Trellix

3-6 November 2025

# EMEA & LTAM Tech Summit

Madrid, Spain

Trellix

# Collaboration Security

## Mitigating Threats in Modern Workspaces

# Speakers


## Matteo Spiga

Solutions Engineer

## Rahul Iyer

Principal, Product Management

Trellix

# Breakout Sessions Content Structure

| |
|---|
| **Solution Presentation** |
| **Architecture** |
| **Key Use-cases** |
| **Demonstration** |
| **Licensing** |
| **Trellix differentiators** |
| **Q&A** |

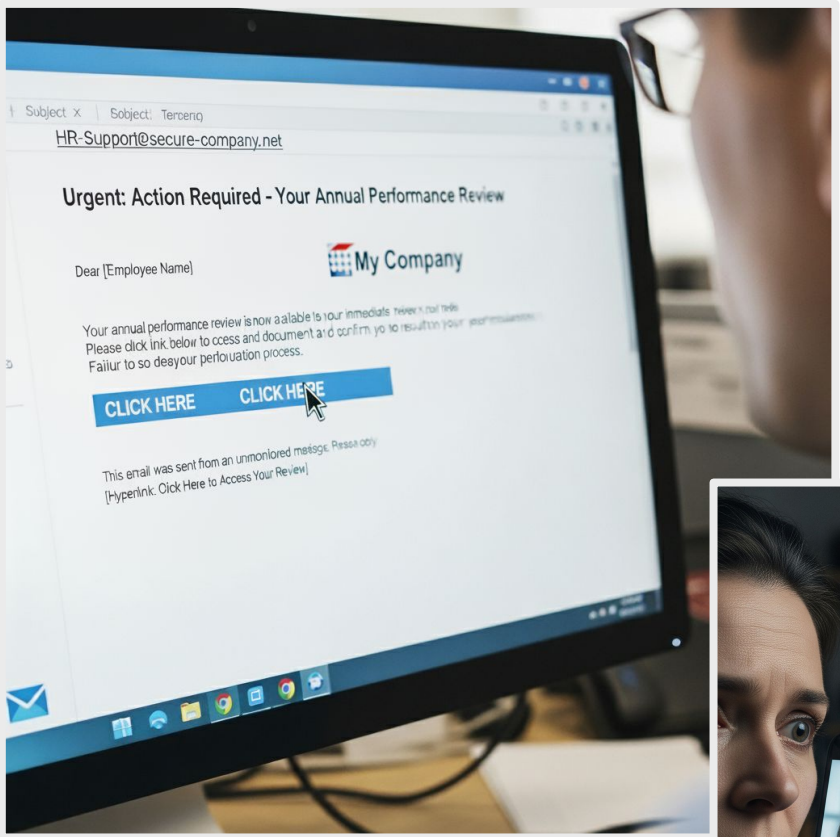
Trellix

Trellix

# Solution Presentation

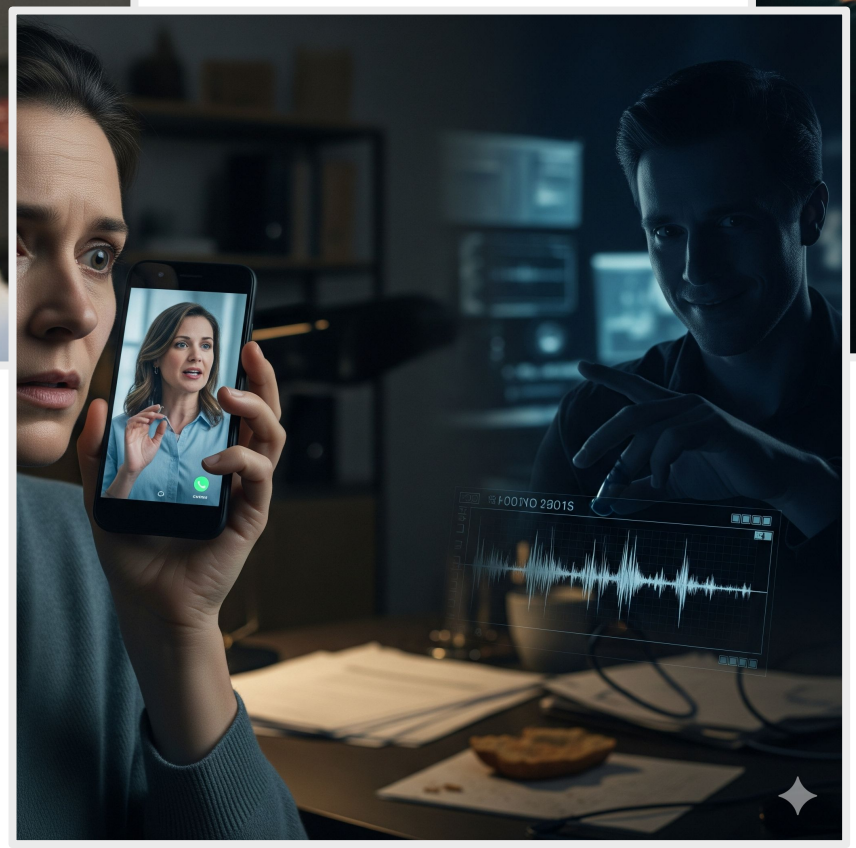
# Collaboration Security

Trellix




Phishing

Deepfake



Advanced techniques

Trellix

# What We're Hearing - How Can We Help?

## Malicious emails and files are still getting through

Phishing-as-a-Service is less than $250/month[1]

## Too much time wasted on false positives

Nearly 1/3 of alerts are false positives[2]

## Despite training, users make mistakes

Email reading time is cut nearly 50% in high stress[3]

Trellix

1. Trellix | 2. IBM | 3. NDSS Symposium

# Cyber threat landscape

## Trellix CyberThreat Report October 2025

- A look into the evolving APT landscape
- Ransomware's new dominance and emerging threats
- Cybercriminals' use of AI-powered malware
- Complex attack chains and exploitation of vulnerabilities


https://www.trellix.com/advanced-research-center/threat-reports/october-2025/

Trellix

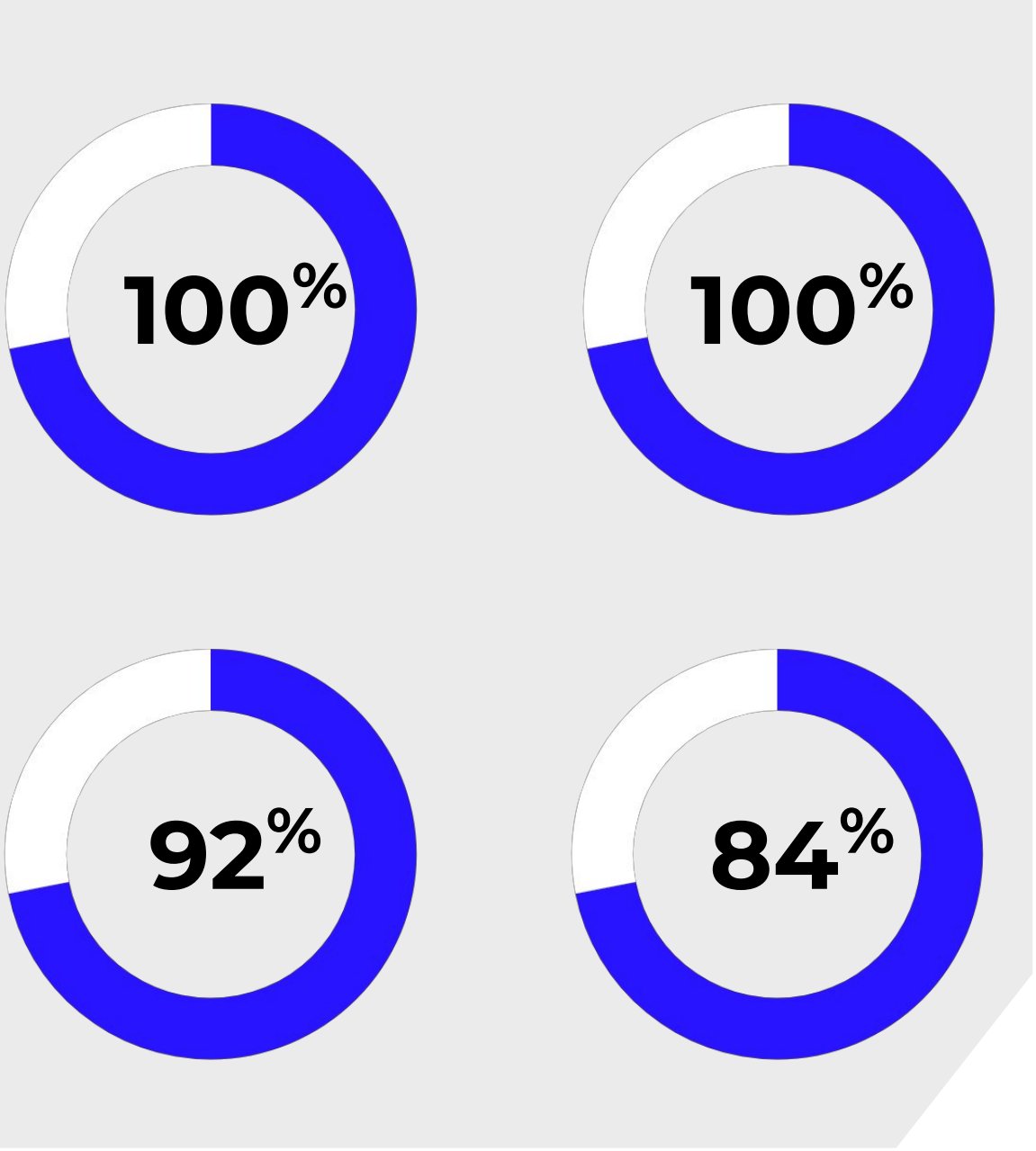
# Mind of CISO
## Decoding the GenAI Impact

**100%** are currently using or plan to use Generative AI

**100%** are concerned about cybercriminals using GenAI to perform cyber attacks

**92%** believe GenAI without clear regulations puts their organizations at greater risk

**84%** believe GenAI could give their organization an advantage over cybercriminals




Trellix

https://www.trellix.com/solutions/mind-of-the-ciso-decoding-the-genai-impact/

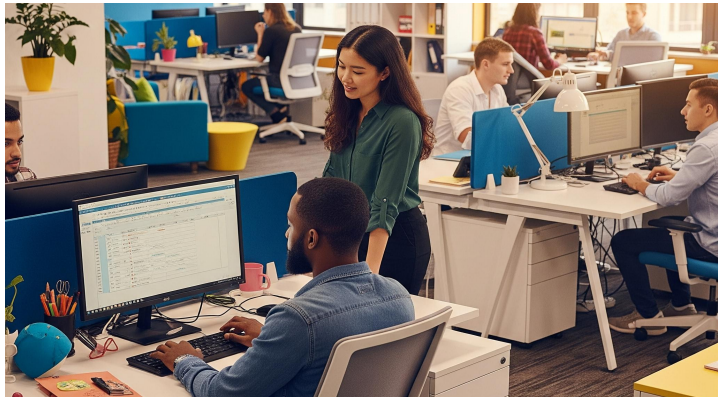
- *People are the weak link in security.*
- But…
- *People are our best defence if they are properly trained and they are properly aware.*

Trellix

# Protection for a New Era of Attackers

## Stop AI-Driven Phishing & Impersonation

- BEC, Impersonation, Malicious URLs, Attachments, Vishing, and QR Codes
- Minimize False Positives
- Extend Protection to Chat, File Shares, and Enterprise Apps



## Improve Response & Resilience

- Accelerate Analysis & Remediation
- Prevent Exfiltration and Leaks with Data Security
- Train a More Alert Workforce

## Fit Your Infrastructure Needs

- Multiple Deployment Options
- SEG, 2nd Hop, and API/ICES
- FedRamp Certified

Trellix

# Mitigate Human Risk Across The Organization

## Email

Catch BEC, impersonations, and other phishing attempts with advanced AI and precise file and URL inspection

## Collaboration & Enterprise Apps

Inspect everything and catch APTs across file sharing, file storage, chat and enterprise applications

## Data Security & Awareness Training

Prevent data leaks and grow a vigilant workforce to catch would be attackers before they can do harm

**Seamlessly integrated into the Trellix Security Platform**

# The World's Most Demanding Trust Trellix[1]

## Technology

- World's Top Public Cloud Service Provider
- Largest Global Telecom Provider
- The Leading Consumer Electronics Company

## Government Agencies

- 4.2 Million DoD mailboxes
- 5 out of 7 G7 Nations
- Half of the World's Largest Aerospace and Defense Contractors

## Financial Services

- World's Largest Investment Manager
- 150+ Large Global Financial Institutions
- Multiple Stock Exchange Entities

## Other Sectors

- 100+ Healthcare Service Providers
- 40+ Global Manufacturing & Industrial Companies
- Double-Digit Energy Service Providers

**Protecting over 25 million mailboxes around the world from top government agencies to Fortune 100 companies**

Trellix

1: As of Q3 2025

Trellix

# Architecture

Trellix IVX

# Precise File/URL Inspection at Scale

## Trellix Intelligent Virtual Execution (IVX)

Deployments

FedRAMP

### Hardened Hypervisor

- Designed for large scale threat analysis
- Custom hypervisor with built-in countermeasures
- Detect sandbox-aware and evasion tactics

### Multi-modal Virtual Execution

- Multiple operating systems and versions
- Multiple applications
- Multiple file-types

### Threat Protection at Scale

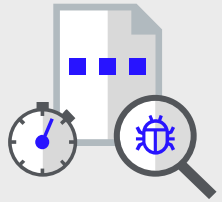
- Multi-stage analysis
- Utilizes most up to date threat intelligence
- Thousands of  simultaneous executions


Trellix

# IVX Multi-stage Inspection Process

## More than just a sandbox

### Find known bad

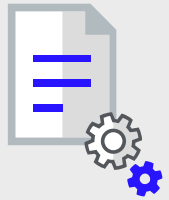


Static Analysis

Lower intensity analytical methods: signatures, reputation, and emulations

Performs high speed analysis at scale

### Find unknown bad



Dynamic Analysis

File executes in a safe and instrumented environment.

Observe file execution and look for malicious behavior.

### Assess malware family similarity


Code Analysis

Remove obfuscation to expose original executable code.

Analyze attributes and instruction sets to identify characteristics similar to known bad behaviors

### Reveal suspicious patterns

Statistical Analysis

Analyze behavioral patterns to identify maliciousness.

Uncover patterns in code to identify emerging threats.

### Verdict


* Remediation actions configurable by integration

Trellix

# Expanded Across Your Organization


Data Shared in Collaboration Apps

Uploads to Enterprise Apps

Files in Enterprise Storage Apps

Files Coming Through Email

Files in Cloud Storage Apps

Suspicious Files from Security Sensors

Suspicious Files from Users

Trellix

# IVX – Specifications

| Product Name | Model | Disk Space | Deployment Type | Throughput | Generation |
|---|---|---|---|---|---|
| Trellix IVX | VX5600 | 4TB | Hardware | Up to **15,840** submissions per day | 6th Gen |
| Trellix IVX | VX12600 | 4TB | Hardware | Up to **120,960** submissions per day | 6th Gen |
| Trellix IVX | VX Bare-Metal | 3.6TB | Cloud – AWS c5.metal | Up to **150,000** submissions per day | 6th Gen |
| Trellix IVX | IVX-VM300 | 1TB | VMWare ESXi | Up to **4,320** submissions per day | 6th Gen |

Trellix

# FX and AX - Hardware Specifications

| Product Name | Model | Disk Space | Deployment Type | Throughput | Generation |
|---|---|---|---|---|---|
| Trellix File Protect | FX2500V | 512GB | Virtual – VMware ESXi | Upto 40,000 files per day | 5th Gen |
| Trellix File Protect | FX2500V | 512GB | Cloud – AWS m5.xlarge | Upto 40,000 files per day | 5th Gen |
| Trellix File Protect | FX2500V | 2TB | Cloud – Azure | Upto 40,000 files per day | 5th Gen |
| Trellix File Protect | FX6500* | 2TB | Hardware | Upto 70,000 files per day | 5th Gen |
| Trellix File Protect | FX6600 | 4TB | Hardware | Upto 87,000 files per day | 6th Gen |
| Trellix Malware Analysis | AX5550* | 4 TB | Hardware | Upto 8,200 analyses per day | 5th Gen |
| Trellix Malware Analysis | AX5600 | 4 TB | Hardware | Upto 10,000 analyses per day | 6th Gen |

Trellix

Trellix

# Key Use-cases

# Use cases

## Practical use cases for on-premise and cloud

### Trellix IVX on-premise

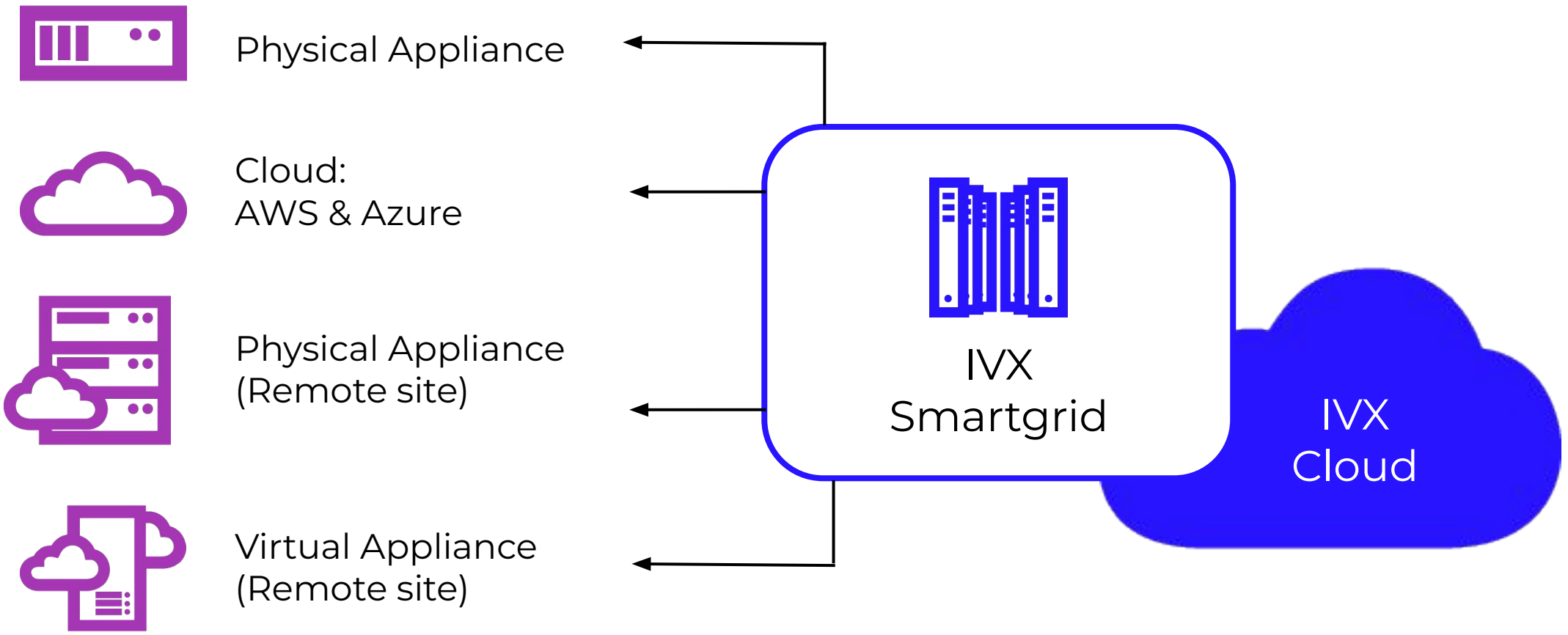
- Inline Network Traffic Inspection
- Internal File Share Protection
- Deep Malware Investigation/Forensics
- Integration with On-Premises Security Stack
- High-Volume or Sensitive Analysis

