most basic security analytics strategy can track metrics like the number of users and roles within access control configurations. You can also measure how rapidly access control policies change. Fluctuations from the norm for both metrics could be a sign of a security issue.

Conclusion

The security analytics described above represent only the most basic metrics you should consider tracking to optimize security operations. There are dozens of others – like mean time to patch, data transfer rates, and network port exposures, to name just a few – that can add critical context to security operations.

But if you're devising a basic security analytics strategy, start with the core essentials, like MTTD, MTTR, MTTC, unidentified device tracking, and access control metrics.

How to avoid security blind spots when logging and monitoring

A.N. Ananth

President, Netsurion

Cybersecurity involves a balancing act between risk aversion and risk tolerance. Going too far to either extreme may increase cost and complexity, or worse: cause the inevitable business and compliance consequences of a successful cyberattack. The decisions that need to be made around logging and monitoring are no exception.

Capturing all data from every device on the network can create bottlenecks, overwhelm log management, and obfuscate signs of network penetration, or malicious activity. Not capturing all the critical log data can result in monitoring that fails to identify attacks before they do damage or assist in forensics after the incident.

Getting logging and monitoring right is so important that it is listed among the Center for Internet Security's critical security controls.

Failing to log creates blind spots

Failing to activate logging creates security blind spots in your network that will only become apparent after the fact (i.e., when an attack is successful). Every component of your extended infrastructure — on premises and remote — should be configured to generate appropriate audit events. These components include operating systems, system utilities, servers, workstations, networking equipment, and security systems (which include anti-malware, firewalls, intrusion detection and prevention systems, and VPNs).

> *Failing to activate logging creates security blind spots in your network that will only become apparent after the fact (i.e., when an attack is successful).*

This applies whether you run your own security information and event management (SIEM) solution for log management or use a managed SIEM with SOC-as-a-Service for 24/7 monitoring, alerting, and reporting. The SIEM relies on log data feeds to provide protection. It can't see alerts on what's not being logged. Responsibility for making devices and apps visible often falls outside of the security organization.

> *Assuming that new apps and devices — including new cloud infrastructure — come with logging set to "on" is another way organizations can fail to send data to the SIEM.*

For example, failure to activate logging can happen if there is a "set it and forget it" mindset. The reality is that networks are always changing. New endpoint devices are continually being added and removed due to personnel changes, addition of new locations, flexible work programs that let employees work from home, new mobility solutions, and the like.

Assuming that new apps and devices — including new cloud infrastructure — come with logging set to "on" is another way organizations can fail to send data to the SIEM. "Always check logging settings" should be standard procedure across the IT organization. A third possibility is failing to understand that logs from an IoT device — in one real example, the badge reader on the entrance to the server room — should be monitored.

Establish a log management and monitoring policy

The best way to avoid logging and monitoring failure — as well as failure to capture the right data — is a log management and monitoring policy, and a culture of policy awareness and adherence. The challenge is determining what log data to capture and monitor with a SIEM, and properly store for auditing purposes.

> *While compliance and audit reporting remain table stakes, today's SIEM solutions have an increased focus on threat detection and forensics.*

Compliance mandates such as PCI DSS initially drove those decisions. US federal legislation and regulatory requirements such as HIPAA and FISMA also come into play. While compliance and audit reporting remain table stakes, today's SIEM solutions have an increased focus on threat detection and forensics.

It takes a blend of art, science, and experience to determine what should be codified in an organization's logging policy. You want to take risk appetite, security relevance, and volume into consideration while finding the balance for logging. This means just enough to satisfy your organization's specific use case and not so much that you're bogged down in data.

The good news is you don't have to start from scratch. For one thing, many network device manufacturers, software vendors, and cloud providers offer suggestions of what event data should be logged for their product or service. You can also get guidance from industry-standard frameworks like NIST SP800-92, MITRE ATT&CK, or the Open Web Application Security Project (OWASP).

For forensic purposes, every log entry should contain at least an actor (username, IP address), an action, a timestamp, and a location (geolocation, browser, code script name).

The key takeaway is that you should be making an informed decision about event data from every network component. The list below is a starting point of events to consider:

- Successful and unsuccessful authentication and access control events
- Account management activities, such as account creation, modification, and deletion
- Session activities
- Starting and stopping processes
- Changes in authorization, user privileges, and configurations
- Devices and software added or removed
- Access, modifications, downloads, and deletion of critical data sets
- Alerts from security systems, including firewalls, IDS/IDP, and anti-malware

For forensic purposes, every log entry should contain at least an actor (username, IP address), an action, a timestamp, and a location (geolocation, browser, code script name).

Proper log management is key for protection and compliance

Also consider how your log files are managed. If you handle personal health or identity information (PHI/PII), consider anonymizing that data to prevent sensitive information from being stored in plain text. You also want to ensure that log files cannot be tampered with. Cyber criminals often change log files to disguise their malicious activities. Encryption at rest and in motion, along with log integrity checks and least-privilege access, can protect log data. To prevent data loss, make sure you back up log data frequently so it will be available for a compliance audit or any needed forensic investigations.

Depending on the regulations or mandates that apply to your business, you will need to store logs for a specified length of time. For example, PCI DSS requires that logs are stored for at least one year, with three months available on demand. The remaining months can reside in long-term storage such as tape stored offsite.

Monitoring considerations: A well-tuned SIEM with a skilled SOC

Log monitoring systems, typically SIEM solutions, oversee network activity, analyze system events, and issue alerts when anomalous behavior is detected. They are optimized for different use cases and one size never fits all. The wrong selection can have a long-lasting impact, be costly to maintain and support, and time-consuming to tune, which is why many SIEM deployments end up abandoned.

Log monitoring systems, typically SIEM solutions, oversee network activity, analyze system events, and issue alerts when anomalous behavior is detected.

Organizations need a well-tuned SIEM to provide the foundational visibility into events in the network environment. Automation produces significant efficiencies when applied to the massive amounts of data that must be correlated and filtered to uncover cyber threats. With automation and artificial intelligence, the SIEM surfaces only those artifacts that need to be further reviewed by a security analyst to determine if the event is a false positive or an actual security event. Threat intelligence then provides context specific to your organization's goals and risk posture. A SIEM should also provide reporting to meet compliance requirements.

It is often unrealistic for most small-to-medium-sized businesses (SMBs) to hire, train, and retain in-house security operations staff and implement the state-of-the-art threat intelligence. For example, in our experience, it takes a minimum of eight to 10 analysts to provide around-the-clock monitoring coverage. Attempting to implement DIY cybersecurity can result in underutilized security software that becomes shelfware and leads to gaping vulnerabilities. For these organizations, a managed SIEM with SOC-as-a-Service for 24/7 monitoring, event analysis, threat intelligence, and log management can be a viable option to speed time to detect security threats and improve resilience.

It is often unrealistic for most small-to-medium-sized businesses (SMBs) to hire, train, and retain in-house security operations staff and implement the state-of-the-art threat intelligence.

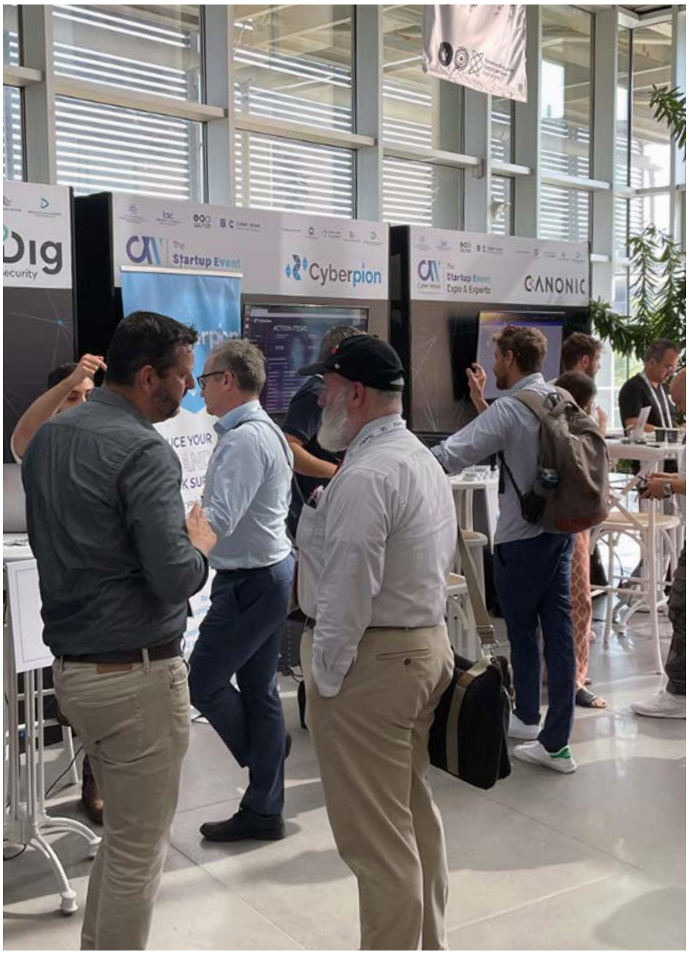
Cyber Week 2022

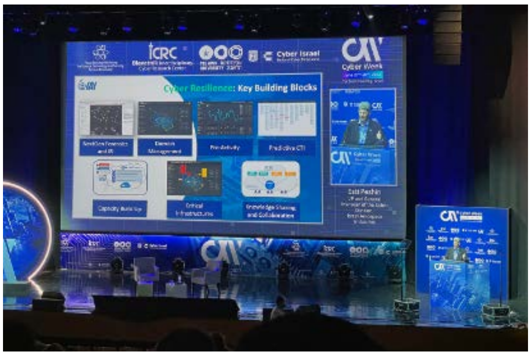
Zeljka Zorz
Editor-in-Chief, (IN)SECURE Magazine

Cyber Week is a large annual international cybersecurity event, hosted each year at Tel Aviv University in Israel. Over the past 12 years, Cyber Week has become internationally acclaimed as one of the top cybersecurity events in the world.

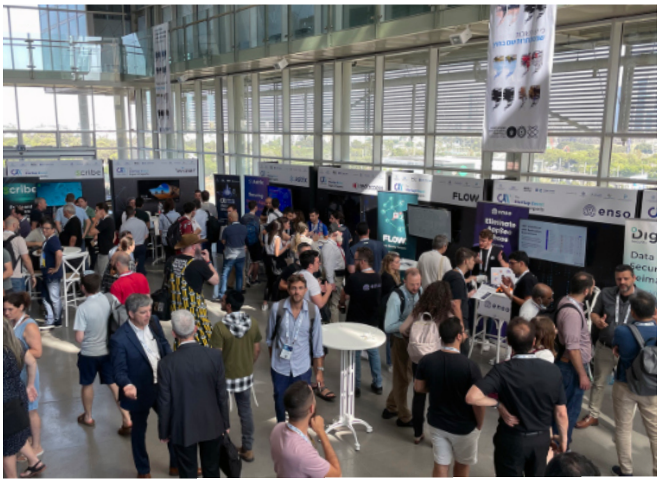
Cyber Week offers a unique gathering of cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials. With over 9,000 attendees from more than 80 countries, this conference offers an exchange of knowledge, methods, and ideas.

