Brigantia Insider Threat Roadshow

The importance of Microsoft 365 and how to protect against insider risk

HORNETSECURITY

MATTHEW FRYE

I have been in the IT Industry for more than 25 years, I worked for a Bristol based MSP for 14 years heading up the support team for the last 10, I was a Microsoft and Hornetsecurity evangelist supporting the products.

Head of Presales and Education

frye@hornetsecurity.com

HORNETSECURITY

Brigantia Insider Threat Roadshow

MICROSOFT 365

The importance of Microsoft 365 and how to protect against insider risk

Amplifying productivity…

HORNETSECURITY

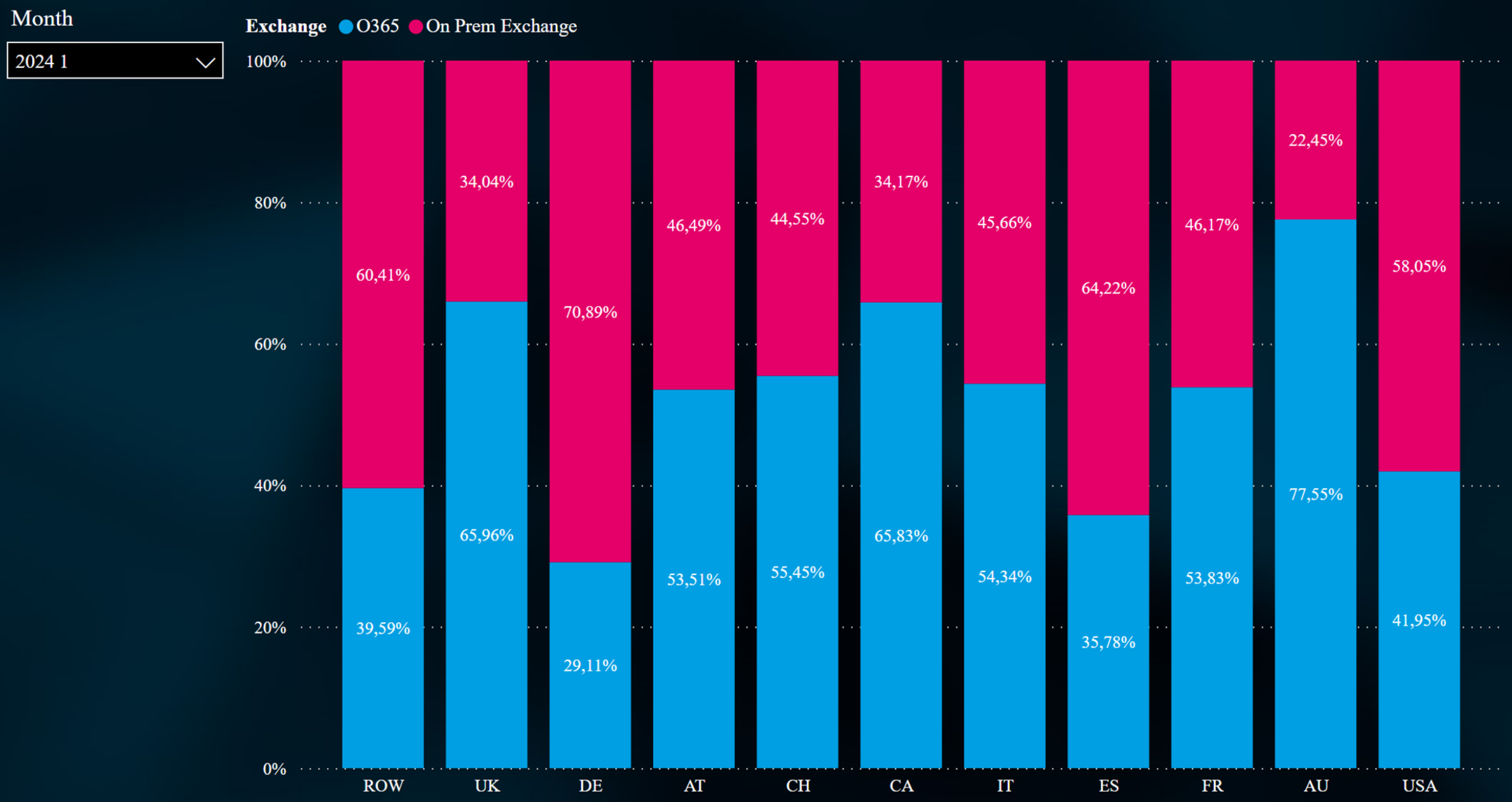
WHY DO YOU NEED MICROSOFT 365 ?

- Unified Communication and Collaboration Platform.
  - Seamless collaboration among team members
- Subscription plans tailored to the needs of businesses.
  - Comprehensive suite of productivity tools
- Scalability and Flexibility.
  - Remote work, Flexible storage, Inclusivity, *Languages, Accessibility*
- Regular updates and enhancements
  - Product Improvements and New features

HORNETSECURITY

STRENGTH OF THE GLOBAL MARKET: MARKET SHARE BY EXCHANGE TYPE

HORNETSECURITY

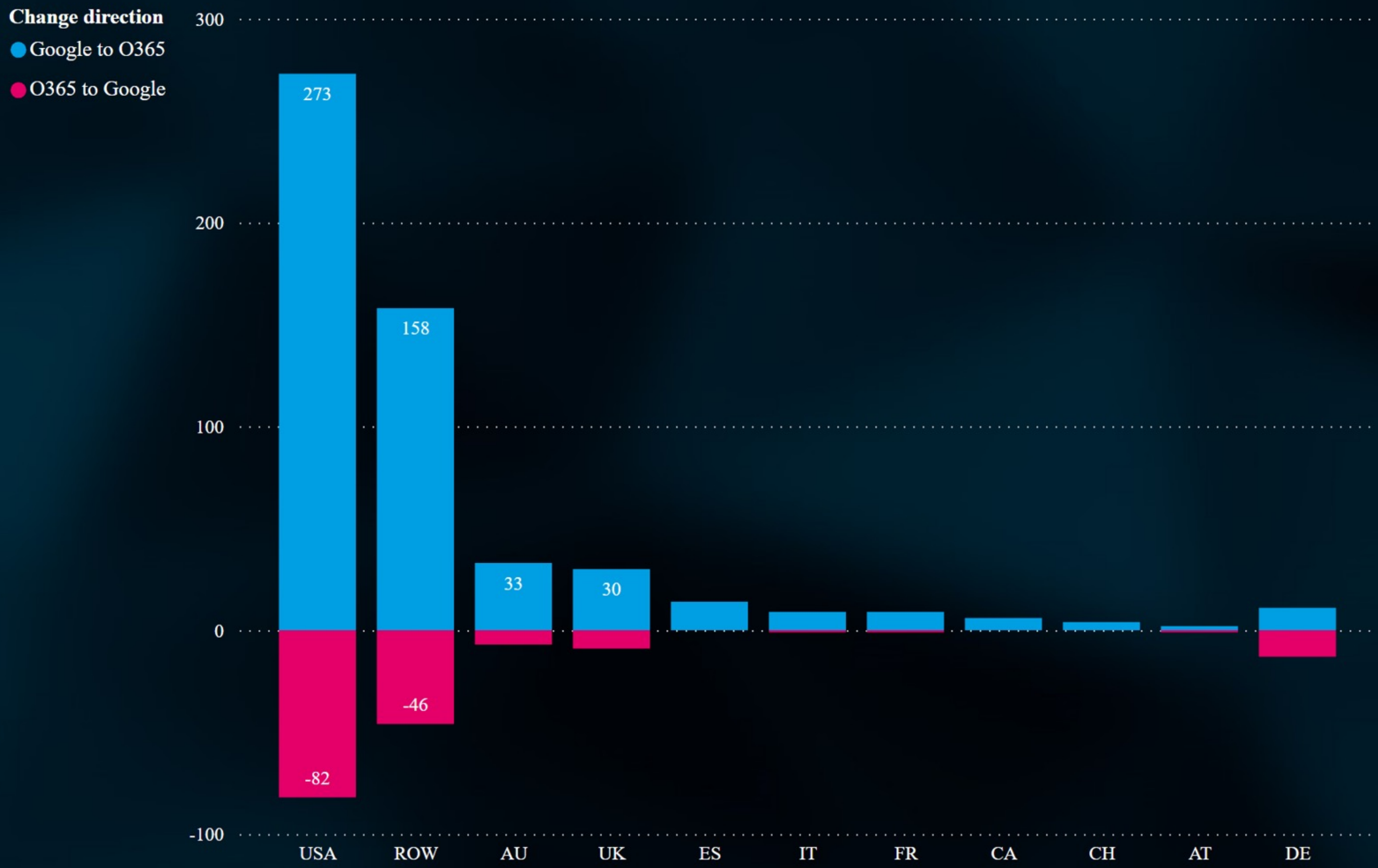


Month: 2024 1

COMPANIES SWITCHING BETWEEN O365 AND GOOGLE

Month

2024 1



Due to the increasing amount of unassignable domains these records were filtered to not skew the chart

INSIDER RISK

What are the risks ?