### Trellix IVX Cloud

- Securing Cloud Collaboration Platforms
- Cloud Storage Malware Scanning
- API-Driven Application Security
- Augmenting Cloud Security Gateways
- Scalable Incident Response and Enrichment

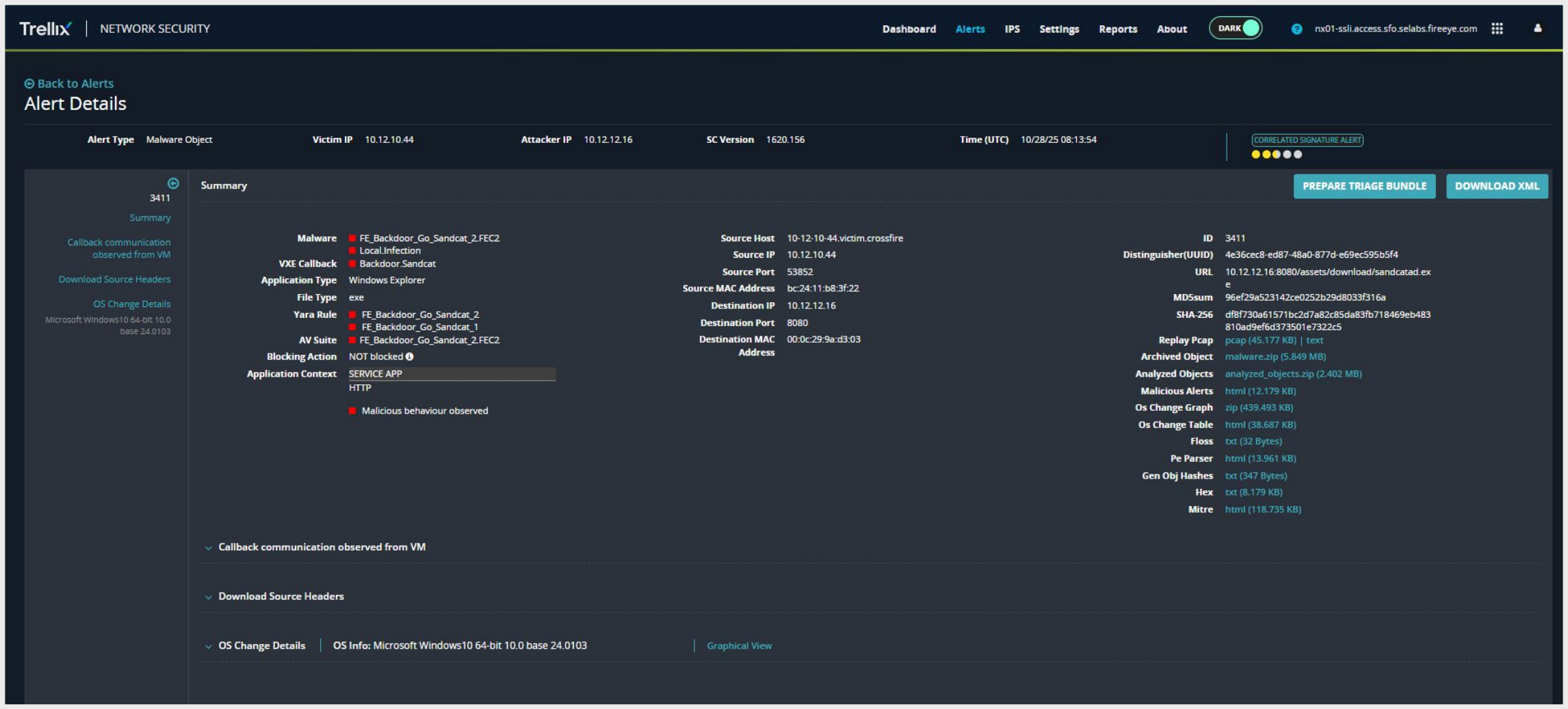
# Inline Network Traffic Inspection

## Integrated and Distributed Network Security



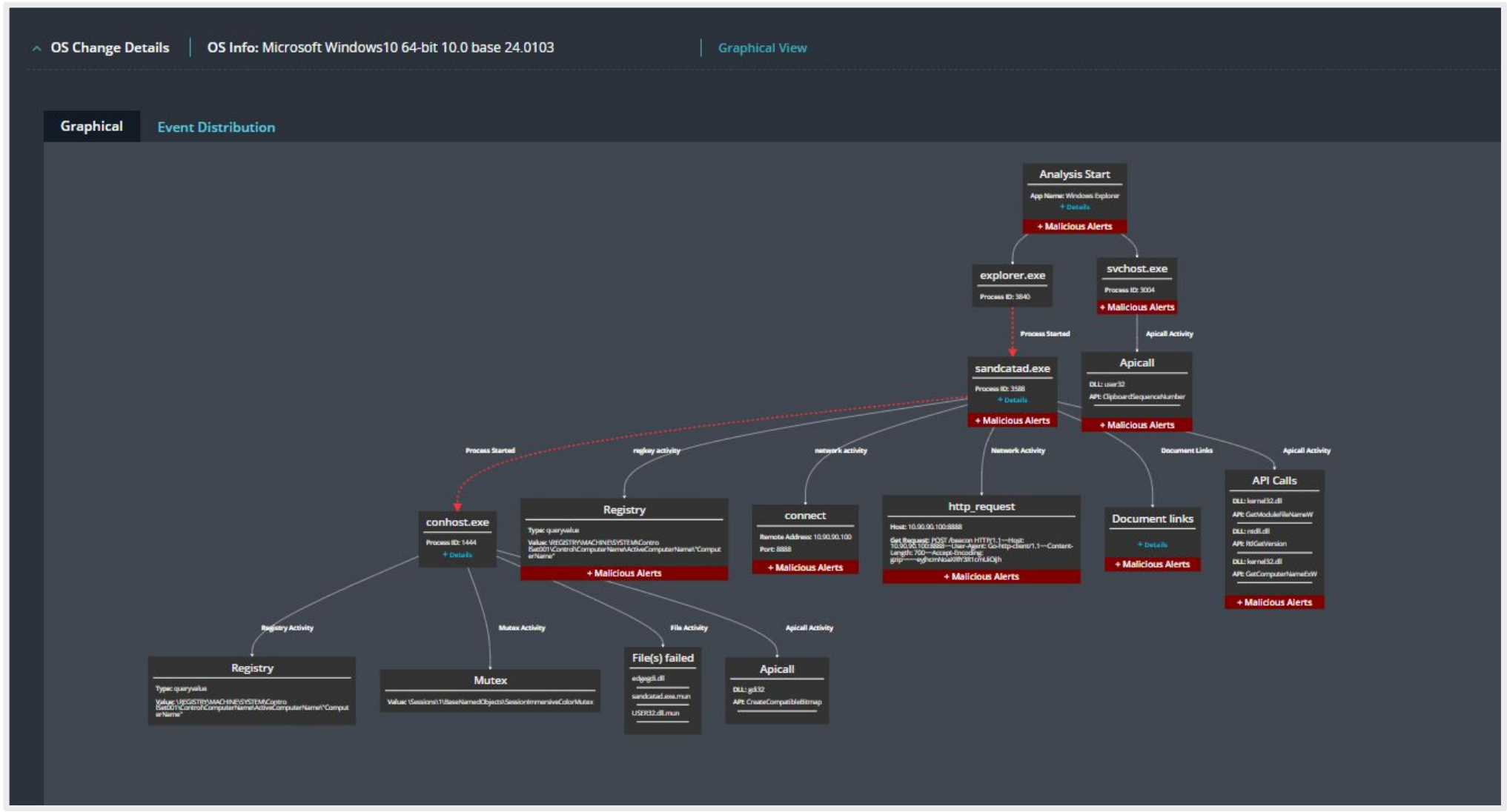
# Deep Malware Investigation/Forensics

## Trellix NX alert use case



# Deep Malware Investigation/Forensics

## Trellix NX alert use case



# Integration with On-Premises Security Stack

## Trellix ePo and TIE

Real-time integration with Trellix Intelligent Virtual Execution (IVX), Intelligent Virtual Execution Cloud (IVX Cloud) to provide detailed assessment and data on malware classification.
These integration allows you to respond to threats and share the information throughout your environment.

## Trellix IPS - Intrusion Prevention System

Trellix IPS offers integration capability with Trellix Intelligent Virtual Execution - Server and Trellix Intelligent Virtual Execution - Cloud which utilize IVX engine's technology to perform malware analysis.

## Skyhigh Secure Web Gateway

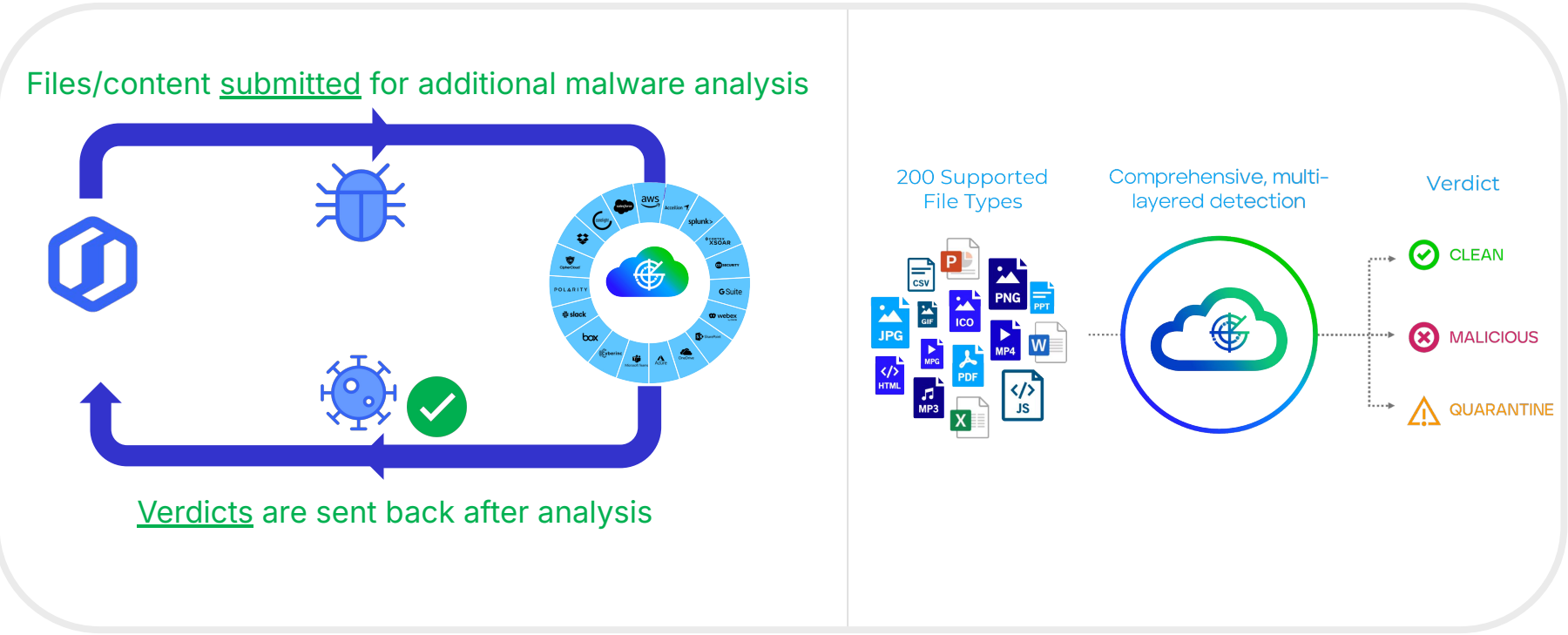
Skyhigh supports integration with Trellix Virtual Execution (VX). For further details please visit Skyhigh website.

# Augmenting Cloud Security Gateways

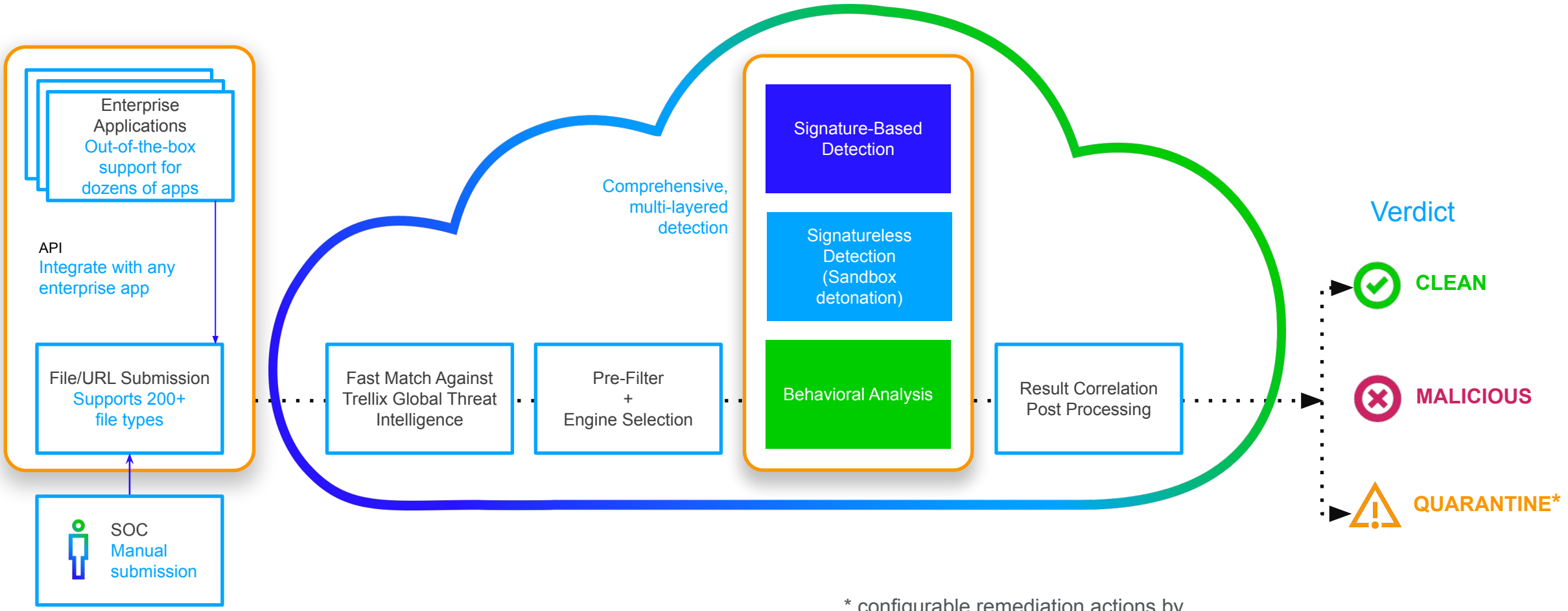
## Skyhigh Security + Trellix provide comprehensive  Anti Malware protection

Skyhigh SWG can easily integrate with Trellix IVX appliances and and IVX cloud services to protect against Zero-Day and Advanced Persistent Threats (APT)

Seamless integration of SWG On-Prem appliances with IVX appliances like legacy ATD and SWG for Cloud with IVX Cloud