Cyber Week is held jointly by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office and the Ministry of Foreign Affairs.





Cyber Week 2022



Cyber Week 2022

Review: Enzoic for Active Directory

Hrvoje Martincic

Senior IT Consultant

Data breaches now happen so often that we don't even pause when reading yet another headline notifying us of the latest one. We react only if the breach happened to a service we use – and maybe not even then. But we should all be aware that once one of our passwords has been compromised and exposed, it should be considered compromised forever.

By gathering and analyzing passwords leaked after many breaches, attackers may work out specific users' password-creation patterns, allowing them to easily guess their passwords. Even worse: they don't need to discover those patterns and attempt to guess passwords, since many users **don't even bother to change their passwords** after a data breach.

By using honeypots or private personas to go into places where bad actors go, Enzoic researchers are continuously investigating data breaches and credential leaks so that organizations that don't have threat researchers can take advantage of the knowledge gleaned during the investigations.

What's new in Enzoic for Active Directory?

One of the strong points of the Enzoic for Active Directory solution is that it's fully compliant with NIST's password guidelines (as set out in **NIST Special Publication 800-63b**, which has been updated in 2020) helping organizations easily achieve industry best practices for passwords.

If you look at those guidelines, you can see that NIST has moved away from old password policy recommendations and has now suggests that users should focus on password blacklists over algorithmic complexity, with an emphasis on ensuring passwords are adequately hashed and salted. Additionally, organizations should not require their employees to reset their passwords unless there is evidence of compromise, and they should monitor new passwords daily, testing them against lists of more recent compromised passwords.

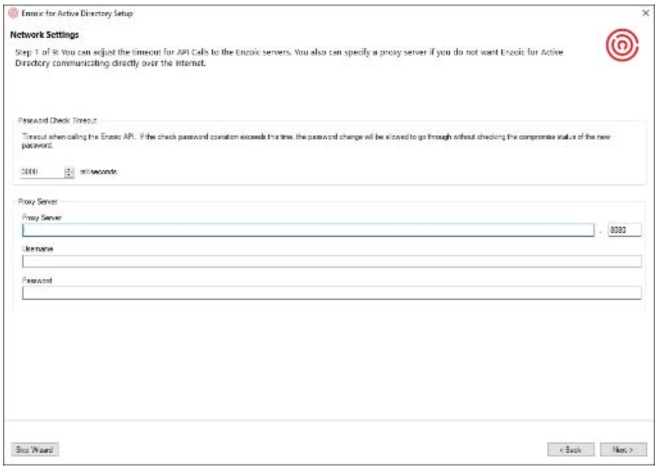
Of particular note is NIST's recommendation of eliminating periodic password resets if you have a method to detect whether credentials in use have become compromised. Here is where a tool like **Enzoic for Active Directory** can come in handy, as it checks passwords when they are created but also continues to check them daily against a constantly updated database.

In its most recent release (v3.2.318.0), Enzoic for Active Directory is going beyond just checking passwords to see whether they've been compromised generally - it now also checks full credential pairs (e.g., email address + password). And, throughout it all, it uses **k-anonymity**, a secure method using partial-hash data exchange to check passwords without the password or the hash leaving the customer's environment or cloud assets.

Installation

A setup assistant (wizard) allows for an easy installation and setup process, and helps users apply their new password policy with ease.

I installed the solution in my test environment via the domain administrator account, as elevated domain privileges are required to access Active Directory to select which users and groups will be monitored.


Enzoic for Active Directory Setup

Network Settings

Step 1 of 9: You can adjust the timeout for API Calls to the Enzoic servers. You also can specify a proxy server if you do not want Enzoic for Active Directory communicating directly over the internet.

Password Check Timeout

Timeout when calling the Enzoic API. If the check password operation exceeds this time, the password change will be allowed to go through without checking the compromise status of the new password.

3000 milliseconds

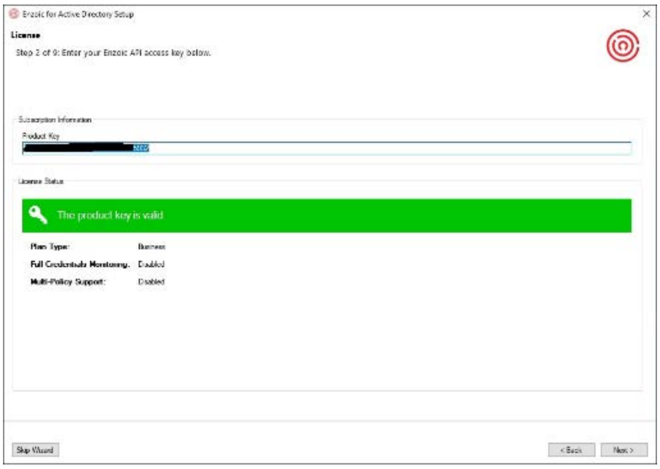
Proxy Server

Proxy Server: _ : 8080

Username: _

Password: _

Figure 1 – Network Settings


Enzoic for Active Directory Setup

License

Step 2 of 9: Enter your Enzoic API access key below.

Subscription Information

Product Key: [redacted]

License Status

The product key is valid

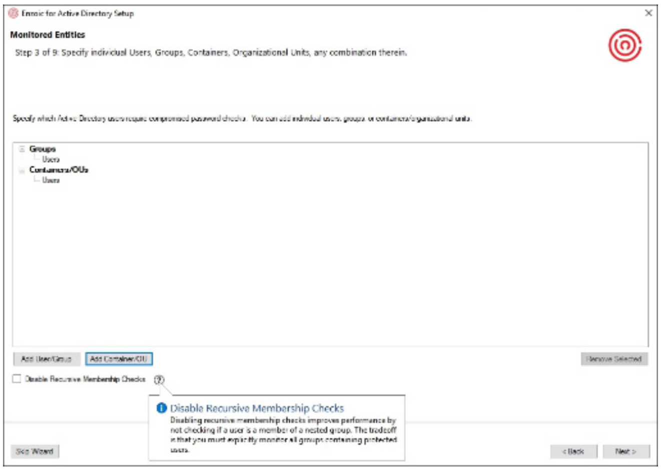
Plan Type: Business

Full Credentials Monitoring: Disabled

Multi-Policy Support: Disabled

Figure 2 – Enter the product key

After entering the necessary network and license information, I was offered the option of setting up groups and users to be monitored, followed by the option of letting the solution automatically choose the right configuration to achieve NIST 800-63b compliance (alternatively, you can customize settings manually).


Enzoic for Active Directory Setup

Monitored Entities

Step 3 of 9: Specify individual Users, Groups, Containers, Organizational Units, any combination therein.

Specify which Active Directory users require compromised password checks. You can add individual users, groups, or containers/organizational units.

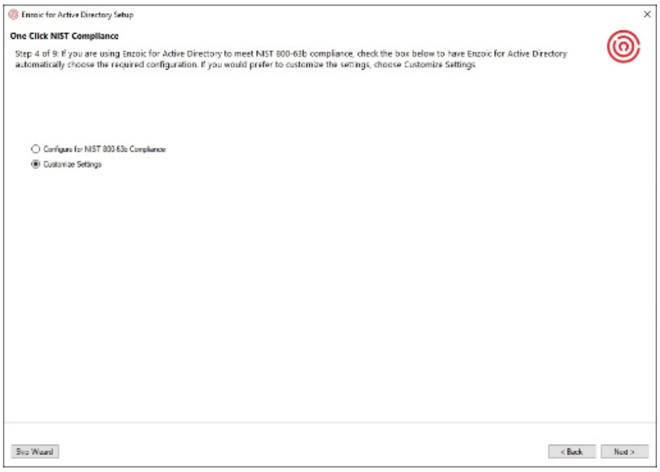
- Groups
  - Users
- Containers/OUs
  - Users

☐ Disable Recursive Membership Checks

Disable Recursive Membership Checks

Disabling recursive membership checks improves performance by not checking if a user is a member of a nested group. The tradeoff is that you must explicitly monitor all groups containing protected users.

Figure 3 - Setting up groups and users to be monitored


Enzoic for Active Directory Setup

One Click NIST Compliance

Step 4 of 9: If you are using Enzoic for Active Directory to meet NIST 800-63b compliance, check the box below to have Enzoic for Active Directory automatically choose the required configuration. If you would prefer to customize the settings, choose Customize Settings

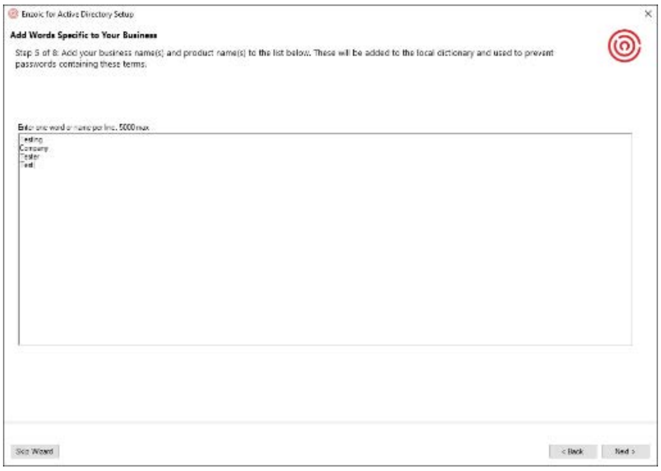
○ Configure for NIST 800-63b Compliance

● Customize Settings

Figure 4 – One Click NIST Compliance

By choosing the "One Click NIST Compliance" option, you can set up a new, NIST-compliant password policy in mere minutes (though not with just one click).

To begin with, you'll need to add words specific to your business (e.g., company name, product name, etc.) to a list that will be used to create a local custom password dictionary. The solution will use that local dictionary to prevent employees from creating predictable and easily guessable passwords that could be easily connected to your company. By cutting this link, you are limiting options for the attacker. All dictionary and compromised passwords are automatically handled by Enzoic, so your custom dictionary can be concise.


Enzoic for Active Directory Setup

Add Words Specific to Your Business

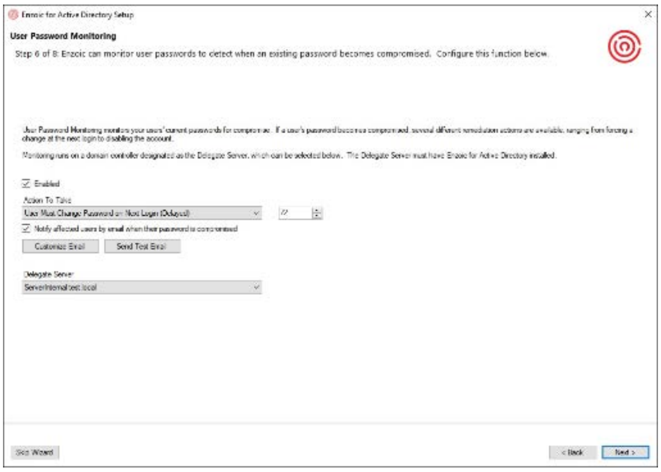
Step 5 of 8: Add your business name(s) and product name(s) to the list below. These will be added to the local dictionary and used to prevent passwords containing these terms.