HORNETSECURITY

INSIDER RISK

- M365 environments are particularly vulnerable to insider threats
  - SharePoint, Teams, Exchange Online and OneDrive.
    - Sharing is SUPER easy
    - *Management is SUPER difficult especially for SMB/SME*
- Human aspect
  - Malicious intent, outages, shutdowns, lost or stolen devices, accidental overwriting of data.
- Unauthorized data access
  - Phishing & ransomware, malware & viruses, third-party apps
- Purview Insider Risk Management ?
  - Expensive (E5 tier!), Difficult and convoluted, overkill for SMBs/SMEs ?
    - *One solution to review itself ?*

HORNETSECURITY

WHY DO YOU NEED 365 PERMISSION MANAGEMENT?

REAL-LIFE CASES THAT CAN LEAD TO CRITICAL COMPLIANCE STATES IN MICROSOFT 365:

INHERITED GROUP ACCESS

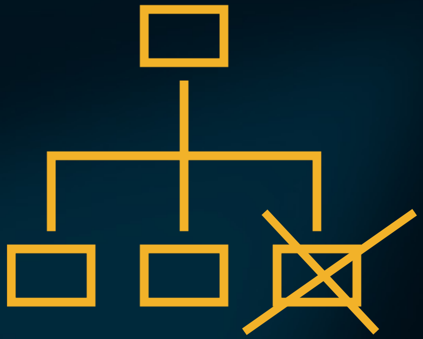
A new employee is added to an existing group. This gives them access to all sites, folders and files for that the group has access to which can have confidential information.

HORNETSECURITY

WHY DO YOU NEED 365 PERMISSION MANAGEMENT?

REAL-LIFE CASES THAT CAN LEAD TO CRITICAL COMPLIANCE STATES IN MICROSOFT 365:

EMPLOYEE LEAVES THE COMPANY



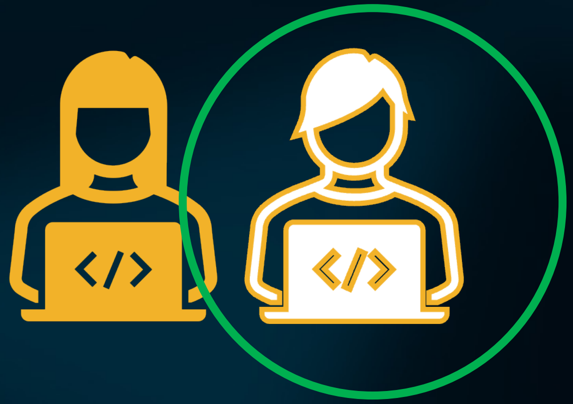
An employee with access to confidential information leaves the company. Even though the user's password is reset by IT, the employee’s access is still active for some time after.

HORNETSECURITY

WHY DO YOU NEED 365 PERMISSION MANAGEMENT?

REAL-LIFE CASES THAT CAN LEAD TO CRITICAL COMPLIANCE STATES IN MICROSOFT 365:

ALLOW COLLABORATION WITH CONTROL



In M365 you can only decide if you want to allow collaboration with external users or block it entirely.
These options do not work in the real world.

WHY DO YOU NEED 365 PERMISSION MANAGEMENT?

REAL-LIFE CASES THAT CAN LEAD TO CRITICAL COMPLIANCE STATES IN MICROSOFT 365:

DEFAULT SITE CONFIGURATION IN M365

Some default settings in M365 can be disastrous: for example, the default behavior in Teams is to create anonymous publicly accessible links whenever someone shares a file over chat.

HORNETSECURITY

MICROSOFT 365– TEAMS FILE SHARING

Any file shared via Microsoft Teams gets automatically uploaded to OneDrive and stays there, by default accessible to everyone with a link, indefinitely.

WHY DO YOU NEED PERMISSION MANAGEMENT?

- Access only ever increases and never gets reduced!
  - No user goes into Teams and says, *"We no longer work with this freelancer, let's remove his access!"*
- Audits are never done by the people who understand the data and access granted to it!
  - No CISO knows which external user needs access to what, and with hundreds of shares happening every day, *traditional audits become outdated within a matter of hours!*
- M365 has an All or Nothing approach to controlling sharing with no wiggle room for the Real World
  - With Admins forced to leave control up to the users to do what's best, it's only a *matter of time until critical data gets leaked!*

365 PERMISSION MANAGER

ELEVATE YOUR COMPLIANCE FOR MICROSOFT 365

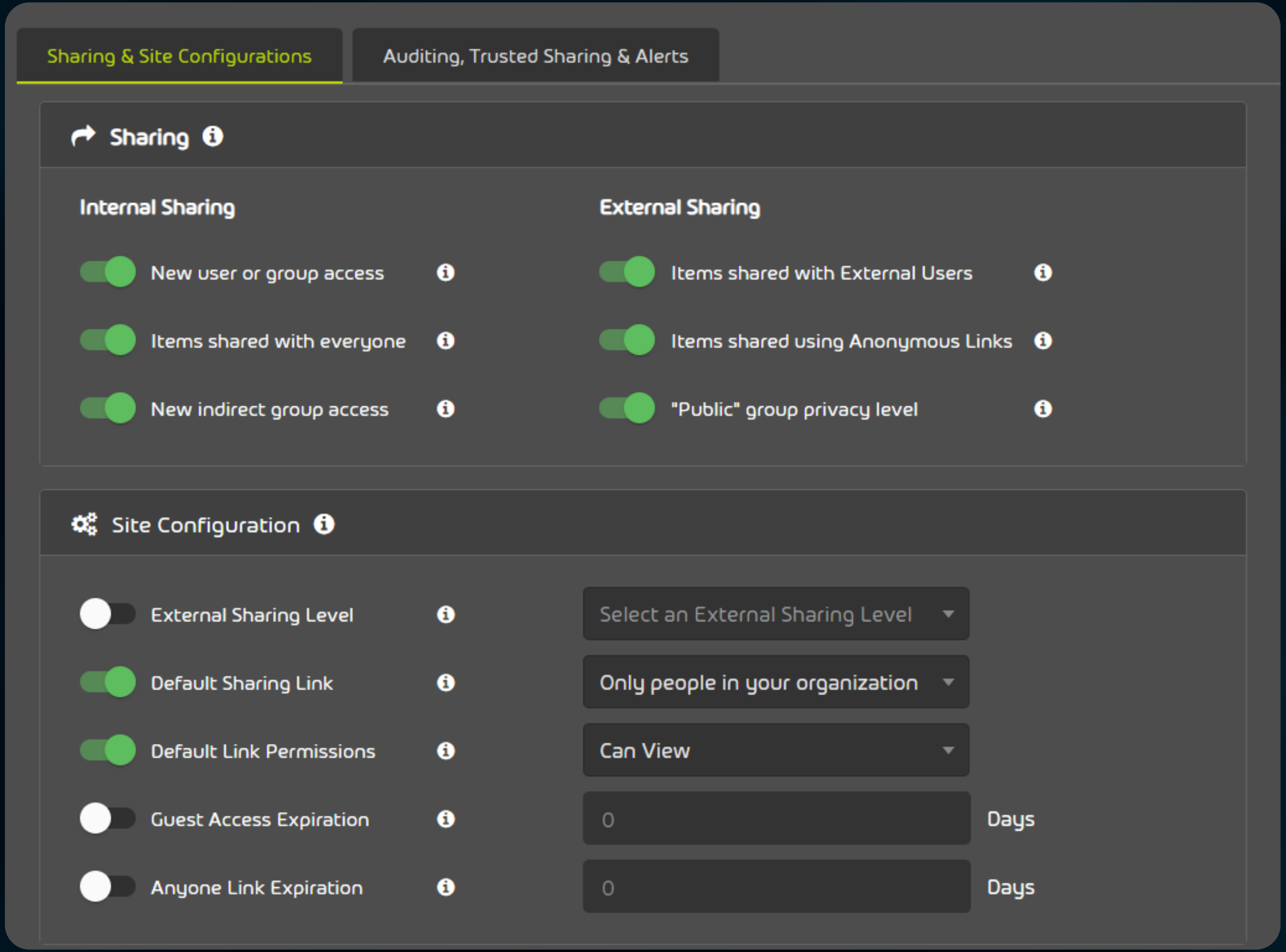
HORNETSECURITY

365 PERMISSION MANAGER – COMPLIANCE POLICIES

DEFINE SHARING POLICIES

- Assign out-of-the-box best practice or custom defined compliance polices to SharePoint sites, Teams, or OneDrive accounts

