Roglit 25

Celovita zaščita M365 storitev - Check Point Email & Collaboration Security

Duško Topić - Unistar

Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem

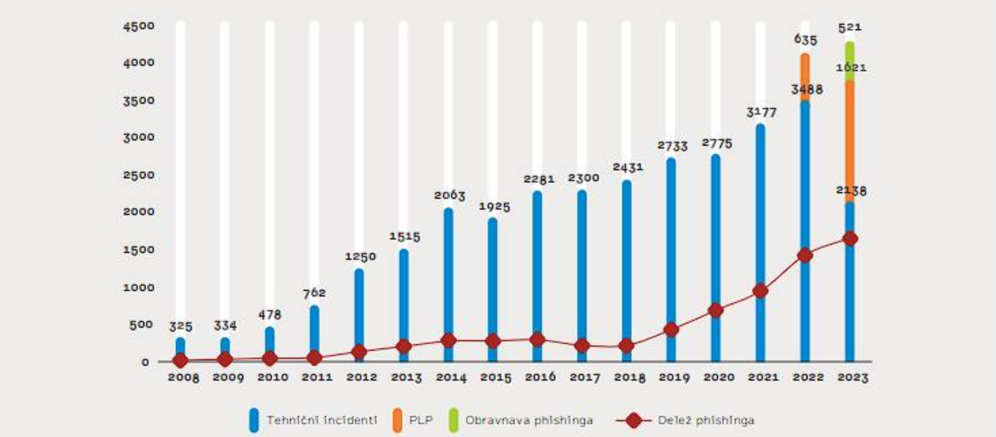
ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Agenda

- Vrste napadov
- Možne rešitve
- Check Point Harmony Email & Collaboration
- Onboarding (POC)
- Primeri v praksi

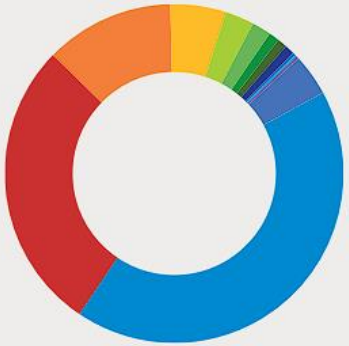
Incidenti skozi leta

INCIDENTI SKOZI LETA

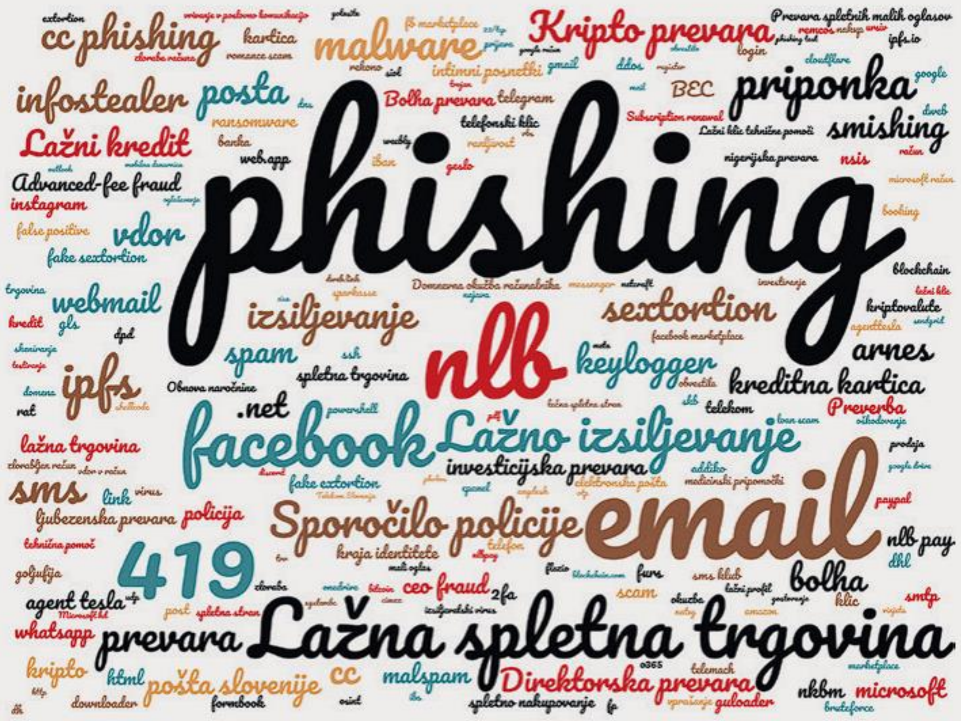


PRIJAVITELJI PO SEKTORJIH

924 (12%) fizična oseba	40 (2%) operater elektronskih komunikacij	5 (0%) digitalna infrastruktura
606 (12%) druge pravne osebe	22 (1%) zdravstvo	2 (0%) pitna voda
269 (12%) bančništvo	20 (1%) energija	2 (0%) oblačno računalništvo
116 (5%) raziskovanje in izobraževanje	20 (1%) promet	1 (0%) finančni trgi
60 (3%) državni organi	6 (0%) digitalni trg	86 (4%) drugo



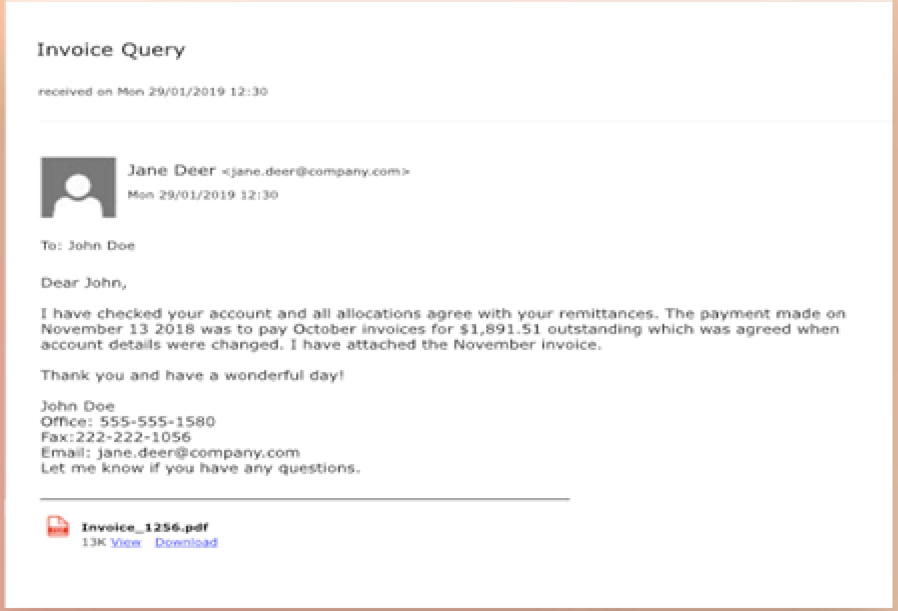
KLJUČNE BESEDE V OBRAVNAVANIH INCIDENTIH



Roglit25

Vrste napadov

- **Malware Phishing**
  (lažno predstavljanje zlonamerne opreme)



Invoice Query

received on Mon 29/01/2019 12:30

Jane Deer <jane.deer@company.com>
Mon 29/01/2019 12:30

To: John Doe

Dear John,

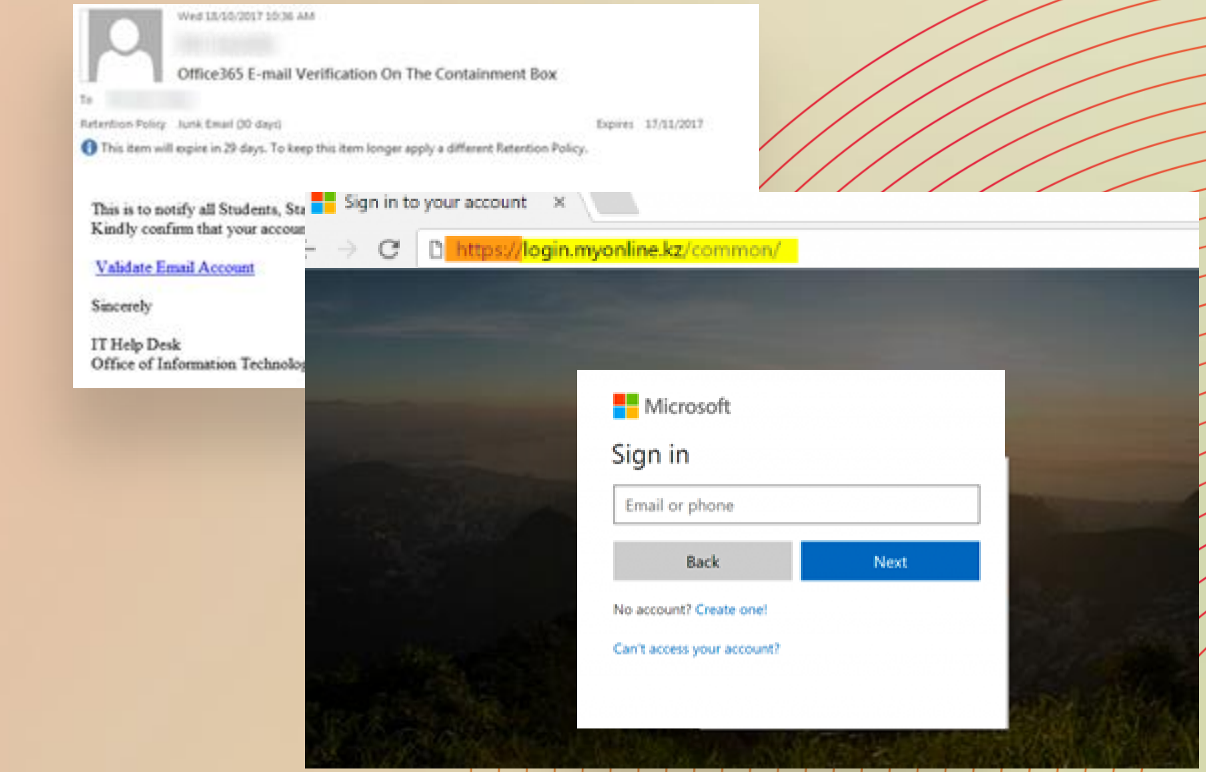
I have checked your account and all allocations agree with your remittances. The payment made on November 13 2018 was to pay October invoices for $1,891.51 outstanding which was agreed when account details were changed. I have attached the November invoice.

Thank you and have a wonderful day!

John Doe
Office: 555-555-1580
Fax:222-222-1056
Email: jane.deer@company.com
Let me know if you have any questions.

Invoice_1256.pdf
13K View Download

- **Credential Harvesting**
  (zbiranje poverilnic)



Wed 18/10/2017 10:36 AM
[redacted]
Office365 E-mail Verification On The Containment Box
To [redacted]
Retention Policy Junk Email (30 days) Expires 17/11/2017
This item will expire in 29 days. To keep this item longer apply a different Retention Policy.

This is to notify all Students, Sta
Kindly confirm that your accou

Validate Email Account

Sincerely

IT Help Desk
Office of Information Technolog

Sign in to your account ×

https://login.myonline.kz/common/

Microsoft

Sign in

Email or phone

Back Next

No account? Create one!

