Trellix

# Collaborate with Ease Across All Applications Without Sacrificing Security

**Boubker El Mouttahid**

Global Technical Director,
Skyhigh Security

**Filippo Sitzia**

EMEA Solution Architect,
Trellix

**Andreas Zengel**

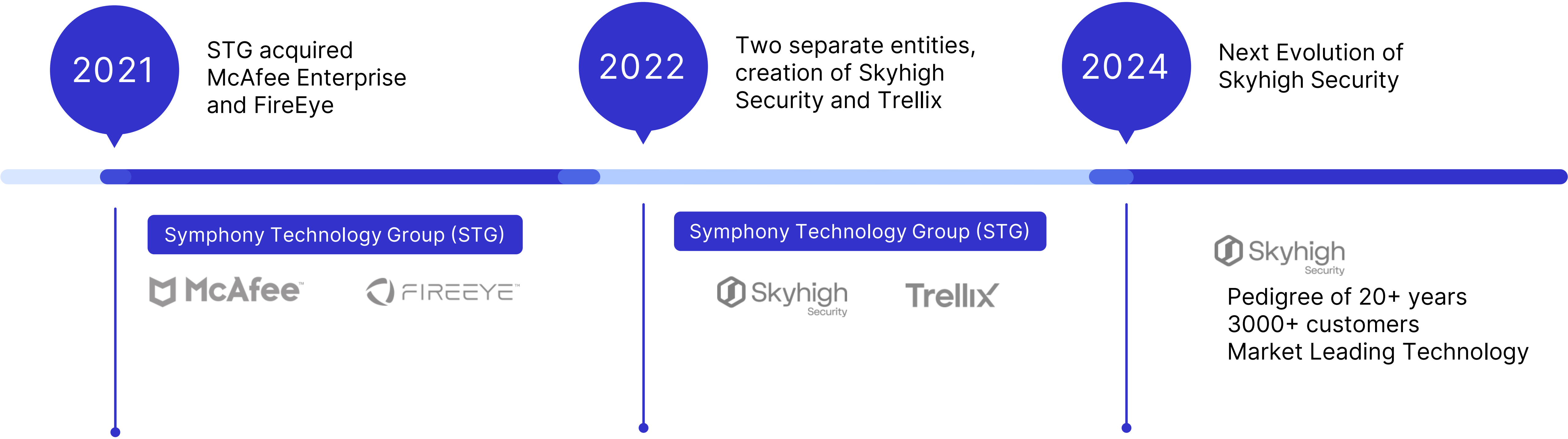
Director Sales Engineering,
Skyhigh Security

June 2024

# Agenda

- Skyhigh Security Vision and Platform overview
- Skyhigh & Trellix ePO Integrations / DLP
- Advanced Threat Defense with Skyhigh Web  & Trellix IVX
- Skyhigh SSE & Trellix Hellix (XDR) Integration
- Conclusion / Q&A

# Skyhigh Security Journey



2021

STG acquired McAfee Enterprise and FireEye

Symphony Technology Group (STG)

McAfee FIREEYE

2022

Two separate entities, creation of Skyhigh Security and Trellix

Symphony Technology Group (STG)

Skyhigh Security Trellix

2024

Next Evolution of Skyhigh Security

Skyhigh Security

Pedigree of 20+ years
3000+ customers
Market Leading Technology

# Skyhigh Security Mission

Skyhigh
Security

## Our Mission

We protect all of an organization's data, regardless of where it resides, against both internal and external threats.

We go beyond data access and focus on data use, allowing organizations to securely connect and collaborate from any device and from anywhere.

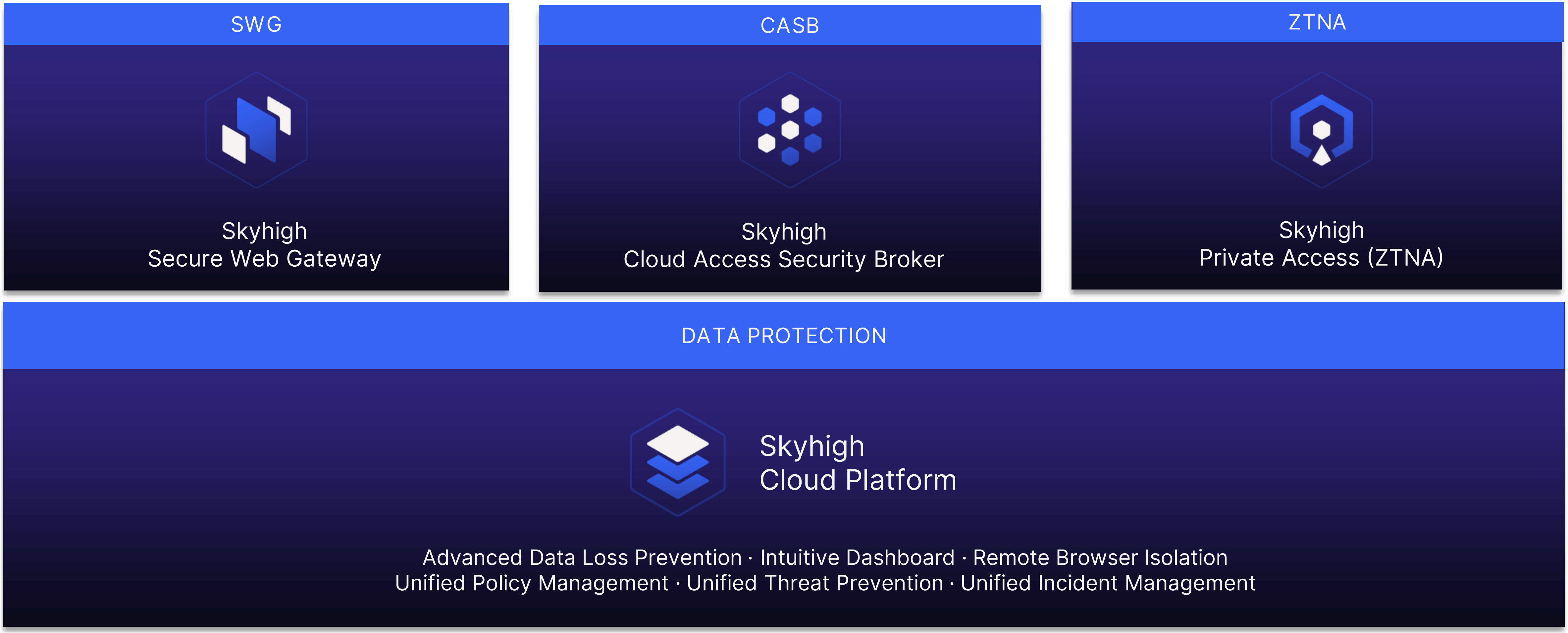
By 2026 –

85% of organizations seeking to secure their Web, SaaS and Private Applications will obtain the security capabilities from a security service edge (SSE) offering.

45% of organizations will prioritize advanced data security features for inspection and protection of data at rest and in motion as a selection criterion for SSE.