HORNETSECURITY



Sharing & Site Configurations | Auditing, Trusted Sharing & Alerts

Sharing

Internal Sharing

- New user or group access: on
- Items shared with everyone: on
- New indirect group access: on

External Sharing

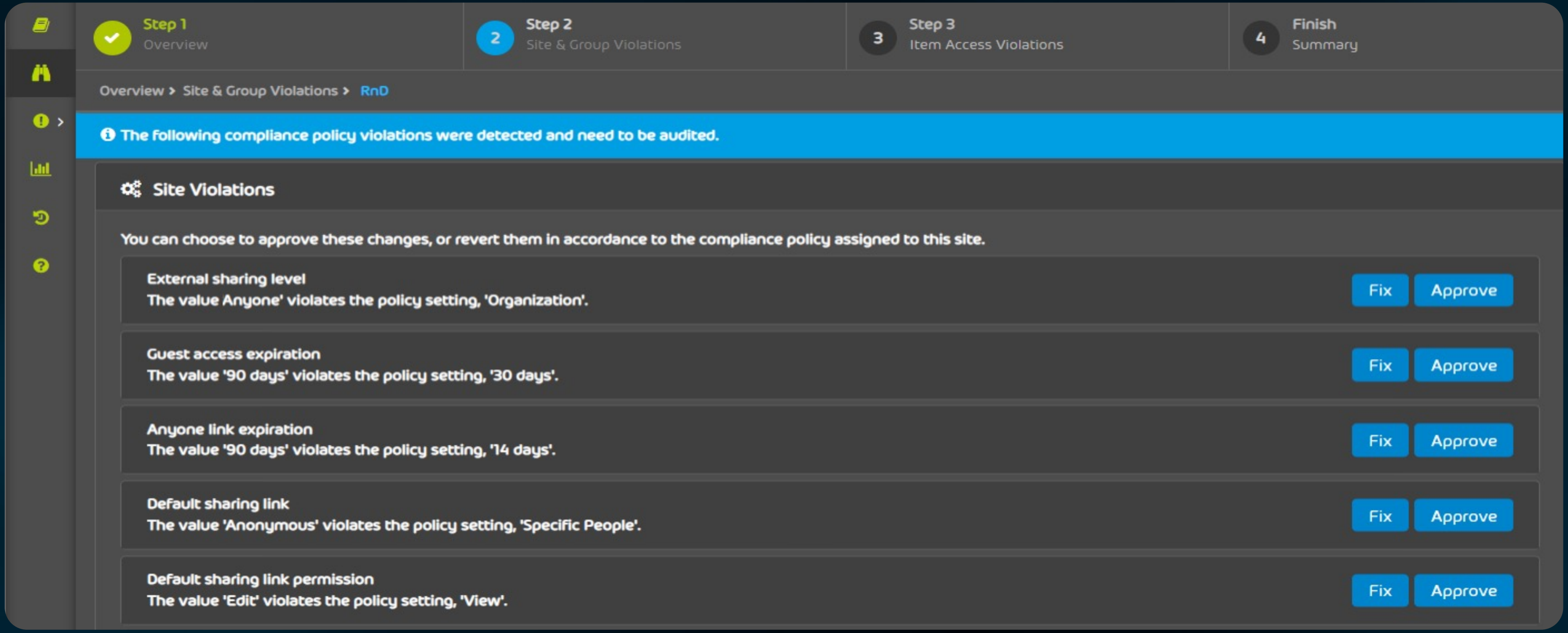
- Items shared with External Users: on
- Items shared using Anonymous Links: on
- "Public" group privacy level: on

Site Configuration

External Sharing Level	off	Select an External Sharing Level
Default Sharing Link	on	Only people in your organization
Default Link Permissions	on	Can View
Guest Access Expiration	off	0 Days
Anyone Link Expiration	off	0 Days

365 PERMISSION MANAGER – AUDIT FUNCTION

IDENTIFY & AUDIT POLICY VIOLATIONS



The following compliance policy violations were detected and need to be audited.

Site Violations

You can choose to approve these changes, or revert them in accordance to the compliance policy assigned to this site.

External sharing level
The value Anyone' violates the policy setting, 'Organization'.
Fix Approve

Guest access expiration
The value '90 days' violates the policy setting, '30 days'.
Fix Approve

Anyone link expiration
The value '90 days' violates the policy setting, '14 days'.
Fix Approve

Default sharing link
The value 'Anonymous' violates the policy setting, 'Specific People'.
Fix Approve

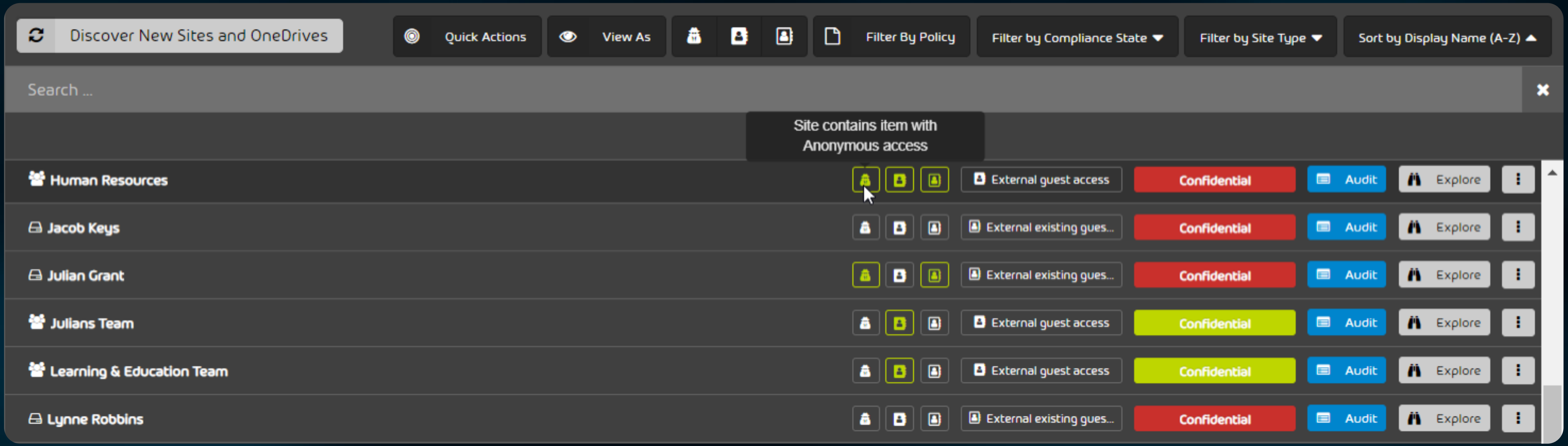
Default sharing link permission
The value 'Edit' violates the policy setting, 'View'.
Fix Approve

- Quickly and easily “fix” or “approve” violations
  - *Done by the People who know the data !!*

HORNETSECURITY

365 PERMISSION MANAGER – EXPLORE SITES

GET A USER-FRIENDLY PERMISSIONS AND COMPLIANCE STATE OVERVIEW


Discover New Sites and OneDrives
Quick Actions
View As
Filter By Policy
Filter by Compliance State
Filter by Site Type
Sort by Display Name (A-Z)
Search ...

Site contains item with Anonymous access

Human Resources	External guest access	Confidential	Audit	Explore
Jacob Keys	External existing gues...	Confidential	Audit	Explore
Julian Grant	External existing gues...	Confidential	Audit	Explore
Julians Team	External guest access	Confidential	Audit	Explore
Learning & Education Team	External guest access	Confidential	Audit	Explore
Lynne Robbins	External existing gues...	Confidential	Audit	Explore

- Use **advanced filtering** to quickly check which objects are accessible by anonymous external users or guests
- Get a detailed access overview of user, group and nested group permissions

HORNETSECURITY

365 PERMISSION MANAGER – QUICK ACTIONS

HORNETSECURITY

Perform bulk actions to manage permissions

- ✓ **Copy User Permissions:** Copy direct permissions from one user to another.
- ✓ **Revoke Access for a User or Group:** Recommended when offboarding Users or Groups, or when ending collaboration with an external user.
- ✓ **Set Site Permissions:** Select who are the Site owners, who can edit, who can view.
- ✓ **Clean Up Orphaned Users:** Remove permissions for Users who have been deleted but are still listed on SharePoint Site permissions.
- ✓ **Set External Sharing Level:** Setting the External Sharing Level of a Site or OneDrive Account.
- ✓ **Remove "Everyone" Permissions:** for all items across all SharePoint Sites and OneDrive Accounts.