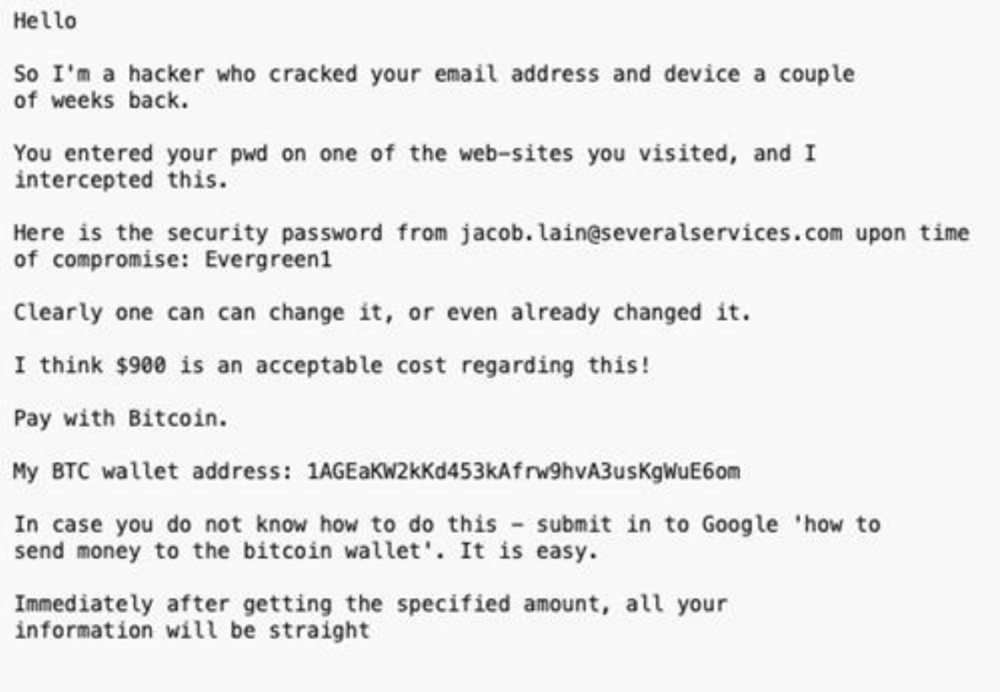
Can't access your account?

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit25

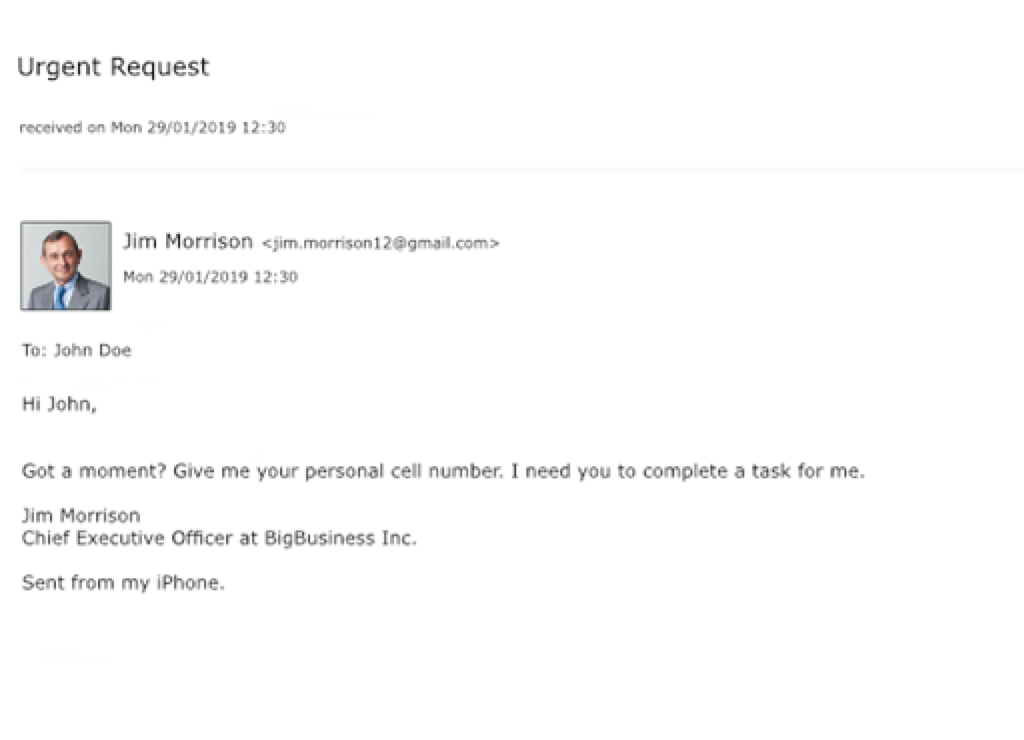
Vrste napadov

- **Extortion Emails (izsiljevalska sporočila)**



```
Hello

So I'm a hacker who cracked your email address and device a couple
of weeks back.

You entered your pwd on one of the web-sites you visited, and I
intercepted this.

Here is the security password from jacob.lain@severalservices.com upon time
of compromise: Evergreen1

Clearly one can can change it, or even already changed it.

I think $900 is an acceptable cost regarding this!

Pay with Bitcoin.

My BTC wallet address: 1AGEaKW2kKd453kAfrw9hvA3usKgWuE6om

In case you do not know how to do this - submit in to Google 'how to
send money to the bitcoin wallet'. It is easy.

Immediately after getting the specified amount, all your
information will be straight
```

- **BEC (Business Email Compromise) (lažno predstavljanje)**



Urgent Request

received on Mon 29/01/2019 12:30

Jim Morrison <jim.morrison12@gmail.com>
Mon 29/01/2019 12:30

To: John Doe

Hi John,

Got a moment? Give me your personal cell number. I need you to complete a task for me.

Jim Morrison
Chief Executive Officer at BigBusiness Inc.

Sent from my iPhone.

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Kaj narediti?

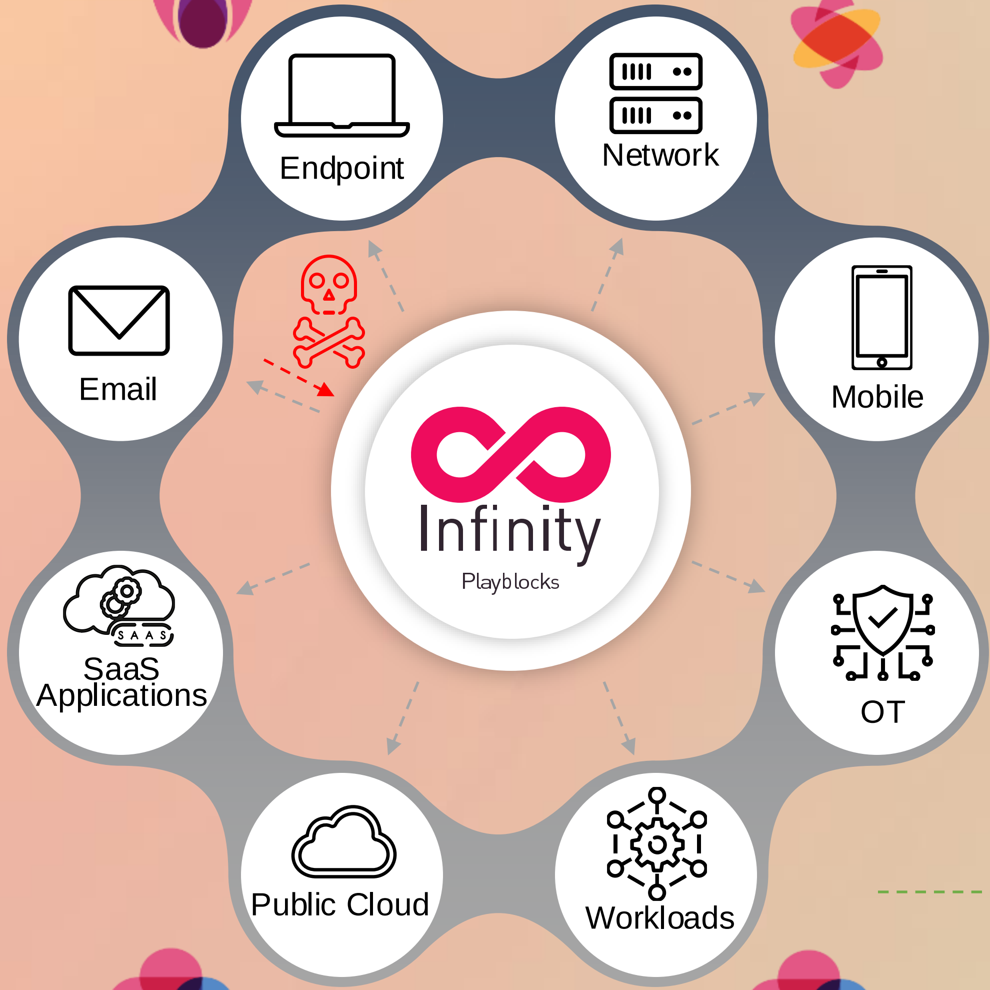
Nenehno izobraževanje zaposlenih ter opozarjanje o najnovejših varnostnih grožnjah

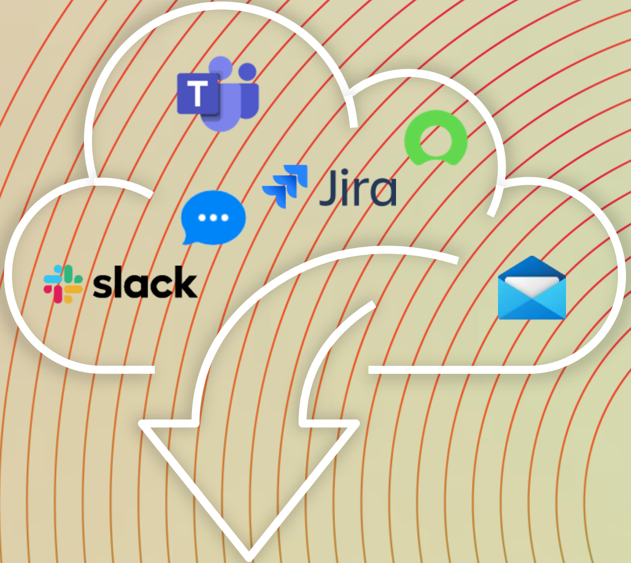
Izbrati ustrezno rešitev, ki:

- **Se uči iz zgodovine mailov (User behaviour)**
- **Analizira vsebino maila, priponk, povezav..**
- **Prepozna, da se je nekdo „vrinil“ ali preusmeril komunikacijo (BEC)**
- **Zazna istočasno prijavo iz različnih lokacij**
- **Deluje na širokem spektru (mail, endpoint, mobilne naprave...)**
- **Zazna in prepreči napad, ki v sisteme namestijo program, ki zašifrira vse dokumente**