Enter one word or name per line. 5000 max

Testing
Company
Tester
Test

Figure 5 – Creating a list of words specific to your business

Next, you are given the option to enable User Password Monitoring and select the remediation actions users will have to go through if their password becomes compromised. I like the option to add a delay before automatically requiring a password change or disabling the account.


Enzoic for Active Directory Setup

User Password Monitoring

Step 6 of 8: Enzoic can monitor user passwords to detect when an existing password becomes compromised. Configure this function below.

User Password Monitoring monitors your users' current passwords for compromise. If a user's password becomes compromised, several different remediation actions are available, ranging from forcing a change at the next login to disabling the account.

Monitoring runs on a domain controller designated as the Delegate Server, which can be selected below. The Delegate Server must have Enzoic for Active Directory installed.

☑ Enabled

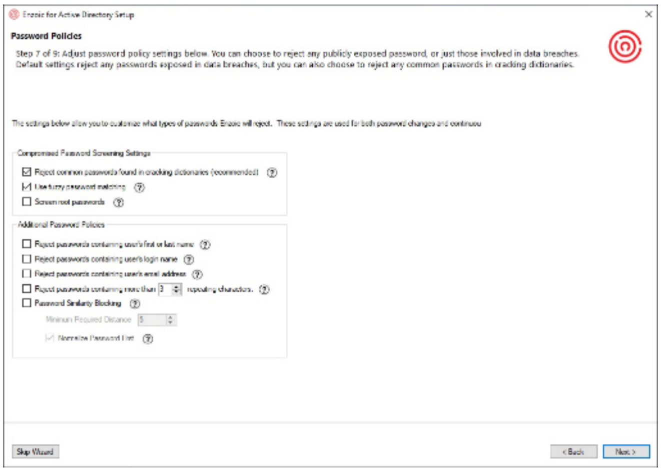
Action To Take: User Must Change Password on Next Login (Delayed) 72

☑ Notify affected users by email when their password is compromised

Delegate Server: Server.internal.test.local

Figure 6 - Setting up User Password Monitoring

The alternative to "One Click NIST Compliance" is to choose your own settings. This includes deciding if you want to enable User Password Monitoring (as pictured above) and which individual password policy settings for your organization's policies and requirements:


Enzoic for Active Directory Setup

Password Policies

Step 7 of 9: Adjust password policy settings below. You can choose to reject any publicly exposed password, or just those involved in data breaches. Default settings reject any passwords exposed in data breaches, but you can also choose to reject any common passwords in cracking dictionaries.

The settings below allow you to customize what types of passwords Enzoic will reject. These settings are used for both password changes and continuou

Compromised Password Screening Settings

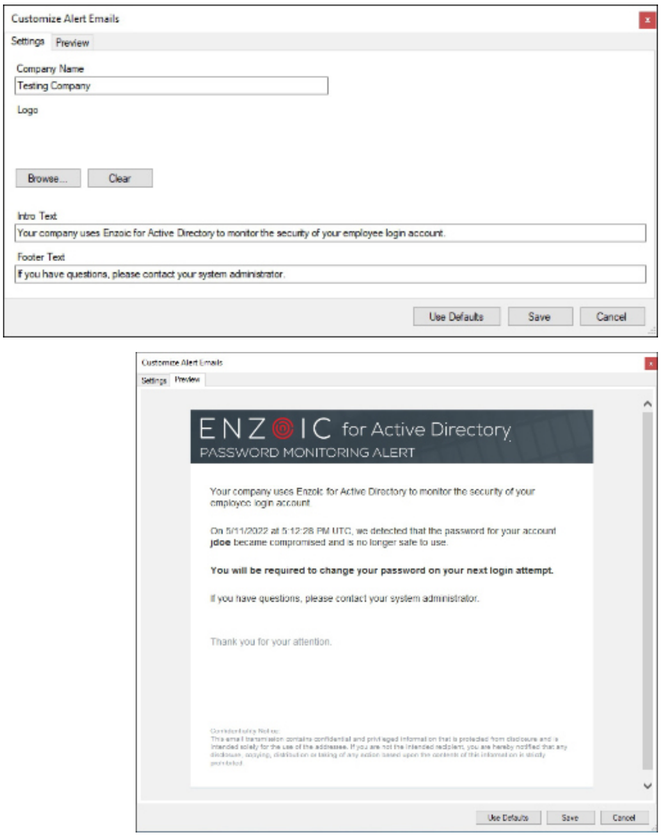
- ☑ Reject common passwords found in cracking dictionaries (recommended)
- ☑ Use fuzzy password matching
- ☐ Screen root passwords

Additional Password Policies

- ☐ Reject passwords containing user's first or last name
- ☐ Reject passwords containing user's login name
- ☐ Reject passwords containing user's email address
- ☐ Reject passwords containing more than 3 repeating characters.
- ☐ Password Similarity Blocking
  - Minimum Required Distance 5
  - ☑ Normalize Password List

Figure 7 – Choosing specific password policies

Regardless of your installation path of choice, you can customize and preview the email alerts that will be sent to your employees if their password is no longer safe to use:


Customize Alert Emails

Settings | Preview

Company Name: Testing Company

Logo

Intro Text: Your company uses Enzoic for Active Directory to monitor the security of your employee login account.

Footer Text: If you have questions, please contact your system administrator.

Customize Alert Emails

Settings | Preview

ENZOIC for Active Directory
PASSWORD MONITORING ALERT

Your company uses Enzoic for Active Directory to monitor the security of your employee login account.

On 5/11/2022 at 5:12:28 PM UTC, we detected that the password for your account **jdoe** became compromised and is no longer safe to use.

You will be required to change your password on your next login attempt.

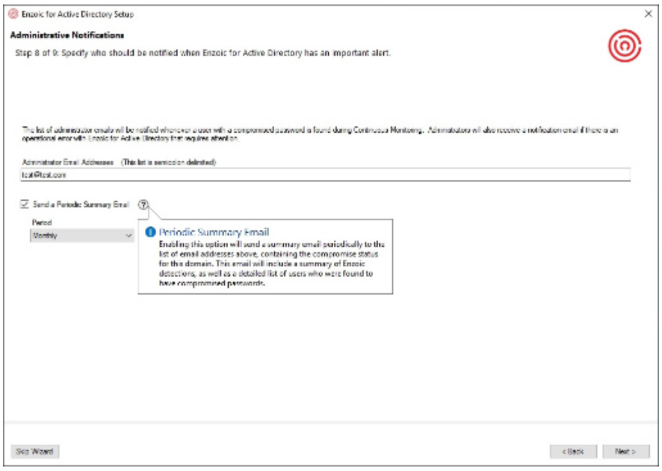
If you have questions, please contact your system administrator.

Thank you for your attention.

Confidentiality Notice:
This email transmission contains confidential and privileged information that is protected from disclosure and is intended solely for the use of the addressee. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking of any action based upon the contents of this information is strictly prohibited.

Figure 8 and 9 - Customizing and preview of email alerts

Next, you must specify which administrators will be notified when the solution has an important alert:



Enzoic for Active Directory Setup

Administrative Notifications

Step 8 of 9: Specify who should be notified when Enzoic for Active Directory has an important alert.

The list of administrator emails will be notified whenever a user with a compromised password is found during Continuous Monitoring. Administrators will also receive a notification email if there is an operational error with Enzoic for Active Directory that requires attention.

Administrator Email Addresses (This list is semicolon delimited)

test@test.com

☑ Send a Periodic Summary Email

Period: Monthly

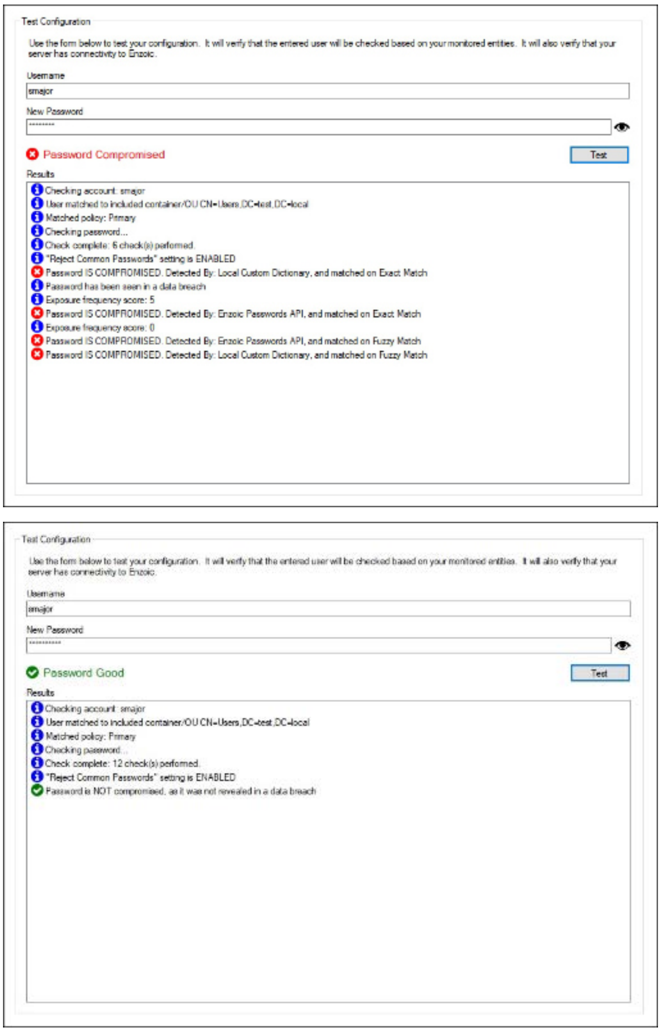
Periodic Summary Email
Enabling this option will send a summary email periodically to the list of email addresses above, containing the compromise status for this domain. This email will include a summary of Enzoic detections, as well as a detailed list of users who were found to have compromised passwords.

Figure 10 - Administrative Notification settings

Admins who have been added to the list to receive administrative notifications will be notified every time a monitored user with a compromised password is found in the system during Continuous Monitoring, although most organizations will set up the automatic remediation that handles requiring a password reset at noted above. Admins will also receive notifications in case of operational error with the software, as they must resolve the situation.

You can also make it so they receive a periodic summary email that will provide additional insight by delivering a compromise status for the monitored domain, a summary of Enzoic's detections and a list of users with compromised passwords in a specified time frame. This can be helpful for documenting password policy compliance for auditors.

Finally, you can test the settings configured during the installation. The test checks whether the password chosen by a specific user complies with your password policy and whether it has been compromised (by comparing it against Enzoic's database of billions of common and compromised credentials). Enzoic suggests most checks take around 250 milliseconds, and I can confirm the password check takes well under a second:



Test Configuration

Use the form below to test your configuration. It will verify that the entered user will be checked based on your monitored entities. It will also verify that your server has connectivity to Enzoic.