COMPLIANCE

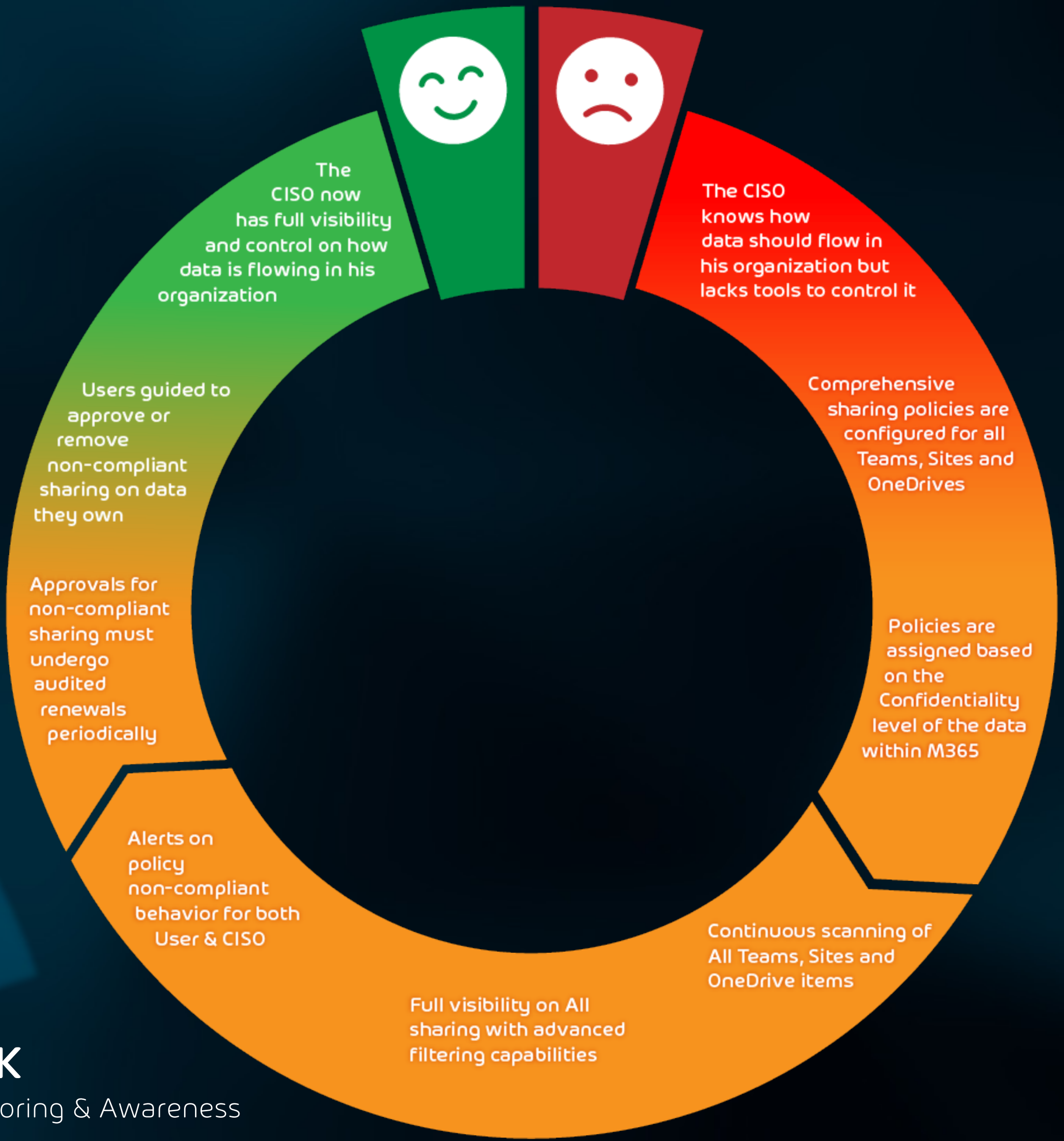
Fixing & Reporting

- Policy enforcement by Site Owners
- Fully Audited approval renewals
- Instantly Revoke user access
- Orphaned user clean-up
- Sharing Link clean-up
- Reset permissions inheritance in bulk
- User Access reporting
- Exhaustive Permissions reporting
- Publicly exposed data reporting

GOVERNANCE

Information Control & Blueprints

- Configure Any Permissions
- Set External sharing level
- Set Sharing link Access
- Set Sharing link Permissions
- Set Guest Access Expiration
- Set Anyone Link expiration
- Set Group Privacy level



The CISO knows how data should flow in his organization but lacks tools to control it

Comprehensive sharing policies are configured for all Teams, Sites and OneDrives

Policies are assigned based on the Confidentiality level of the data within M365

Continuous scanning of All Teams, Sites and OneDrive items

Full visibility on All sharing with advanced filtering capabilities

Alerts on policy non-compliant behavior for both User & CISO

Approvals for non-compliant sharing must undergo audited renewals periodically

Users guided to approve or remove non-compliant sharing on data they own

The CISO now has full visibility and control on how data is flowing in his organization

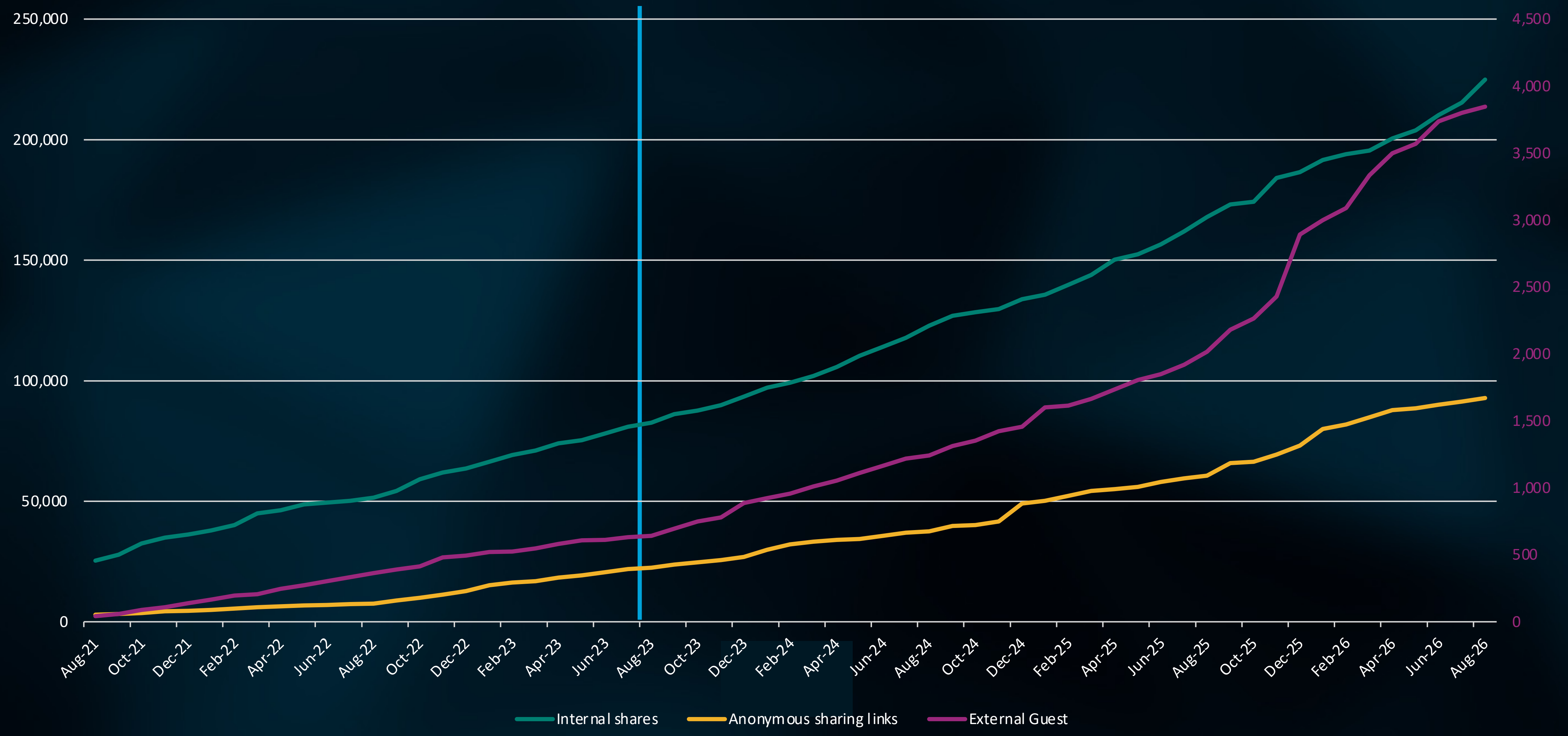
RISK

Monitoring & Awareness

- Single pane of glass File Explorer
- View Access as a specific User
- Monitor New user access
- Restrict Company-wide sharing
- Alert on External user access
- Control Anonymous link usage