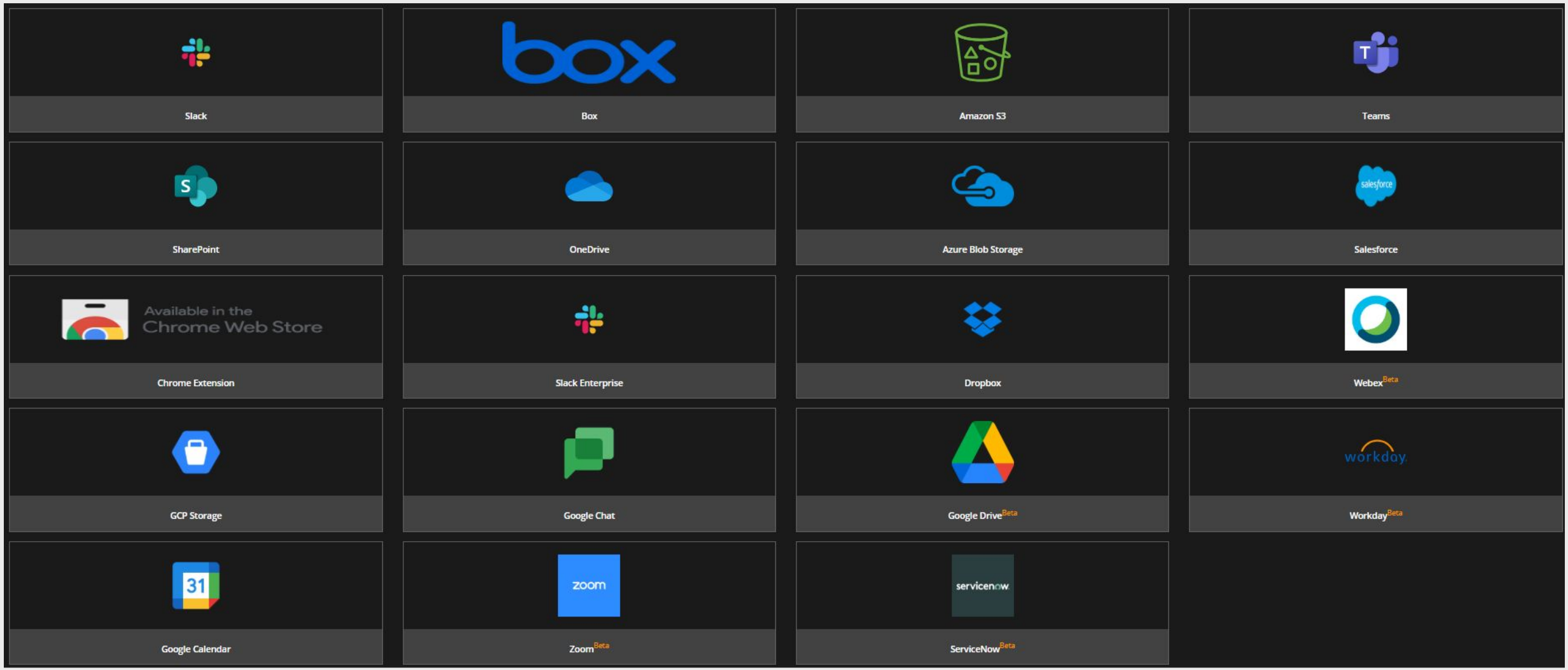
# Trellix IVX Cloud




* configurable remediation actions by integrations where applicable

Trellix

# Securing Cloud Collaboration Platforms

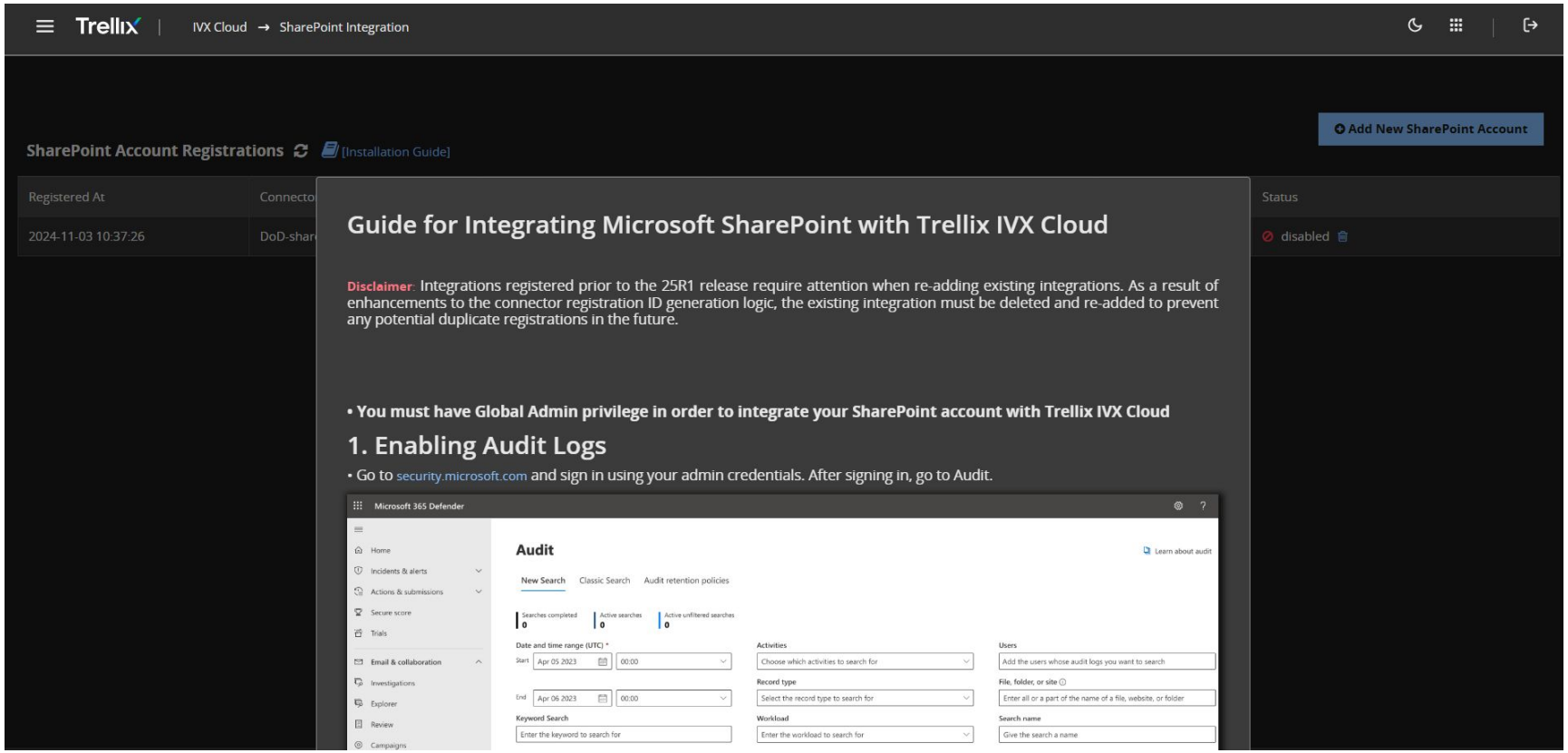


# Securing Cloud Collaboration Platforms

## Integration guidelines

Click on a third-party tool, then click Installation Guide.

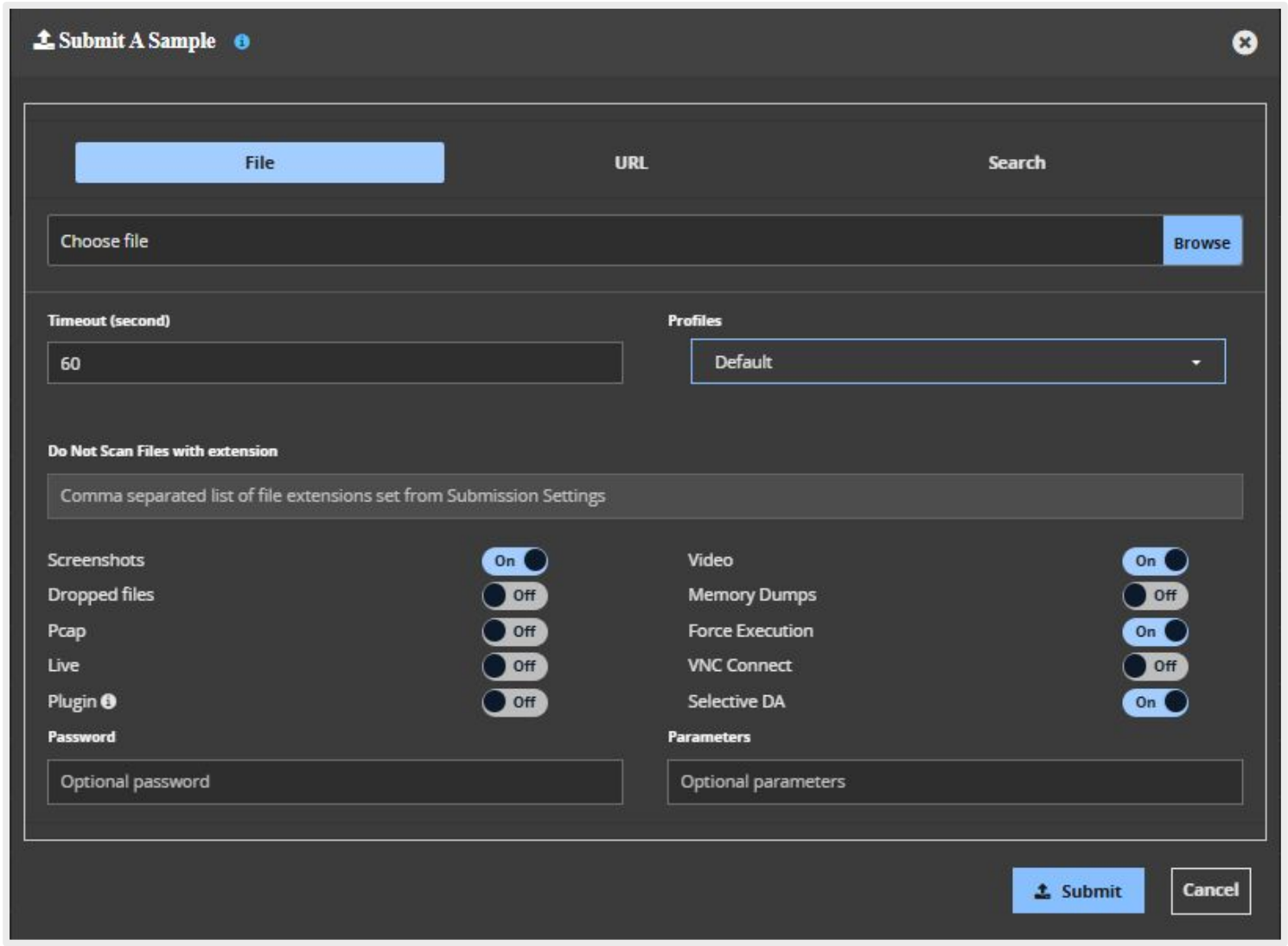
Follow the instructions to set up the integration.



# Scalable Incident Response and Enrichment

## Manual Submission

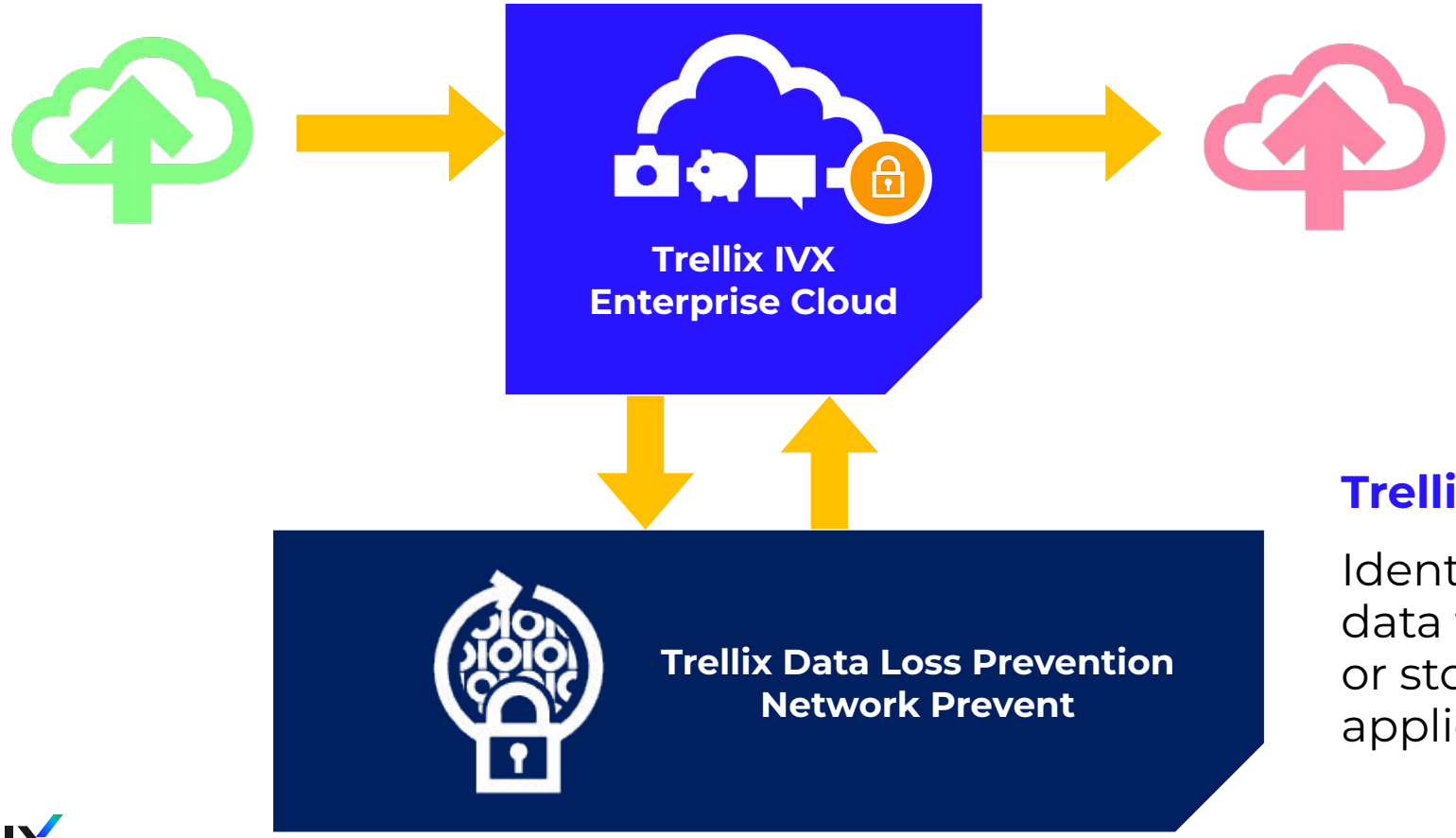
The Submissions page allows you to submit files or URLs manually to IVX Cloud for analysis



# Outbound Data Loss Prevention: Cloud Apps

## Trellix IVX Enterprise Cloud

Monitors and controls data transfers to cloud applications




**Stops sensitive data exfiltration before breaches occur**

## Trellix DLP Network Prevent

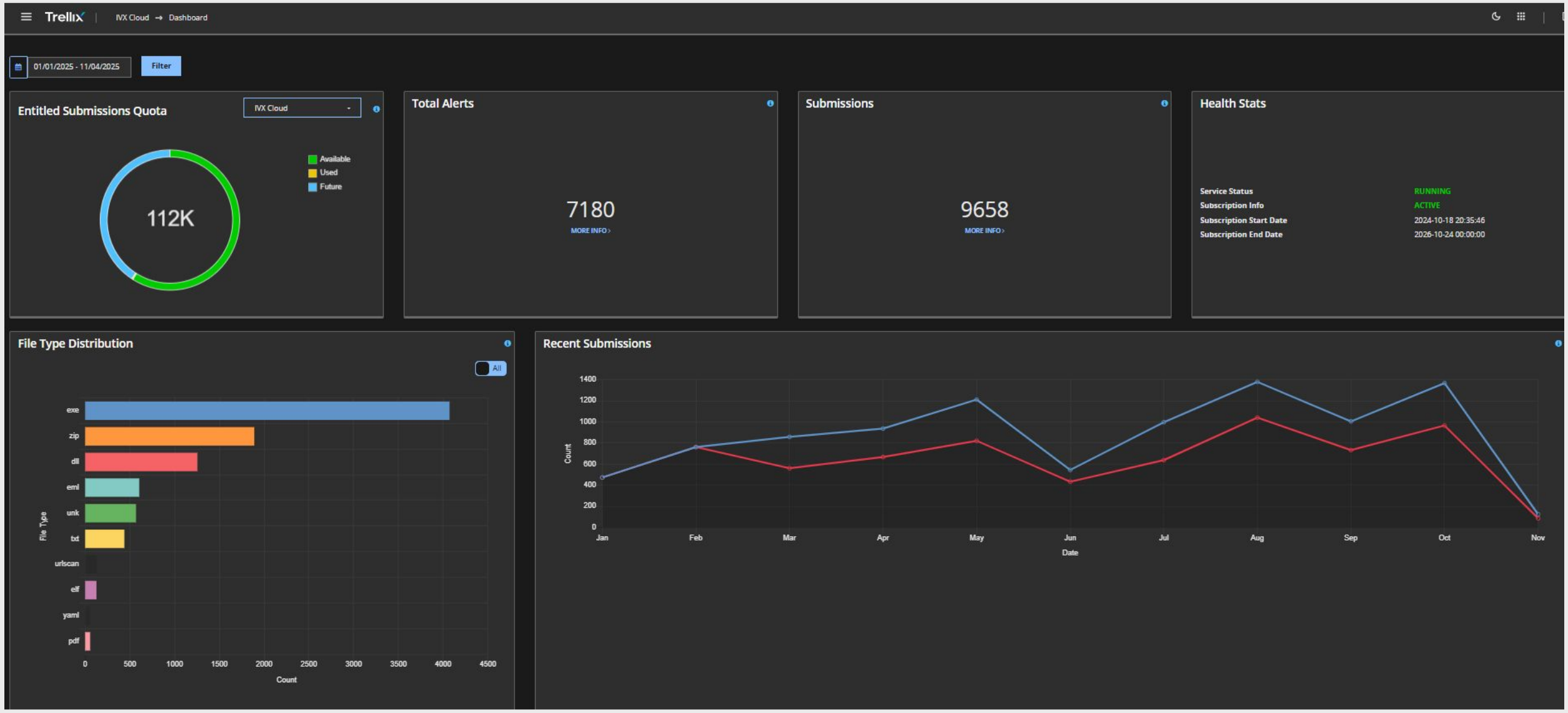
Identifies and blocks sensitive data from being transferred or stored in cloud applications