Username: smajor

New Password: *********

Password Compromised

Results

```
Checking account: smajor
User matched to included container/OU CN=Users,DC=test,DC=local
Matched policy: Primary
Checking password...
Check complete: 6 check(s) performed.
"Reject Common Passwords" setting is ENABLED
Password IS COMPROMISED. Detected By: Local Custom Dictionary, and matched on Exact Match
Password has been seen in a data breach
Exposure frequency score: 5
Password IS COMPROMISED. Detected By: Enzoic Passwords API, and matched on Exact Match
Exposure frequency score: 0
Password IS COMPROMISED. Detected By: Enzoic Passwords API, and matched on Fuzzy Match
Password IS COMPROMISED. Detected By: Local Custom Dictionary, and matched on Fuzzy Match
```

Test Configuration

Use the form below to test your configuration. It will verify that the entered user will be checked based on your monitored entities. It will also verify that your server has connectivity to Enzoic.

Username: smajor

New Password: **********

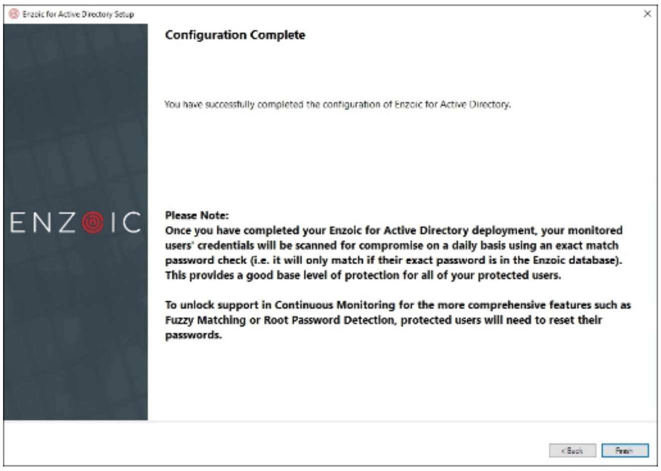
Password Good

Results

```
Checking account: smajor
User matched to included container/OU CN=Users,DC=test,DC=local
Matched policy: Primary
Checking password...
Check complete: 12 check(s) performed.
"Reject Common Passwords" setting is ENABLED
Password is NOT compromised, as it was not revealed in a data breach
```

Figure 11 and 12 – Testing a password

And that's it! The software is installed, up and running, applied to a Windows domain environment, protecting monitored users right away.



Enzoic for Active Directory Setup

Configuration Complete

You have successfully completed the configuration of Enzoic for Active Directory.

Please Note:
Once you have completed your Enzoic for Active Directory deployment, your monitored users' credentials will be scanned for compromise on a daily basis using an exact match password check (i.e. it will only match if their exact password is in the Enzoic database). This provides a good base level of protection for all of your protected users.

To unlock support in Continuous Monitoring for the more comprehensive features such as Fuzzy Matching or Root Password Detection, protected users will need to reset their passwords.

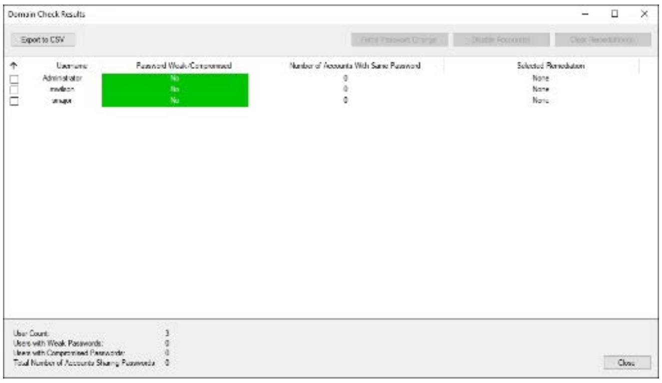
Figure 13 - Completed installation (with some limitations)

Enzoic states that to fully unlock the potential of the software – e.g., more comprehensive features such as “Fuzzy Matching” and “Root Password Detection” - a password reset is required for all monitored users. As a domain-wide user password reset is not possible in all environments nor convenient right after the installation, Enzoic made the right choice to leave these features disabled. It’s on administrators to decide if/when to enable them.

Use

Once installation and setup are complete, Enzoic for Active Directory will ask you if you want to run an initial scan of your domain to identify monitored users with compromised passwords.

This scan will reveal users with the compromised or weak passwords and accounts that share passwords, and I recommend running it right away.

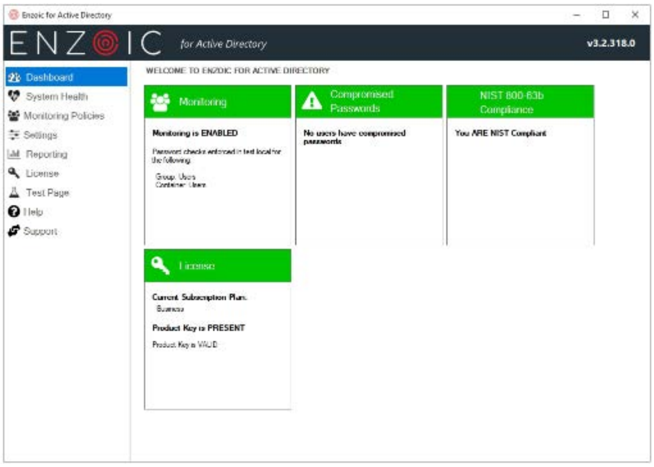


↑	Username	Password Weak/Compromised	Number of Accounts With Same Password	Selected Remediation
□	Administrator	No	0	None
□	[illegible]	No	0	None
□	[illegible]	No	0	None

User Count:	3
Users with Weak Passwords:	0
Users with Compromised Passwords:	0
Total Number of Accounts Sharing Passwords	0

Figure 14 – The results of the initial scan of the domain

Looking at the dashboard, I can say that Enzoic tried and succeed in keeping things simple and tidy. I could argue that the color scheme could be toned down, but that’s not an issue – just a personal preference.



WELCOME TO ENZOIC FOR ACTIVE DIRECTORY

Monitoring is ENABLED

Password checks enforced in test.local for the following:

Group: Users
Container: Users

No users have compromised passwords

You ARE NIST Compliant

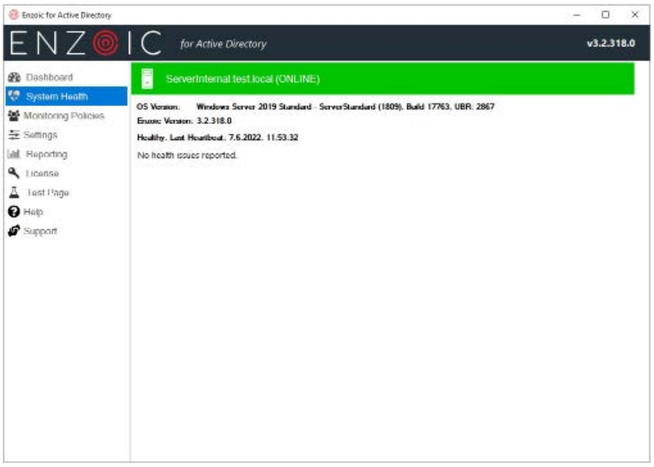
Current Subscription Plan:
Business

Product Key is PRESENT

Product Key is VALID

Figure 15 – The solution’s dashboard

The System Health tab provides an overview of possible issues with the Enzoic for Active Directory, enabling you to quickly detect and diagnose them.



ServerInternal.test.local (ONLINE)

OS Version: Windows Server 2019 Standard - ServerStandard (1809), Build 17763, UBR: 2867

Enzoic Version: 3.2.318.0

Healthy. Last Heartbeat: 7.6.2022. 11.53.32

No health issues reported.

Figure 16 - System Health info

All the options you have initially chosen during the installation and setup process can be changed.

In the Monitoring Policies tab you can add additional policies (if supported by your software license), but also configure the monitoring policy to fit your needs.

- Monitored Entities – Fine tune Active Directory users and groups to be monitored

- Password Changes – Enable protection for monitored entities during password change

- Password Monitoring – Enable continuous, daily checking of how it behaves when it finds compromised user passwords

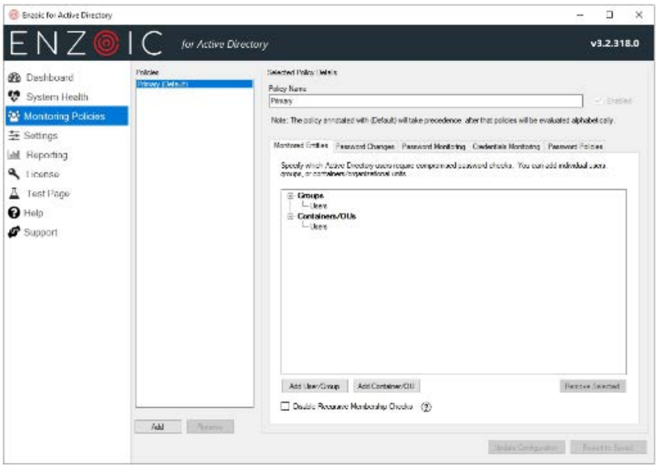
- Credentials Monitoring – Customize actions when full credentials (username + password pair) are compromised.

- Password Policies – Customize what types of passwords will be rejected

User Credentials Monitoring

User Credentials Monitoring checks every day if the exact email/password combination has become compromised. Since this type of compromise presents a level of high risk, I would always recommend disabling the user until the situation is investigated either by admins or dedicated security team.

Access to full credentials is a treasure trove for attackers, as it greatly simplifies access to the target system. This is exactly why taking advantage of the User Credentials Monitoring option provides an additional level of protection most organizations should be using.



Policies: Primary (Default)

Selected Policy Details

Policy Name: Primary ☑ Enabled

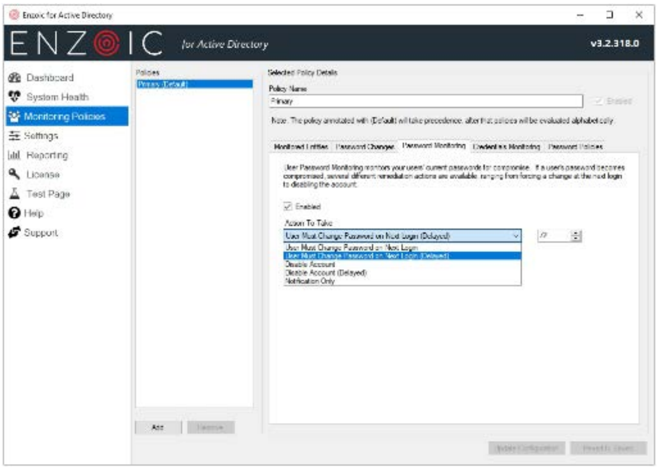
Note: The policy annotated with (Default) will take precedence, after that policies will be evaluated alphabetically.

Specify which Active Directory users require compromised password checks. You can add individual users, groups, or containers/organizational units.

```
⊟ Groups
   └ Users
⊟ Containers/OUs
   └ Users
```

☐ Double Recursive Membership Checks (?)

Figure 17 – Choose monitored users and groups



Policies: Primary (Default)

Selected Policy Details

Policy Name: Primary ☑ Enabled

Note: The policy annotated with (Default) will take precedence, after that policies will be evaluated alphabetically.