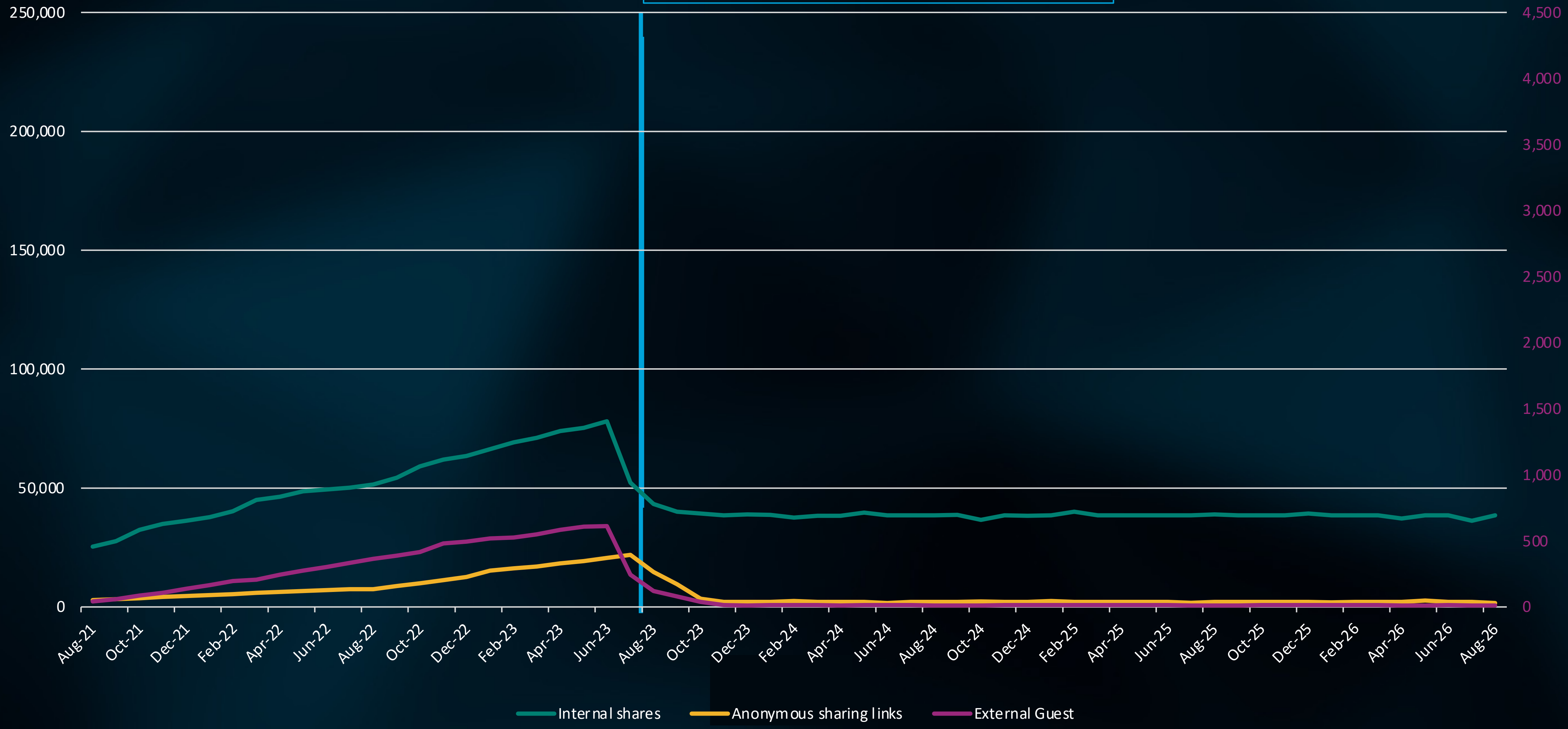
COMPANY X ALREADY HAS MORE THAN 2 MILLION FILES THAT CAN BE SHARED TODAY

82.540 Internal Shares
22.341 Anonymus Sharing Links
641 External Guest



THE INTRODUCTION OF PERMISSION MANAGER REDUCES THE NUMBER OF RELEASES

39.038 Internal Shares
2.055 Anonymus Sharing Links
13 External Guest

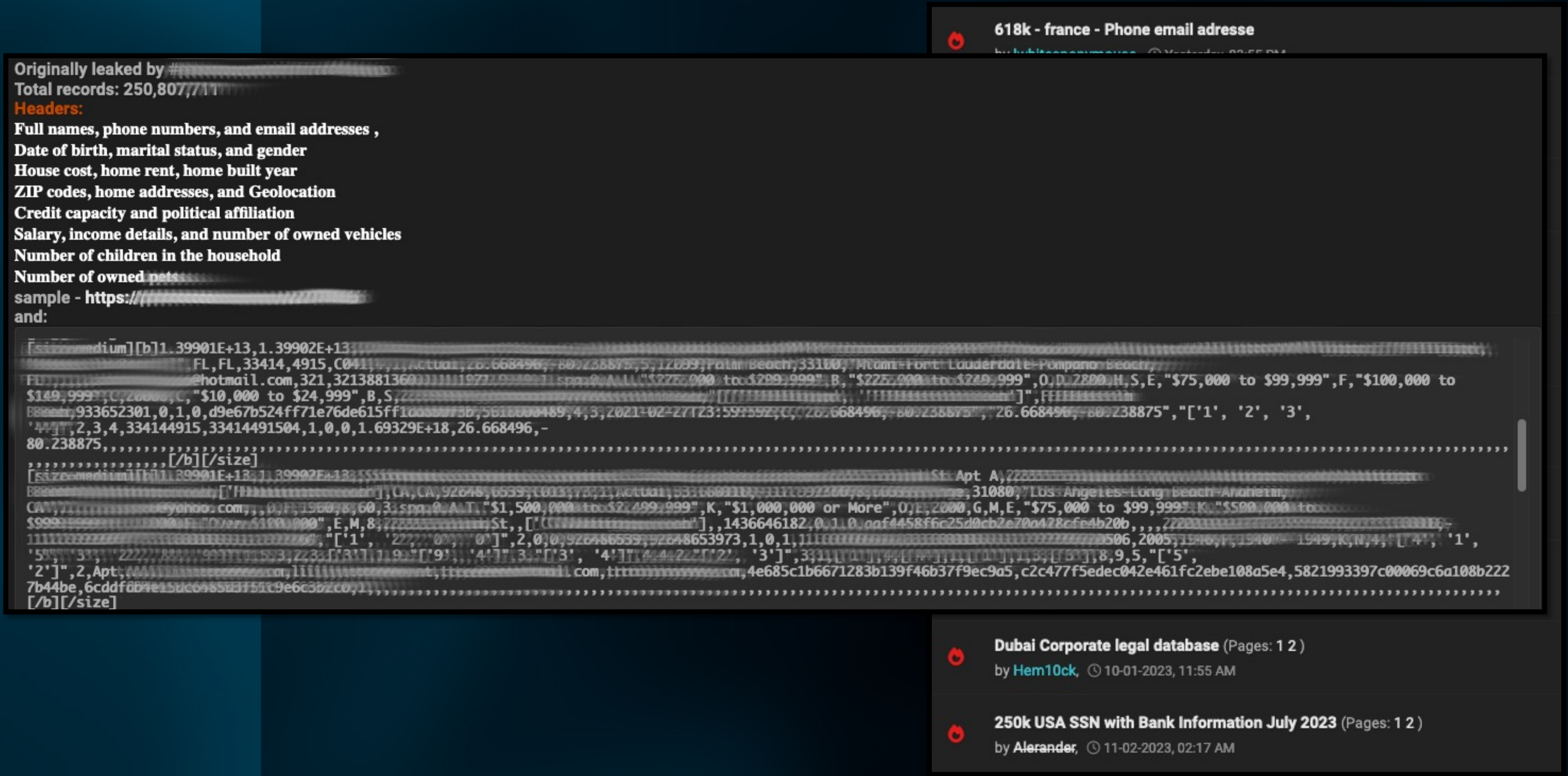


INSIDER RISK …………. OTHER CONSIDERATIONS

- The Outsider - inside
  - Once a Threat actor gets inside, *"are they are an insider risk ?"*

- Out an open gate
  - Misdirection, *"are misdirected emails really such a big thing?*

HOW EASY IS IT FOR THREAT ACTORS TO LAUNCH ATTACKS?