—2024 Gartner® Magic Quadrant™ for Security Service Edge

# Skyhigh Security Service Edge (SSE) Portfolio



SWG

Skyhigh
Secure Web Gateway

CASB

Skyhigh
Cloud Access Security Broker

ZTNA

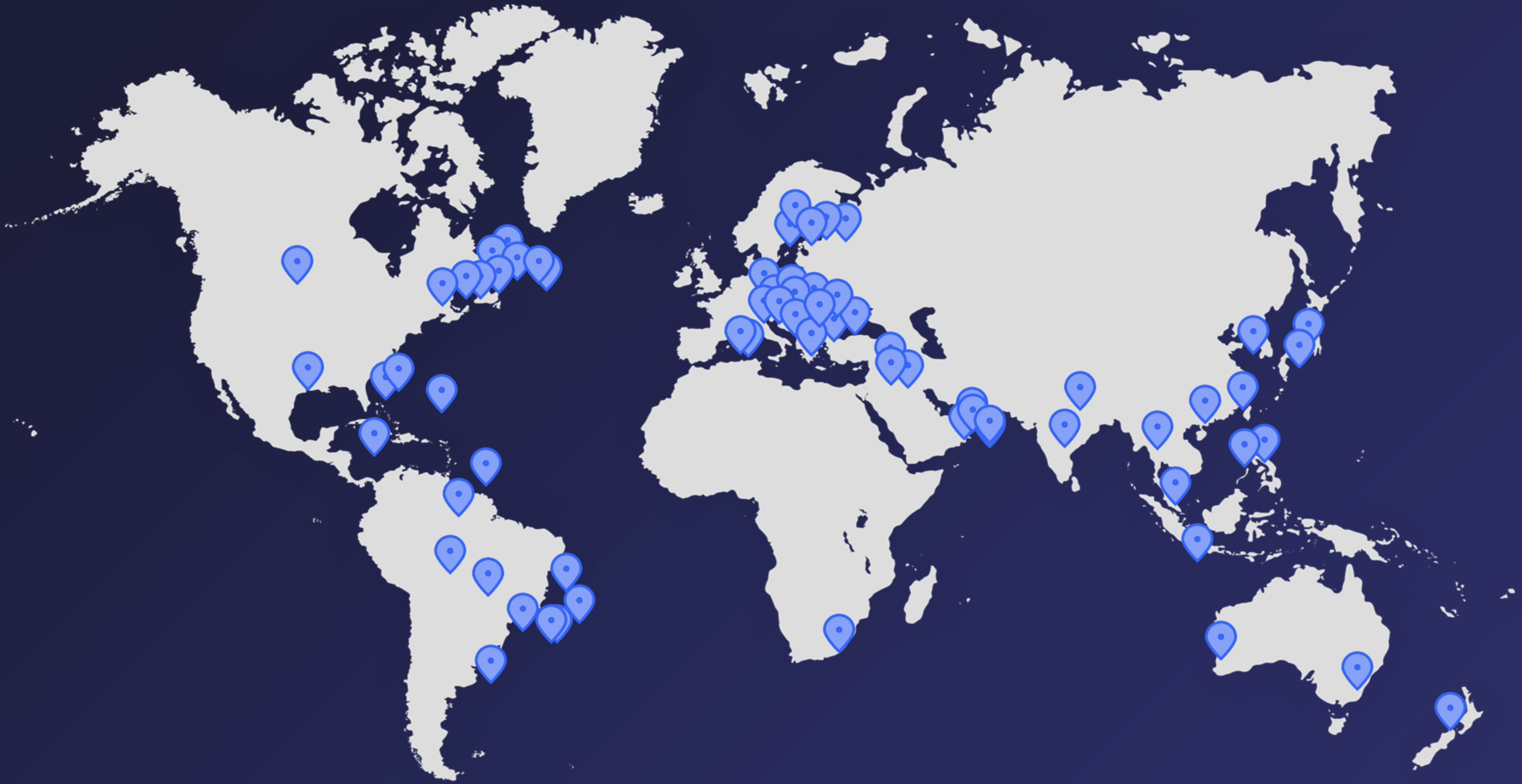
Skyhigh
Private Access (ZTNA)

DATA PROTECTION

Skyhigh
Cloud Platform

Advanced Data Loss Prevention · Intuitive Dashboard · Remote Browser Isolation
Unified Policy Management · Unified Threat Prevention · Unified Incident Management

# 100+ Points of Presence Globally



# Our Differentiation

- Unified Data Protection & Most Advanced DLP Techniques
- Flexible Deployment SWG (On-prem, Hybrid, Cloud)
- Best-in-Class Malware Protection
- Industry’s Largest CASB API coverage
- Single Converged Platform
- Wide ecosystem of Enterprise Integrations

# Security and Performance at Scale

**8.6B+**

Shadow Events Monitored Every Day

**100+**

Cloud-Native Security Points of Presence Worldwide

**230M+**

Files Scanned Every Day

**2B+**

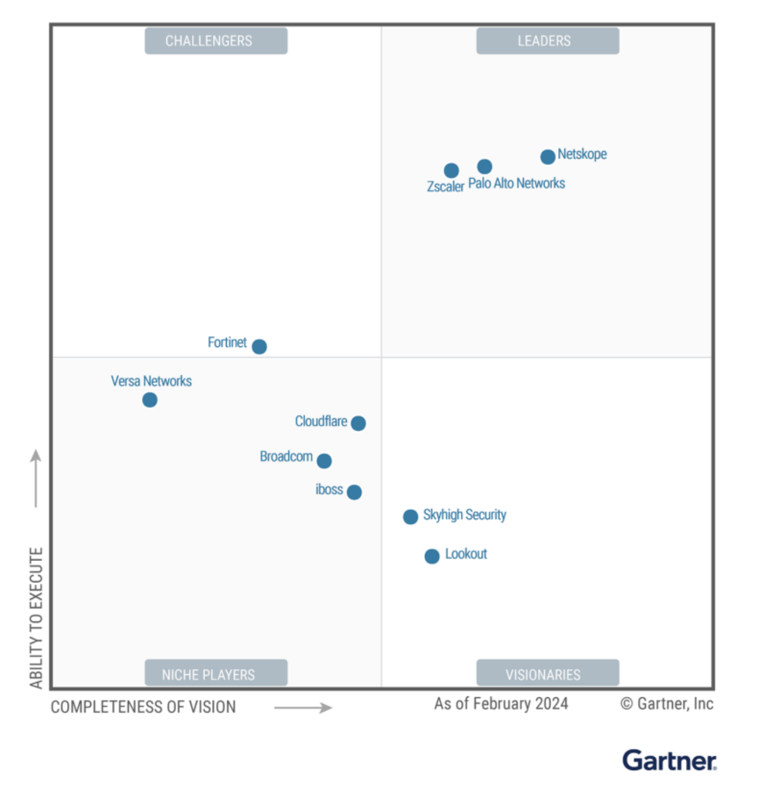
Sanctioned Events Monitored Every Day

# Validated By Analysts

## Skyhigh Security Named “Visionary” - 2 Years in a Row

Gartner

2024 Gartner® Magic Quadrant$^{\text{TM}}$ for Security Service Edge



Gartner

2024 Gartner® Critical Capabilities for Security Service Edge

**#1 in “Protect Data” Use Case**

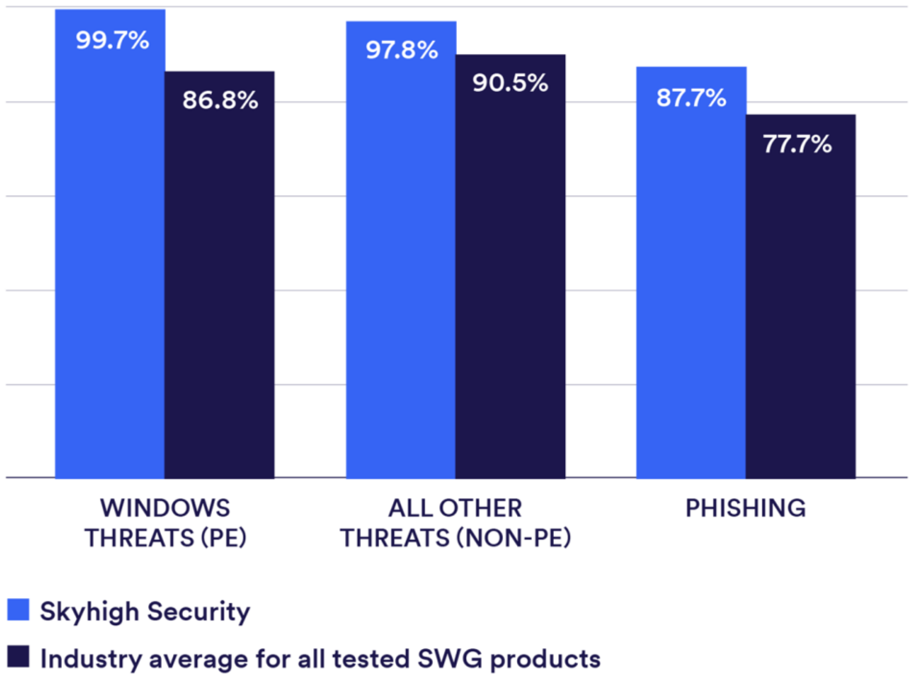
**#1 in 4 out of 10 Critical Capabilities**

- Visibility and Control of activities
- Data Security
- SSPM
- Enterprise Integration

# Validated by Industry Experts

AV-TEST

## Skyhigh Beats the Average in All Test Categories



> Considering all the results of the products tested by AV-TEST, Skyhigh is among the top performers in that product category and offers strong protection against the used test cases.