Avtomatizirana varnost

Roglit25



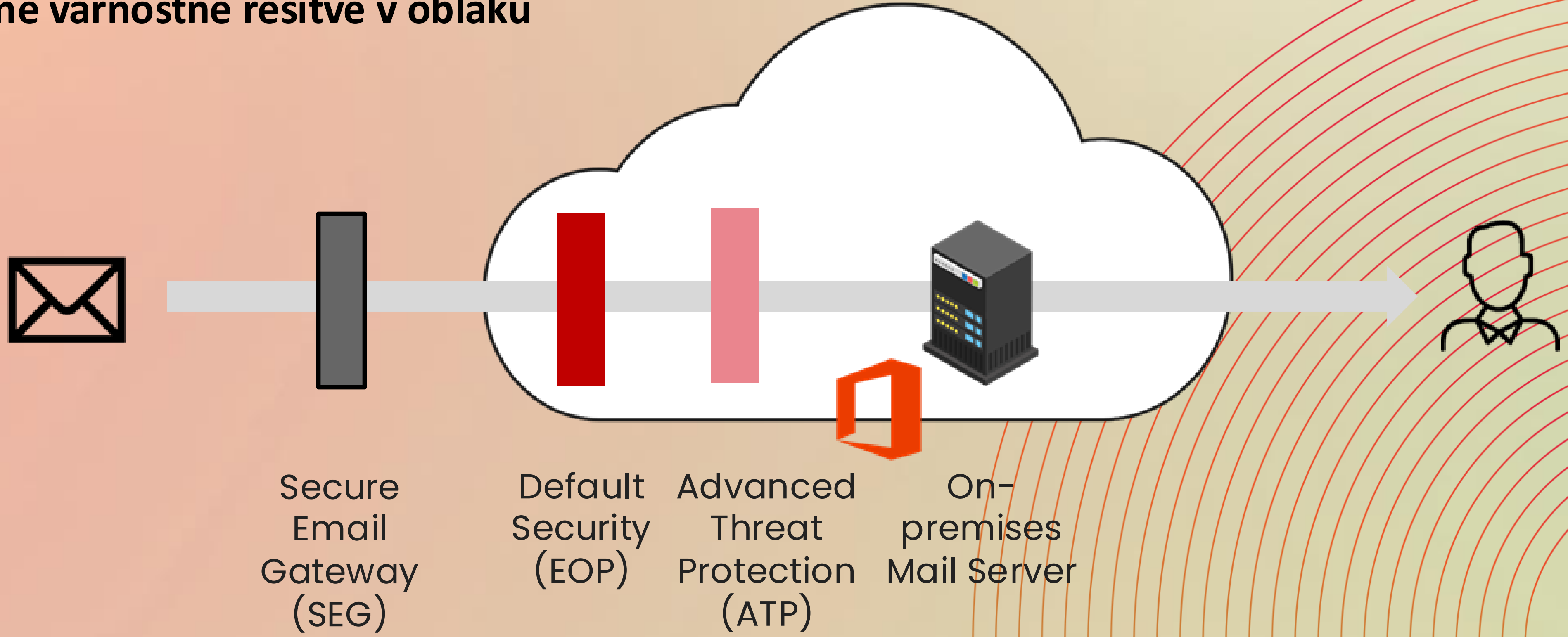


ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Možne rešitve

On-premise Email Gateway

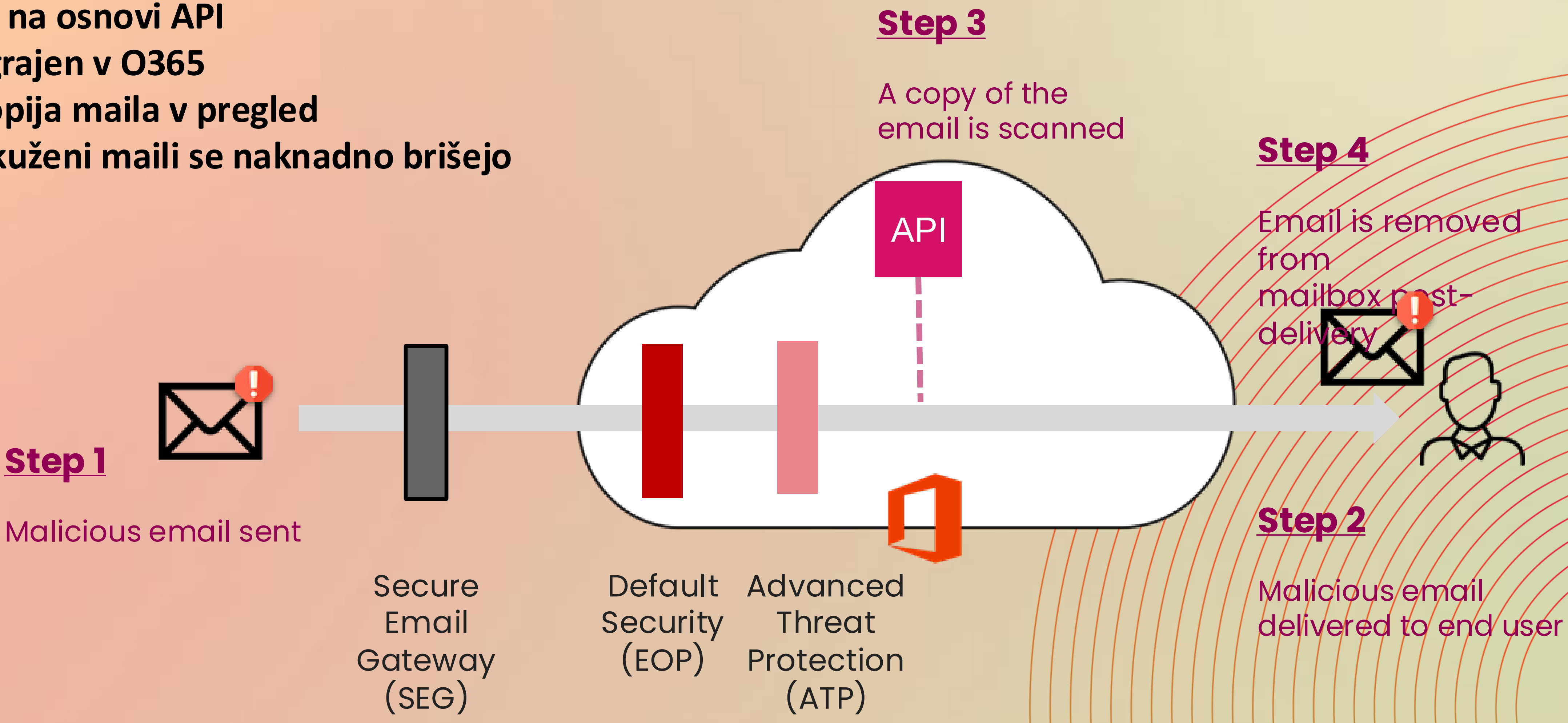
- **Potreba po lastni infrastrukturi**
- **Onemogočene varnostne rešitve v oblaku**



Možne rešitve

Varnost na osnovi API

- Vgrajen v O365
- Kopija maila v pregled
- Okuženi maili se naknadno brišejo

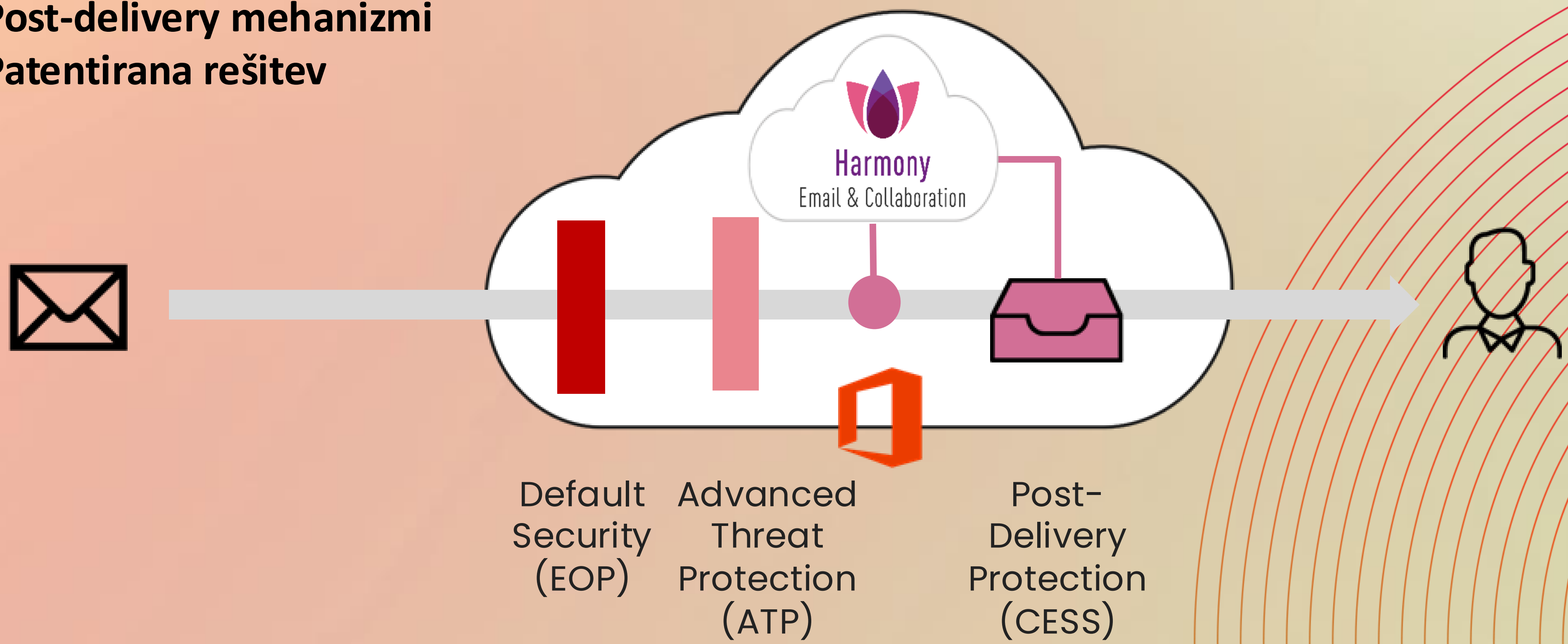


Step 3
A copy of the email is scanned
API
Step 4
Email is removed from mailbox post-delivery
Step 1
Malicious email sent
Step 2
Malicious email delivered to end user
Secure Email Gateway (SEG)
Default Security (EOP)
Advanced Threat Protection (ATP)

Možne rešitve

Harmony Email & Collaboration

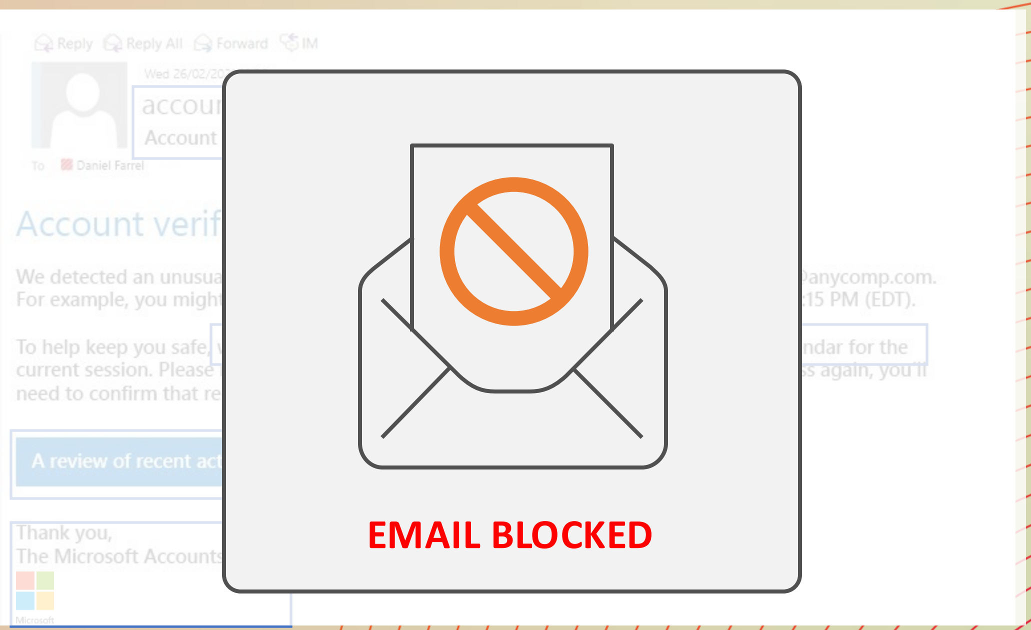
- **Vgrajen v O365 “inline” način**
- **Okužen mail ne prispe do uporabnika**
- **Post-delivery mehanizmi**
- **Patentirana rešitev**