618k - france - Phone email adresse

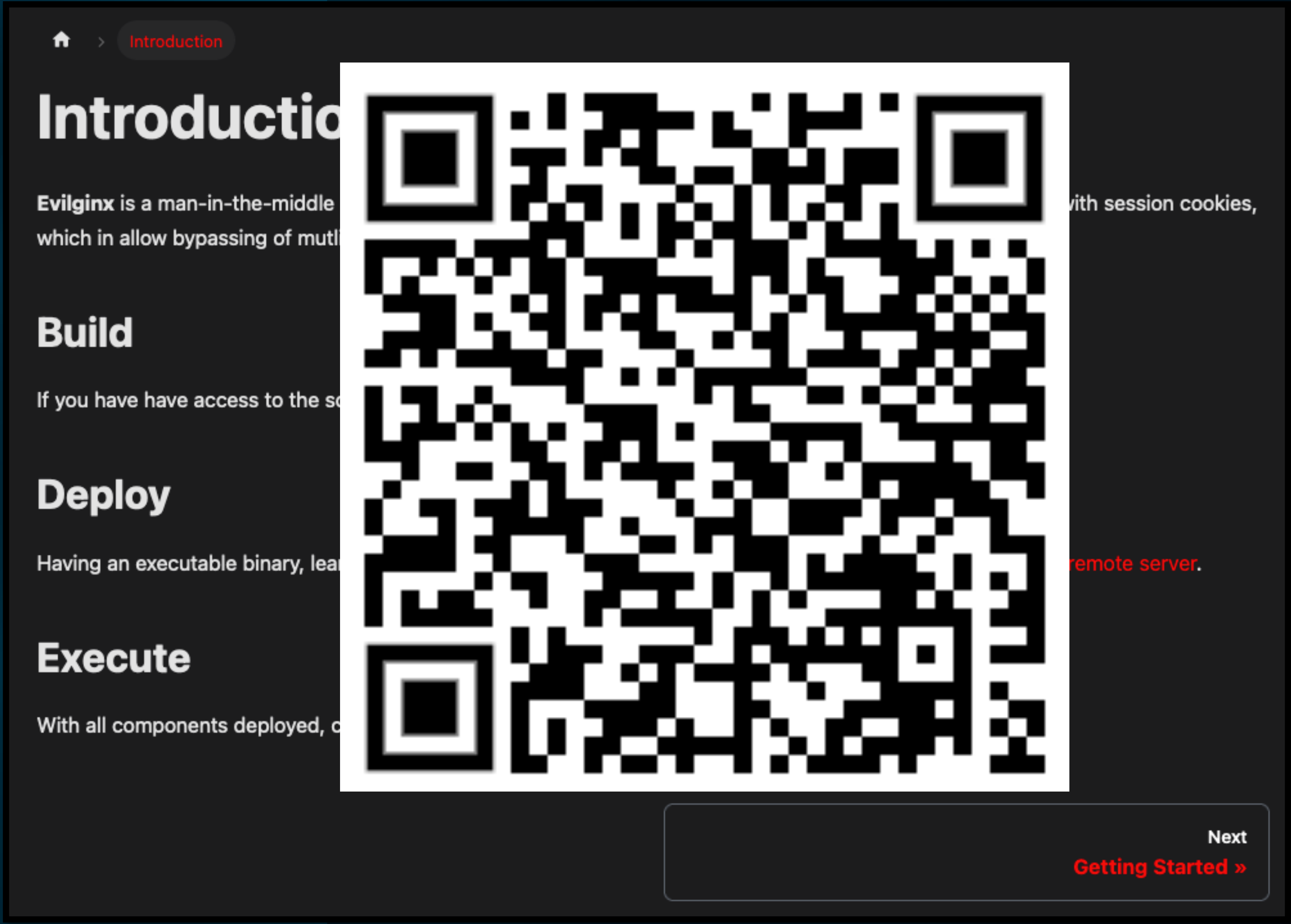
Originally leaked by [redacted]
Total records: 250,807[redacted]
Headers:
Full names, phone numbers, and email addresses ,
Date of birth, marital status, and gender
House cost, home rent, home built year
ZIP codes, home addresses, and Geolocation
Credit capacity and political affiliation
Salary, income details, and number of owned vehicles
Number of children in the household
Number of owned [redacted]
sample - https://[redacted]
and:

```
[redacted]dium][b]1.39901E+13,1.39902E+13,[redacted]
[redacted]",FL,FL,33414,4915,C041[redacted]
[redacted]@hotmail.com,321,3213881360[redacted]"$75,000 to $99,999",F,"$100,000 to
$149,999[redacted],"$10,000 to $24,999",B,S,[redacted]
[redacted],933652301,0,1,0,d9e67b524ff71e76de615ff1[redacted]38875","['1', '2', '3',
'4'[redacted],2,3,4,334144915,33414491504,1,0,0,1.69329E+18,26.668496,-
80.238875,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,[/b][/size]
[redacted]St Apt A,[redacted]
[redacted],31080,[redacted]
CA[redacted]yahoo.com,[redacted],60,3[redacted]"$1,500,000[redacted]",K,"$1,000,000 or More",O[redacted],2000,G,M,E,"$75,000 to $99,999[redacted]
$999[redacted]",E,M,8,[redacted]St,,[[redacted]],,1436646182[redacted]
[redacted],"['1',[redacted]0']",2,0,0,[redacted]653973,1,0,1,[redacted]506,2005,[redacted] '1',
'5'[redacted],3,[redacted]['9', '4']",3,"['3', '4'][redacted]'3']",3[redacted],8,9,5,"['5',
'2']",2,Apt,[redacted],4e685c1b6671283b139f46b37f9ec9a5,c2c477f5edec042e461fc2ebe108a5e4,5821993397c00069c6a108b222
7b44be,6cddf[redacted],,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
[/b][/size]
```

Dubai Corporate legal database (Pages: 1 2)
by Hem10ck, 10-01-2023, 11:55 AM

250k USA SSN with Bank Information July 2023 (Pages: 1 2)
by Alerander, 11-02-2023, 02:17 AM

HOW EASY IS IT FOR THREAT ACTORS TO LAUNCH ATTACKS?



Introductio

Evilginx is a man-in-the-middle ith session cookies,
which in allow bypassing of mutl

Build

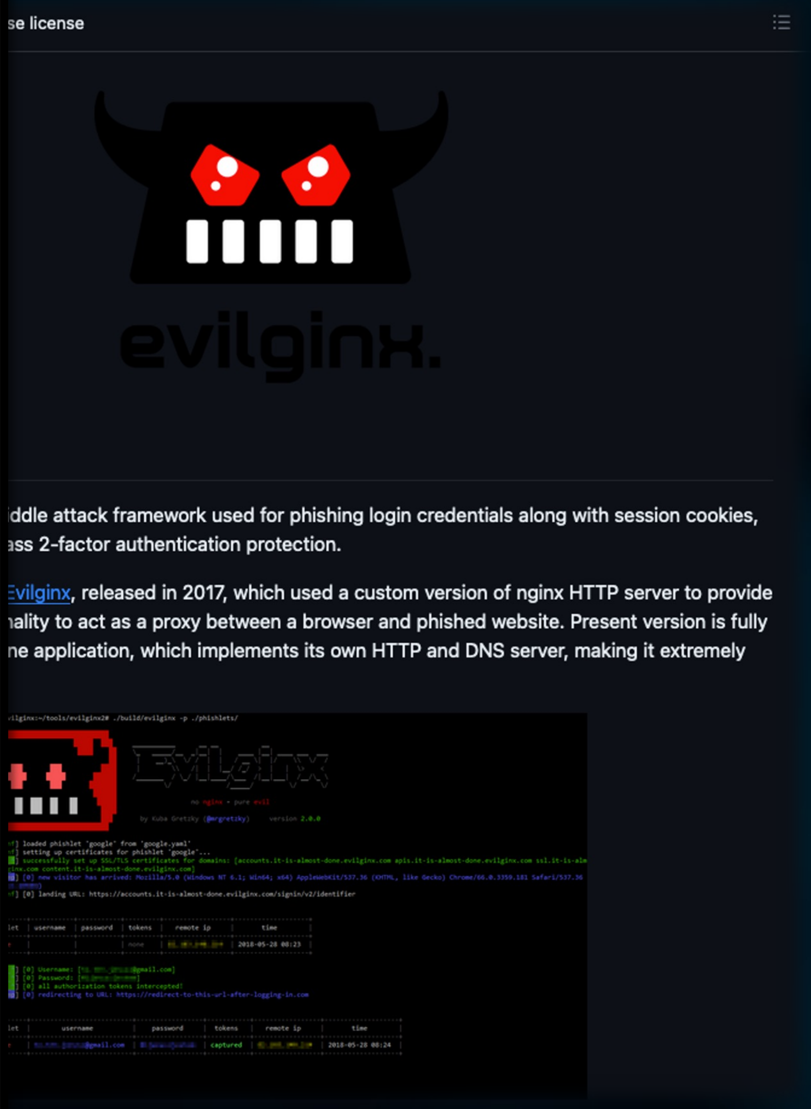
If you have have access to the sc

Deploy

Having an executable binary, lea remote server.