AV-TEST: Evaluation of Skyhigh SSE, November 2023

# Recognized by Industry

2024 Globee® Awards for Cybersecurity

2024 Cloud Security Awards

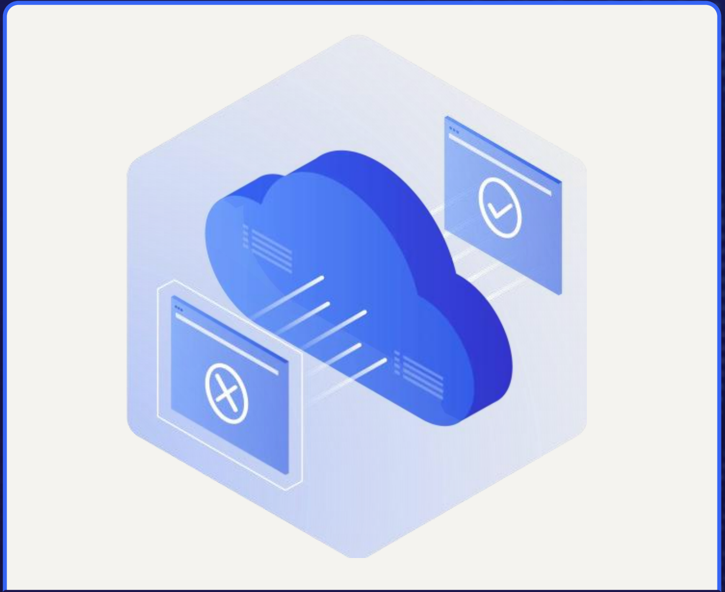
2024 Constellation ShortList ™ for SSE Q1