Harmony
Email & Collaboration
Default Security (EOP)
Advanced Threat Protection (ATP)
Post-Delivery Protection (CESS)

Harmony Email & Collaboration

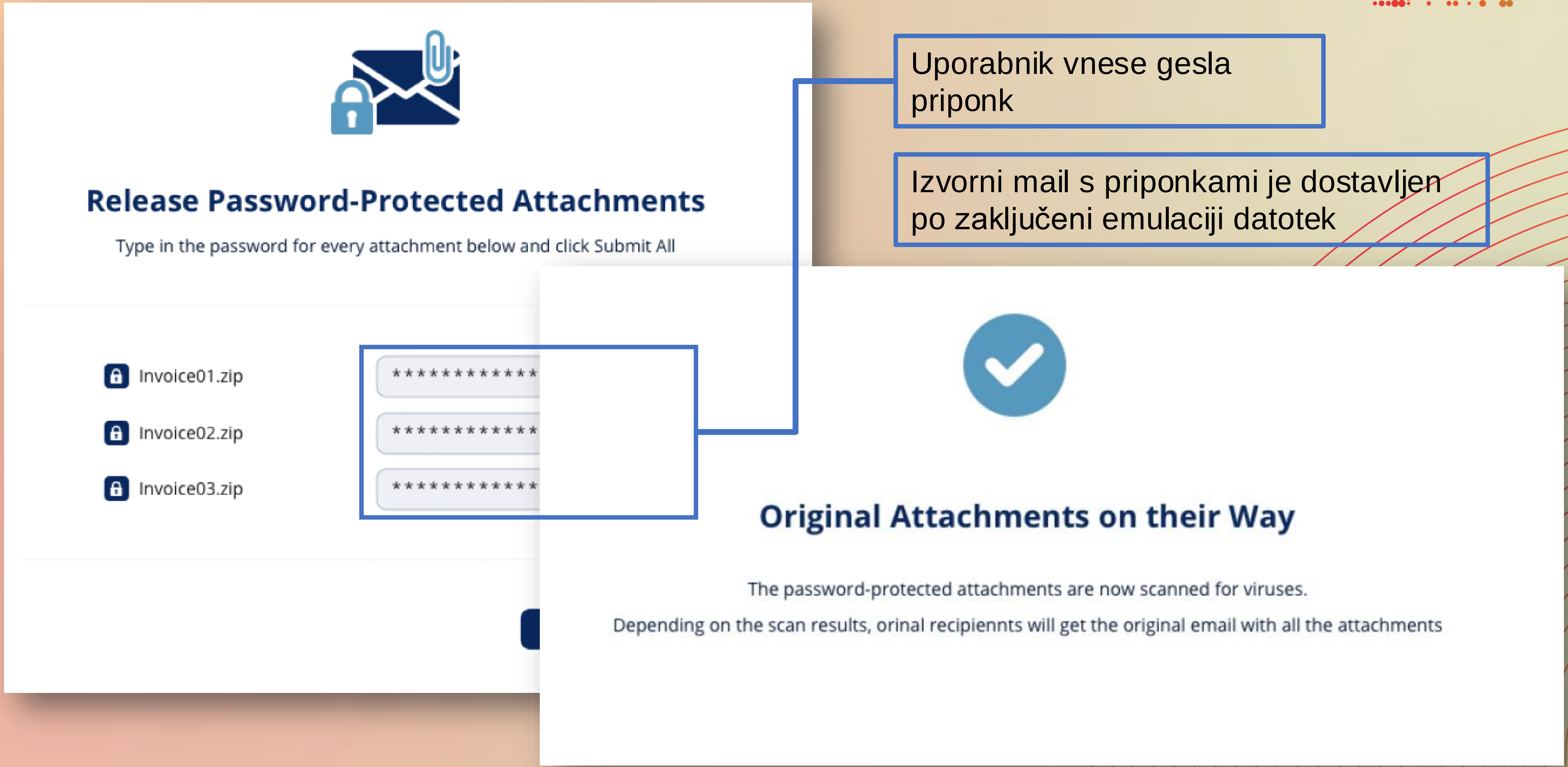
Roglit25

- Zaznava Phishing z uporabo ThreatCloud AI, analizira prek 300 indikatorjev
  - IP Reputation
  - URL Reputation ✓
  - Subject Content
  - HTML Inspection
  - Natural Language Processing ✓
  - Domain Reputation ✓
  - Lookalike Icon
  - Brand Impersonation ✓
  - URL Emulation
  - File Emulation
  - …



ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Harmony Email & Collaboration



Release Password-Protected Attachments

Type in the password for every attachment below and click Submit All

Invoice01.zip	************
Invoice02.zip	************
Invoice03.zip	************

Original Attachments on their Way

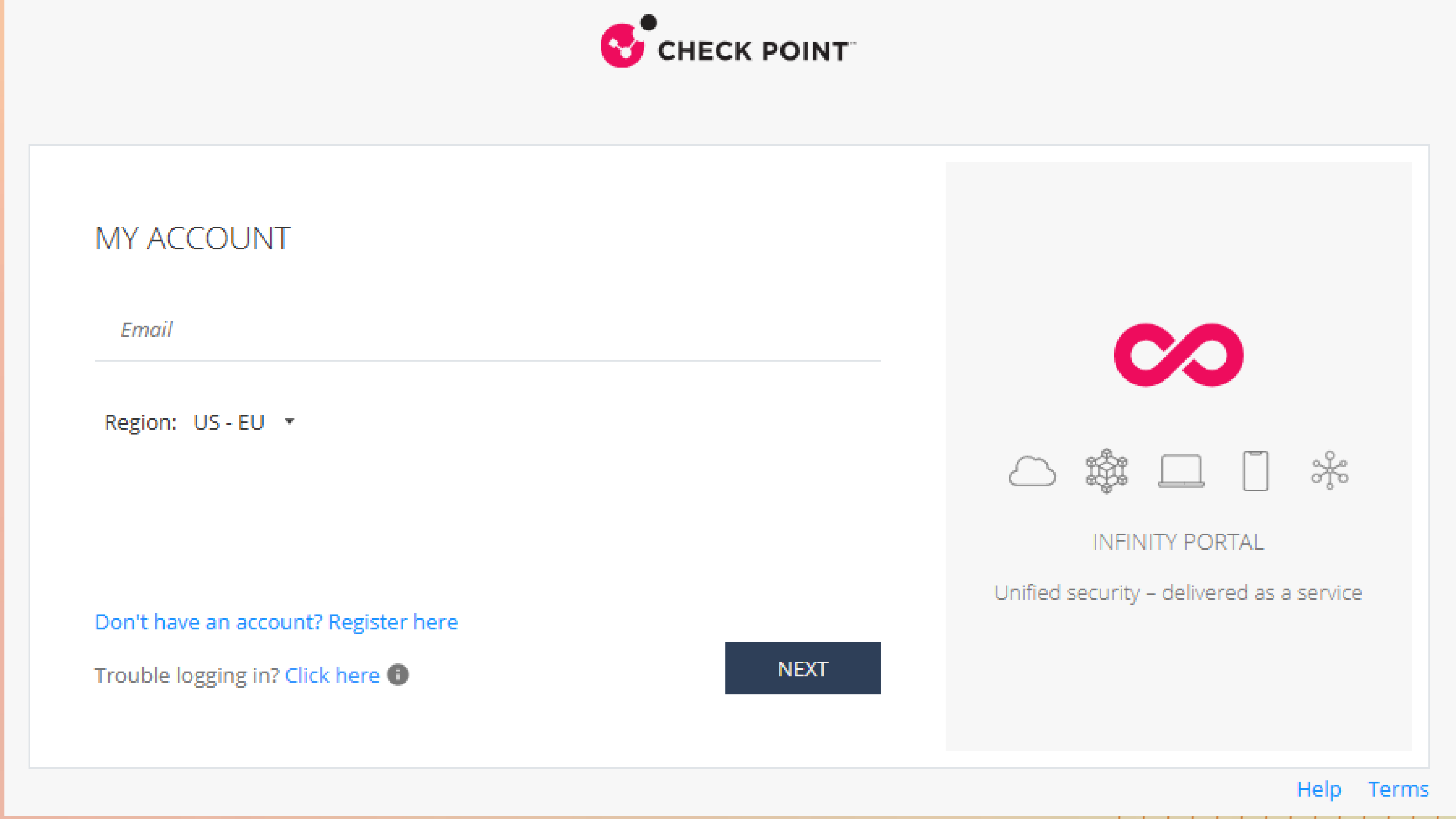
The password-protected attachments are now scanned for viruses.

Depending on the scan results, orinal recipiennts will get the original email with all the attachments