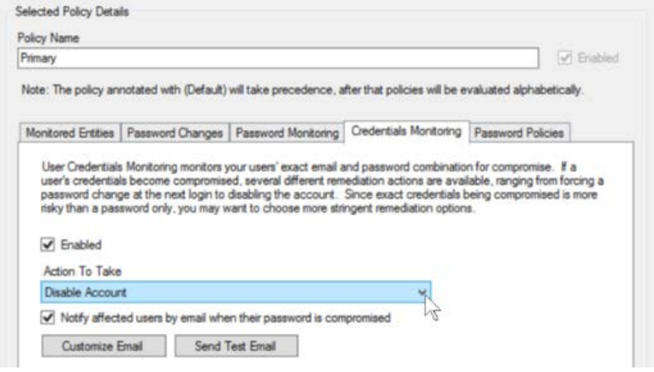
User Password Monitoring monitors your users' current passwords for compromise. If a user's password becomes compromised, several different remediation actions are available, ranging from forcing a change at the next login to disabling the account.

☑ Enabled

Action To Take: User Must Change Password on Next Login (Delayed)

User Must Change Password on Next Login
User Must Change Password on Next Login (Delayed)
Disable Account
Disable Account (Delayed)
Notification Only

Figure 18 – Enable or disable Password Monitoring



Selected Policy Details

Policy Name: Primary ☑ Enabled

Note: The policy annotated with (Default) will take precedence, after that policies will be evaluated alphabetically.

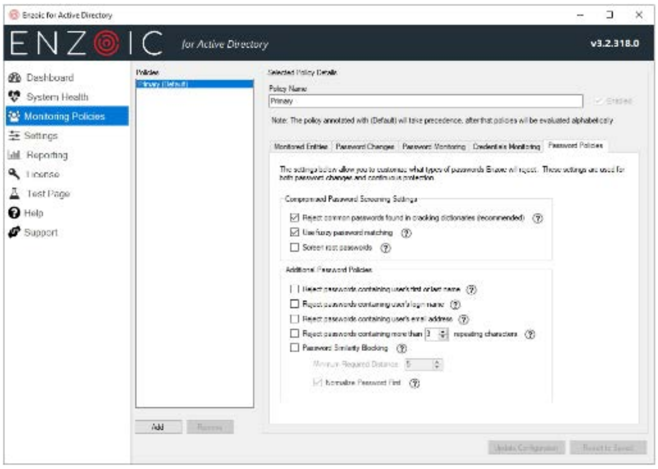
User Credentials Monitoring monitors your users' exact email and password combination for compromise. If a user's credentials become compromised, several different remediation actions are available, ranging from forcing a password change at the next login to disabling the account. Since exact credentials being compromised is more risky than a password only, you may want to choose more stringent remediation options.

☑ Enabled

Action To Take: Disable Account

☑ Notify affected users by email when their password is compromised

Figure 19 - Add checking of full credentials (email/password combo)



Policies: Primary (Default)

Selected Policy Details

Policy Name: Primary ☑ Enabled

Note: The policy annotated with (Default) will take precedence, after that policies will be evaluated alphabetically.

The settings below allow you to customize what types of passwords Enzoic will reject. These settings are used for both password changes and continuous protection.

Compromised Password Screening Settings

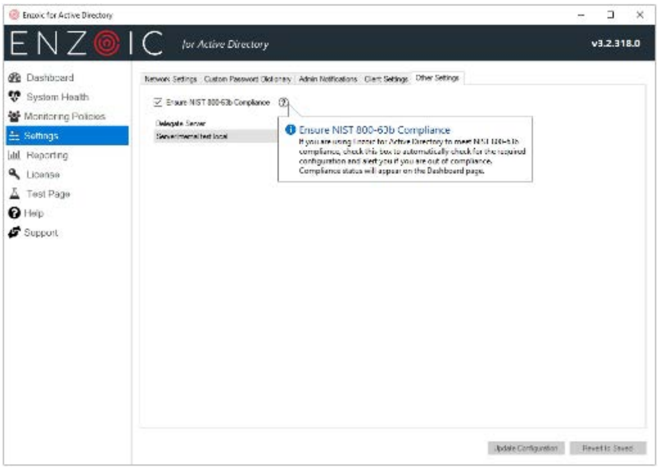
☑ Reject common passwords found in cracking dictionaries (recommended) (?)
☑ Use fuzzy password matching (?)
☐ Screen root passwords (?)

Additional Password Policies

☐ Reject passwords containing user's first or last name (?)
☐ Reject passwords containing user's login name (?)
☐ Reject passwords containing user's email address (?)
☐ Reject passwords containing more than 3 repeating characters (?)
☐ Password Similarity Blocking (?)
Minimum Required Distance: 5
☑ Normalize Password First (?)

Figure 20 - Customize what types of passwords will be rejected

All Settings are configurable here in one place: You can change network settings, add new words to your custom password dictionary, change which admins will be receiving alerts, and make sure your password policies will adhere to NIST standards.



☑ Ensure NIST 800-63b Compliance

Delegate Server: Server.internal.test.local

Ensure NIST 800-63b Compliance
If you are using Enzoic for Active Directory to meet NIST 800-63b compliance, check this box to automatically check for the required configuration and alert you if you are out of compliance. Compliance status will appear on the Dashboard page.

Figure 21 - General Settings

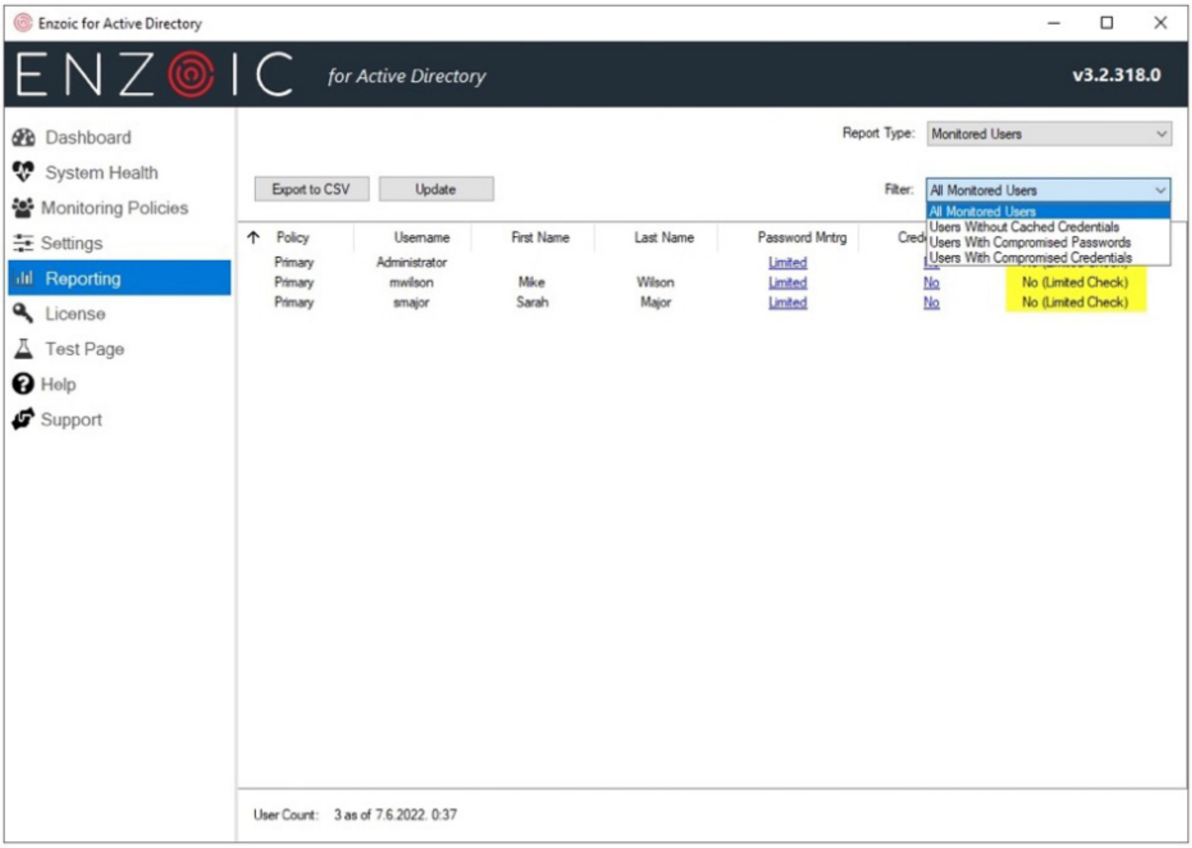
Reports based on "Monitored users," "Password Change," and "Continuous Monitoring" can be generated and exported to CSV:

Verdict

Enzoic for Active Directory combines real-time password policy enforcement with continuous password auditing and automated remediation, allowing you to keep unsafe and compromised passwords out of Active Directory.

By using Enzoic for Active Directory organizations of all types and sizes can implement NIST 800-63b password guideline requirements in minutes and monitor and clean their AD environment of vulnerable or compromised passwords.

In my humble opinion: If you're searching for such a service or if you're looking for a password policy tool that offers protection from leaked credentials with daily updates, Enzoic for Active Directory is a candidate you should strongly consider.



Report Type: Monitored Users

Filter: All Monitored Users
- All Monitored Users
- Users Without Cached Credentials
- Users With Compromised Passwords
- Users With Compromised Credentials

Policy	Username	First Name	Last Name	Password Mntrg	Cred	
Primary	Administrator			Limited	[illegible]	[illegible]
Primary	mwilson	Mike	Wilson	Limited	No	No (Limited Check)
Primary	smajor	Sarah	Major	Limited	No	No (Limited Check)

User Count: 3 as of 7.6.2022. 0:37

Figure 22 - Reporting options

Industry news

Crossword Cybersecurity Supply Chain Cyber practice improves supply chain resilience for organizations

In response to client demand and the substantial increase in supply chain cyber threat levels, the integrated practice provides a set of controls, processes and tools, along with a range of managed services, advice and training to massively reduce the risk of direct cyber-attacks as well as threats via third parties across a company's supply chain.

The practice provides an end-to-end approach to supply chain cybersecurity and includes a standard operating model (SOM) and a substantially updated version of Rizikon Assurance, Crossword's SaaS platform used by supplier management and cybersecurity teams and across an organization to underpin the controls, tools and data needed to reduce supply chain risk.

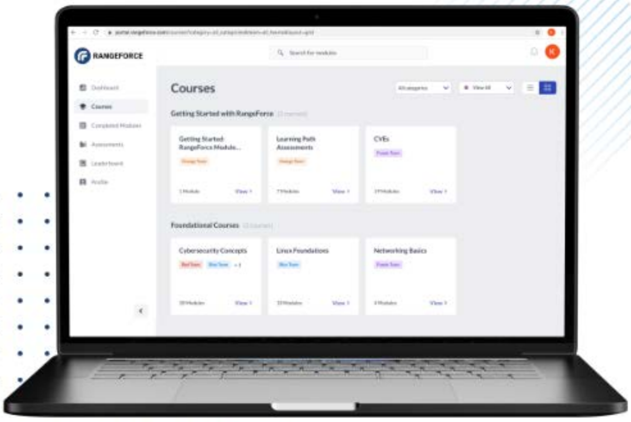
Cato Networks detects and interrupts ransomware with network-based ransomware protection

With this announcement, Cato's heuristic algorithms inspect all SMB protocol flows for ransomware. SMB is the protocol used by Windows to share files and folders.