2024 CRN Coolest Cloud 100 List

2024 CRN Hottest Cloud 100 List

2024 BIG Innovation Award

# Skyhigh Security - AI Focus



VISIBILITY
Shadow IT

PROTECTION
DLP and Content

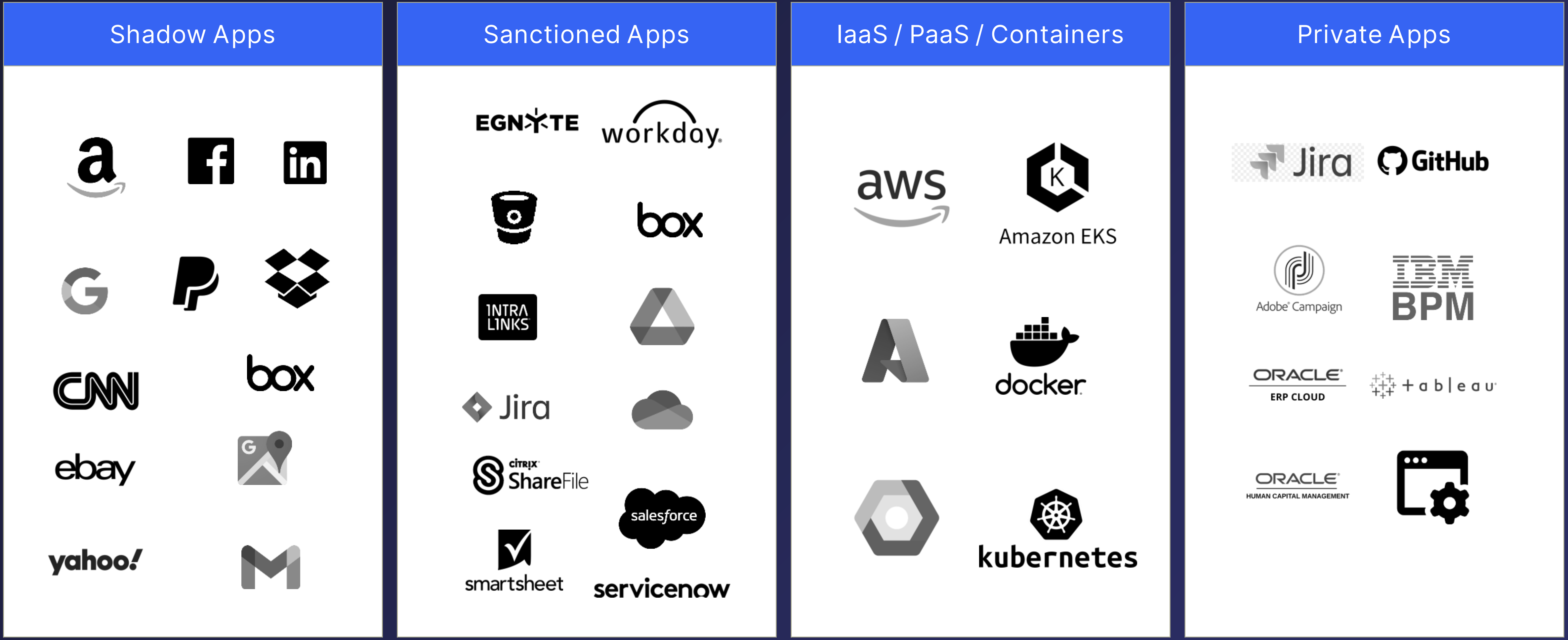
OPTIMIZATION
Ease of use and Detection

# Skyhigh/Trellix ePO Integrations / DLP

Boubker El Mouttahid

Global Technical Director, Skyhigh Security

# Data isn’t just on endpoints anymore



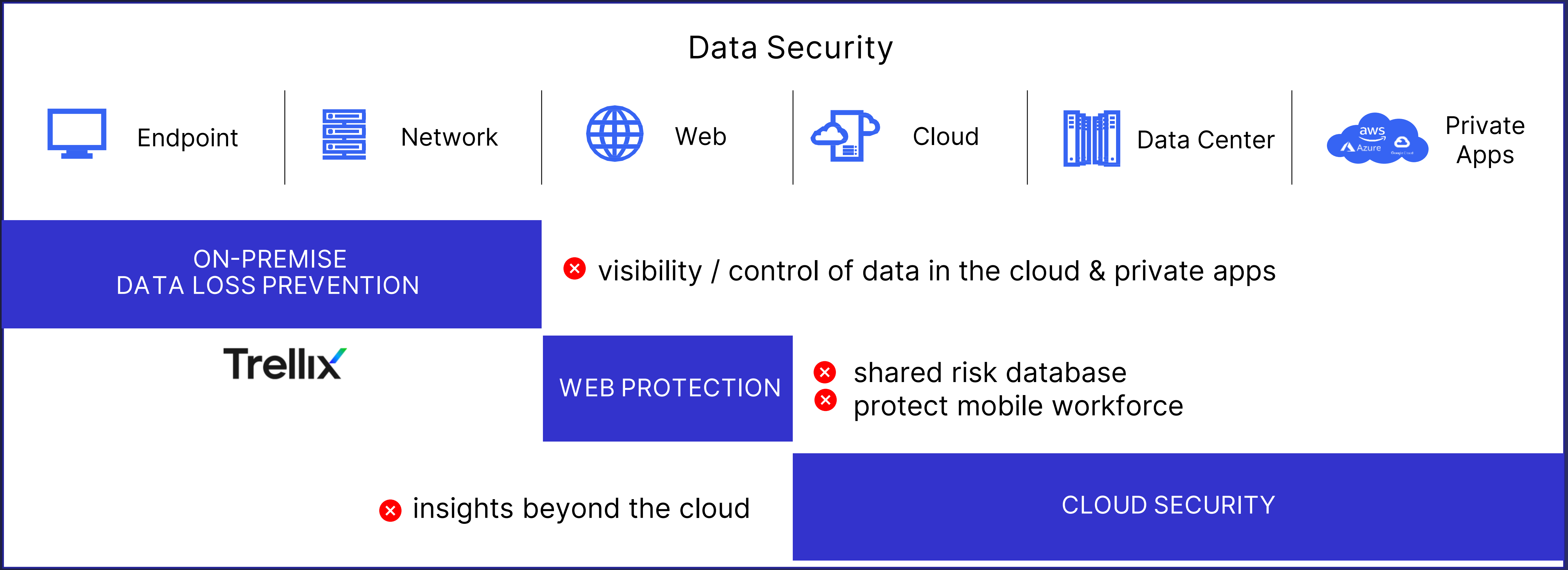
## Shadow Apps

## Sanctioned Apps

## IaaS / PaaS / Containers

## Private Apps

# Point solutions create security gaps



Data Security

Endpoint | Network | Web | Cloud | Data Center | Private Apps

ON-PREMISE
DATA LOSS PREVENTION

☒ visibility / control of data in the cloud & private apps

Trellix

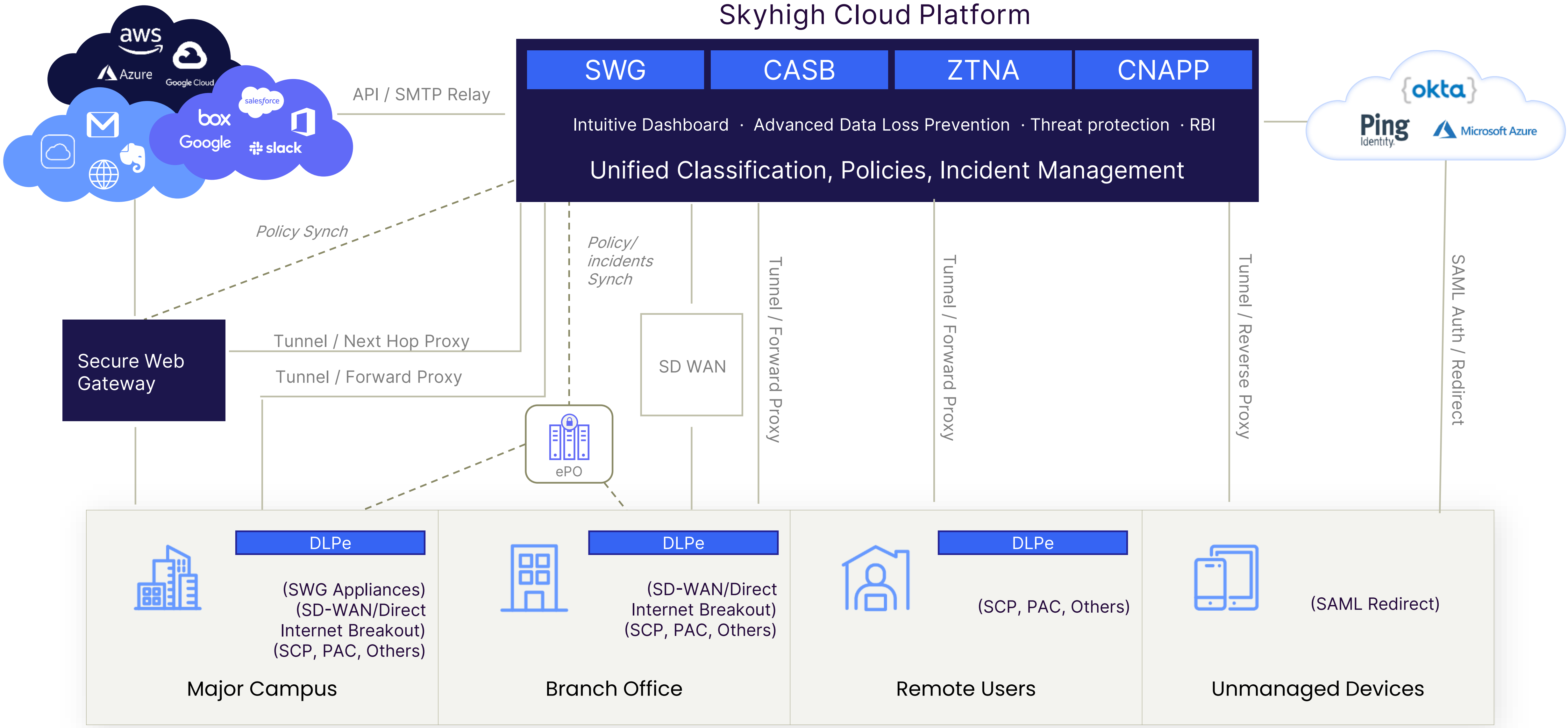
WEB PROTECTION

☒ shared risk database
☒ protect mobile workforce

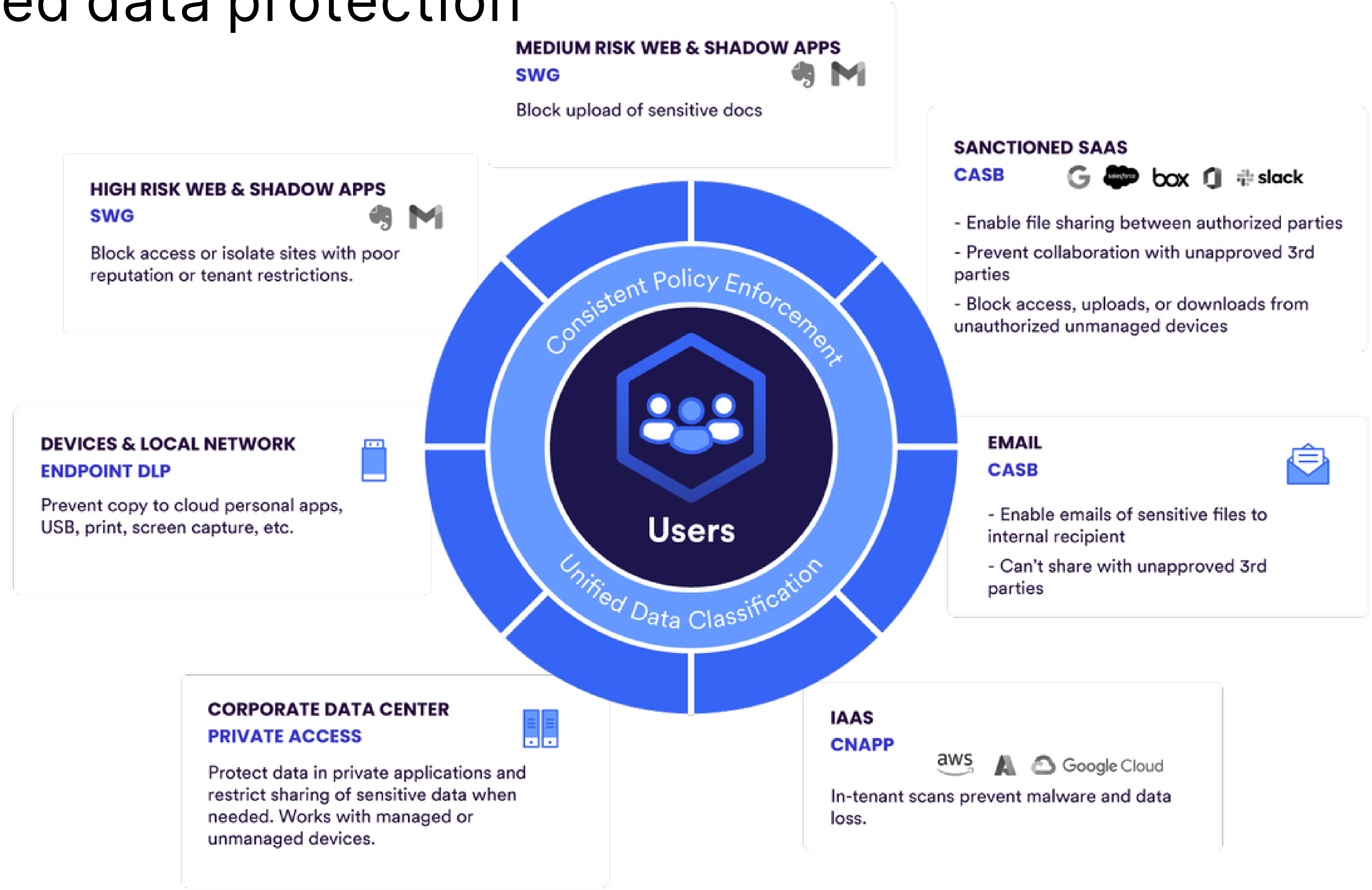
☒ insights beyond the cloud

CLOUD SECURITY

# Our unified DLP architecture



# Unified data protection



**MEDIUM RISK WEB & SHADOW APPS**
**SWG**
Block upload of sensitive docs

**HIGH RISK WEB & SHADOW APPS**
**SWG**
Block access or isolate sites with poor reputation or tenant restrictions.

**SANCTIONED SAAS**
**CASB**
- Enable file sharing between authorized parties
- Prevent collaboration with unapproved 3rd parties
- Block access, uploads, or downloads from unauthorized unmanaged devices