Uporabnik vnese gesla priponk

Izvorni mail s priponkami je dostavljen po zaključeni emulaciji datotek

Onboarding



CHECK POINT

MY ACCOUNT

Email

Region: US - EU

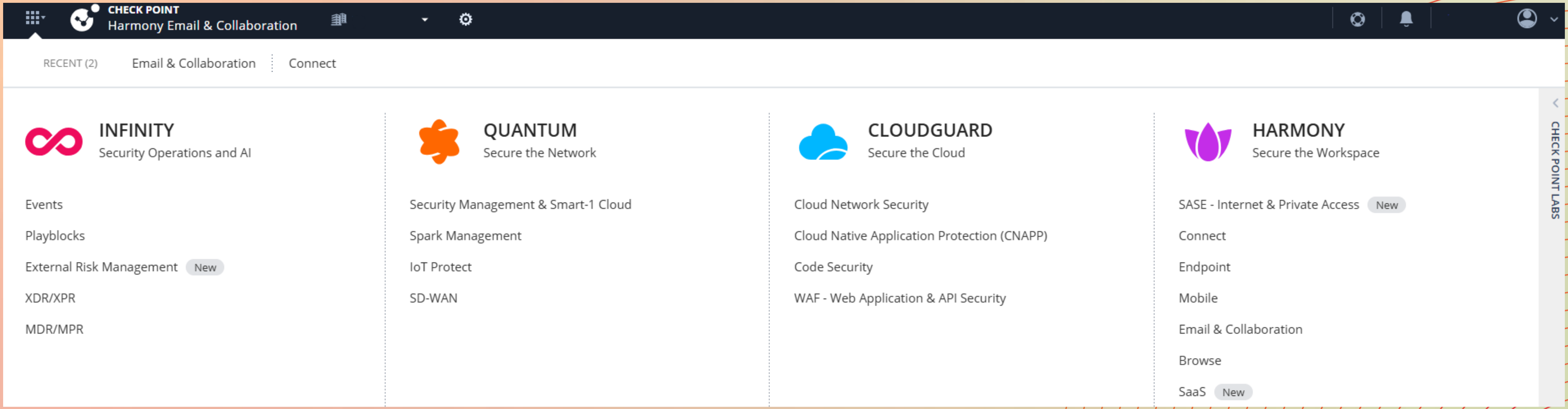
Don't have an account? Register here

Trouble logging in? Click here

INFINITY PORTAL

Unified security – delivered as a service

Onboarding



CHECK POINT
Harmony Email & Collaboration

RECENT (2)
Email & Collaboration
Connect

INFINITY
Security Operations and AI

- Events
- Playblocks
- External Risk Management New
- XDR/XPR
- MDR/MPR

QUANTUM
Secure the Network

- Security Management & Smart-1 Cloud
- Spark Management
- IoT Protect
- SD-WAN

CLOUDGUARD
Secure the Cloud

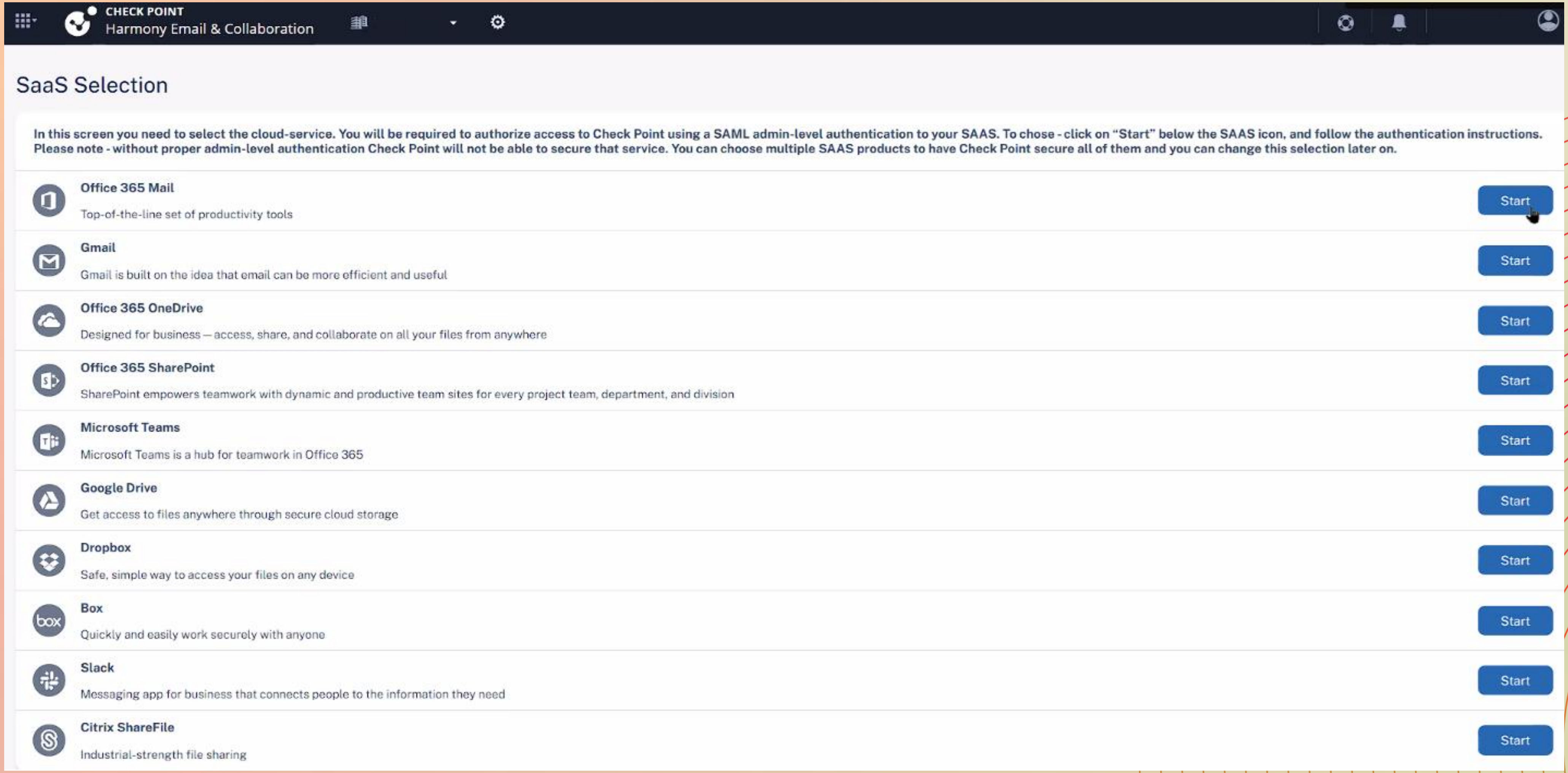
- Cloud Network Security
- Cloud Native Application Protection (CNAPP)
- Code Security
- WAF - Web Application & API Security

HARMONY
Secure the Workspace

- SASE - Internet & Private Access New
- Connect
- Endpoint
- Mobile
- Email & Collaboration
- Browse
- SaaS New

CHECK POINT LABS

Onboarding



SaaS Selection

In this screen you need to select the cloud-service. You will be required to authorize access to Check Point using a SAML admin-level authentication to your SAAS. To chose - click on "Start" below the SAAS icon, and follow the authentication instructions. Please note - without proper admin-level authentication Check Point will not be able to secure that service. You can choose multiple SAAS products to have Check Point secure all of them and you can change this selection later on.

Office 365 Mail
Top-of-the-line set of productivity tools
Start

Gmail
Gmail is built on the idea that email can be more efficient and useful
Start

Office 365 OneDrive
Designed for business — access, share, and collaborate on all your files from anywhere
Start

Office 365 SharePoint
SharePoint empowers teamwork with dynamic and productive team sites for every project team, department, and division
Start

Microsoft Teams
Microsoft Teams is a hub for teamwork in Office 365
Start

Google Drive
Get access to files anywhere through secure cloud storage
Start

Dropbox
Safe, simple way to access your files on any device
Start

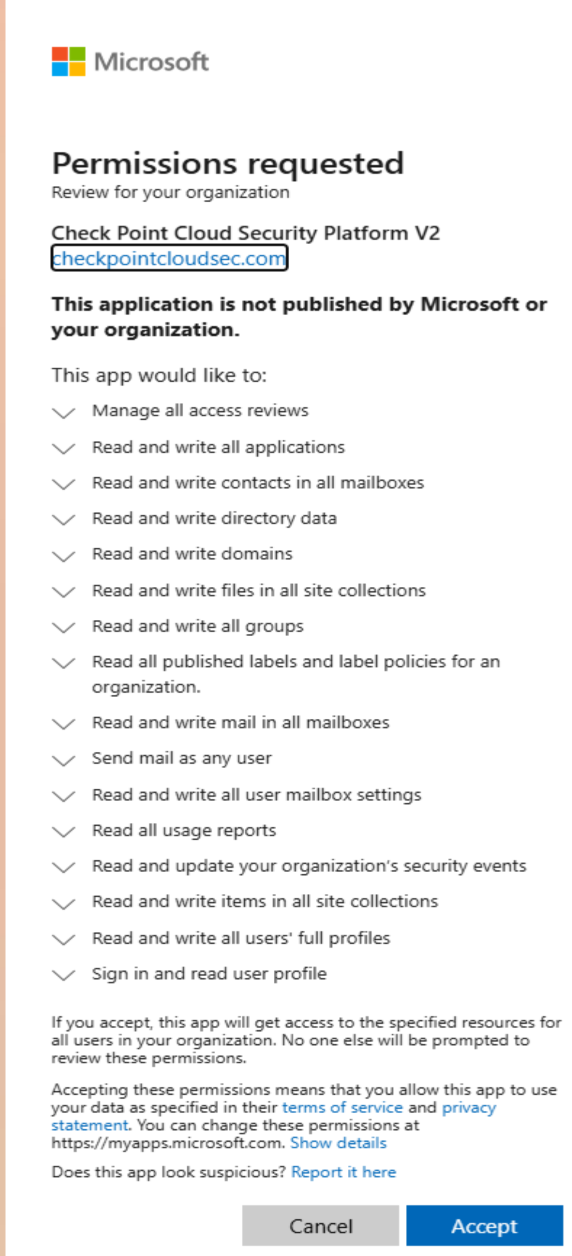
Box
Quickly and easily work securely with anyone
Start

Slack
Messaging app for business that connects people to the information they need
Start

Citrix ShareFile
Industrial-strength file sharing
Start

Onboarding

- **Potrditev pravic za posamezno aplikacijo**



Permissions requested

Review for your organization

Check Point Cloud Security Platform V2
checkpointcloudsec.com

This application is not published by Microsoft or your organization.

This app would like to:

- Manage all access reviews
- Read and write all applications
- Read and write contacts in all mailboxes
- Read and write directory data
- Read and write domains
- Read and write files in all site collections
- Read and write all groups
- Read all published labels and label policies for an organization.
- Read and write mail in all mailboxes
- Send mail as any user
- Read and write all user mailbox settings
- Read all usage reports
- Read and update your organization's security events
- Read and write items in all site collections
- Read and write all users' full profiles
- Sign in and read user profile

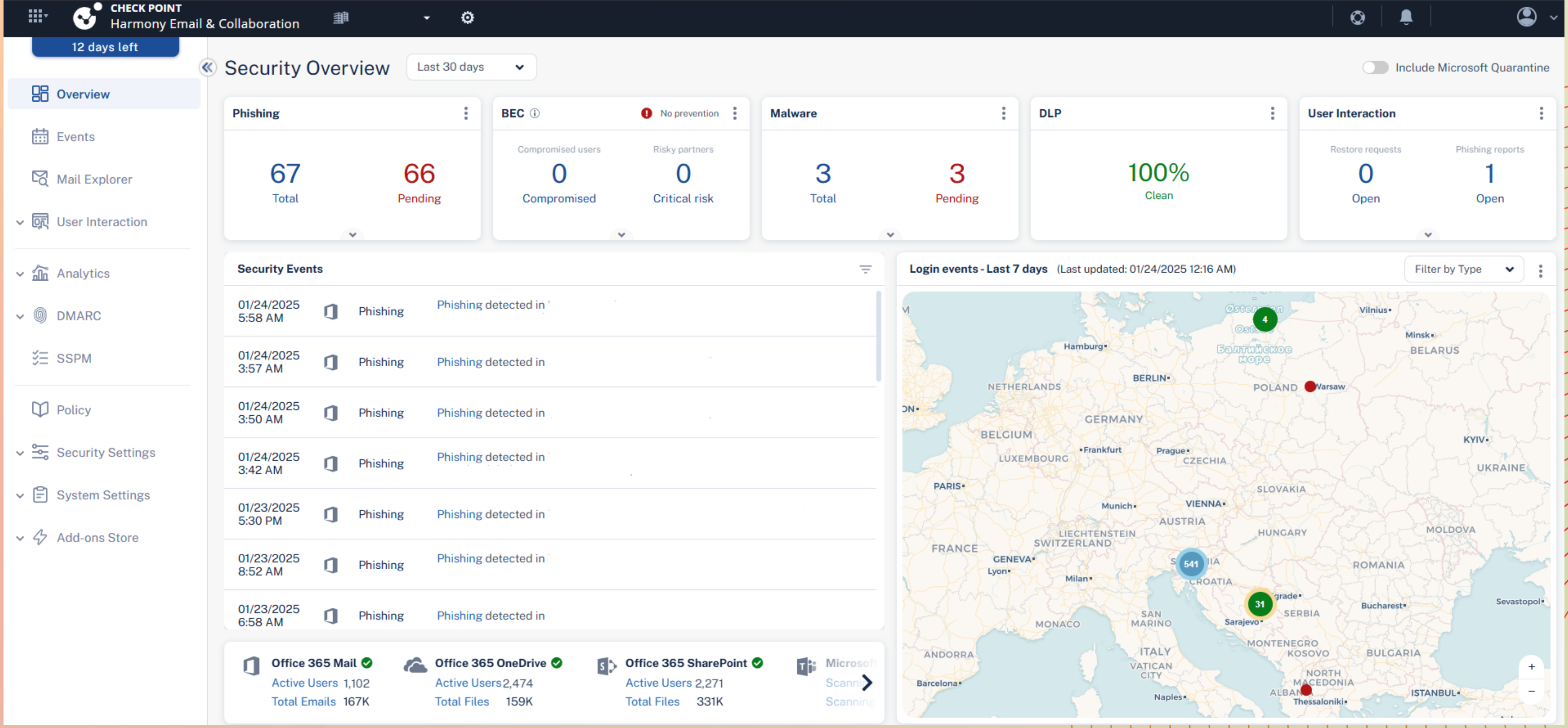
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Onboarding - Dashboard