Cato researchers trained and tested these algorithms against Cato's massive data warehouse, a data lake of end-to-end attributes for all traffic flows processed by the Cato SASE Cloud. Being the network, Cato has visibility into data normally blocked by firewalls and NATs. More than a trillion flows from all Cato-connected edges – sites, users, IoT devices, cloud-connected resources, and the Internet resources – populate Cato's data lake.

Once trained, the machine-learning heuristic algorithms inspect live SMB traffic flows for a combination of network attributes.

RangeForce platform updates enable users to conduct offensive and defensive attack scenarios



RangeForce announced it has enhanced its team threat exercises platform with new capabilities that make it easier for organizations to accelerate the skills development of their security teams through multi-user detection and response exercises of emulated attacks.

RangeForce team threat exercises enable security teams to configure the security stack to be protected, choose an attack scenario, execute the threat exercise, review post-exercise results and develop a targeted training plan.

Using high-intensity, real-world attack scenarios that require teams of security professionals to find and stop cyber threats, RangeForce threat exercises create realistic digital artifacts of both signal and noise that require teams to demonstrate their cyber readiness.

Immersive Labs Cyber Team Sim prepares teams for real-life cyber attacks

Immersive Labs announced the launch of technical multiplayer simulations, including scenarios for both offensive and defensive teams in complex environments.

This capability offers security teams the ability to use their own tool sets for a more relevant hands-on experience. The simulations run on Immersive Labs' award-winning Cyber Workforce Optimization platform that evaluates and improves an organization's cyber readiness and resilience.

The new capability, Cyber Team Sim, enables organizations to prepare teams for real-life cyber attacks through regular, collaborative practice in complex and realistic virtual scenarios. The new simulations are supported by Immersive Labs' acquisition of Snap Labs in 2021, which brought the technology to create complex custom virtual environments on demand. New scenarios are released to simulate the latest vulnerabilities and prepare the workforce to defend against developing threats.

The Immersive Labs' platform helps security and executive leadership to identify skill gaps and opportunities to improve judgment in various scenarios so that they can remedy areas of weakness ahead of real-world attacks. Available now, Cyber Team Sim includes analysis of technical tasks and evaluation of the collaboration among the red or blue teams.

CyberArk Endpoint Privilege Manager protects Linux systems by enforcing least privilege policies

Linux is widely applicable to various types of operations – everything from smartphones to cloud computing – and runs 90% of all public cloud workloads. In a recent survey, 83.1% of developers said Linux is the platform they prefer to work on. It's so popular that in 2021, Linux ran on 100% of the world's 500 supercomputers.

However, many Linux administrators find it challenging to enforce least privilege policies on DevOps engineers or application owners that access Linux servers while maintaining least privilege controls on Linux machines without creating friction for end users.

CyberArk Endpoint Privilege Manager for Linux is a SaaS solution that provides configuration and enforcement of least privilege policy. Linux administrators benefit from capabilities that enable them to quickly build the right policy rules for their users and reduce the manual work typically required to maintain these policies.

Endpoint Privilege Manager for Linux can monitor and automatically detect privileged activity. It then helps administrators decide whether privileged access rights should be approved or blocked, and easily update the policy accordingly. Security teams and Linux administrators gain critical visibility and control over what users can run and execute on Linux systems.

Enveil ZeroReveal ML Encrypted Training enables secure usage of cross-silo data sources

The enterprise-ready product extends the boundary of trusted compute by enabling encrypted federated learning and the secure usage of disparate, decentralized datasets for machine learning applications.

Designed to address specific customer pain points, ZMET allows organizations to train models in an encrypted capacity while ensuring the model development process, the model itself, and the interests to all parties involved remain protected. The product expansion, an extension of Enveil's machine learning solution suite, comes on the heels of the company's $25 million Series B funding announcement.

Normalyze emerges from stealth and raises $22.2 million to help organizations manage sensitive data

This round brings the company's total funding to $26.6M to date. Normalyze is an agentless platform that helps organizations better manage sensitive data—and attack paths to it —in today's complex, multi-cloud environments, protecting customers from large and damaging data breaches.

Palo Alto Networks adds new cloud security features to help organizations secure web applications

Over the last two years, organizations have expanded their use of cloud environments by more than 25%. Many are now struggling to manage the technical complexity of cloud migration, including the ability to secure their applications across the entire application development lifecycle.

Palo Alto Networks announced the addition of Out-of-Band Web Application and API Security (Out-of-Band WAAS) to Prisma Cloud to help organizations secure web applications with maximum flexibility.

Until now, a primary industry approach to securing web applications has been to deploy inline web application firewalls (WAFs). Some organizations are reluctant to introduce WAFs or API security solutions inline, however, due to performance and scalability concerns. With this announcement, Prisma Cloud can provide organizations with deep web and API security both inline and out of band, allowing them to choose how to protect their applications in the cloud.

CyberStrong 3.20 empowers customers to automate the assessment process

CyberSaint released CyberStrong version 3.20, providing customers with the ability to further automate the assessment process via continuous control automation with Tenable and Microsoft Azure Security Center integrations.

“CyberSaint’s continuous control automation functionality changes the way that security and risk teams perform assessments, and ultimately, manage cyber risk,” said Jerry Layden, CEO of CyberSaint. “Being first-to-market with this technology is exciting for us, and positions us to redefine the cyber and IT risk management market at large.”

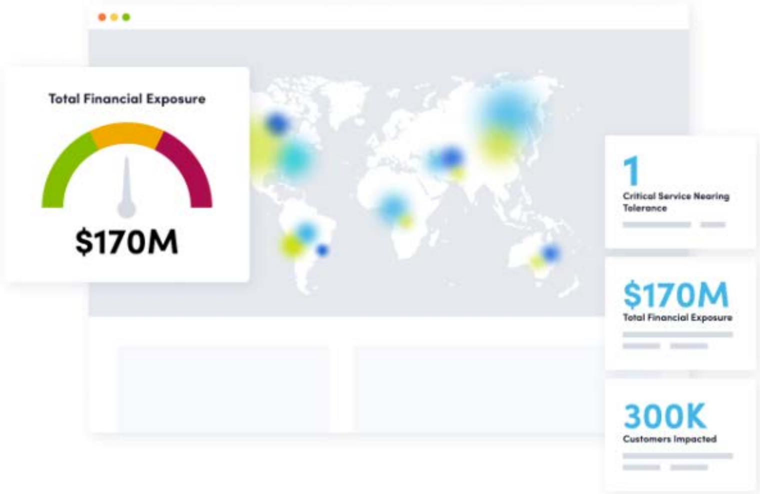
Until now, the process of assessing an organization’s cybersecurity risk posture against a framework or standard has been manual. CyberStrong’s continuous control automation leverages natural language processing (NLP) to map telemetry coming in from various security products, such as Tenable and Microsoft Azure Security Center, to controls in a customer environment, automating scores at the control level and pulling in evidence.

Menlo Security HEAT Security Assessment Toolkit provides insight into current exposure to HEAT attacks

The HEAT Security Assessment Toolkit provides a lightweight penetration and exposure assessment to help an organization better understand their susceptibility to HEAT attacks.

“HEAT attacks are defined by the techniques that adversaries are increasingly using to evade detection by traditional security tools,” said Mark Guntrip, senior director of cybersecurity strategy, Menlo Security. “HEAT techniques can be used individually or in combination for any type of attack that targets the user, endpoint, or applications, including ransomware. The HEAT Security Assessment Toolkit is critical to helping companies ensure they are protected against these attacks.”

Fusion Risk Management announces new capabilities to improve incident response for organizations



The new Intelligent Incident Manager is a purpose-built solution that enables organizations to identify the full scope of an incident and recognize impacted assets or known outages.

The expanded Dynamic Response features build on existing capabilities to drive data-driven response plays that are tailored to any business issue. The new functionality leverages dynamic response strategies instead of static plans to quickly react in line with the situation when disruption occurs.

Response strategies are dynamic runbooks of procedures compiled in real-time based on a unified picture of business operations and the current operating environment. Organizations will now be able to reduce time spent on response planning through flexible diagnostic and remediation procedures that can be flexibly combined into plays based on what the situation commands.

Inspectiv raises $8.6 million to help companies protect against security threats

Inspectiv is a vulnerability detection platform that combines intelligence from crowdsourced security testing and proprietary vulnerability scanning to help companies continuously identify, remediate, and protect against security threats.

The new Series A funding round, led by StepStone Group with Fika Ventures, Freestyle and Mucker Capital, brings Inspectiv's total funding to more than $16 million. These investments — including follow-on funding from seed-stage investors — are an endorsement of Inspectiv's rapid success in the security field and position the platform for its next stage of growth.

Resecurity's cybersecurity solutions now available in the Microsoft Azure marketplace

Resecurity's AI-powered solutions provide proactive alerts and comprehensive visibility of digital risks targeting the enterprise ecosystem.

Microsoft's Azure Marketplace is the most comprehensive marketplace on the planet, offering thousands of certified cloud applications and software to over four million active users and subscribers. By joining the Microsoft Azure marketplace, Resecurity's software solutions will be easily accessible to the millions of Microsoft Azure customers needing comprehensive cybersecurity management and monitoring.

Darktrace adds early warning system to its Antigena Email solution

Darktrace announced that its Antigena Email product has added an early warning system, allowing members of the Darktrace community to contribute and benefit from insights gleaned from across the fleet.

This new capability is now available to Antigena Email users and includes the extension of anonymized, learned domain behavioral profiles across Darktrace's expansive and diverse group of global customers.

"Darktrace stops all kinds of cyber-attacks against organizations in every sector in over 110 countries globally. That represents a huge bank of knowledge about how malicious payloads behave in the very earliest stage of a cyber-attack," commented Jack Stockdale, OBE, Darktrace CTO. "Antigena Email has now realized the vision of leveraging collaborative, anonymized insights to leave attackers with nowhere to hide."

Ninety-four percent of cyber-attacks begin in the inbox. As organizations continue to rely on email as a primary workplace collaboration tool and attacks become increasingly novel and sophisticated, email security technologies that rely on behavior rather than threat intelligence become more imperative.

Darktrace's Self-Learning AI observes emails to build bespoke behavioral profiles for each customer and leverages these behavioral profiles, rather than a ledger of binary 'good' or 'bad,' to accurately determine whether each email belongs in a recipient's inbox. Antigena Email uniquely analyzes domains within email addresses and links in email bodies and attachments to evaluate their popularity and typical presence in the inbox.

Cloudflare One enhancements strengthen zero trust security for organizations

New features for Cloudflare One include sophisticated email security protection, data loss prevention tools, cloud access security broker (CASB), and private network discovery. Now, any organization can use Cloudflare One for a comprehensive and deeply-integrated zero trust security and networking solution to protect and accelerate the performance of devices, applications, and entire networks to keep workforces secure and productive.