**DEVICES & LOCAL NETWORK**
**ENDPOINT DLP**
Prevent copy to cloud personal apps, USB, print, screen capture, etc.

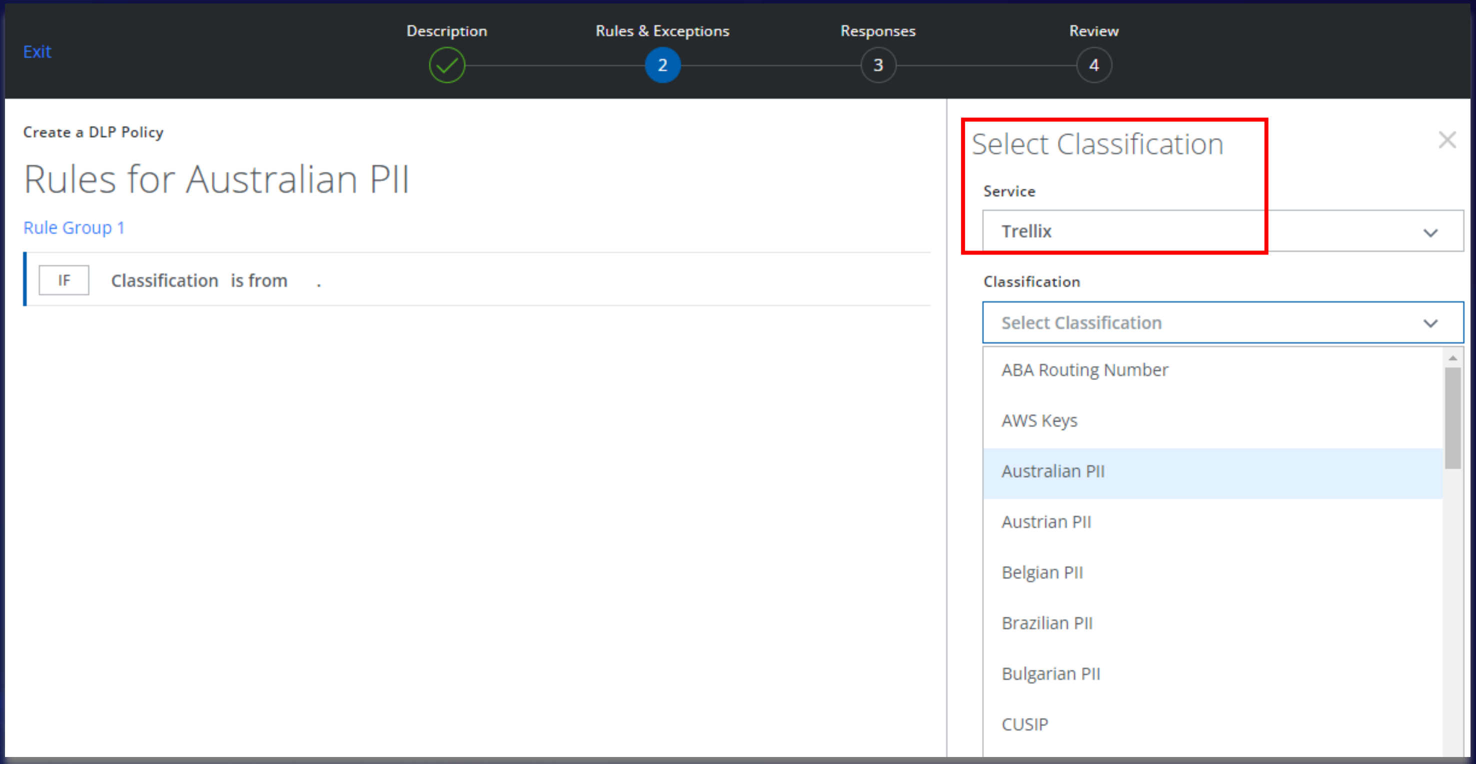
**EMAIL**
**CASB**
- Enable emails of sensitive files to internal recipient
- Can't share with unapproved 3rd parties

**CORPORATE DATA CENTER**
**PRIVATE ACCESS**
Protect data in private applications and restrict sharing of sensitive data when needed. Works with managed or unmanaged devices.

**IAAS**
**CNAPP**
In-tenant scans prevent malware and data loss.

# Skyhigh / Trellix DLP integrations: Classifications

- Unified data classification
- DLP Data classifications created in Trellix on-prem ePO can be used in SSE policies (CASB ,  SWG, RBI, ZTNA)



Create a DLP Policy

Rules for Australian PII

Rule Group 1

IF Classification is from .

Select Classification

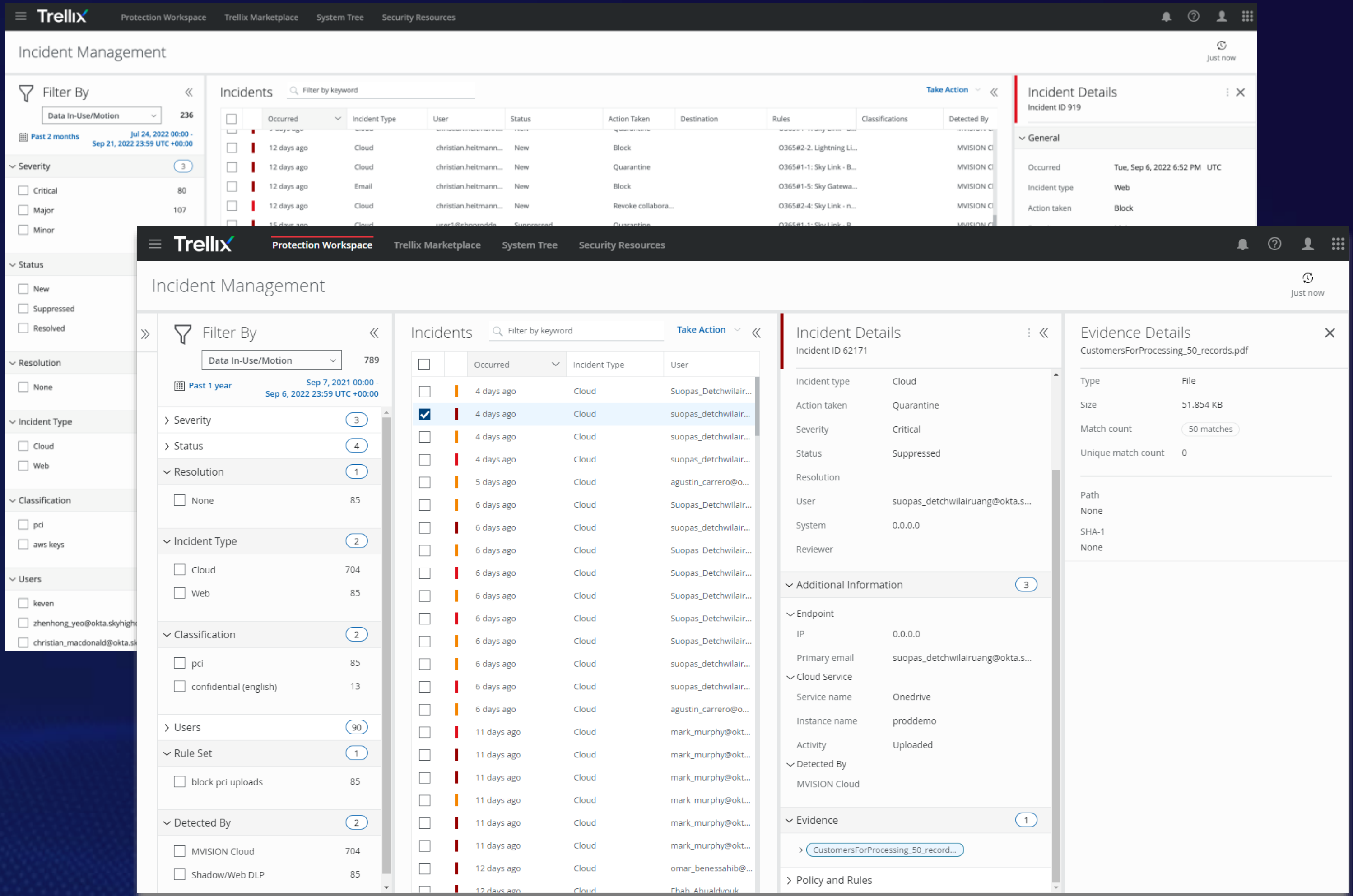
Service: Trellix

Classification: Select Classification

# Skyhigh / Trellix DLP integrations: Incidents

- Unified Incidents

All Web, ZTNA and CASB Incidents can be shown in Trellix on premise / Cloud ePO ePO



Incident Management

Filter By

Data In-Use/Motion 236

Past 2 months Jul 24, 2022 00:00 - Sep 21, 2022 23:59 UTC +00:00

Severity (3)
- □ Critical 80
- □ Major 107
- □ Minor

Status
- □ New
- □ Suppressed
- □ Resolved

Resolution
- □ None

Incident Type
- □ Cloud
- □ Web

Classification
- □ pci
- □ aws keys

Users
- □ keven
- □ zhenhong_yeo@okta.skyhigh
- □ christian_macdonald@okta.sk

Incidents

| | Occurred | Incident Type | User | Status | Action Taken | Destination | Rules | Classifications | Detected By |
|---|---|---|---|---|---|---|---|---|---|
| □ | 12 days ago | Cloud | christian.heitmann... | New | Block | | O365#2-2. Lightning Li... | | MVISION Cl |
| □ | 12 days ago | Cloud | christian.heitmann... | New | Quarantine | | O365#1-1: Sky Link - B... | | MVISION Cl |
| □ | 12 days ago | Email | christian.heitmann... | New | Block | | O365#1-5: Sky Gatewa... | | MVISION Cl |
| □ | 12 days ago | Cloud | christian.heitmann... | New | Revoke collabora... | | O365#2-4: Sky Link - n... | | MVISION Cl |