Roglit25



CHECK POINT
Harmony Email & Collaboration

12 days left

- Overview
- Events
- Mail Explorer
- User Interaction
- Analytics
- DMARC
- SSPM
- Policy
- Security Settings
- System Settings
- Add-ons Store

Security Overview

Last 30 days

Include Microsoft Quarantine

Phishing
67 Total
66 Pending

BEC ⓘ ● No prevention
Compromised users: 0 Compromised
Risky partners: 0 Critical risk

Malware
3 Total
3 Pending

DLP
100% Clean

User Interaction
Restore requests: 0 Open
Phishing reports: 1 Open

Security Events

01/24/2025 5:58 AM	Phishing	Phishing detected in
01/24/2025 3:57 AM	Phishing	Phishing detected in
01/24/2025 3:50 AM	Phishing	Phishing detected in
01/24/2025 3:42 AM	Phishing	Phishing detected in
01/23/2025 5:30 PM	Phishing	Phishing detected in
01/23/2025 8:52 AM	Phishing	Phishing detected in
01/23/2025 6:58 AM	Phishing	Phishing detected in

Office 365 Mail ✓
Active Users 1,102
Total Emails 167K

Office 365 OneDrive ✓
Active Users 2,474
Total Files 159K

Office 365 SharePoint ✓
Active Users 2,271
Total Files 331K

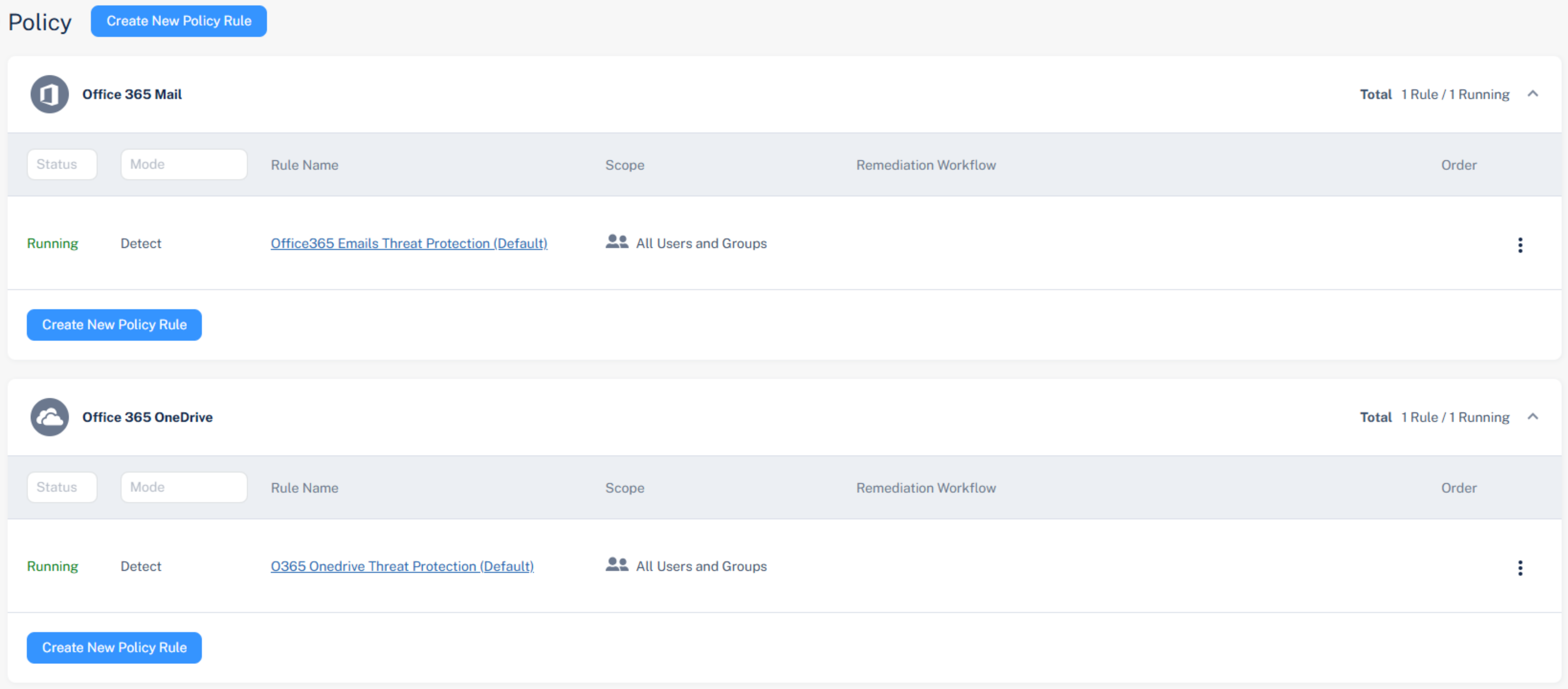
Microsof
Scann
Scanning

Login events - Last 7 days (Last updated: 01/24/2025 12:16 AM)

Filter by Type

ACTUAL I.T.   UNISTAR PRO   ITELIS   astec   ACTUAL I.T. GROUP A DBA Group Company

Onboarding - Policy



Policy Create New Policy Rule

Office 365 Mail **Total** 1 Rule / 1 Running

Status	Mode	Rule Name	Scope	Remediation Workflow	Order
Running	Detect	Office365 Emails Threat Protection (Default)	All Users and Groups		

Create New Policy Rule

Office 365 OneDrive **Total** 1 Rule / 1 Running

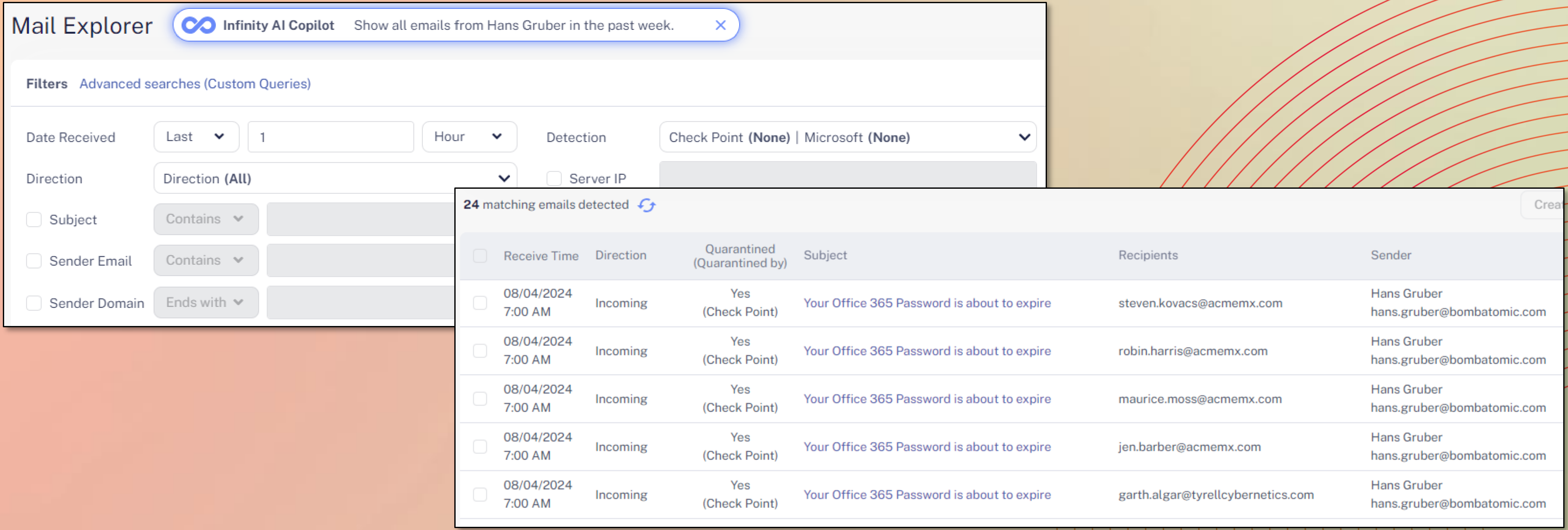
Status	Mode	Rule Name	Scope	Remediation Workflow	Order
Running	Detect	O365 Onedrive Threat Protection (Default)	All Users and Groups		

Create New Policy Rule

Roglit25

Primer 1 – AI Assistant

- **Nastavitev filtrov za iskanje v naravnem jeziku**



Mail Explorer

Infinity AI Copilot   Show all emails from Hans Gruber in the past week. ✕

Filters   Advanced searches (Custom Queries)