"When I sit with customers, they share that one of the most daunting aspects of Zero Trust security is simply where to begin. Making matters worse, every vendor has a different definition for Zero Trust, turning a critical approach to security into a misunderstood and overused term," said Matthew Prince, co-founder and CEO of Cloudflare. "We believe Zero Trust must extend to the entire network, all the way from email to data centers, and accelerate user and endpoint connections, not slow people down. And we want to give every customer a step-by-step guide for what they can do today, this week, and this month to make themselves more secure regardless of what vendor they use."

Arcserve N Series appliances allow organizations to protect their digital assets

Arcserve N Series hyper-converged data protection appliances combine orchestrated recovery using Arcserve UDP, the flexible scale-out design of Nutanix, and ransomware protection of the backup system with Sophos Intercept X Advanced cybersecurity.

Converging industry-leading data protection technologies in a single appliance, the new Arcserve N Series allows organizations to simplify their IT environments and secure data with an all-in-one backup and recovery appliance. Arcserve N Series enables customers to protect any type and number of workloads across physical, virtual, and cloud environments.

Businesses are challenged to manage exponential data growth and maintain the high performance of critical systems while protecting vital information from ever-increasing ransomware threats. Available immediately, the new N Series appliances, named N1100-4, and N1200-4, offer a new approach to storing, managing, and protecting data that reduces complexity and TCO.

Portnox unveils new cloud-native tool to help midmarket businesses simplify network security

Portnox released a cloud-native Terminal Access Controller Access Control Server (TACACS+) solution to help midmarket businesses manage network device administration and access management across increasingly distributed networks.

Continuing its commitment to delivering network security products that are easy for the mid-market to use, scale and maintain, the new cloud-native Portnox TACACS+-as-a-Service offering empowers users to easily enforce network authentication, authorization, and accounting (AAA) services and policies for network devices – functionality once only available to large enterprises. Offering a free entry-level tier, Portnox now allows any organization to deploy this must-have network security technology for up to 100 network devices – such as wireless access points and wired switches – under the authority of a single administrator.

IOTech Edge XRT 2.0 simplifies the development of time-critical OT applications

Edge XRT 2.0 greatly simplifies the development of OT applications and enables faster time-to-market for new edge systems. It is hardware agnostic, independent of the silicon provider (Intel or ARM) and operating system. Users have complete deployment flexibility. They can deploy it as a native application, containerized and/or into a virtualized environment.

With its small memory footprint and efficient use of computing resources, Edge XRT 2.0 is also suitable for microcontroller-based applications where CPU and memory resources are limited. This makes it ideal for use cases such as connected commercial or consumer electronic devices (e.g., refrigeration unit), medical device applications or automotive engine management systems.

GLEIF partners with PharmaLedger to secure sensitive healthcare data with digital ID

A collaboration between GLEIF and PharmaLedger has resulted in the Legal Entity Identifier (LEI) becoming a critical component of a new healthcare service blockchain platform.

The partnership enables a digitally trusted ecosystem, designed to support innovation, and benefit all global healthcare stakeholders involved – from manufacturers to patients. The digital trust enabled by the verifiable LEI (vLEI) promises to vastly increase the operational efficiency of the global healthcare industry. This also results in the digital exchange of data and documentation relating to a wide range of use cases, including patient health, clinical drug trials and supply chain partnerships.

PharmaLedger, a project sponsored by the Innovative Medicines Initiative (IMI) and the European Federation of Pharmaceutical Industries and Associations (EFPIA), brings together 12 global pharmaceutical companies and 17 public and private entities. PharmaLedger has been a key participant in GLEIF's cross-industry vLEI development program and will be one of the first service providers globally to integrate GLEIF's new organizational identity credential into its system.

Schneider Electric and Claroty launch a solution that protects smart buildings from cyber risks

Schneider Electric launched Cybersecurity Solutions for Buildings, a solution that helps all buildings customers secure their building management systems (BMS) to protect their people, assets and operations.

The joint solution with Claroty, the security company for cyber-physical systems across industrial, healthcare, and commercial environments, will combine award-winning technology with Schneider Electric industry expertise and services to identify all facility-wide assets, deliver unmatched risk and vulnerability management capabilities, and provide continuous threat monitoring to protect enterprise investments.

Fifty percent of today's buildings are likely to be still in use by 2050. This is driving commercial buildings to digitize their assets, including modernizing their building management system. In fact, IoT technology for buildings is expected to grow from an existing 1.7 billion connected devices at the end of 2020 to over 3 billion by 2025. As these commercial buildings evolve into smart buildings of the future, they share at least one common trait: heightened exposure to risks.

An offensive mindset is crucial for effective cyber defense

John DeSimone

President of Cybersecurity, Intelligence and Services, Raytheon Intelligence & Space

As ransomware attacks continue to increase and cybercriminals are becoming more sophisticated, the federal government has implemented a more proactive approach when it comes to cybersecurity. As evidenced by its stated strategy to adopt a zero trust architecture, the federal government is taking measures to reduce the risk of cyberattacks against its digital infrastructure, and setting specific security goals for agencies to quickly detect, isolate and respond to threats. This approach is also exemplified by the extension of its Industrial Control Systems Cybersecurity Initiative, which is aimed at facilitating the deployment of technologies and systems that provide cyber-related threat visibility, indicators, detections and warnings to the water infrastructure.

There are three main components for organizations to consider when developing a defensive strategy based on an offensive cyber model: re-envisioning recruitment, thinking like a hacker, and promoting offensive training in tangent with defensive training.

An offensive mindset is key to ensuring the best cyber defense. To ensure success, there are three main components for organizations to consider when developing a defensive strategy based on an offensive cyber model: re-envisioning recruitment, thinking like a hacker, and promoting offensive training in tangent with defensive training.

Re-envisioning recruitment

According to ISACA's State of Cybersecurity 2022 report, 63% of respondents have unfilled cybersecurity positions, up eight percentage points from 2021. Yet, the cyber skills gap is widening with each passing year. This demand for talent calls for organizations to take advantage of those who are looking for more growth and a career change, especially in the cyber industry. Ultimately, cybersecurity is a creative field with ever-evolving problems and solutions, so hiring people with new ways of looking at problems and an eagerness to learn is much more valuable than a specific degree or tenure.

This means companies should consider building programs that help recruit individuals that may not exactly meet the usual cyber standards and help them develop the skills they are looking for in employees. There is also an opportunity to further train those job candidates who interview, but just miss the mark of what the role requires to succeed – again, helping to build the skills they are looking for in such positions. It is also important to offer new opportunities for current employees, advocating transferable skills from one department to the next. Entice cyber employees, who are considering giving their notice, with these new opportunities, providing confidence that there is still growth to be had. Such efforts take a proactive approach to addressing the current threat landscape.

Thinking like a hacker

Threat intelligence is a key component to developing an offensive mindset. That's why proactive cybersecurity auditing can be one of the best courses of action in stopping cyberattacks before they can impact an organization. To implement the right changes to cybersecurity strategy, an organization needs to understand fully existing network vulnerabilities.

This can be accomplished through a few different tactics, including penetration testing and vulnerability scanning. Penetration testing involves a person purposefully hacking into a network to identify weaknesses to an organization's system, while vulnerability scanning consists of an automated test that looks for potential security vulnerabilities. Both tactics enable organizations to better grasp the mind of a hacker and understand the "how" behind a potential attack. Something else to be considered – under the right circumstances – is the possibility of hiring a former hacker. Their insight could prove to be extremely helpful, as aptitude in identifying weaknesses can be a useful asset. Many former hackers find roles as a penetration tester / red team member fulfills their desire to expose system flaws while doing so legally, for the betterment of security.

Promoting offensive training in tangent with defensive training

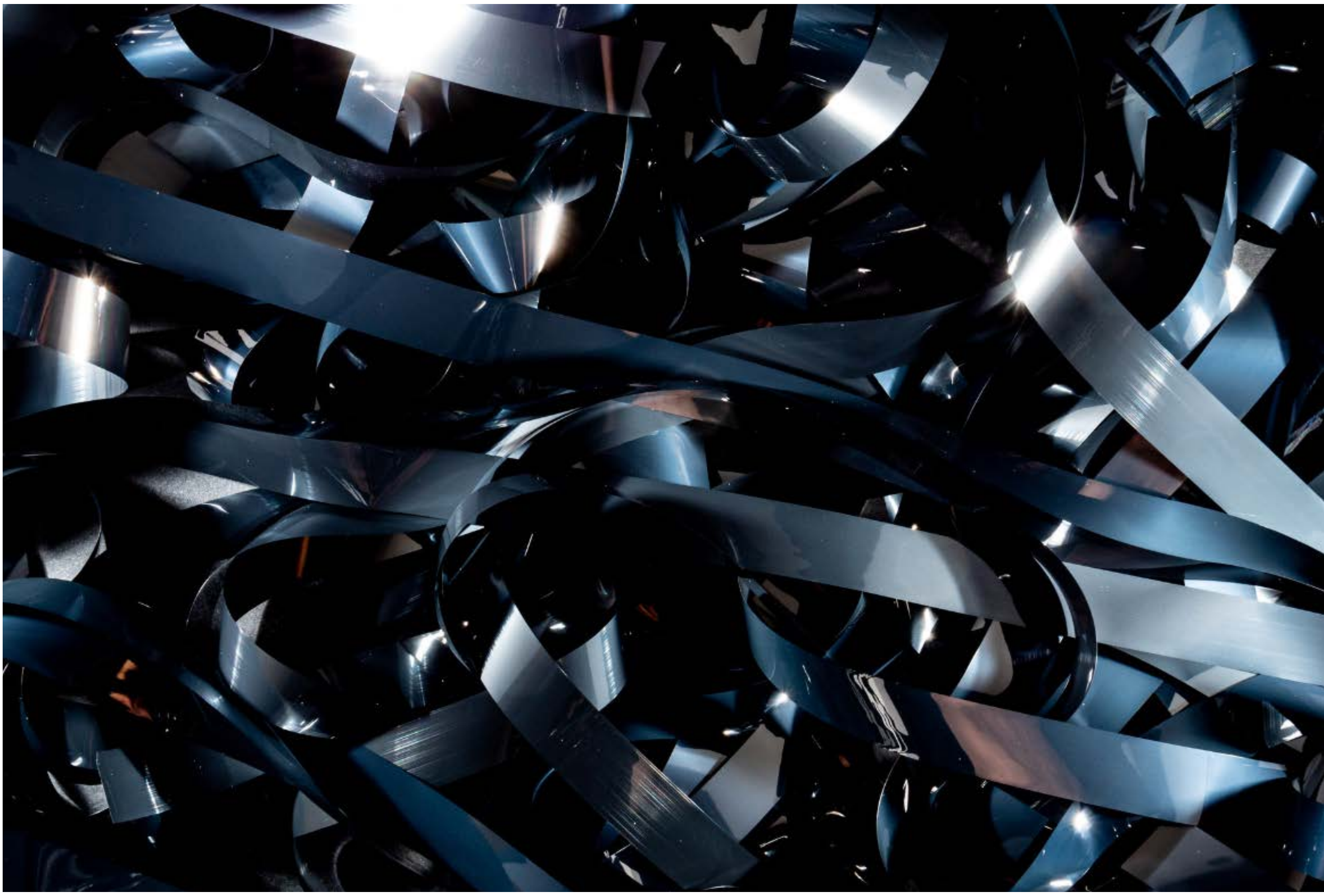
While we're seeing changes on a national level to better protect our way of life through the push for zero trust frameworks, there also needs to be better recognition of honing offensive capabilities across all sectors, ensuring they are being taught right next to defensive approaches.