Incident Details

Incident ID 919

General

| | |
|---|---|
| Occurred | Tue, Sep 6, 2022 6:52 PM UTC |
| Incident type | Web |
| Action taken | Block |

Incident Management

Filter By

Data In-Use/Motion 789

Past 1 year Sep 7, 2021 00:00 - Sep 6, 2022 23:59 UTC +00:00

- Severity (3)
- Status (4)
- Resolution (1)
  - □ None 85
- Incident Type (2)
  - □ Cloud 704
  - □ Web 85
- Classification (2)
  - □ pci 85
  - □ confidential (english) 13
- Users (90)
- Rule Set (1)
  - □ block pci uploads 85
- Detected By (2)
  - □ MVISION Cloud 704
  - □ Shadow/Web DLP 85

Incidents

| □ | Occurred | Incident Type | User |
|---|---|---|---|
| □ | 4 days ago | Cloud | Suopas_Detchwilair... |
| ☑ | 4 days ago | Cloud | suopas_detchwilair... |
| □ | 4 days ago | Cloud | suopas_detchwilair... |
| □ | 4 days ago | Cloud | suopas_detchwilair... |
| □ | 5 days ago | Cloud | agustin_carrero@o... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | suopas_detchwilair... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | Suopas_Detchwilair... |
| □ | 6 days ago | Cloud | suopas_detchwilair... |
| □ | 6 days ago | Cloud | suopas_detchwilair... |
| □ | 6 days ago | Cloud | agustin_carrero@o... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 11 days ago | Cloud | mark_murphy@okt... |
| □ | 12 days ago | Cloud | omar_benessahib@... |
| □ | 12 days ago | Cloud | Ehab_Abualdvouk |

Incident Details

Incident ID 62171

| | |
|---|---|
| Incident type | Cloud |
| Action taken | Quarantine |
| Severity | Critical |
| Status | Suppressed |
| Resolution | |
| User | suopas_detchwilairuang@okta.s... |
| System | 0.0.0.0 |
| Reviewer | |

Additional Information (3)

Endpoint

| | |
|---|---|
| IP | 0.0.0.0 |
| Primary email | suopas_detchwilairuang@okta.s... |

Cloud Service

| | |
|---|---|
| Service name | Onedrive |
| Instance name | proddemo |
| Activity | Uploaded |

Detected By

MVISION Cloud

Evidence (1)

CustomersForProcessing_50_record...

Policy and Rules

Evidence Details

CustomersForProcessing_50_records.pdf

| | |
|---|---|
| Type | File |
| Size | 51.854 KB |
| Match count | 50 matches |
| Unique match count | 0 |

Path

None

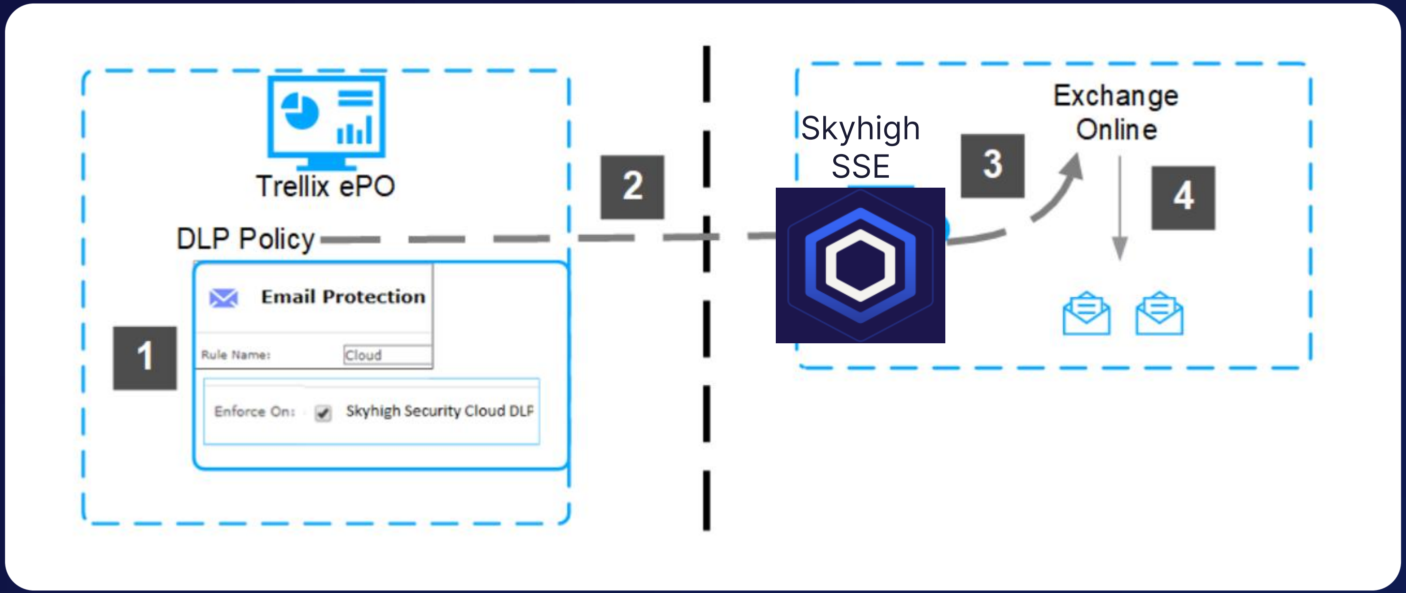
SHA-1

None

Trellix | Skyhigh Security

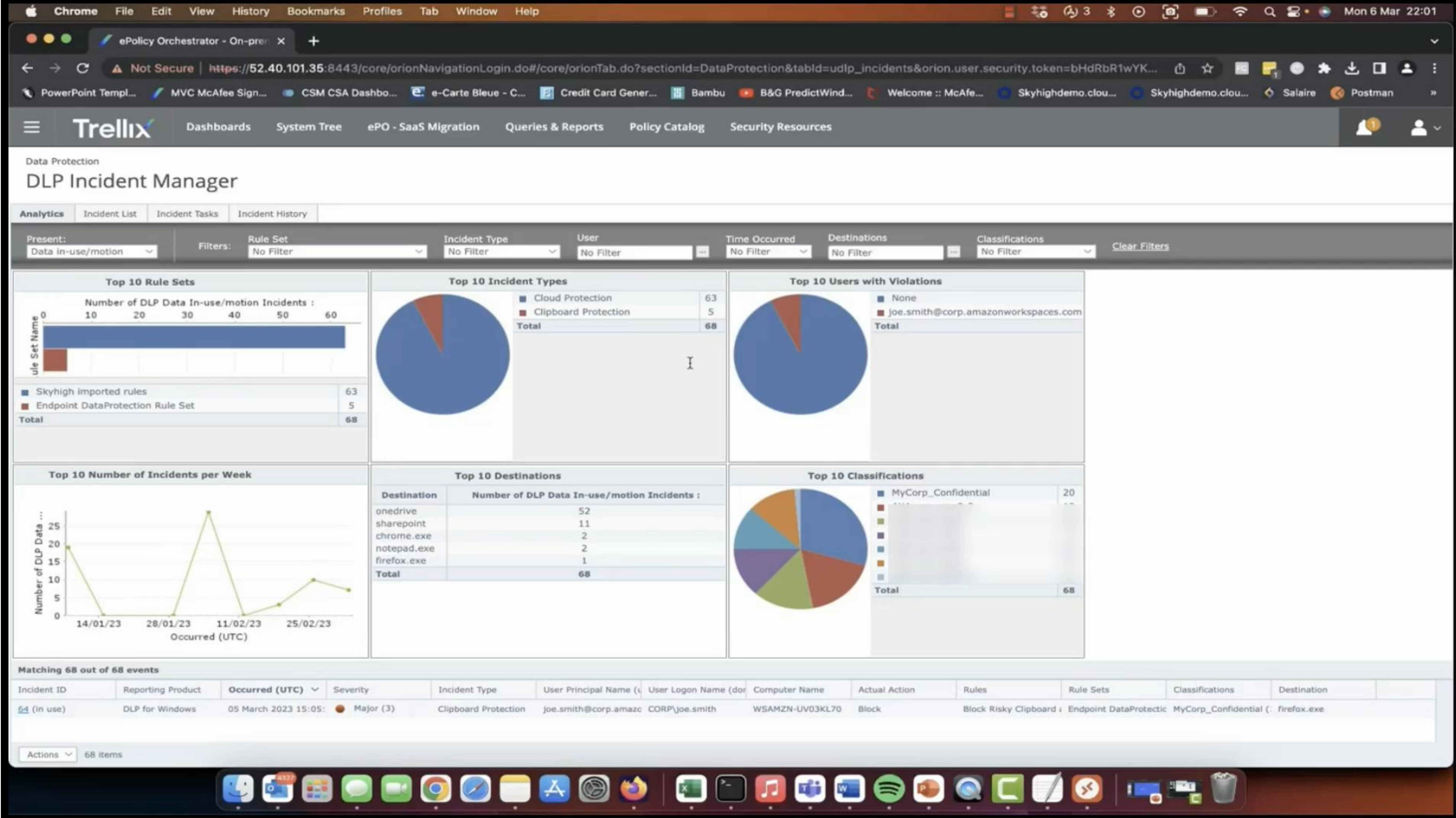
# Apply a Trellix email DLP policy to Exchange Online using Skyhigh

- The Trellix DLP administrator creates a DLP policy with email rules and associated Skyhigh Security Cloud reactions
- The Trellix DLP administrator applies the Trellix DLP policy to Skyhigh Security Cloud.
- The Skyhigh Security Cloud administrator enables DLP policy for Exchange Online within the Skyhigh Security Cloud UI.
- The DLP Policy is applied to Exchange Online content in the customers connected account.