Trellix

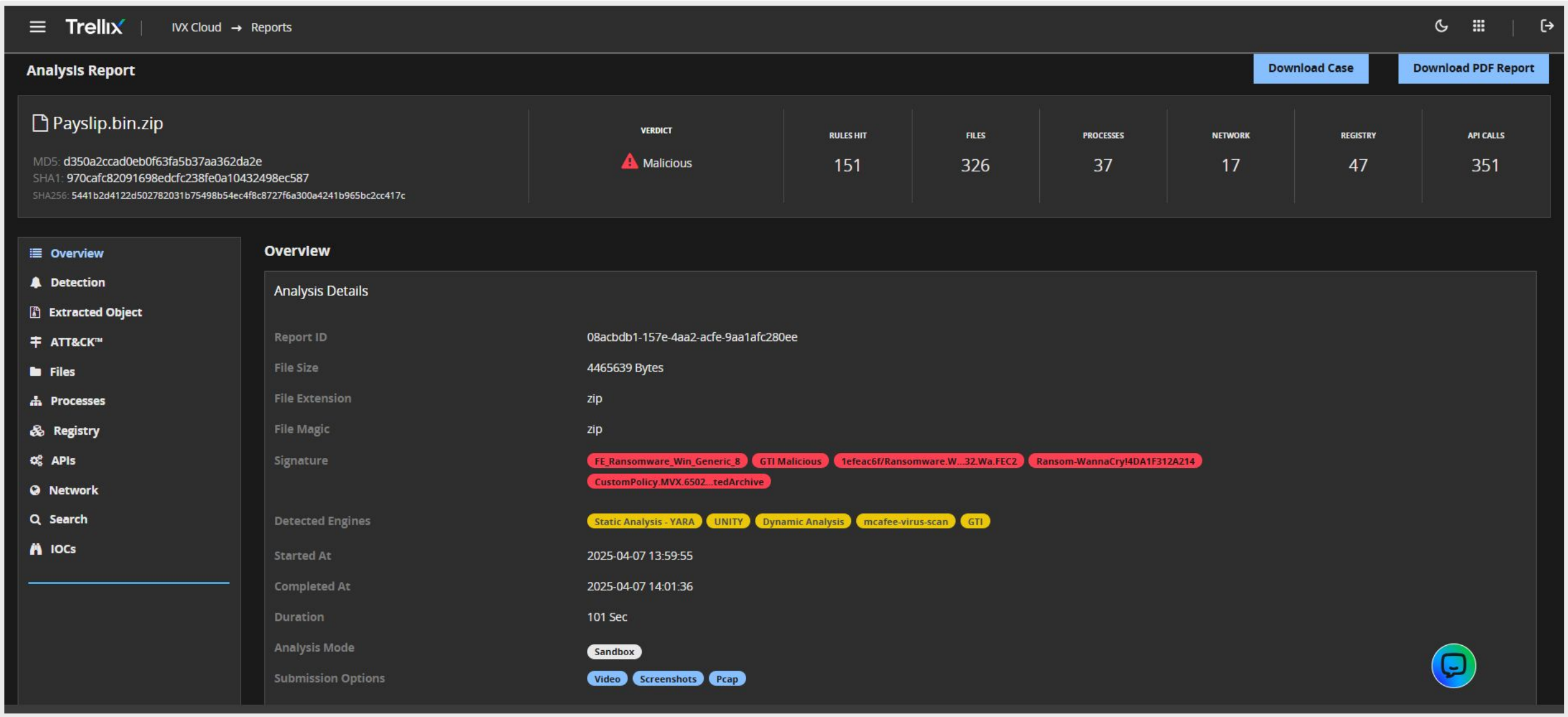

# DEMO

Trellix IVX

Trellix


Trellix
IVX Cloud → Dashboard
01/01/2025 - 11/04/2025
Filter
Entitled Submissions Quota
IVX Cloud
112K
Available
Used
Future
Total Alerts
7180
MORE INFO
Submissions
9658
MORE INFO
Health Stats
Service Status
RUNNING
Subscription Info
ACTIVE
Subscription Start Date
2024-10-18 20:35:46
Subscription End Date
2026-10-24 00:00:00
File Type Distribution
All
exe
zip
dll
eml
unk
txt
urlscan
elf
yaml
pdf
File Type
0
500
1000
1500
2000
2500
3000
3500
4000
4500
Count
Recent Submissions
1400
1200
1000
800
600
400
200
0
Count
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Date

Trellix


Trellix
IVX Cloud → Reports
Analysis Report
Download Case
Download PDF Report
Payslip.bin.zip
MD5: d350a2ccad0eb0f63fa5b37aa362da2e
SHA1: 970cafc82091698edcfc238fe0a10432498ec587
SHA256: 5441b2d4122d502782031b75498b54ec4f8c8727f6a300a4241b965bc2cc417c
VERDICT
Malicious
RULES HIT
151
FILES
326
PROCESSES
37
NETWORK
17
REGISTRY
47
API CALLS
351
Overview
Detection
Extracted Object
ATT&CK™
Files
Processes
Registry
APIs
Network
Search
IOCs
Overview
Analysis Details
Report ID
08acbdb1-157e-4aa2-acfe-9aa1afc280ee
File Size
4465639 Bytes
File Extension
zip
File Magic
zip
Signature
FE_Ransomware_Win_Generic_8
GTI Malicious
1efeac6f/Ransomware.W...32.Wa.FEC2
Ransom-WannaCry!4DA1F312A214
CustomPolicy.MVX.6502...tedArchive
Detected Engines
Static Analysis - YARA
UNITY
Dynamic Analysis
mcafee-virus-scan
GTI
Started At
2025-04-07 13:59:55
Completed At
2025-04-07 14:01:36
Duration
101 Sec
Analysis Mode
Sandbox
Submission Options
Video
Screenshots
Pcap

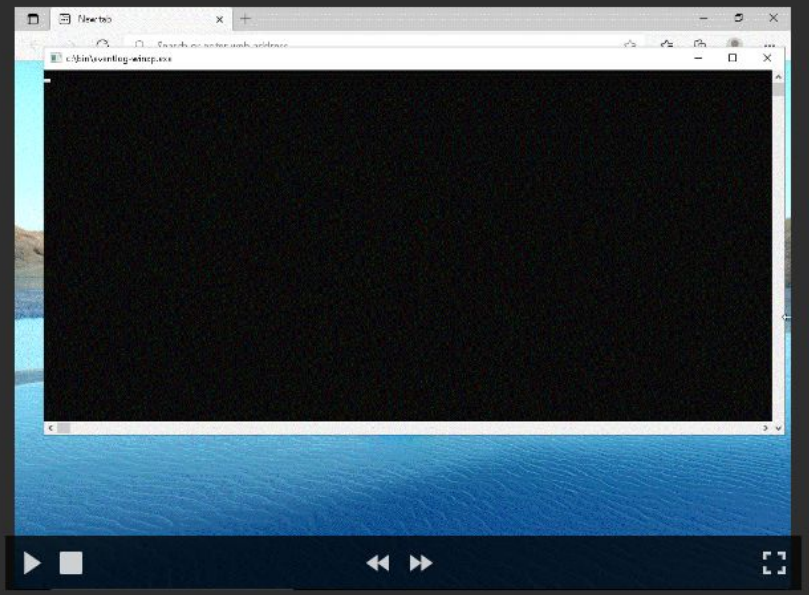
Trellix | IVX Cloud → Reports

## Connector Information

| | |
|---|---|
| Connector Registration ID | DoD-box-82de70c4a397 |
| File Owner | IVX Demo |
| Email | ivxclouddemo@trellix.com |
| File Path | All Files > Test-Malicious > Payslip.bin.zip |

## Screen Activity

**Payslip.bin.zip** wannacry.bin



Trellix

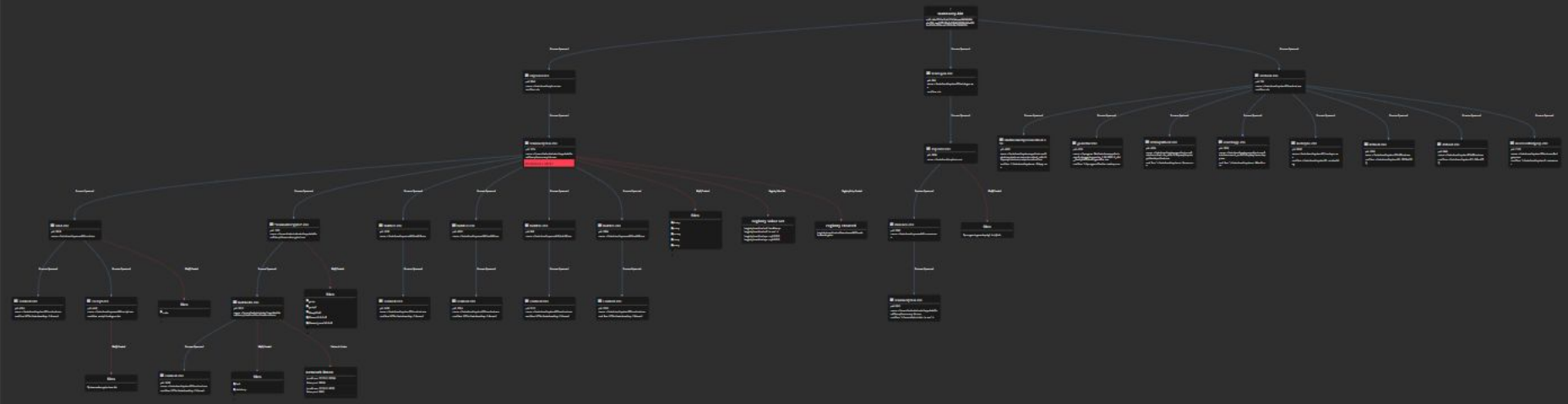
## Process Graph

**wannacry.bin**

**Win10x64 WinXP**

File Name wannacry.bin

MD5 4da1f312a214c07143abeeafb695d904



Trellix

# Licensing

New Bundles, SKUs, Example BOM,
No Pricing Discussion!

# Trellix IVX Offerings - Cloud

| SKU | Capabilities |
|---|---|
| **IVX** | IVX Enterprise Cloud - PER USER:<br><br>Up to twenty (20) submissions per User per month of the Product Term, aggregated across all of Customer's Users |
| **IVX-BP** | IVX Enterprise Cloud - Banded Submission Pack |
| **CDR-BP*** | Content Disarm and Reconstruction - Add On |

***CDR-BP Scheduled for December 2025 Release**

Trellix

# Trellix IVX Offerings - Server

| SKU | Capabilities |
|---|---|
| **5600IVX-T** | 5600 IVX Enterprise Appliance |
| **5600IVX-S-T** | 5600 IVX Enterprise SW and DTI - Subscription(T) |
| **12600IVX-T** | 12600 IVX Enterprise Appliance(T) |
| **12600IVX-S-T** | 12600 IVX Enterprise SW and DTI - Subscription(T) |
| **IVX-VM300** | Trellix Intelligent Virtual Execution VM 300 - (Available 16 - 32 - 48 - 64 Core) |
| **NFEAX-T** | IVX Investigator Subscription (Formerly AX) |
| **NFAX5600-T** | IVX Investigator 5600 Appliance (Formerly AX) |

# Trellix FX Offerings - Server

| SKU | Capabilities |
|---|---|
| **NWEFX-T** | File Security - Subscription (Per Appliance) |
| **NWFX6600-T** | File Protect 6600 Appliance (Per Appliance) |
| **NWFX-VA-T** | IVX File Share Connector Virtual (Per Appliance instance) |