Those who operate in cybersecurity roles for the private sector or critical infrastructure companies are performing cyber defense, but there's the notion of active defense – more proactively identifying and containing threats before they have a chance to breach systems. That takes an understanding of how hackers think to know how to find the threats before they're inside, since the zero trust principle of "assume breach" acknowledges that attackers will get in.

However, those seeking legitimate, ethical careers in cyber are generally taught how to defend networks. But unless one knows how to penetrate various security layers, they're not thinking like an attacker. Giving employees offensive cyber training in a setting where they have permission to try to break in can be liberating and help them develop the instincts and know-how they need to be the best possible cyber defenders. Moving forward, this must be a standard practice, ensuring offensive training is promoted in unison with defensive training. That experience of how to break into something using offensive cyber tactics is what sparks original thinking on ways to defend, which is just as valuable as understanding an attackers' methods and motivations.

Giving employees offensive cyber training in a setting where they have permission to try to break in can be liberating and help them develop the instincts and know-how they need to be the best possible cyber defenders.

The threat environment is continuously evolving due to current events and the rise of more sophisticated cybercrimes. As such, an offensive mindset is crucial to defend organizations fully against attacks on the enterprise and national level. For success, organizations need to act now by changing how they recruit and train employees, understanding the motivations of a hacker, and ensuring offensive strategies are being deployed alongside defensive ones.



The SaaS-to-SaaS supply chain is a wild, wild mess

Yoni Shohet

CEO, Valence Security

Cloud migration and IT democratization have created a continuously growing network of interconnected business applications, integrated to digitize and automate business workflows. Employees in the digital transformation age are now compelled to choose their best-of-breed applications, independently adopting and connecting SaaS applications, no/low code platforms like Workato and Zapier, and SaaS marketplace third-party apps in order to increase productivity, creating a convoluted web of ever-growing app-to-app integrations. This expanding new network is built in the cloud and is based on third-party vendor integrations, introducing the SaaS-to-SaaS supply chain as the future of enterprise interconnectivity.

Massive amounts of data are now flowing between these applications in the highly dynamic cloud environment, and the modern enterprise cannot revert to the days of data silos and isolated applications. However, with every new connection and automated workflow, a new and concerning risk surface grows with indiscriminate and shadow connectivity. A ubiquitous phenomenon of the interconnectivity era, CISOs should take heed and consider the challenges introduced by the size, expansion, security and governance ramifications of the SaaS-to-SaaS supply chain.

> *Massive amounts of data are now flowing between these applications in the highly dynamic cloud environment, and the modern enterprise cannot revert to the days of data silos and isolated applications.*

Zero trust for non-humans

For years, security teams have focused on securing human-to-app interactions, adopting security controls such as managed devices, endpoint security, CASB, ZTNA, MFA and IdPs. These solutions provided value for their original purpose, but the SaaS-to-SaaS supply chain today thrives on application integration, non-human identities and app-to-app connectivity - leaving out the human element in order to streamline and automate work processes.

The SaaS-to-SaaS supply chain continues to grow uninhibited, without alerting security teams on new risks and connections created by non-human identities that cannot be resolved using traditional security controls designed for human-to-app interactions. The continuous increase in non-human identities in app-to-app integrations and their robust access to sensitive data-intensive platforms heighten attackers' motivation to exploit these new attack surfaces.

Security teams struggle with handling the scale and sophistication of impending attacks. Blind to these threats and with application adoption becoming as easy as signing a form, employees are no longer inclined to request CISO consent to adopt new apps, and CISOs are not able to govern third-party access due to the ease of bypassing existing controls. The number of supply chain attacks via third-party vendors has skyrocketed over the past few years, as malicious actors leverage non-human identities to gain unauthorized access to business applications.

Third-party API takeover attacks

Enterprise budgets and organizational resources are heavily routed to fortifying internal security postures, while critical assets are left exposed to external threats due to these unmanaged third-party integrations. The infamous Solarwinds attack brought organizational reliance on third-party integrations to the forefront, leading to an inevitable backlash against existing, woefully unsuitable solutions for third-party risk management. As part of the attack campaign, the abuse of application credentials, like in the case of Microsoft Azure, and the focus on API takeover attacks targeting third-party vendors like Mimecast, highlight how attackers leverage such integrations to gain unauthorized access to critical business applications.

Securing the hyper-automated enterprise

The SaaS-to-SaaS supply chain with its unique characteristics is prone not only to third-party breaches, but also to various other ways by which malicious actors may leverage it as an attack vector.

As organizations strive for automated business workflows, hyper-automation, no/low code and enterprise application integration (EAI) platforms are the methods of choice for connectivity. These platforms are now configured by citizen developers, without security governance and oversight, potentially leading to misconfigurations and sensitive data exposure. Attackers actively target such platforms as they hold the keys to the kingdom with their high privileges across the enterprises' most critical business applications.

Malicious OAuth token access

Attackers have found that human error and employee trust are lucrative opportunities for exploits and trickery, and target employee independence with SaaS marketplaces for phishing campaigns. With the increasing adoption of multifactor authentication (MFA), traditional account takeover techniques have become less efficient as it's no longer enough to have a username and password to gain access. Attackers leverage marketplaces and third-party apps to trick employees into installing malicious apps via sophisticated consent phishing campaigns that provide them with OAuth tokens with high privileges, bypassing many security controls, such as MFA.

It all comes down to managing trust

The SaaS-to-SaaS supply chain will continue to grow and provide enterprises with value at scale, simplifying and automating processes, enabling robust data collection, and maximizing the benefits of enterprise software. That said, security teams cannot continue to ignore the pitfalls and challenges of this wild, wild mess, as it creates organizational dependency on external vendors, leading users to trust third parties for integration and interconnectivity while potentially jeopardizing their most important assets.

The shift from human to non-human interactions necessitates a corresponding shift in the paradigm used to secure these integrations, without impeding workflows. These challenges cannot be mitigated and resolved in silos. Security teams must gain more visibility and control by bolstering their collaboration with business application teams, decentralized owners, citizen developers and end users to ensure the secure growth of the SaaS-to-SaaS supply chain and enhance innovation, increase productivity, and enable organizations to reap the benefits of their digital transformation journey.

> *The shift from human to non-human interactions necessitates a corresponding shift in the paradigm used to secure these integrations, without impeding workflows.*

How the blurring of the supply chain opens your doors to attackers—and how you can close them

Jordan LaRose

Director of Consulting and IR, Americas, WithSecure

There have been more than 200 dedicated supply-chain attacks over the past decade. Some of these campaigns have affected countless supplier networks and millions of customers - SolarWinds, Kaseya and the recent Log4j debacle come to mind.

But given how distributed work has become, especially since the beginning of the Covid-19 pandemic, what exactly isn't part of the "supply chain" now? Likewise, what workplace doesn't include aspects of "remote work", even if it's being done in a cubicle on the 30th floor of a skyscraper?

Dependence on cloud-hosted platforms, weaker authentication solutions, and public tools has become endemic, and there's no turning back now. The dense ecosystem we find ourselves in - where everything is bleeding into everything else and companies rarely have more than one degree of separation from each other - will only become denser.

But if the supply chain is anything that potentially gives you an opportunity to hop to another target, just about everything – including you – is part of the supply chain.

Certainly, the suppliers your business rely on most should rise above the others when it comes to considering the security of your organization. But if the supply chain is anything that potentially gives you an opportunity to hop to another target, just about everything – including you – is part of the supply chain. And to an attacker, all the weaknesses in that chain look like the same thing: opportunity.

The cost of being more productive

While attackers are motivated by opportunity, companies must deal with the blurring of the clear lines that used to be a foundation of cyber security for a related reason: productivity.

For instance, more and more organizations use GitHub for their code pipeline. This is true even when internal solutions like GitLab are available because GitHub is a more convenient way for developers to upload and manage code.

IT pros know it's possible to lock down a public tool, but no one is going to argue it's secure by default. In fact, the opposite is true. And software like GitHub presents a variety of openings for those who seek to do you and your business harm.

Attackers look at GitHub and may not see a server that will be their actual attack vector or even where they find a way to implant the backdoor. But it is a key intelligence source for hardcoded developer credentials, crucial information about the inner workings of a software package, and more. This view could give an advanced threat actor insights both into how to build an effective backdoor and where it could be inserted for easy, reliable access without being detected.

GitHub also gifts attackers with lists of developers that have access to a repository. This list doubles as a perfect set of targets to approach once a foothold in the corporate network has been achieved. Now, with one breached laptop containing one GitHub login, an entire code repository - and by extension its host organization - can be compromised.

Similarly, the explosion of formal or informal "bring your own device" policies, alongside developers logging into easily reachable services from their own devices, dramatically widens your company's attack surface, as it removes the crucial segmentation that acts as a defense for internal services.

Think like an attacker and then like a C-level executive

With services like GitHub, AWS, and others forming a complex web of supply chain threats, it can be extremely difficult to convey these risks concisely to decision makers in your organization. That's why communication is key when discussing a topic that's constantly in the news like supply chain attacks. When you only have minutes to sell your security message, concise communication – a story that gets to the crux of the matter – is crucial.

Security professionals often love details about their job, even when their audience doesn't. The challenge is to establish the context and need for investment in security while tying them to the company's goals instead of scaremongering about the nightmares no one wants to imagine.

Focusing on the largest revenue-generating organizations and the biggest revenue-generating products will naturally draw the attention of those who sit on the C-level. That creates the opportunity to explore the threats that could land in those spheres and how to tackle them without sacrificing too much productivity.

What's crucial to understand in the supply chain is the elements you control, where the bottlenecks are, and where you can introduce key mitigations to prevent a small flaw from spiraling into full domain compromise. It's also crucial to educate executives about how vast and amorphous the supply chain can be, because attackers are well aware.

If your company uses Microsoft Teams, for instance, everyone in your organizational chart is likely to know it. However, they may not be aware that Microsoft, the host of that pervasive cloud service, is now part of your supply chain. Now any potential risk to one of the world's largest software companies that does business in most countries around the world is a potential risk to you.

We're all in this together, for better or worse

Thinking about the supply chain probably doesn't feel like a spiritual pursuit. But contemplating security, especially information security, from an attacker's perspective can create a feeling of oneness.

From the perspective of those who make their living attacking our businesses, you can see that every company we work with and every tool we use is a potential weak link in our security. Thus, individual organizations cannot make risk decisions without impacting every organization upstream and downstream from yours. However, the scope of these decisions can often create an impossibly large risk profile, so understanding your key suppliers and those that you supply is often your biggest step towards effective supply chain security.

> *Thinking about the supply chain probably doesn't feel like a spiritual pursuit. But contemplating security, especially information security, from an attacker's perspective can create a feeling of oneness.*

This realization isn't likely to reward anyone with inner peace. But recognizing that the rewards of productivity come with the risk of interdependence is a key step toward reducing attackers' opportunities before they overwhelm us.