Rule Name: Cloud

Enforce On: ☑ Skyhigh Security Cloud DLF


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 6 Mar 22:01
ePolicy Orchestrator - On-prer
Not Secure https://52.40.101.35:8443/core/orionNavigationLogin.do#/core/orionTab.do?sectionId=DataProtection&tabId=udlp_incidents&orion.user.security.token=bHdRbR1wYK...
PowerPoint Templ... MVC McAfee Sign... CSM CSA Dashbo... e-Carte Bleue - C... Credit Card Gener... Bambu B&G PredictWind... Welcome :: McAfe... Skyhighdemo.clou... Skyhighdemo.clou... Salaire Postman
Trellix
Dashboards System Tree ePO - SaaS Migration Queries & Reports Policy Catalog Security Resources

Data Protection

DLP Incident Manager

Analytics | Incident List | Incident Tasks | Incident History

Present: Data in-use/motion

Filters: Rule Set: No Filter | Incident Type: No Filter | User: No Filter | Time Occurred: No Filter | Destinations: No Filter | Classifications: No Filter | Clear Filters

**Top 10 Rule Sets**

Number of DLP Data In-use/motion Incidents :
0
10
20
30
40
50
60
ule Set Name

| | |
|---|---|
| 🟦 Skyhigh imported rules | 63 |
| 🟥 Endpoint DataProtection Rule Set | 5 |
| Total | 68 |

**Top 10 Incident Types**

| | |
|---|---|
| 🟦 Cloud Protection | 63 |
| 🟥 Clipboard Protection | 5 |
| Total | 68 |

**Top 10 Users with Violations**

| | |
|---|---|
| 🟦 None | |
| 🟥 joe.smith@corp.amazonworkspaces.com | |
| Total | |

**Top 10 Number of Incidents per Week**

**Top 10 Destinations**

| Destination | Number of DLP Data In-use/motion Incidents : |
|---|---|
| onedrive | 52 |
| sharepoint | 11 |
| chrome.exe | 2 |
| notepad.exe | 2 |
| firefox.exe | 1 |
| Total | 68 |

**Top 10 Classifications**

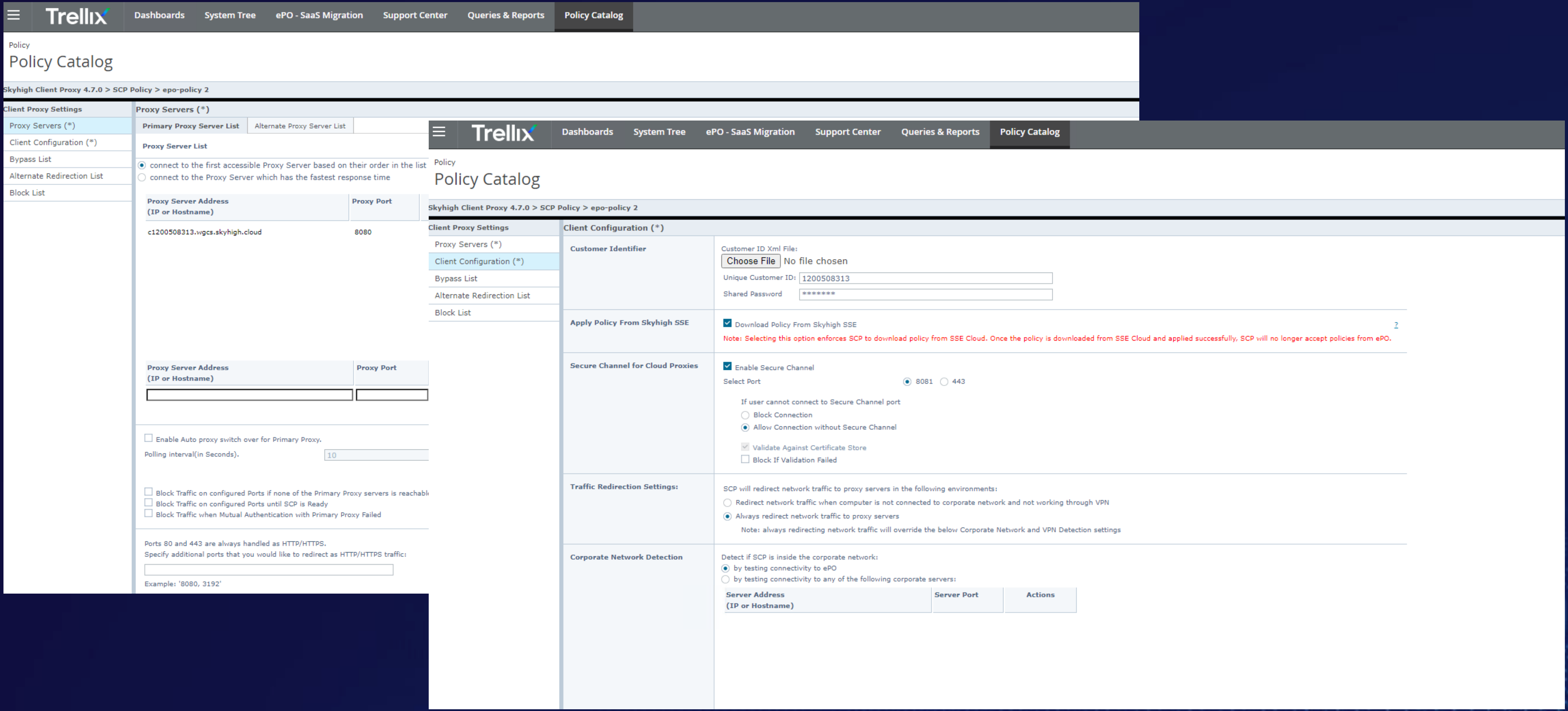
| | |
|---|---|
| 🟦 MyCorp_Confidential | 20 |
| [redacted] | |
| Total | 68 |

Matching 68 out of 68 events

| Incident ID | Reporting Product | Occurred (UTC) | Severity | Incident Type | User Principal Name (u | User Logon Name (dor | Computer Name | Actual Action | Rules | Rule Sets | Classifications | Destination |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 64 (in use) | DLP for Windows | 05 March 2023 15:05: | ● Major (3) | Clipboard Protection | joe.smith@corp.amazc | CORP\joe.smith | WSAMZN-UV03KL70 | Block | Block Risky Clipboard ε | Endpoint DataProtectic | MyCorp_Confidential (: | firefox.exe |

Actions 68 items

# Install the Client Proxy extension on Trellix ePO on-premise



Policy

Policy Catalog

Skyhigh Client Proxy 4.7.0 > SCP Policy > epo-policy 2

**Client Proxy Settings**

- Proxy Servers (*)
- Client Configuration (*)
- Bypass List
- Alternate Redirection List
- Block List

**Proxy Servers (*)**

Primary Proxy Server List | Alternate Proxy Server List

**Proxy Server List**

● connect to the first accessible Proxy Server based on their order in the list
○ connect to the Proxy Server which has the fastest response time

| Proxy Server Address (IP or Hostname) | Proxy Port |
|---|---|
| c1200508313.wgcs.skyhigh.cloud | 8080 |

| Proxy Server Address (IP or Hostname) | Proxy Port |
|---|---|
| | |

□ Enable Auto proxy switch over for Primary Proxy.