Execute

With all components deployed, c



iddle attack framework used for phishing login credentials along with session cookies,
ass 2-factor authentication protection.

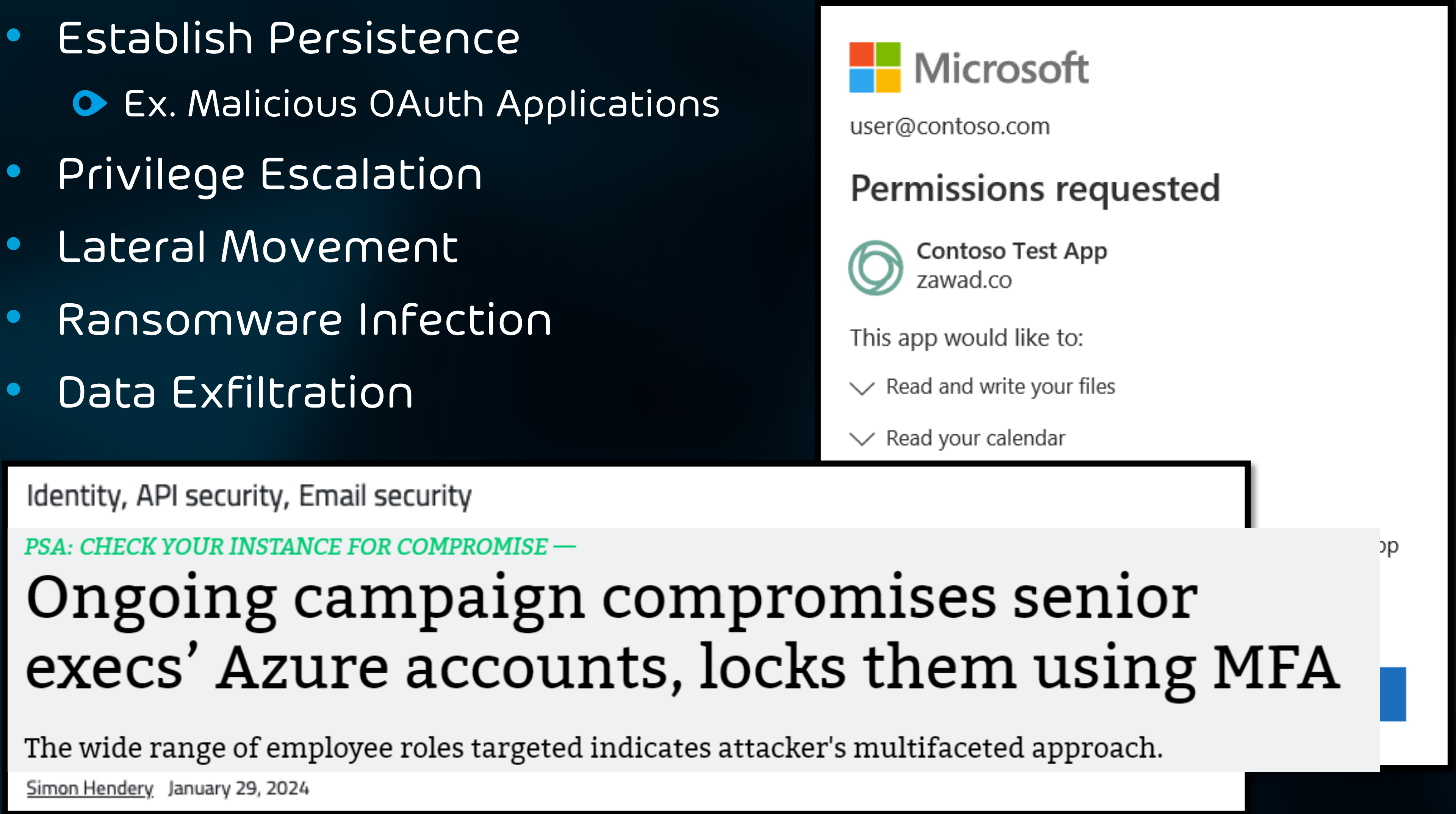
Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide
nality to act as a proxy between a browser and phished website. Present version is fully
ne application, which implements its own HTTP and DNS server, making it extremely

```
vilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                              Evilginx

                        no nginx - pure evil

              by Kuba Gretzky (@mrgretzky)     version 2.0.0

nf] loaded phishlet 'google' from 'google.yaml'
nf] setting up certificates for phishlet 'google'...
  ] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ginx.com content.it-is-almost-done.evilginx.com]
  ] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
[redacted])
nf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier

let | username | password | tokens |  remote ip  |       time
e   |          |          | none   | [redacted]  | 2018-05-28 08:23

  ] [0] Username: [[redacted]@gmail.com]
  ] [0] Password: [[redacted]]
  ] [0] all authorization tokens intercepted!
  ] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com

let |       username        |   password   |  tokens  |  remote ip  |       time
e   | [redacted]@gmail.com  | [redacted]   | captured | [redacted]  | 2018-05-28 08:24
```

HORNETSECURITY

WHAT CAN THE ATTACKER DO NOW?

- Establish Persistence
  - Ex. Malicious OAuth Applications
- Privilege Escalation
- Lateral Movement
- Ransomware Infection
- Data Exfiltration



Microsoft

user@contoso.com

Permissions requested

Contoso Test App
zawad.co

This app would like to:

Read and write your files

Read your calendar

op

Identity, API security, Email security

PSA: CHECK YOUR INSTANCE FOR COMPROMISE —

Ongoing campaign compromises senior execs’ Azure accounts, locks them using MFA

The wide range of employee roles targeted indicates attacker's multifaceted approach.

Simon Hendery January 29, 2024

SHORT STORY: MISDIRECTED EMAILS CAN CAUSE SECURITY INCIDENTS AND COMPLIANCE VIOLATIONS

HORNETSECURITY

⏭

Emails are often sent in a rush, without paying attention to details and relying on "muscle memory"

✕

This can result in sending emails to the wrong recipients

⚠

If a misdirected email contains sensitive information, this can lead to a compliance violation or be used for a data breach.

MISDIRECTED EMAILS CAN LEAD TO DATA BREACHES WITH SEVERE CONSEQUENCES

HORNETSECURITY

Data loss

Identity theft

Monetary loss

Data breaches caused by misdirected emails can be costly to your business in financial terms and also result in loss of reputation and trust.

Regulations, including the GDPR in Europe, have shown their strict side when it comes to protecting sensitive data. And with the NIS 2 directive on the horizon, regulations are getting even stricter.

HORNETSECURITY

WHAT CAN YOU DO ?

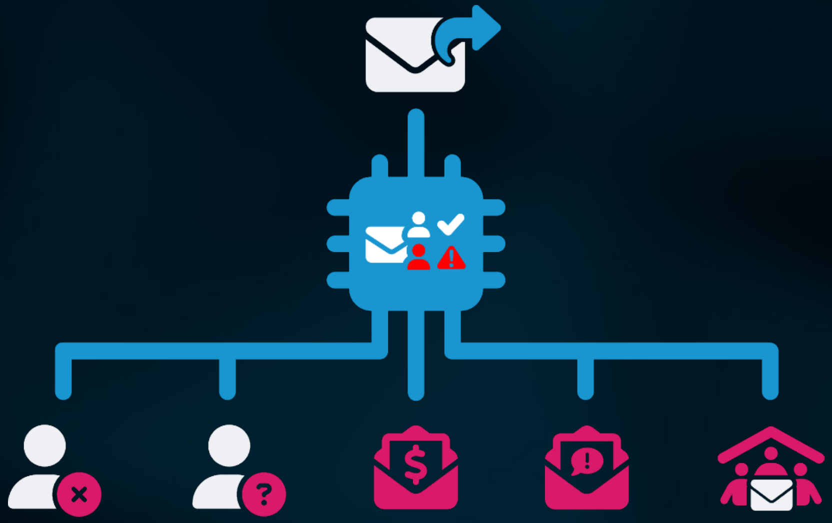
REAL-TIME EMAIL ANALYSIS

AI Recipient Validation is an **AI-based, self-learning service** that continuously learns the user's email communication patterns in the background and warns the user in different instances, including:

- An unintended recipient is being addressed
- An email contains sensitive data like Personal Identifiable Information
- A user is about to reply to a large distribution list
- The email contains inappropriate language

AI-BASED ADJUSTMENT MECHANISMS

- AI Recipient Validation factors in user behavior and responses to automatically adjust warnings and suggestions issued in upcoming communications.
- This prevents users from receiving similar warnings multiple times.