Date Received: Last ⌄ | 1 | Hour ⌄

Detection: Check Point **(None)** | Microsoft **(None)** ⌄

Direction: Direction **(All)** ⌄

□ Server IP

□ Subject: Contains ⌄

□ Sender Email: Contains ⌄

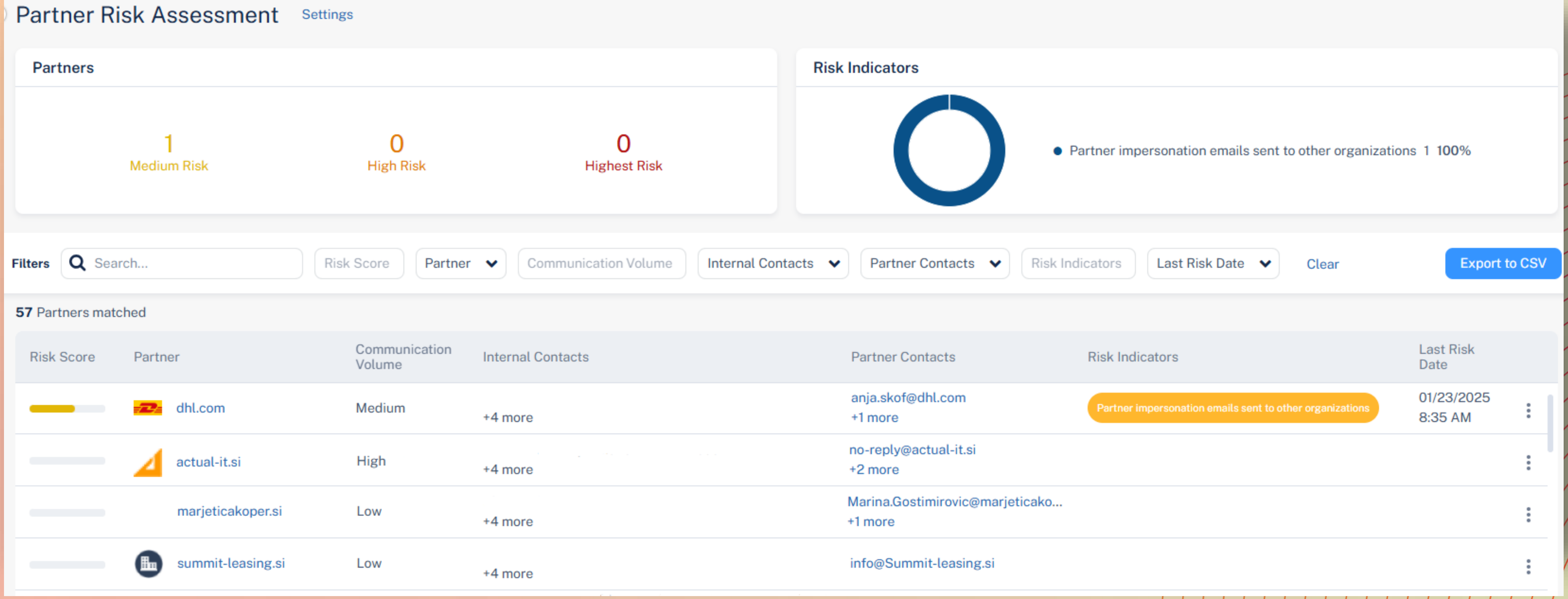
□ Sender Domain: Ends with ⌄

24 matching emails detected

□	Receive Time	Direction	Quarantined (Quarantined by)	Subject	Recipients	Sender
□	08/04/2024 7:00 AM	Incoming	Yes (Check Point)	Your Office 365 Password is about to expire	steven.kovacs@acmemx.com	Hans Gruber hans.gruber@bombatomic.com
□	08/04/2024 7:00 AM	Incoming	Yes (Check Point)	Your Office 365 Password is about to expire	robin.harris@acmemx.com	Hans Gruber hans.gruber@bombatomic.com
□	08/04/2024 7:00 AM	Incoming	Yes (Check Point)	Your Office 365 Password is about to expire	maurice.moss@acmemx.com	Hans Gruber hans.gruber@bombatomic.com
□	08/04/2024 7:00 AM	Incoming	Yes (Check Point)	Your Office 365 Password is about to expire	jen.barber@acmemx.com	Hans Gruber hans.gruber@bombatomic.com
□	08/04/2024 7:00 AM	Incoming	Yes (Check Point)	Your Office 365 Password is about to expire	garth.algar@tyrellcybernetics.com	Hans Gruber hans.gruber@bombatomic.com

ACTUAL I.T.   UNISTAR PRO   ITELIS   astec   ACTUAL I.T. GROUP A DBA Group Company

Primer 2 – Partner Risk Assesment



Partner Risk Assessment

Settings

Partners

1 Medium Risk

0 High Risk

0 Highest Risk

Risk Indicators

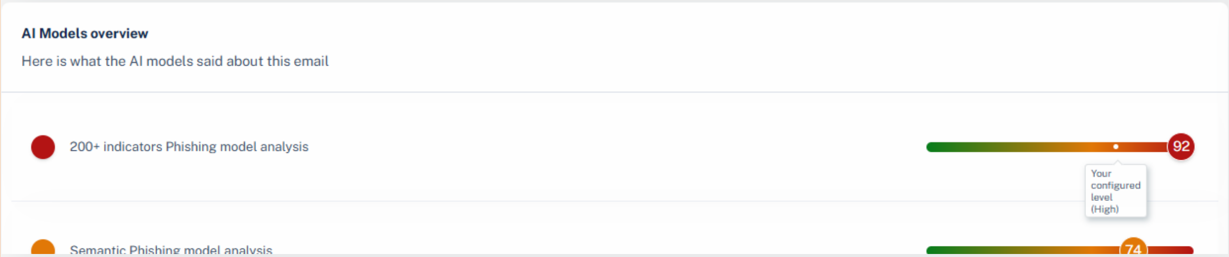
● Partner impersonation emails sent to other organizations 1 100%

Filters | Search... | Risk Score | Partner | Communication Volume | Internal Contacts | Partner Contacts | Risk Indicators | Last Risk Date | Clear | Export to CSV

57 Partners matched

Risk Score	Partner	Communication Volume	Internal Contacts	Partner Contacts	Risk Indicators	Last Risk Date
	dhl.com	Medium	+4 more	anja.skof@dhl.com +1 more	Partner impersonation emails sent to other organizations	01/23/2025 8:35 AM
	actual-it.si	High	+4 more	no-reply@actual-it.si +2 more		
	marjeticakoper.si	Low	+4 more	Marina.Gostimirovic@marjeticako... +1 more		
	summit-leasing.si	Low	+4 more	info@Summit-leasing.si		

Primer 3 – Phishing

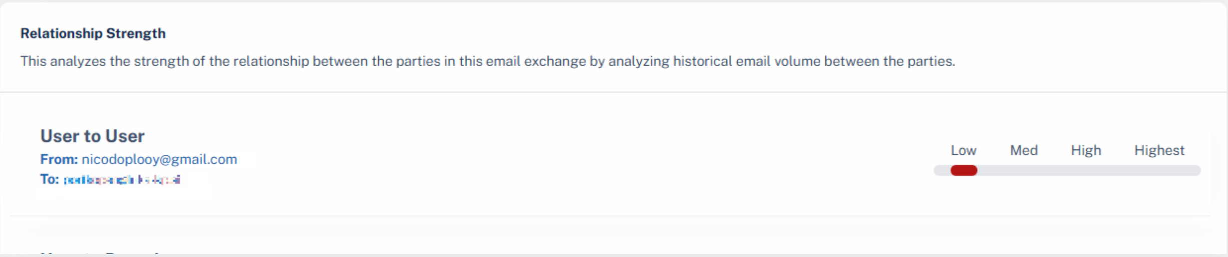


AI Models overview

Here is what the AI models said about this email

● 200+ indicators Phishing model analysis — 92

● Semantic Phishing model analysis — 74



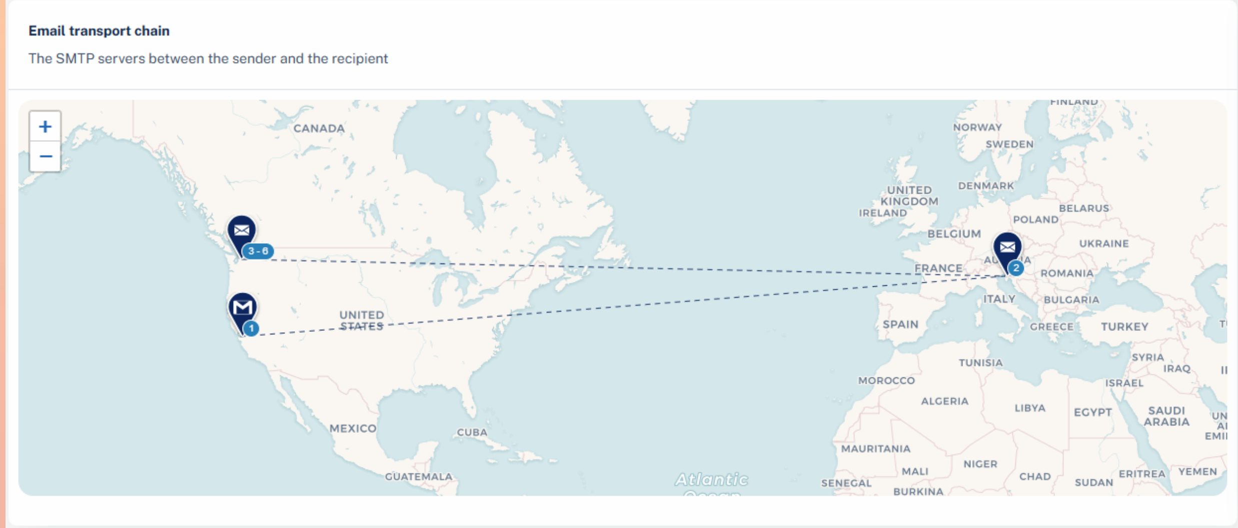
Relationship Strength

This analyzes the strength of the relationship between the parties in this email exchange by analyzing historical email volume between the parties.

User to User

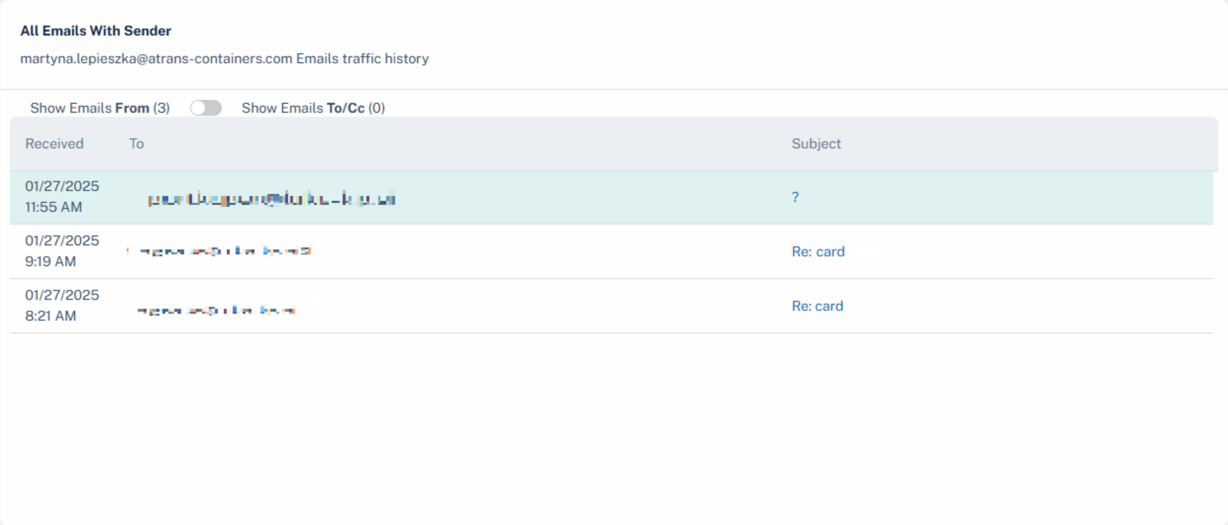
From: nicodoplooy@gmail.com

To: [redacted]