Trellix

Trellix

# Architecture

Trellix Email Security

# Email Cloud Deployment Options

Scan/Block

1. **Primary SEG with Full Hygiene.**


Scan/Block

2. **Full Hygiene inline, second hop, behind a 3rd party SEG.**


Scan/Drop

3. **Full Hygiene in BCC mode and sends alerts.**


4. **MS365/Google Workspace Native API Integration (ICES)**

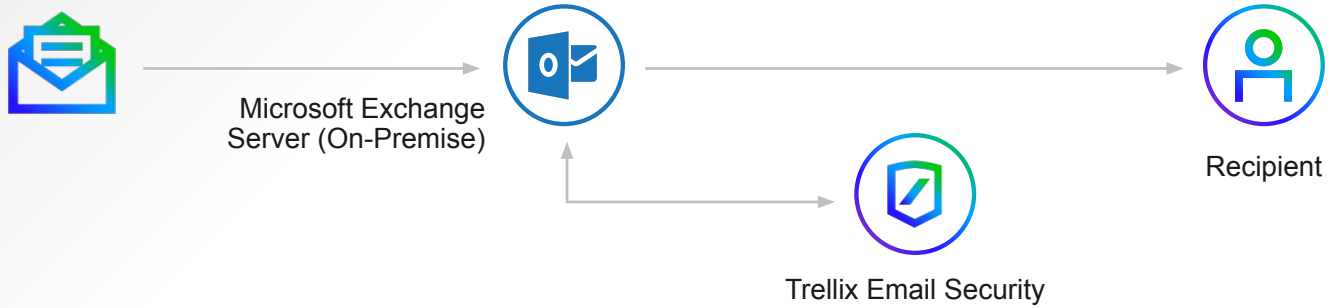
Google Workspace  Microsoft 365

Trellix

# Email Server Deployment Options

1. **On prem Inline mode**


2. **On prem in BCC/Monitor modes**

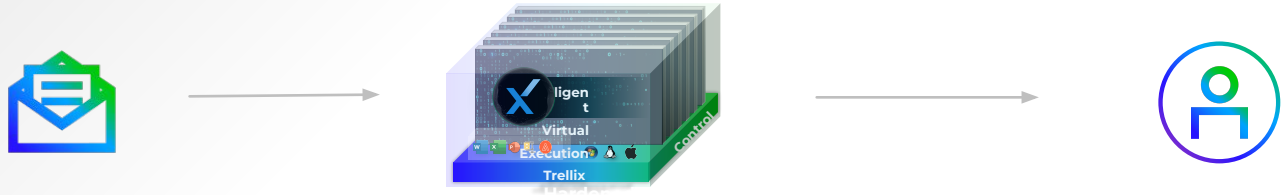



3. **Appliance deployments (Form factors)**


Trellix

# Email Security with IVX Deployment Options

1. **Included with Email Security Cloud**




2. **On-premises In-Line Server**

Collaboration & Enterprise Applications


Collaboration & Enterprise Applications

3. **Cloud and Virtual In-Line**

Collaboration & Enterprise Applications

aws
AWS Bare Metalc5.meta
NUTANIX
vmware


Collaboration & Enterprise Applications

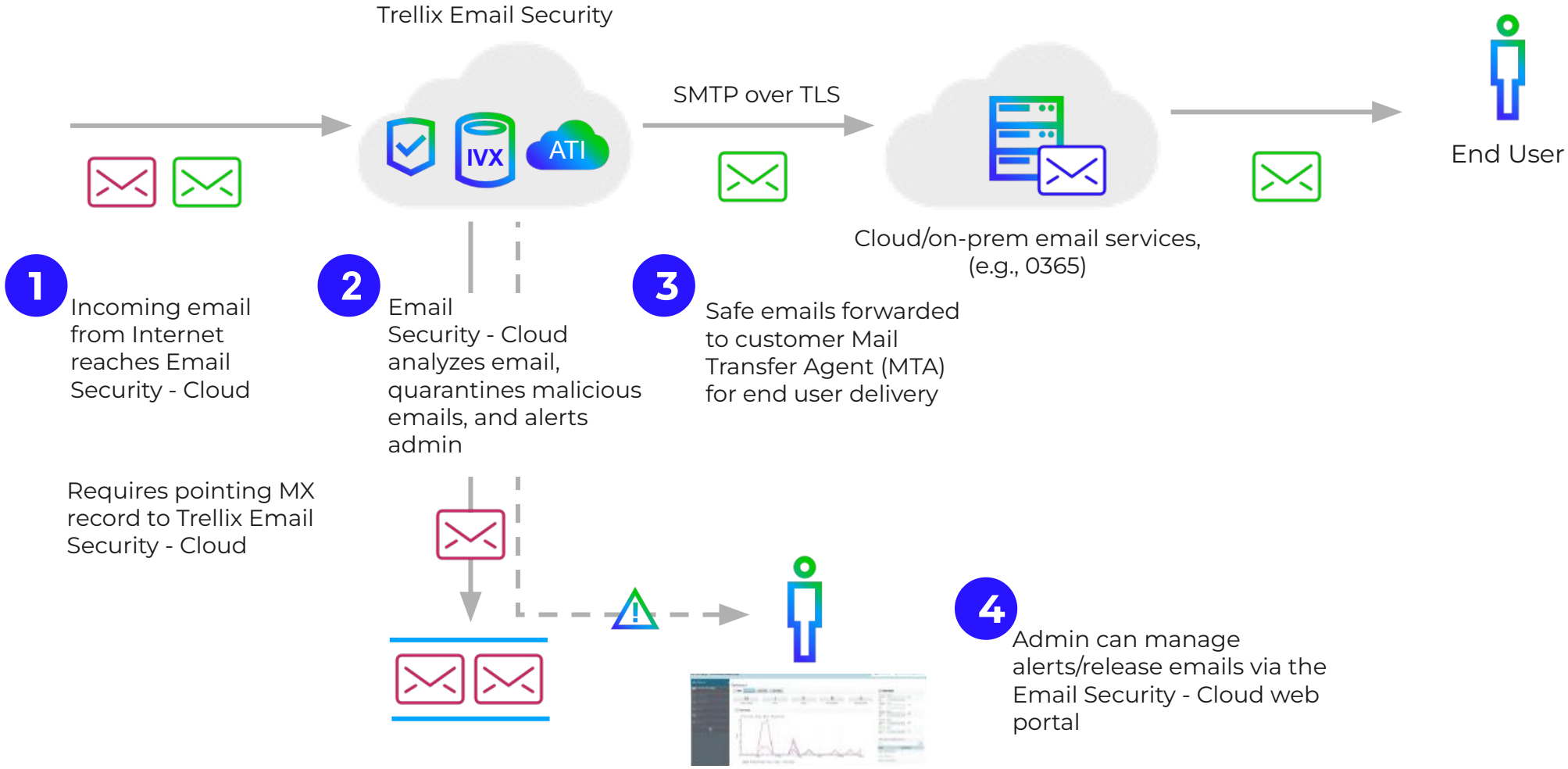
Trellix

Trellix

# Trellix Email Security Cloud

# Email Security - Cloud Inline Deployment

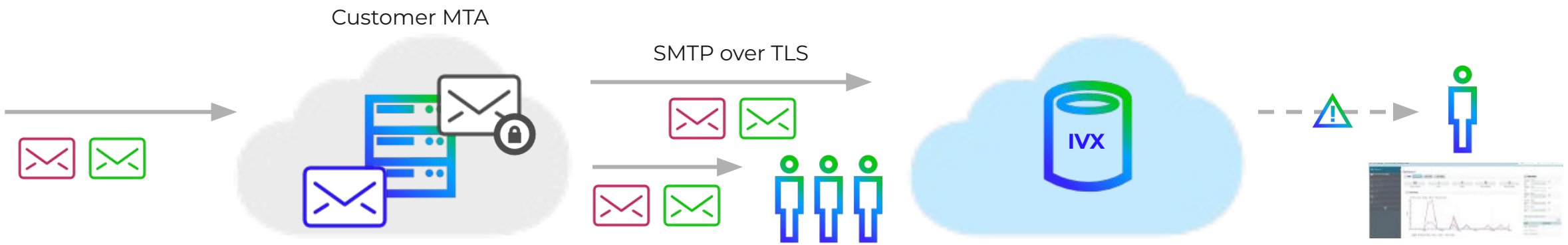
## Inline Blocking Deployment




Trellix

# Email Security - Cloud BCC Deployment

## BCC (Monitor) Deployment

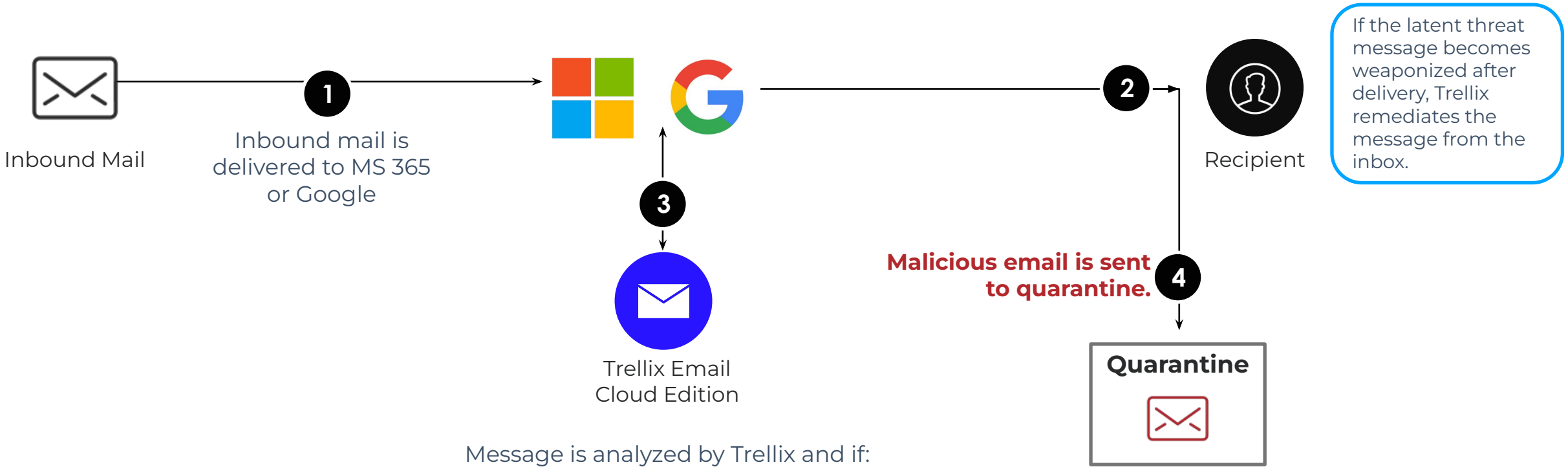



1. Incoming email from Internet reaches customer MTA with antivirus/antispam(AV/AS)
2. Customer MTA delivers email to end users
3. Customer MTA configured with **BCC transport rule**, also forwards a copy of email to Email Security - Cloud for analysis
4. Admin receives alerts through email and can manage alerts via the Email Security - Cloud web portal

Trellix

# Email Security - Cloud API Deployment

## Native API Integration: Microsoft 365 or Google Workspace




Trellix

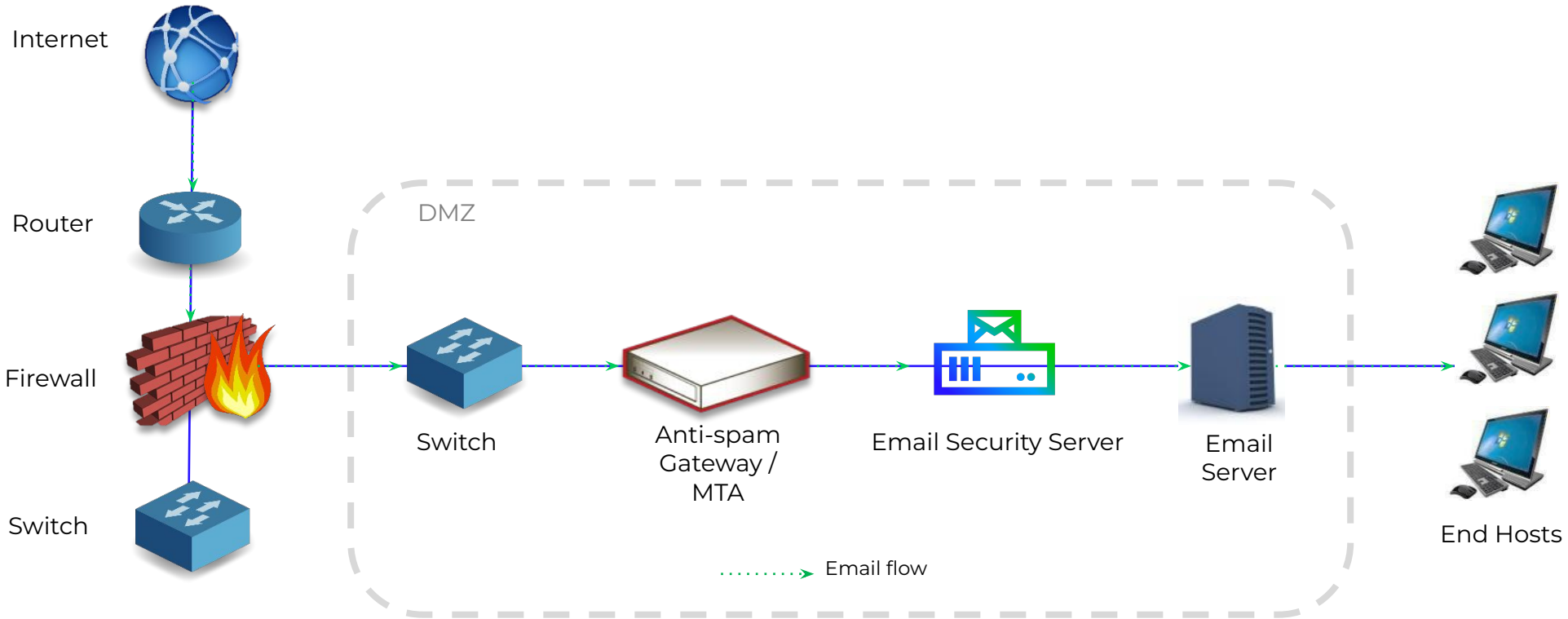
Trellix

# Trellix Email Security Server

# Email Security Server - Deployment Options

## Inline MTA

- Email Security Server sits in the flow of email traffic
- Detection and protection of advanced attacks
- Malicious emails automatically quarantined
- Malicious emails never reach end user

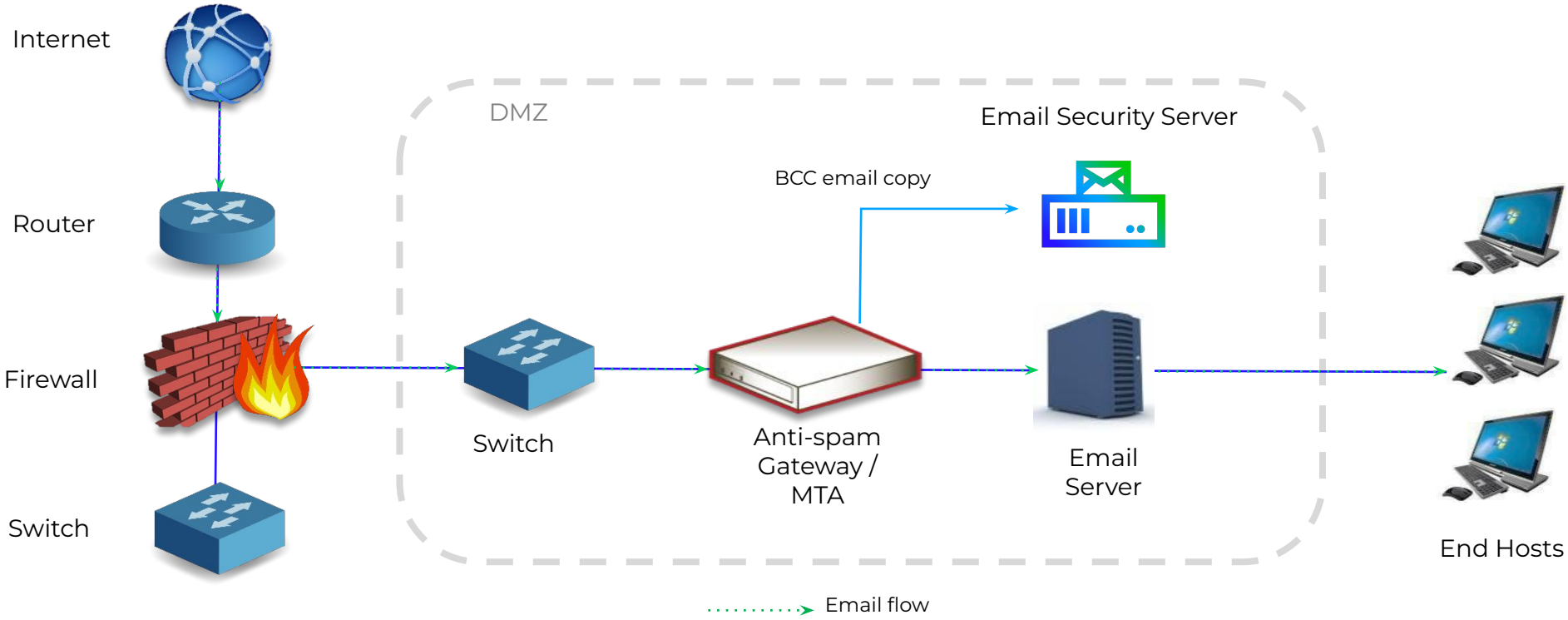



Trellix

# Email Security Server - Deployment Options

## Out-of-Band / BCC Mode

- Email Security Server receives a copy of emails from MTA
- Detection of advanced attacks
- Admins notified of malicious emails

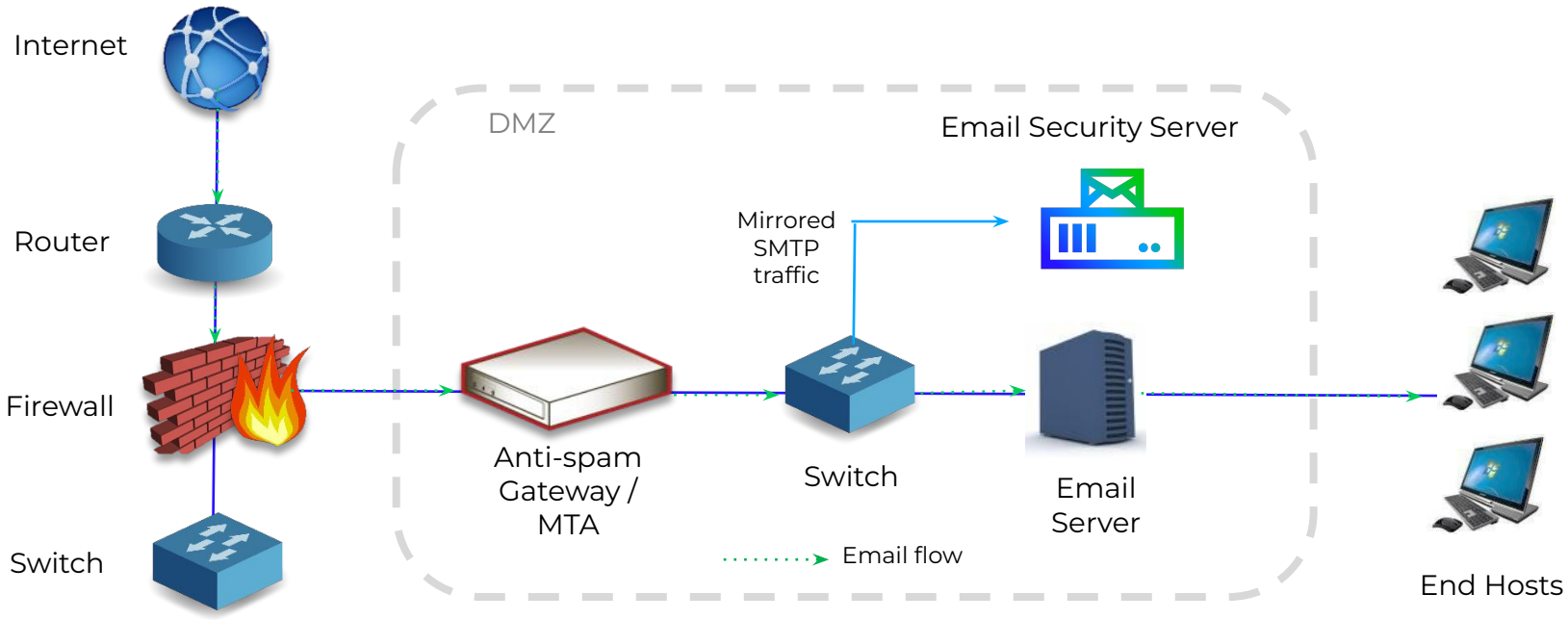



Trellix

# Email Security Server - Deployment Options

## SPAN Mode

- Email Security Server reads SMTP traffic mirrored from SPAN port of switch to assemble and analyze emails
- Detection of advanced attacks
- Admins notified of malicious emails




Trellix

Trellix

# Key Use-cases

# Accelerate Analysis & Remediation

## Remediate at Scale

- Intelligent detection automatically identifies and groups campaigns for one click remediation
- Take action on up to 10,000 emails at once
- Manage policies and inheritances for all domains in a single table

## Quickly Gain Actionable Intelligence

- Automated triage and threat summaries with agentic AI
- Learn what to do next based on best practices
- Interact with natural language for deeper insight and Q&A

## Jump Start Investigations Across the Platform

- Stream email and collaboration metadata to Trellix Helix Connect to accelerate investigation and response workflows

Trellix

# Improve Response & Organizational Resilience

Reduce the time it takes to detect and take action against threats and transform your workforce into your strongest security asset with intuitive data security and timely, relevant phishing simulations

- Accelerate Analysis & Remediation
- Prevent Exfiltration and Leaks with Data Security
- Train a More Alert Workforce

# Stop Phishing From Getting Through

## Sender Relationship, Domain, and Impersonation

Check reputations, sender history, domain, and sender authenticity, examining content for impersonation tactics like typosquatting and spoofing

## Context and Sentiment

Combine GenAI, ML, and NLP to detect subtle cues of malicious intent

## Imagery

Discern the slightest pixel variations, accurately spot modified graphics, and inspect embedded URLs with intelligent virtual execution

## QR Codes and Embedded URLs

Open and inspect QR paths and URLs, including URL rewrite, click protection, and deep inspection of multi-hop and other methods to thwart obfuscation

## Post-Delivery

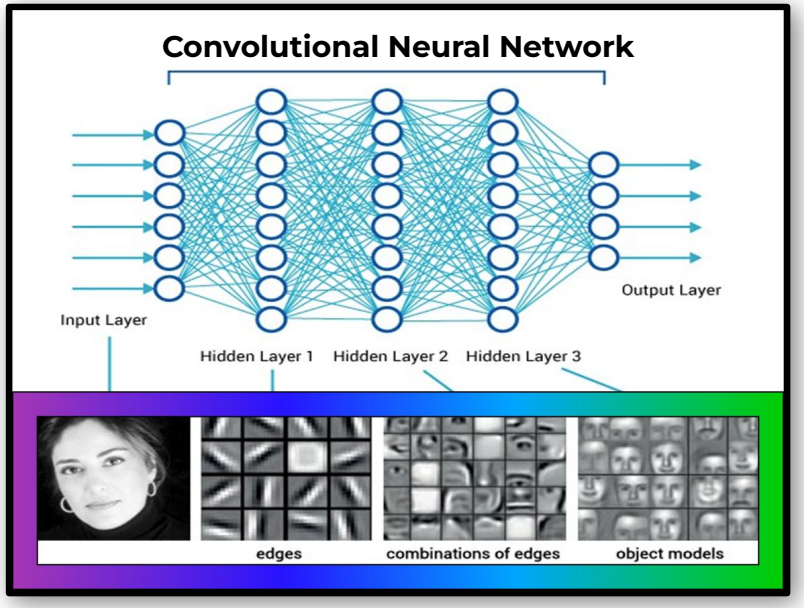
Run an additional scan including multi-hop inspection of URLs to catch post-delivery weaponization

## Deep File Inspection

Deep file inspection and virtual execution across 200 environments at enterprise speed capable of over 2,000+ simultaneous executions

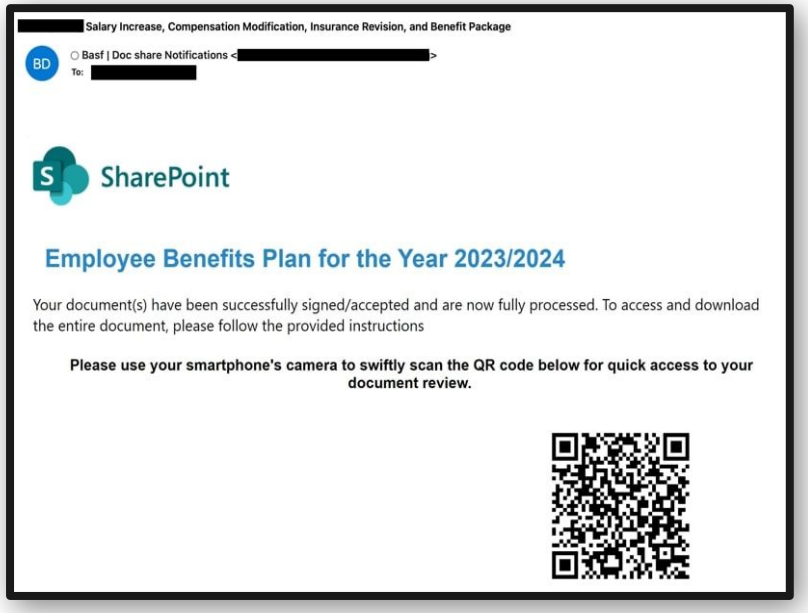
Trellix

# Hidden in Imagery or Behind QR Codes




## Deep, Multi-layer Image Analysis

Convolutional neural networks (CNN) synthesize layers of an image, down to the individual pixel. These are compared with existing brand and web imagery for a highly effective technique to uncover common impersonations techniques involving vendor web sites and login pages.




## Embedded URL Detection

Using computer vision, AI that trains computers to "see" and interpret the visual world, QR codes or other images are identified and their URLs are traced and analyzed for malicious intent.

Instructions embedded in an image are similarly followed, tracing the results to uncover nefarious activity.