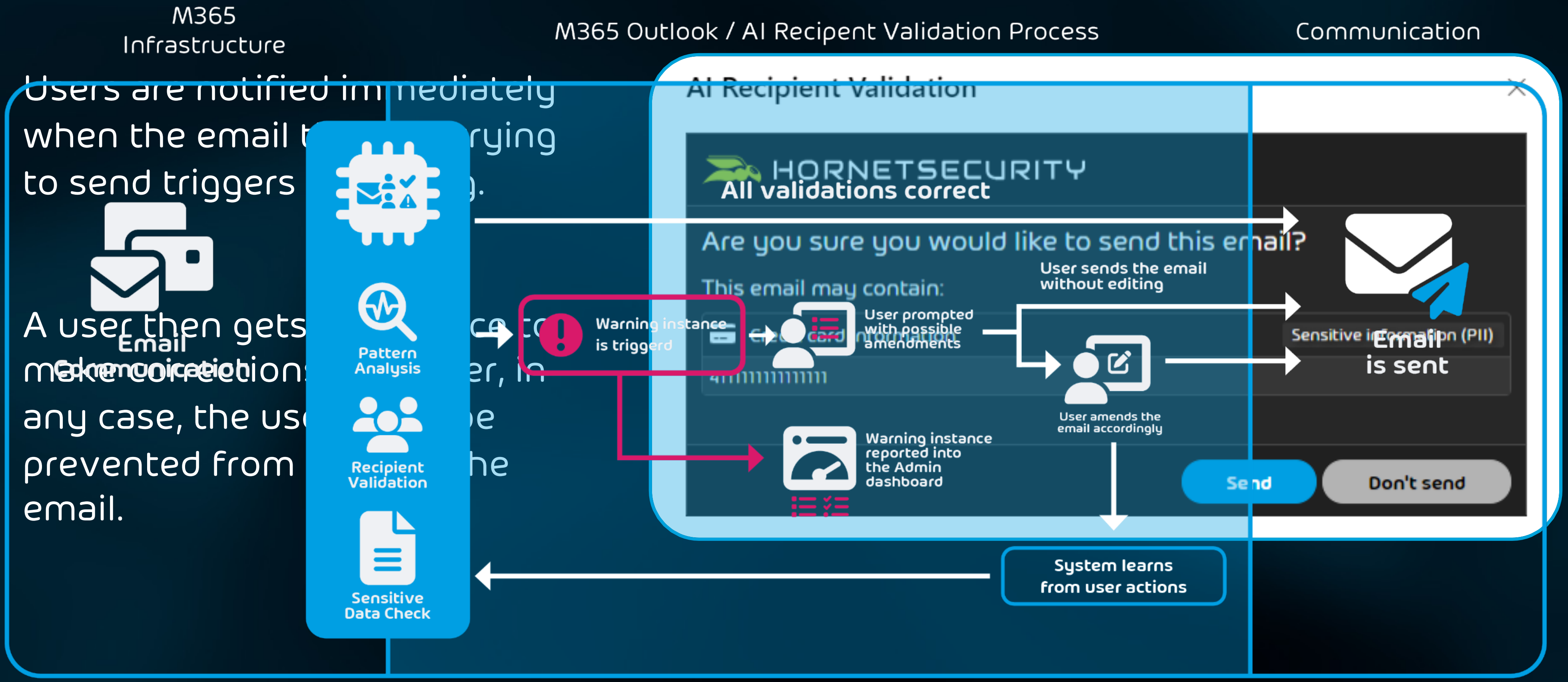


FEATURES AT A GLANCE

HORNETSECURITY

INSTANT FEEDBACK AND CHANCE FOR CORRECTION

- Users are notified immediately when the email t rying to send triggers).
- A user then gets ce to make corrections er, in any case, the us be prevented from he email.


AI Recipient Validation

HORNETSECURITY

Are you sure you would like to send this email?

This email may contain:

Credit card information

4111111111111

Sensitive information (PII)

Send

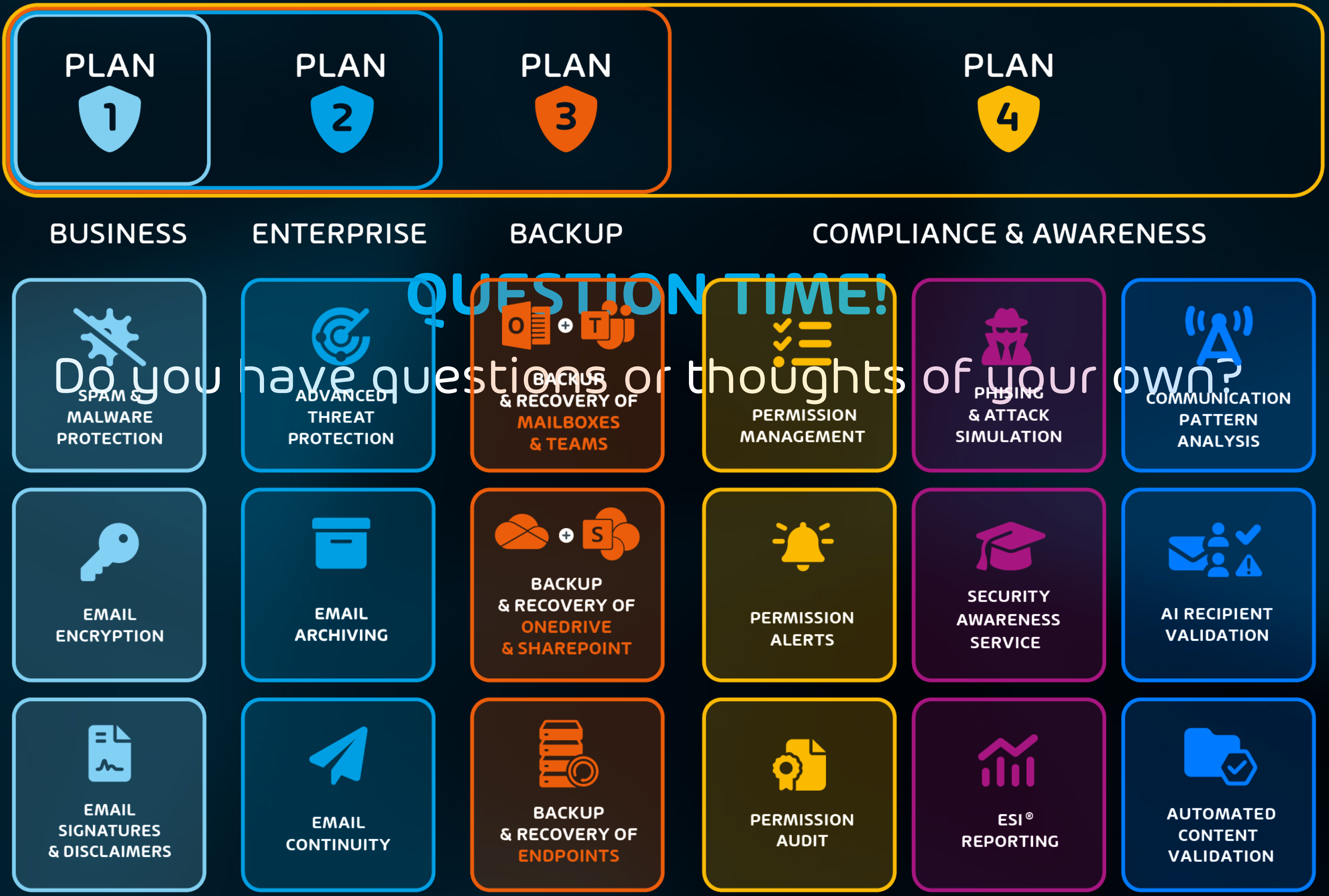
Don't send

365 TOTAL PROTECTION SUITE PLANS

NEXT-GEN SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS FOR MICROSOFT 365

QUESTION TIME!

Do you have questions or thoughts of your own?



PLAN 1 – BUSINESS

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

PLAN 2 – ENTERPRISE

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 3 – BACKUP

- BACKUP & RECOVERY OF MAILBOXES & TEAMS
- BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT
- BACKUP & RECOVERY OF ENDPOINTS

PLAN 4 – COMPLIANCE & AWARENESS

- PERMISSION MANAGEMENT
- PERMISSION ALERTS
- PERMISSION AUDIT
- PHISING & ATTACK SIMULATION
- SECURITY AWARENESS SERVICE
- ESI® REPORTING
- COMMUNICATION PATTERN ANALYSIS
- AI RECIPIENT VALIDATION
- AUTOMATED CONTENT VALIDATION