Email transport chain

The SMTP servers between the sender and the recipient

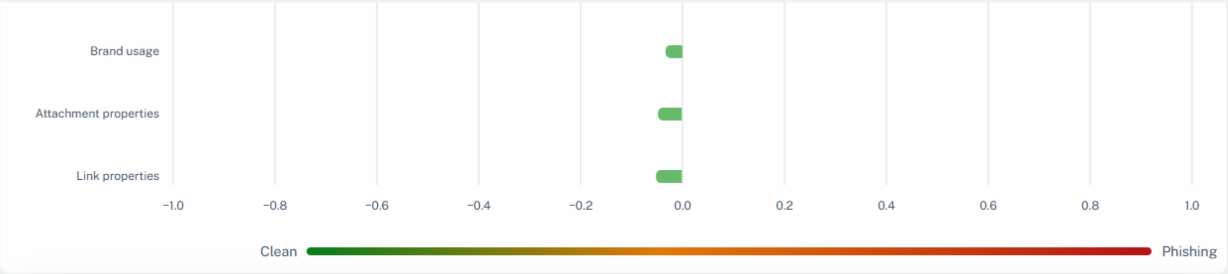


All Emails With Sender

martyna.lepieszka@atrans-containers.com Emails traffic history

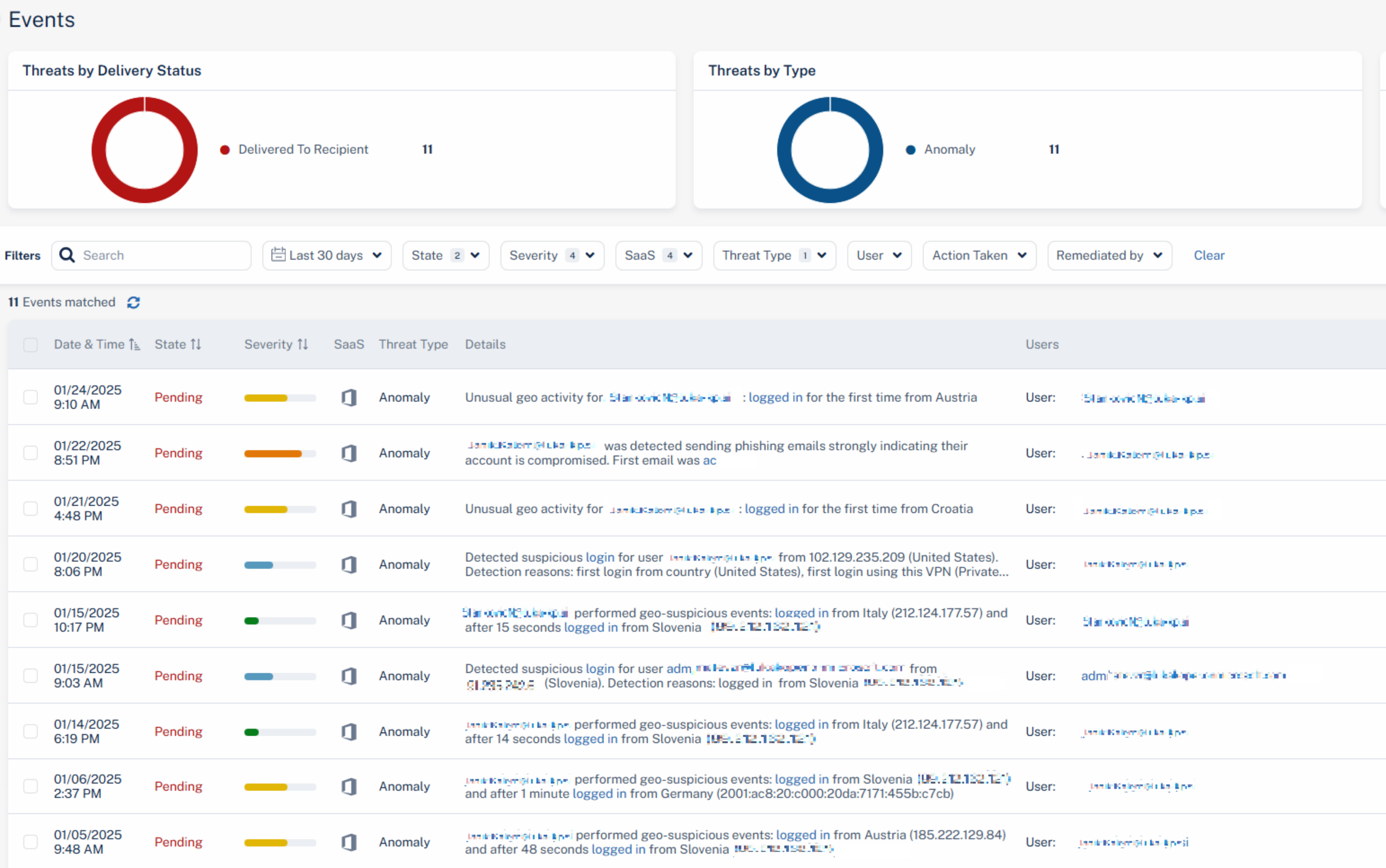
Show Emails **From** (3) ○ Show Emails **To/Cc** (0)

Received	To	Subject
01/27/2025 11:55 AM	[redacted]	?
01/27/2025 9:19 AM	[redacted]	Re: card
01/27/2025 8:21 AM	[redacted]	Re: card



Primer 4 – GEO Location analitika

Roglit25



Events

Threats by Delivery Status

● Delivered To Recipient	11

Threats by Type

● Anomaly	11

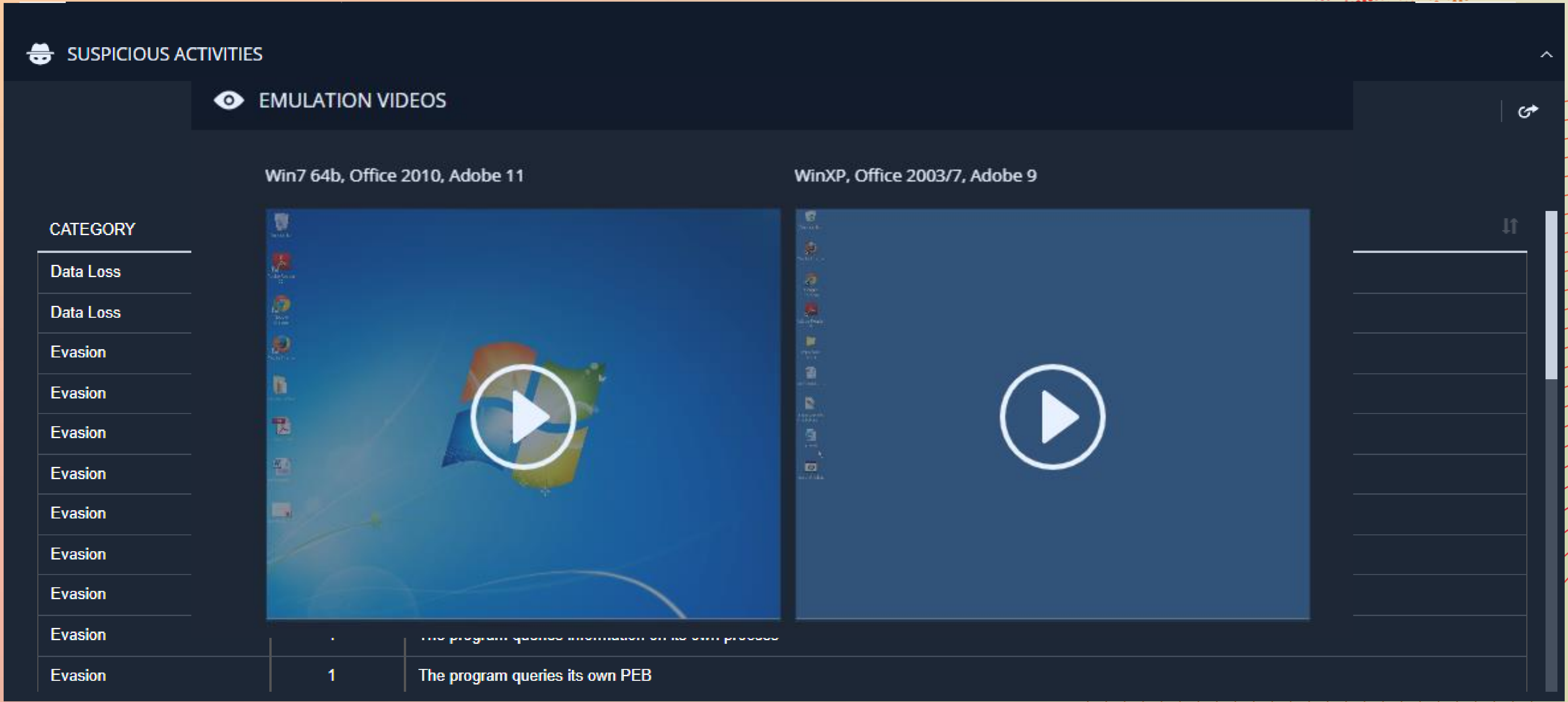
Filters | Search | Last 30 days | State 2 | Severity 4 | SaaS 4 | Threat Type 1 | User | Action Taken | Remediated by | Clear

11 Events matched

□	Date & Time	State	Severity	SaaS	Threat Type	Details	Users
□	01/24/2025 9:10 AM	Pending			Anomaly	Unusual geo activity for [redacted] : logged in for the first time from Austria	User: [redacted]
□	01/22/2025 8:51 PM	Pending			Anomaly	[redacted] was detected sending phishing emails strongly indicating their account is compromised. First email was ac	User: [redacted]
□	01/21/2025 4:48 PM	Pending			Anomaly	Unusual geo activity for [redacted] : logged in for the first time from Croatia	User: [redacted]
□	01/20/2025 8:06 PM	Pending			Anomaly	Detected suspicious login for user [redacted] from 102.129.235.209 (United States). Detection reasons: first login from country (United States), first login using this VPN (Private...	User: [redacted]
□	01/15/2025 10:17 PM	Pending			Anomaly	[redacted] performed geo-suspicious events: logged in from Italy (212.124.177.57) and after 15 seconds logged in from Slovenia [redacted]	User: [redacted]
□	01/15/2025 9:03 AM	Pending			Anomaly	Detected suspicious login for user adm [redacted] from [redacted] (Slovenia). Detection reasons: logged in from Slovenia [redacted]	User: adm [redacted]
□	01/14/2025 6:19 PM	Pending			Anomaly	[redacted] performed geo-suspicious events: logged in from Italy (212.124.177.57) and after 14 seconds logged in from Slovenia [redacted]	User: [redacted]
□	01/06/2025 2:37 PM	Pending			Anomaly	[redacted] performed geo-suspicious events: logged in from Slovenia [redacted] and after 1 minute logged in from Germany (2001:ac8:20:c000:20da:7171:455b:c7cb)	User: [redacted]
□	01/05/2025 9:48 AM	Pending			Anomaly	[redacted] performed geo-suspicious events: logged in from Austria (185.222.129.84) and after 48 seconds logged in from Slovenia [redacted]	User: [redacted]

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Primer 5 – Sharepoint



SUSPICIOUS ACTIVITIES

EMULATION VIDEOS

Win7 64b, Office 2010, Adobe 11
WinXP, Office 2003/7, Adobe 9

CATEGORY		
Data Loss		
Data Loss		
Evasion		
Evasion		
Evasion		
Evasion		
Evasion		
Evasion		
Evasion		
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PEB

Vprašanja

Hvala za vašo pozornost!