Trellix

# BEC & Impersonation Detection

## Relationship Analysis

Analyzes reputations and relationships, tracking sender history to identify anomalous patterns.

- How often do the two parties communicate?
- Across our customers, how often do customers receive mail from the sender?
- What does normal traffic volume look like?

## Domain Analysis

Checks for impersonations

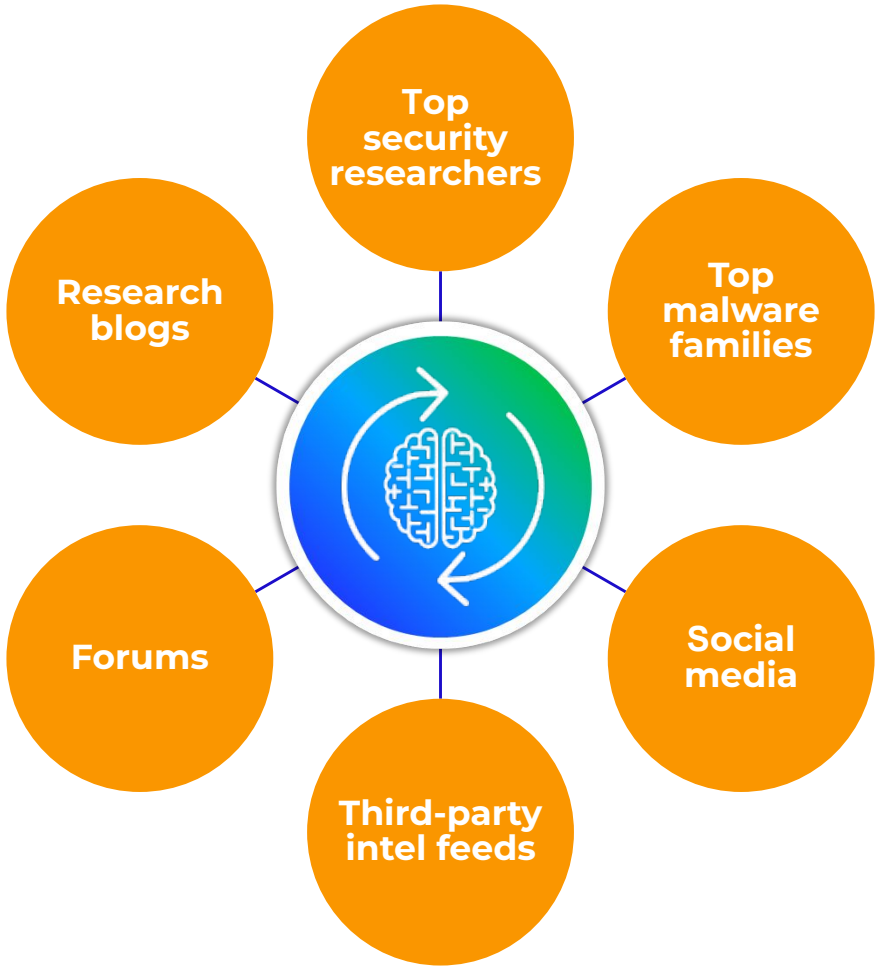
- When was the sender domain created or first observed?
- Typosquatting and/or sender display/username spoofed?

## Context and Sentiment Analysis

Combines a layered approach of GenAI, ML, and NLP to detect subtle cues of malicious intent in the words used when no payload exists

- Tones of urgency or panic
- Attempts to communicate outside corporate systems
- Conversational patterns and much more

# Real-Time URL Understanding




## Pre-Delivery

Checks against Trellix's massive known URL database to identify previously identified malicious URLs

- Process +10M URLs / Day
- Extensive multi-hop analysis plus impersonation detections
- Trellix continually monitors social media and other threat research blogs for the latest insights into attacker techniques and emerging campaigns

## Post-Delivery Weaponization

Thwarts would be attackers hoping to avoid initial checks by activating their malicious sites after an email has entered targets' inbox

- In addition to pre-delivery checks, URL rewrite is applied for click-time detection
- Trellix modifies the URL to point to Trellix's security infrastructure rather than the original page

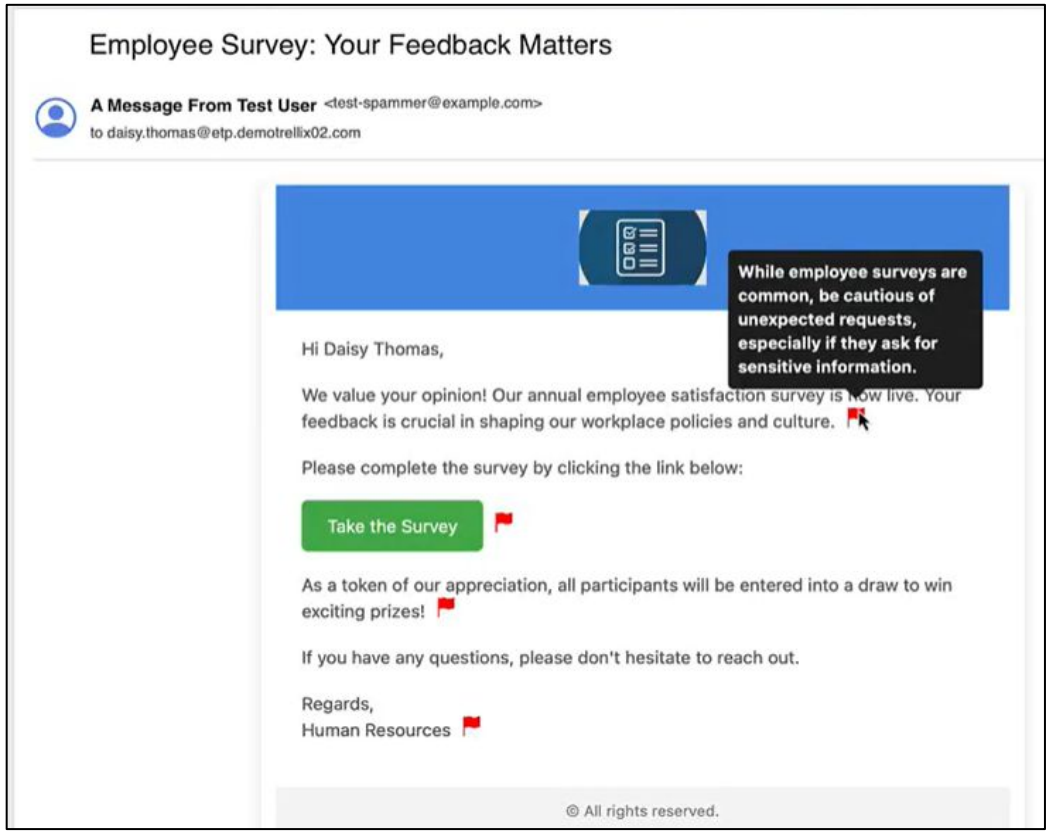
  Safe: User is allowed to proceed to original as intended
  Suspicious: User is sent to a warning page indicating risk
  Malicious: User is sent to a page informing of malicious content and blocked

- Claw-back (M365 & Google): In ICES mode, if an email is later discovered as malicious through other means, Trellix is able to scan user inboxes for similar messages and retract them post-delivery

Trellix

# Train a More Alert Workforce

## Trellix Phishing Simulator *(add on feature to Email Security Cloud)*




### Educate on the Latest Threats

Use GenAI to develop real-world attack simulations based on the latest phishing techniques to help enhance realism and identify areas of potential risk.

### Reinforce Vigilance and Awareness

Employees receive immediate feedback with interactive training and specific guidance to reinforce education.

### Effortless Deployment

Simplify campaign rollouts through automation, AI-powered tools, pre-built templates, and intuitive wizards to enable low-touch campaign creation and deployment.

### Actionable Analytics

Move beyond basic click rate tracking to performance insights. Track repeat offenders, measure training effectiveness, and generate executive-ready reports that demonstrate ROI.

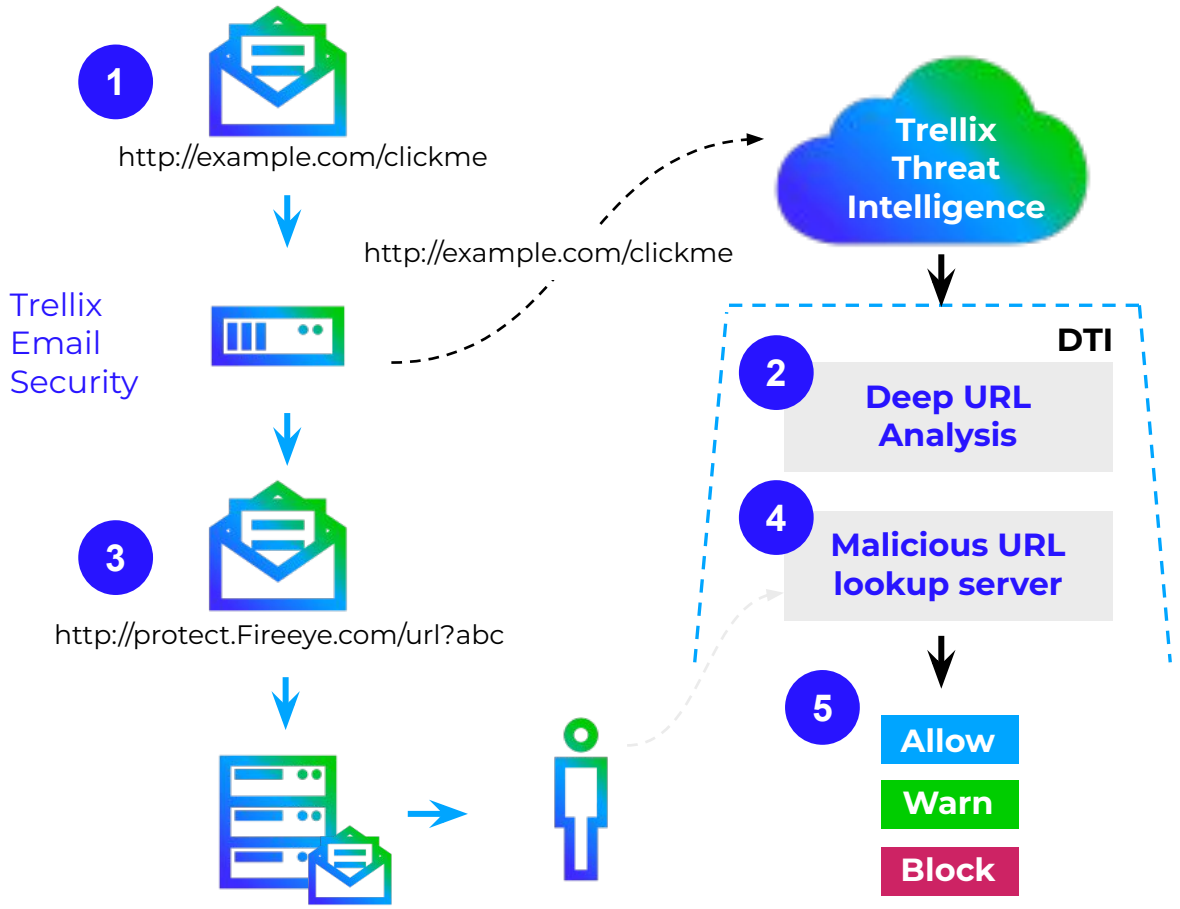
### Address Cyber Insurance Needs

Many cyber insurance policies require phishing simulators or give discounts based on usage.

Trellix

# Advanced URL Defense

## Detection of Spear Phishing Websites (URLs & Content)




1. ETP checks AUD fast path if suspicious URL is known to be malicious
2. Unknown suspicious URLs submitted to AUD Slow Path for real time analysis
3. URL is rewritten and email delivered to prevent delays (inline deployments only)
4. End user redirected to warning page upon clicking suspicious link
5. Based on results of lookup, URL access either allowed, warned or blocked

## Overview

- Detects zero-day, low-volume, highly-targeted phishing attacks
- Analyzes website content for malicious behavior by scanning the whole phishing site (links, content, etc.)

## Benefits

- High-fidelity detection
- Blocking of multi-stage malware and evolving URL based threats
- Low false positive rate
- Simplified alert prioritization and faster attack prevention

Trellix

# Integrated Investigation and Response

## How We Achieve It

### Clawback emails after delivery

**Receive**
**7:55 am**
email received by inbound mail server

**Detect**
- Spam
- Impersonation
- Known malware
- Malicious URL

**Analyzed**

**7:56 am**
email is analyzed as benign

**7:56 am**
email is clean and delivered to recipient's inbox

**Email is weaponized after delivery to user's inbox!**


**8:15 am**
URL is weaponized post email delivery

Retroactive analysis determines the file is malicious

**Alert**
Admin receives an alert of malicious message after delivery

- Quarantine
- Move
- Delete

**Email Extracted**
using an auto remediate policy and Microsoft 365 and Google Workspace APIs.

Trellix

# Introduction - Phishing Simulator

## Our Understanding

- 80-95% of all social engineering attacks begin with a phish.
- 4,151% increase in malicious emails since the launch of ChatGPT.
- $4.76M is the global average cost of a phishing breach.

## Required Capabilities

- Advanced phishing training with comprehensive strategy.
- Extensive reporting and analytics for actionable insights..
- Simplified security administration, with low-touch creation.

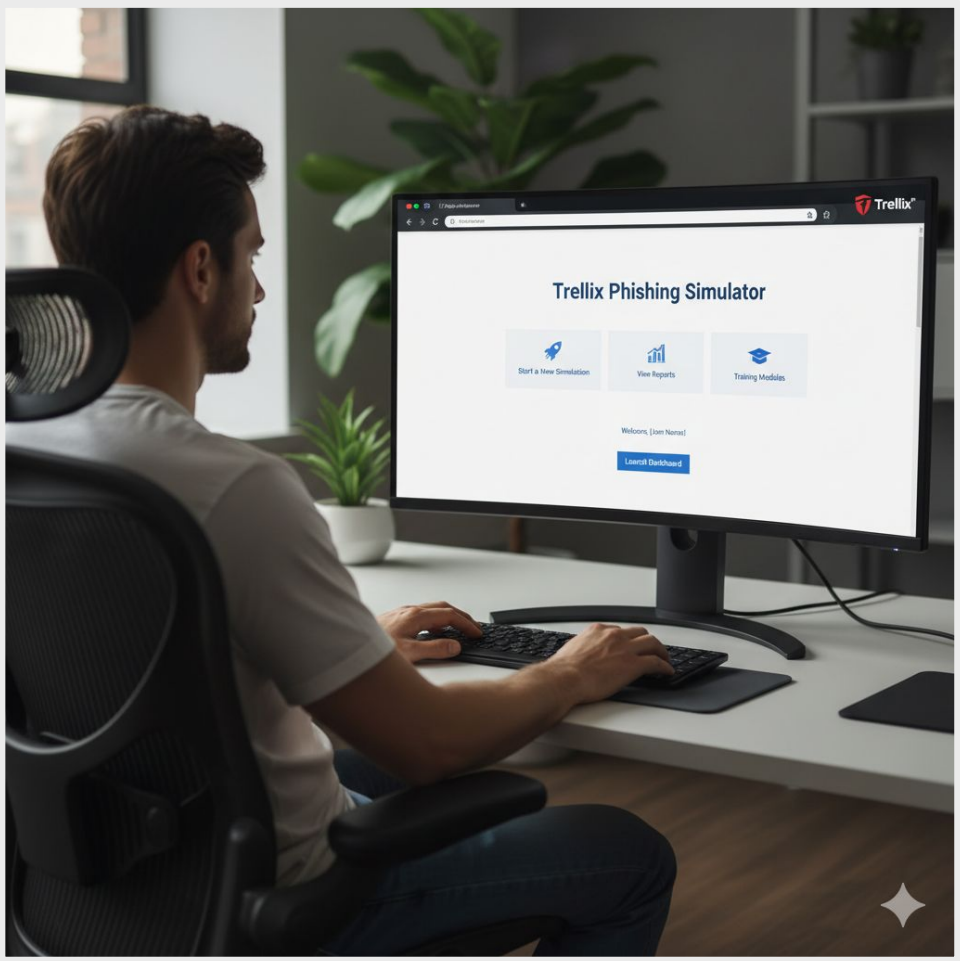
## Business Outcomes

- Strengthened organisation security posture.
- Increase productivity with reduced creation and administrative efforts.
- Reduce security fatigue through cue based training for employees.

Trellix

# Trellix Phishing Simulator

## Promote a More Alert Workforce




**Educate on the Latest Threats**
Use GenAI to develop real-world attack simulations based on the latest phishing techniques to help enhance and identify areas of potential risk.

**Reinforce Vigilance and Awareness**
Employees receive immediate feedback with interactive training and specific guidance to reinforce education.

**Effortless Deployment**
Simplify campaign rollouts through automation, AI-powered tools, pre-built templates, and intuitive wizards to enable low-touch campaign creation and deployment.

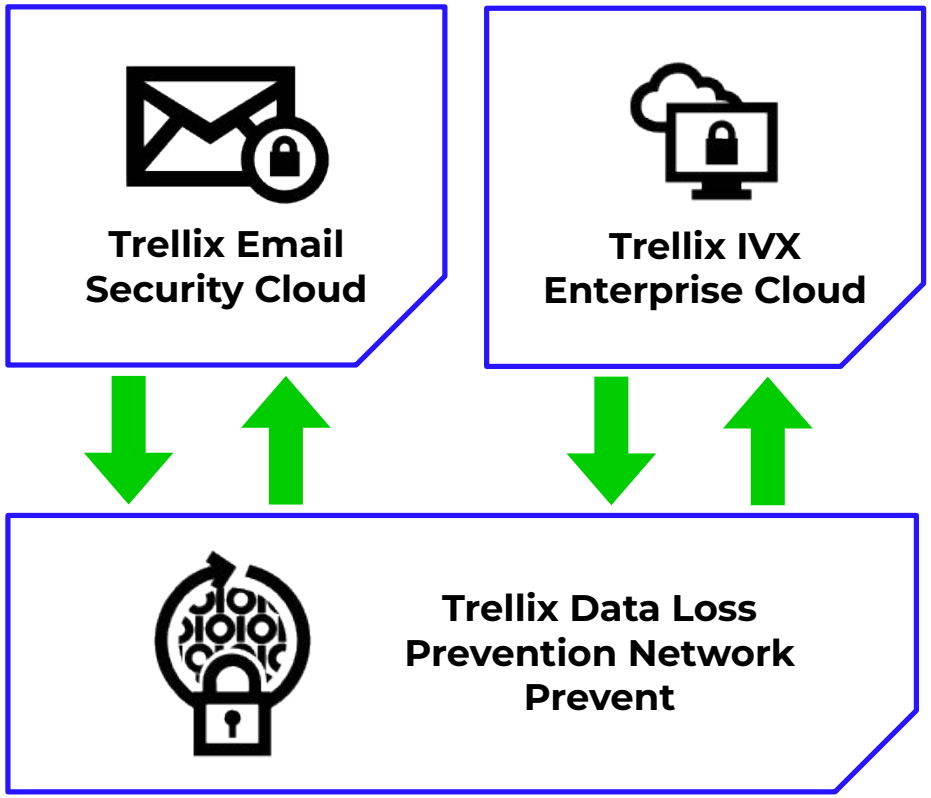
**Actionable Analytics**
Move beyond basic click rate tracking to performance insights. Track repeat offenders, measure training effectiveness, and generate executive-ready reports that demonstrate ROI.

**Address Cyber Insurance Needs**
Many cyber insurance policies require phishing simulators or give discounts based on usage

Trellix

# Prevent Data leaks and Maintain Compliance

## Trellix Data Security




### Protect sensitive business data

Monitor and block data exfiltration by insiders and accidental sharing across your email and collaboration channels.

### Simplify regulatory compliance efforts

Choose from dozens of pre-built policies for all major compliance frameworks to strengthen your compliance posture.

### Gain granular policy control

Leverage the flexibility to easily customize pre-built policies or create new ones using a simple policy builder.

### Simple, reliable deployment and control

API-based integration provides enterprise-grade protection that is easier and more reliable to deploy than complex SMTP routing.

### Accelerate incident investigations

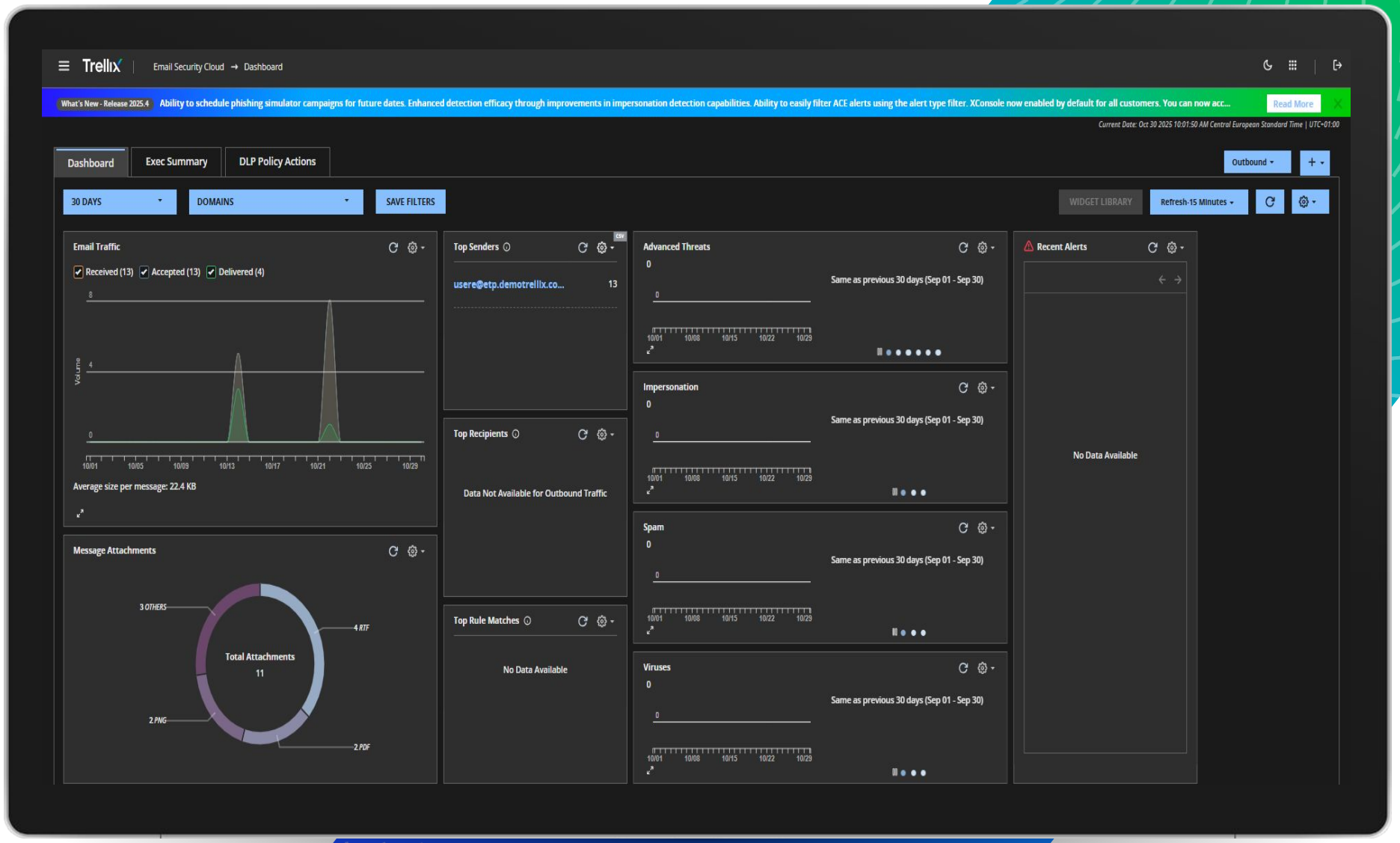
Captured data events provide admin teams with greater visibility and control for forensics directly within the security console.

Trellix

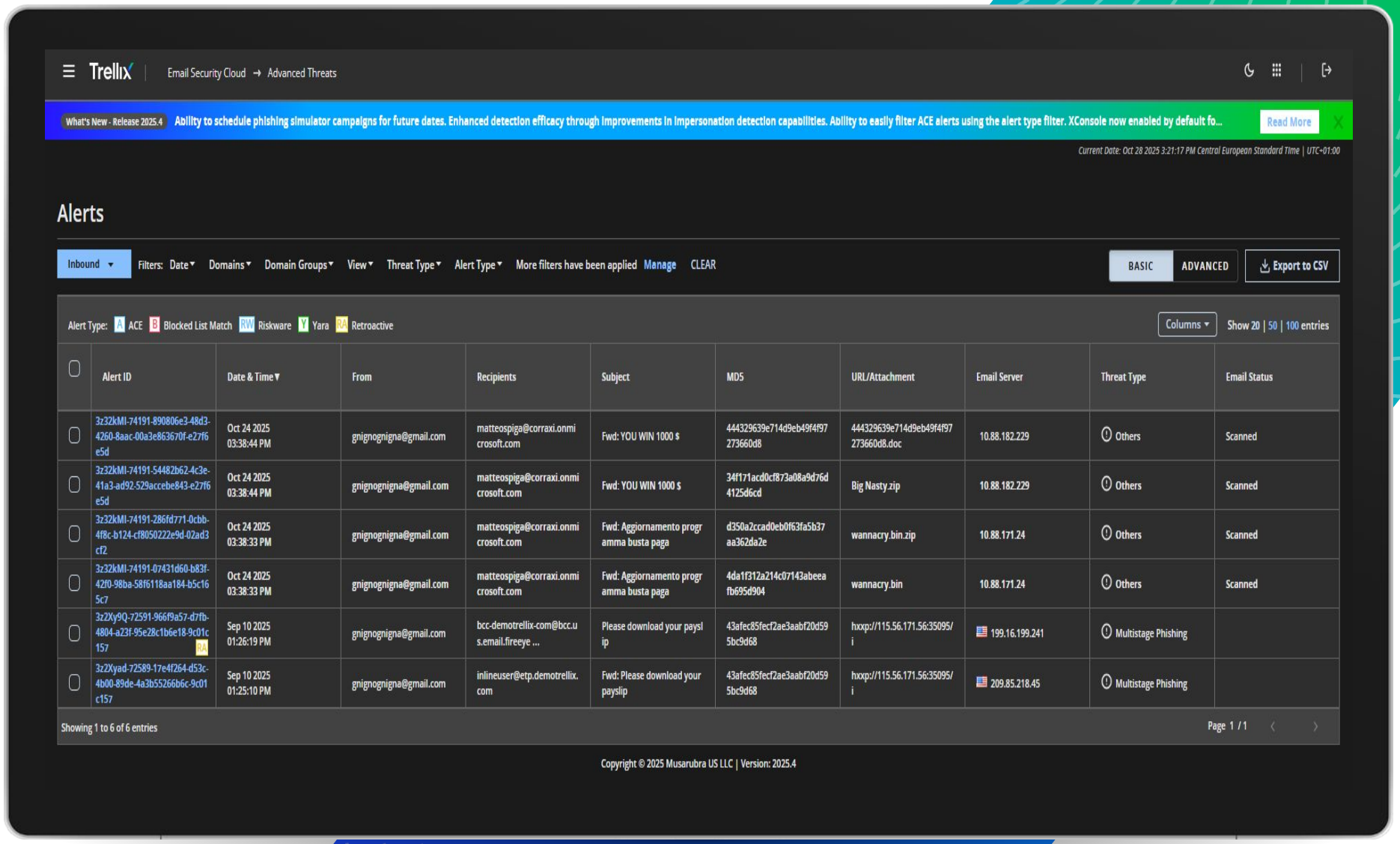

# DEMO

Trellix IVX

Trellix


Trellix
Email Security Cloud → Dashboard
What's New - Release 2025.4
Ability to schedule phishing simulator campaigns for future dates. Enhanced detection efficacy through improvements in impersonation detection capabilities. Ability to easily filter ACE alerts using the alert type filter. XConsole now enabled by default for all customers. You can now acc...
Read More
Current Date: Oct 30 2025 10:01:50 AM Central European Standard Time | UTC+01:00
Dashboard
Exec Summary
DLP Policy Actions
Outbound
30 DAYS
DOMAINS
SAVE FILTERS
WIDGET LIBRARY
Refresh-15 Minutes
Email Traffic
Received (13)
Accepted (13)
Delivered (4)
Volume
Average size per message: 22.4 KB
Top Senders
usere@etp.demotreillx.co...
13
Top Recipients
Data Not Available for Outbound Traffic
Top Rule Matches
No Data Available
Advanced Threats
Same as previous 30 days (Sep 01 - Sep 30)
Impersonation
Same as previous 30 days (Sep 01 - Sep 30)
Spam
Same as previous 30 days (Sep 01 - Sep 30)
Viruses
Same as previous 30 days (Sep 01 - Sep 30)
Recent Alerts
No Data Available
Message Attachments
3 OTHERS
4 RTF
2 PNG
2 PDF
Total Attachments
11

Trellix


Trellix
Email Security Cloud → Advanced Threats
What's New - Release 2025.4
Ability to schedule phishing simulator campaigns for future dates. Enhanced detection efficacy through improvements in impersonation detection capabilities. Ability to easily filter ACE alerts using the alert type filter. XConsole now enabled by default fo...
Read More
Current Date: Oct 28 2025 3:21:17 PM Central European Standard Time | UTC+01:00
Alerts
Inbound
Filters: Date Domains Domain Groups View Threat Type Alert Type More filters have been applied Manage CLEAR
BASIC
ADVANCED
Export to CSV
Alert Type: A ACE B Blocked List Match RW Riskware Y Yara RA Retroactive
Columns
Show 20 | 50 | 100 entries
Alert ID
Date & Time
From
Recipients
Subject
MD5
URL/Attachment
Email Server
Threat Type
Email Status
3z32kMI-74191-890806e3-48d3-4260-8aac-00a3e863670f-e27f6e5d
Oct 24 2025 03:38:44 PM
gnignognigna@gmail.com
matteospiga@corraxi.onmicrosoft.com
Fwd: YOU WIN 1000 $
444329639e714d9eb49f4f97273660d8
444329639e714d9eb49f4f97273660d8.doc
10.88.182.229
Others
Scanned
3z32kMI-74191-54482b62-4c3e-41a3-ad92-529accebe843-e27f6e5d
Oct 24 2025 03:38:44 PM
gnignognigna@gmail.com
matteospiga@corraxi.onmicrosoft.com
Fwd: YOU WIN 1000 $
34f171acd0cf873a08a9d76d4125d6cd
Big Nasty.zip
10.88.182.229
Others
Scanned
3z32kMI-74191-286fd771-0cbb-4f8c-b124-cf8050222e9d-02ad3cf2
Oct 24 2025 03:38:33 PM
gnignognigna@gmail.com
matteospiga@corraxi.onmicrosoft.com
Fwd: Aggiornamento programma busta paga
d350a2ccad0eb0f63fa5b37aa362da2e
wannacry.bin.zip
10.88.171.24
Others
Scanned
3z32kMI-74191-07431d60-b83f-42f0-98ba-58f6118aa184-b5c165c7
Oct 24 2025 03:38:33 PM
gnignognigna@gmail.com
matteospiga@corraxi.onmicrosoft.com
Fwd: Aggiornamento programma busta paga
4da1f312a214c07143abeeafb695d904
wannacry.bin
10.88.171.24
Others
Scanned
3z2Xy9Q-72591-966f9a57-d7fb-4804-a23f-95e28c1b6e18-9c01c157
RA
Sep 10 2025 01:26:19 PM
gnignognigna@gmail.com
bcc-demotrellix-com@bcc.us.email.fireeye ...
Please download your paysl ip
43afec85fecf2ae3aabf20d595bc9d68
hxxp://115.56.171.56:35095/i
199.16.199.241
Multistage Phishing
3z2Xyad-72589-17e4f264-d53c-4b00-89de-4a3b55266b6c-9c01c157
Sep 10 2025 01:25:10 PM
gnignognigna@gmail.com
inlineuser@etp.demotrellix.com
Fwd: Please download your payslip
43afec85fecf2ae3aabf20d595bc9d68
hxxp://115.56.171.56:35095/i
209.85.218.45
Multistage Phishing
Showing 1 to 6 of 6 entries
Page 1 / 1
Copyright © 2025 Musarubra US LLC | Version: 2025.4

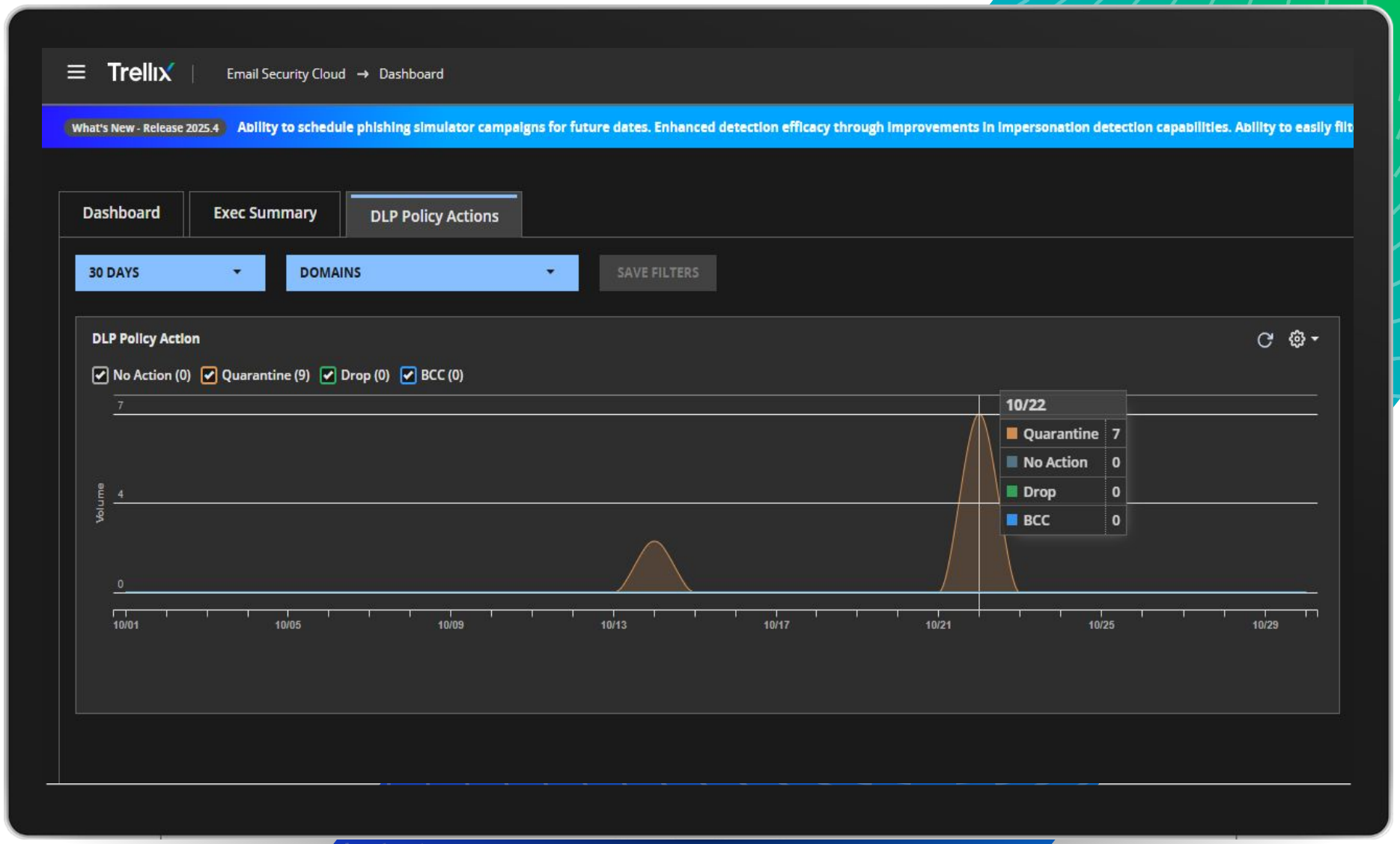
Trellix

# Alerts

## Email analysis results

| | Not Performed | Fail | Pass |
|---|---|---|---|
| Spam | S | S | S |
| Virus | V | V | V |
| Advanced Threats | AT | AT | AT |
| | Not Performed | Drop / Quarantine | Others |
| Policy Action | PA | PA | PA |

Trellix

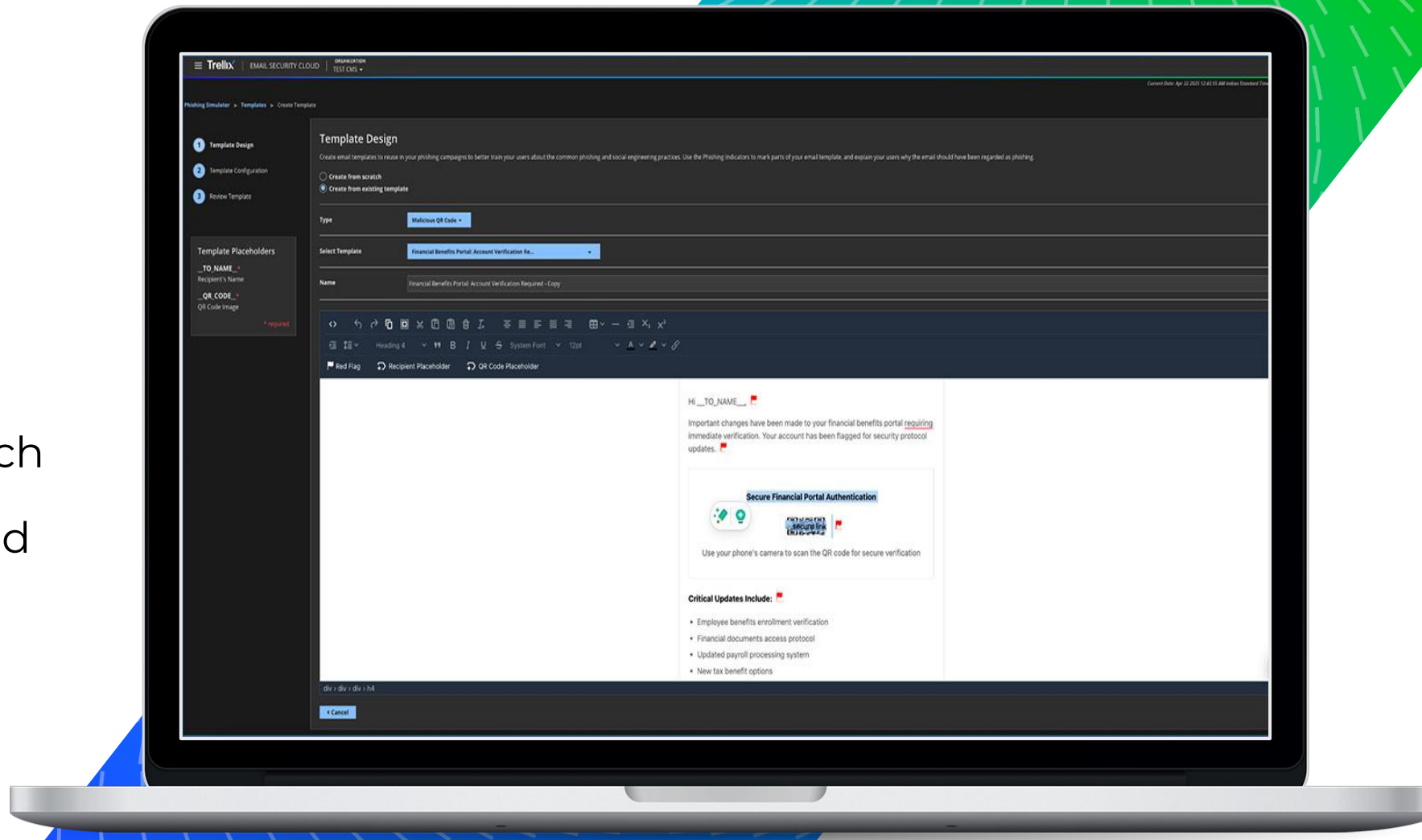

Trellix
Email Security Cloud → Dashboard
What's New - Release 2025.4
Ability to schedule phishing simulator campaigns for future dates. Enhanced detection efficacy through improvements in impersonation detection capabilities. Ability to easily filt
Dashboard
Exec Summary
DLP Policy Actions
30 DAYS
DOMAINS
SAVE FILTERS
DLP Policy Action
No Action (0)
Quarantine (9)
Drop (0)
BCC (0)
7
4
0
Volume
10/01
10/05
10/09
10/13
10/17
10/21
10/25
10/29
10/22
Quarantine 7
No Action 0
Drop 0
BCC 0

Trellix

# Advanced Phishing Simulations

Design simulations based on environment, region, and industry using AI-powered templates.

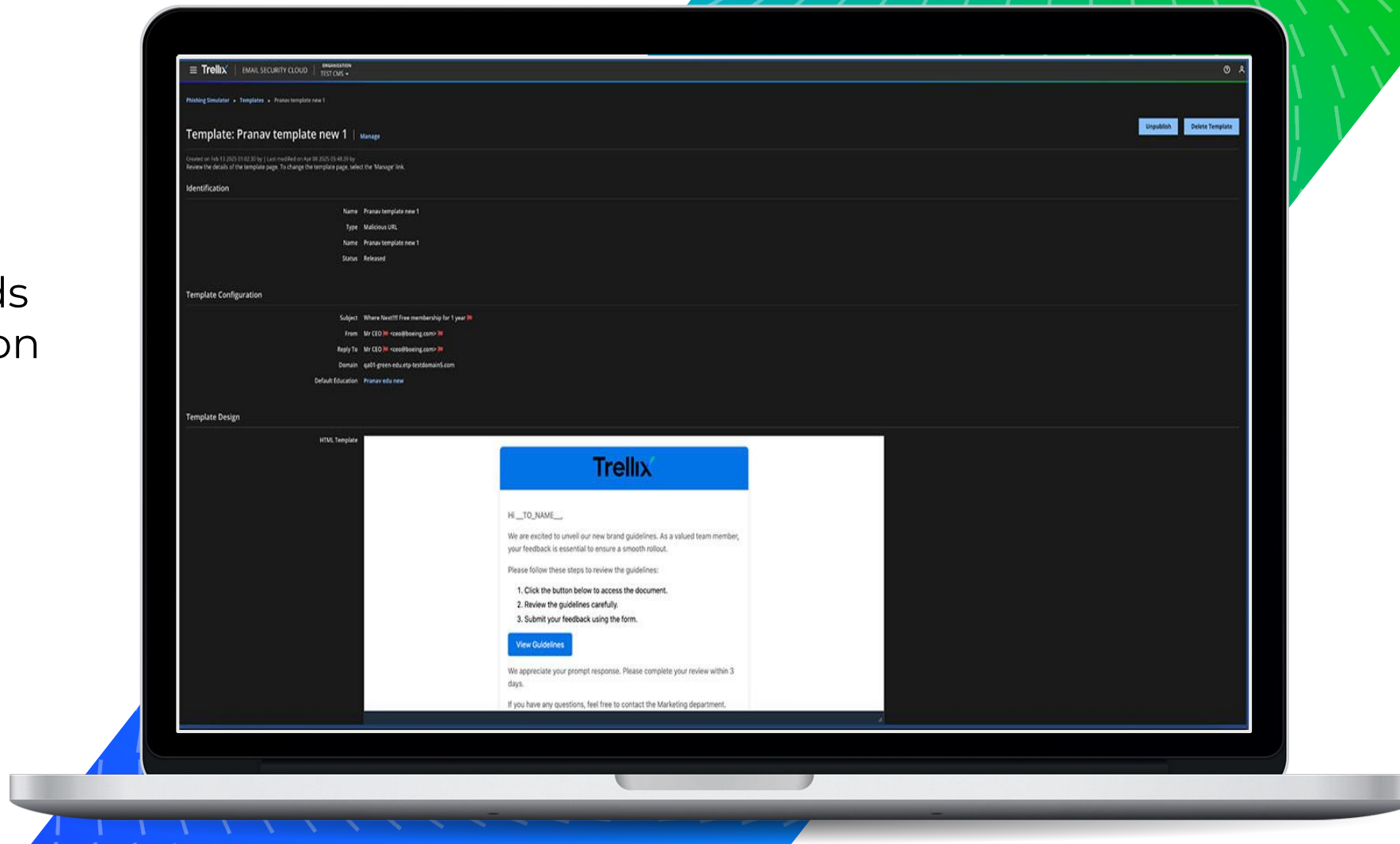
Support attack vectors such as business email compromise, quishing, and more.




Trellix

# Personalized and Effective Training

Provide relevant training tailored to employee needs and interactive remediation training to reinforce learning.

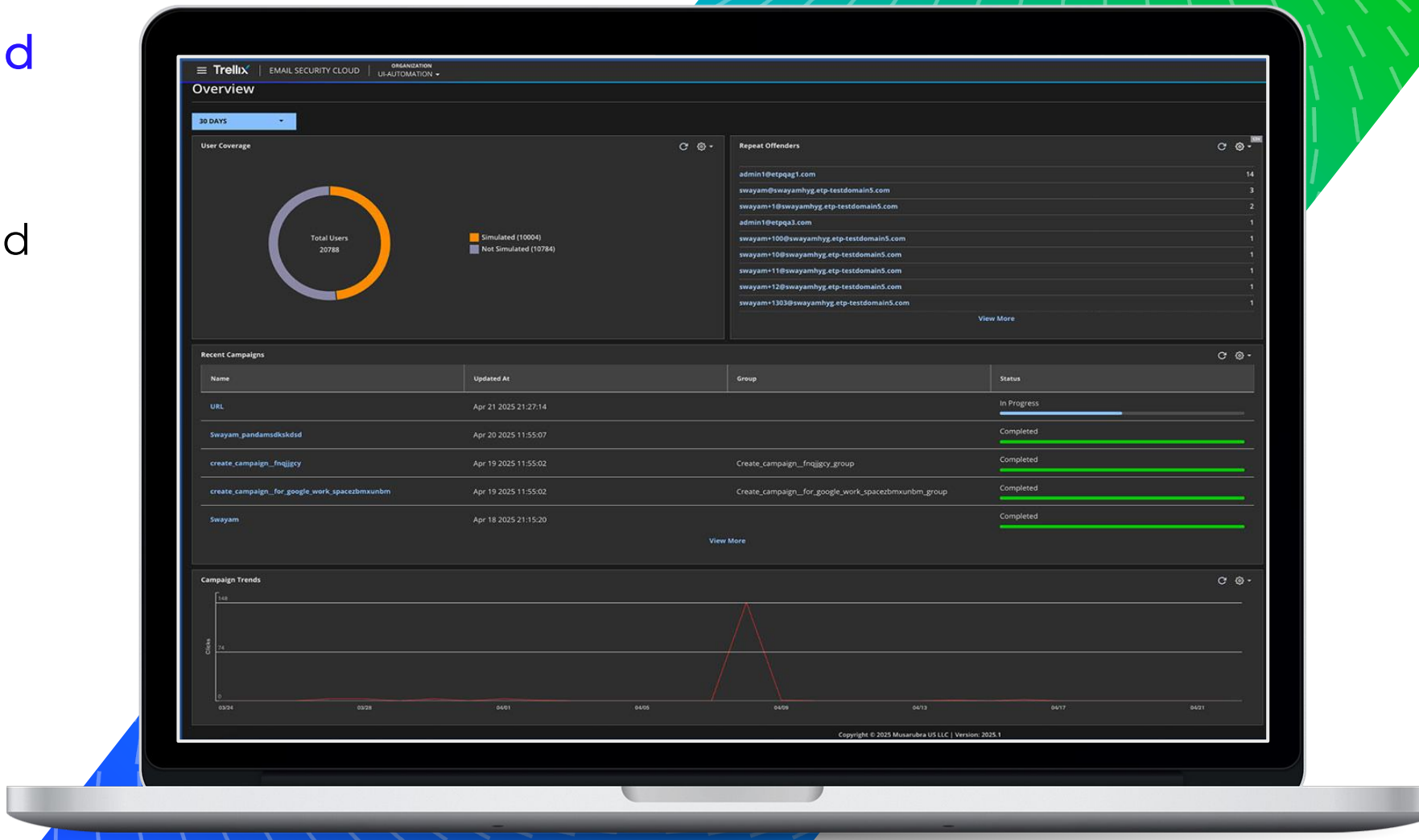



Trellix

# Actionable Analytics and Reporting

Deliver actionable data and metrics through automated reporting.

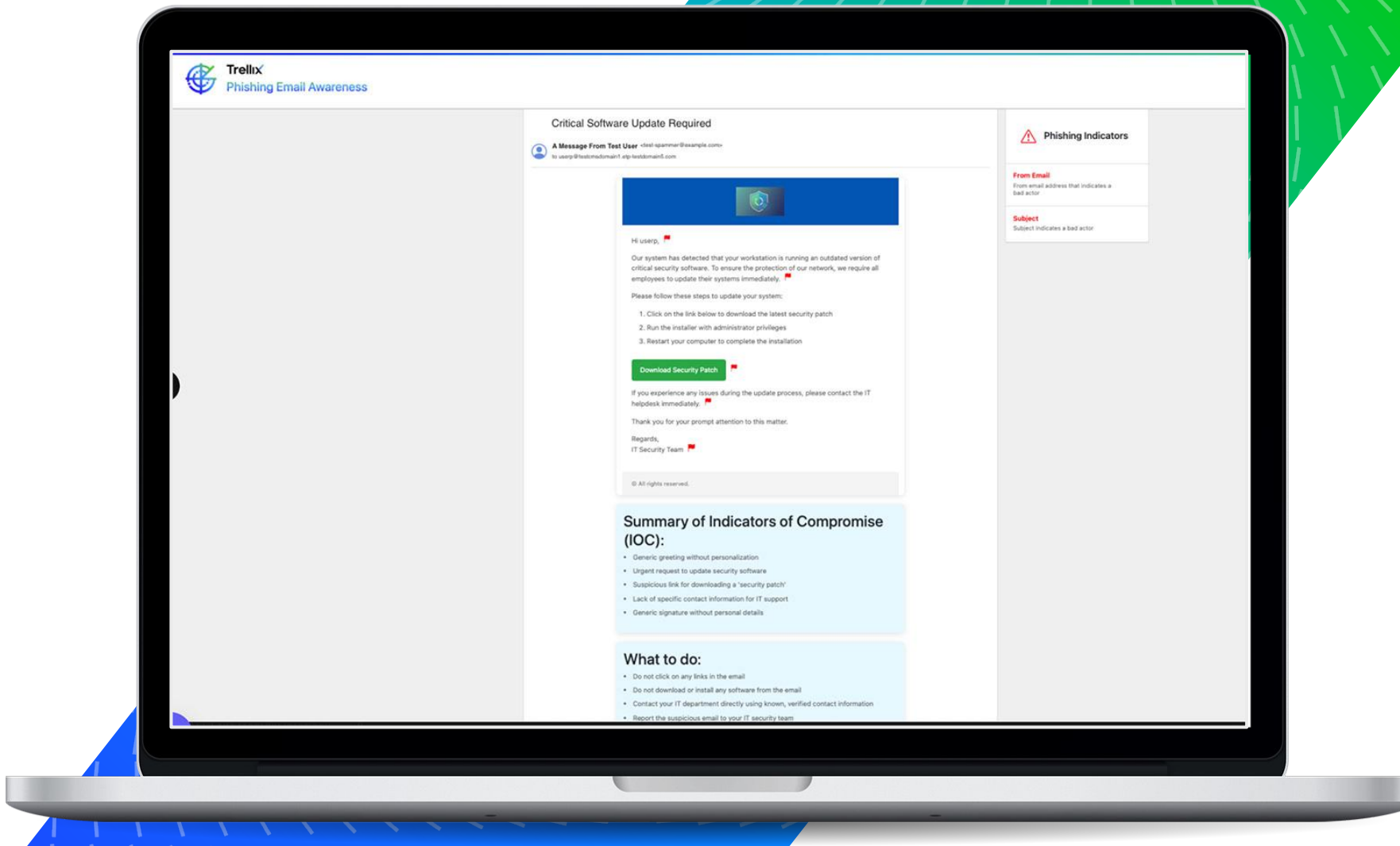
Identify and report on real and simulated phishing attacks.




Trellix

# Enhanced User Experience

Increase administrator productivity with GenAI assistance. Easily build custom employee landing pages with an intuitive training experience.




Trellix

Trellix

# Licensing

New Bundles, SKUs, Example BOM,
No Pricing Discussion!

# Trellix Email Security Offerings - Cloud

## Protecting customers against the #1 attack vector

Trellix Email Security Cloud deployment Types:

- Email Security Cloud with AntiVirus / AntiSpam Edition (deployed as a secure email gateway)
- Email Security Cloud without AntiVirus / AntiSpam Edition (deployed behind secure email gateway)

## Trellix Email Security for Office 365:

Either of the Email Security Cloud deployment types + IVX Enterprise Cloud

| SKU | Capabilities |
|---|---|
| Per user-based subscription pricing | |
| **EMCL** | Email Cloud without AntiVirus/AntiSpam functionality |
| **EMCA** | Email Cloud including AntiVirus/AntiSpam functionality. |
| **EMCLVX** | • Email Security for Office 365 (Protects Office 365 including Email + Sharepoint + Teams + OneDrive)<br>• Email Cloud with AntiVirus/AntiSpam functionality, IVX Enterprise Cloud and Trellix Phishing Simulator |

Trellix

# Trellix Email Security Offerings - Server

## Protecting customers against the #1 attack vector

Trellix Email Security Server

- Email Security Server Edition

Requires either deployment of physical or virtual appliance

| SKU | Capabilities |
|---|---|
| Per user-based subscription pricing | |
| **EMUSE** | Email Security Server Edition |
| **EM-VA-T** | Email Security VM Deployment Option |
| **EM7700-BM-VA** | VM Deployment Option - AMI (Amazon Machine Image) image for c5 Metal AWS instance |
| **EM2500-VA** | VM Deployment option with IVX integrated - No Separate IVX (Intelligent Virtual Execution) is needed. |
| **EM3600 / 5600 / 8600** | Appliance HW unit |

Trellix

Trellix

# Trellix differentiators

# We Catch What Others Miss


Targeted attacks missed by Microsoft across 1,679 customers


Targeted attacks missed by Proofpoint across 962 customers


Targeted attacks missed by IronPort across 871 customers

**“The Trellix detection engines are more capable compared to others and the catch rate is higher.”**

*Dir. Information Security*
*Major Transportation/Logistics company*

Trellix

Source: Trellix Email Security Detection Efficacy Statistics Q1 2025

Trellix

# Vision and Strategy

with Rahul Iyer

Principal, Product Management


Trellix