Polling interval(in Seconds). 10

□ Block Traffic on configured Ports if none of the Primary Proxy servers is reachabl
□ Block Traffic on configured Ports until SCP is Ready
□ Block Traffic when Mutual Authentication with Primary Proxy Failed

Ports 80 and 443 are always handled as HTTP/HTTPS.
Specify additional ports that you would like to redirect as HTTP/HTTPS traffic:

Example: '8080, 3192'

Policy

Policy Catalog

Skyhigh Client Proxy 4.7.0 > SCP Policy > epo-policy 2

**Client Proxy Settings**

- Proxy Servers (*)
- Client Configuration (*)
- Bypass List
- Alternate Redirection List
- Block List

**Client Configuration (*)**

**Customer Identifier**

Customer ID Xml File:
Choose File No file chosen
Unique Customer ID: 1200508313
Shared Password *******

**Apply Policy From Skyhigh SSE**

☑ Download Policy From Skyhigh SSE ?
Note: Selecting this option enforces SCP to download policy from SSE Cloud. Once the policy is downloaded from SSE Cloud and applied successfully, SCP will no longer accept policies from ePO.

**Secure Channel for Cloud Proxies**

☑ Enable Secure Channel
Select Port ● 8081 ○ 443

If user cannot connect to Secure Channel port
○ Block Connection
● Allow Connection without Secure Channel

☑ Validate Against Certificate Store
□ Block If Validation Failed

**Traffic Redirection Settings:**

SCP will redirect network traffic to proxy servers in the following environments:
○ Redirect network traffic when computer is not connected to corporate network and not working through VPN
● Always redirect network traffic to proxy servers
Note: always redirecting network traffic will override the below Corporate Network and VPN Detection settings

**Corporate Network Detection**

Detect if SCP is inside the corporate network:
● by testing connectivity to ePO
○ by testing connectivity to any of the following corporate servers:

| Server Address (IP or Hostname) | Server Port | Actions |
|---|---|---|

# Advance Threat Defense Skyhigh Web / CASB + Trellix IVX

# Proven technology to address three distinct use cases

## IVX for Products

Targeted for Trellix Appliances

- MVX detection created the sandbox market. Detection is our founding competency
- Flexible deployment options that scale for scanning throughput with Network Security, Email Security, Endpoint, etc.
- Clustered architecture instrumented for 200 potential simultaneous executions
- **Product: Trellix IVX**

## IVX for Investigators

Targeted for the SOC

- Used during investigative workflows
- Detonate suspicious content
- Reverse engineer malware
- **Product: Trellix Malware Analysis**

## IVX for Collaboration Security

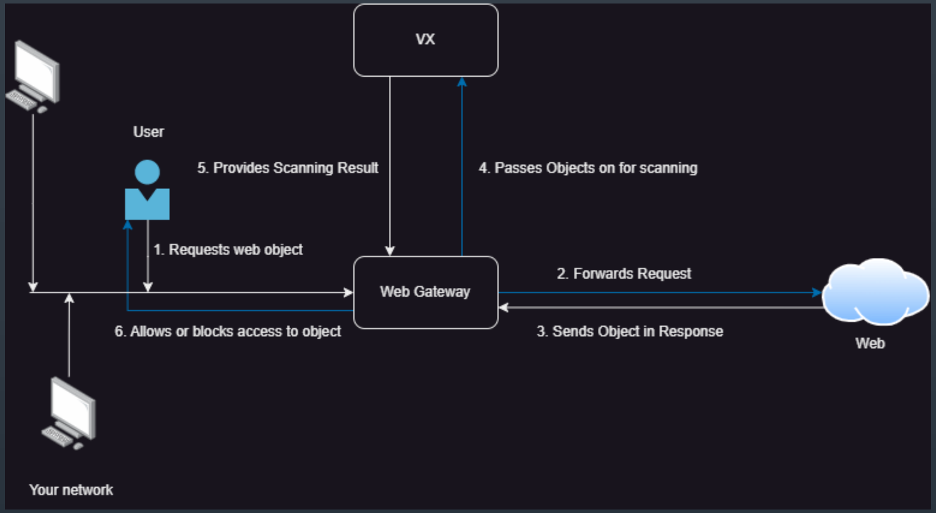
Targeted for Enterprise Applications

- Organizations focused on digitizing their extended enterprise value chain
- Integrates with enterprise applications
- Mitigate the risk of working with external organizations and vendors
- **Products: Trellix IVX Cloud**
  **Trellix File Protect**

# 3rd Party Integrations: Trellix IVX

## Skyhigh SWG for On-Prem and SWG for Cloud

Q3 2024


VX
User
5. Provides Scanning Result
4. Passes Objects on for scanning
1. Requests web object
Web Gateway
2. Forwards Request
3. Sends Object in Response
6. Allows or blocks access to object
Web
Your network

Trellix

| SWG for On-Prem | Q3, 2023 ⟷ | IVX Appliance |
|---|---|---|
| SWG for Cloud | Q3, 2024 ⟷ | IVX Cloud |

## Adds support for new Trellix IVX Appliances and IVX Cloud

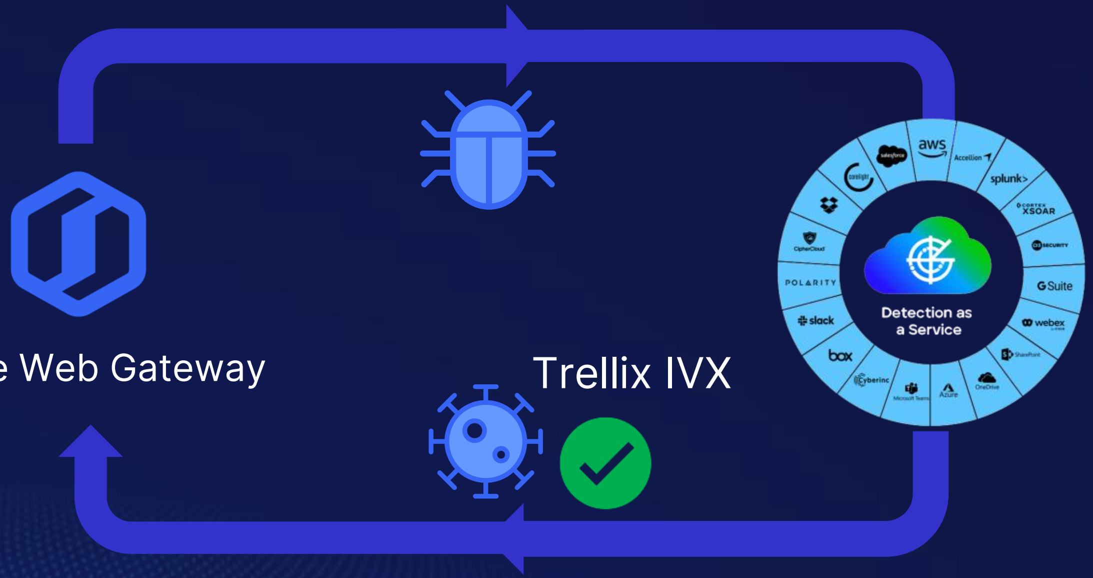
- SWG can easily integrate with Trellix IVX appliances and and IVX cloud services to protect against Zero-Day and Advanced Persistent Threats (APT)
- Seamless integration of SWG On-Prem appliances with IVX appliances like legacy ATD and SWG for Cloud with IVX Cloud

Trellix | Skyhigh Security

# Skyhigh Security + Trellix Provide Comprehensive Anti Malware protection

Threat detection sandbox that pinpoints known and unknown malware

Files/content submitted for additional malware analysis



Secure Web Gateway

Trellix IVX

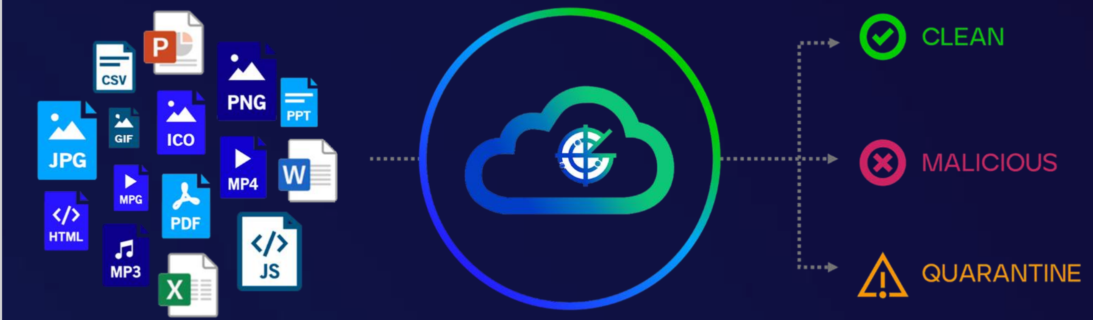
Verdicts are sent back after analysis

## Trellix Intelligent Virtual Execution (IVX)

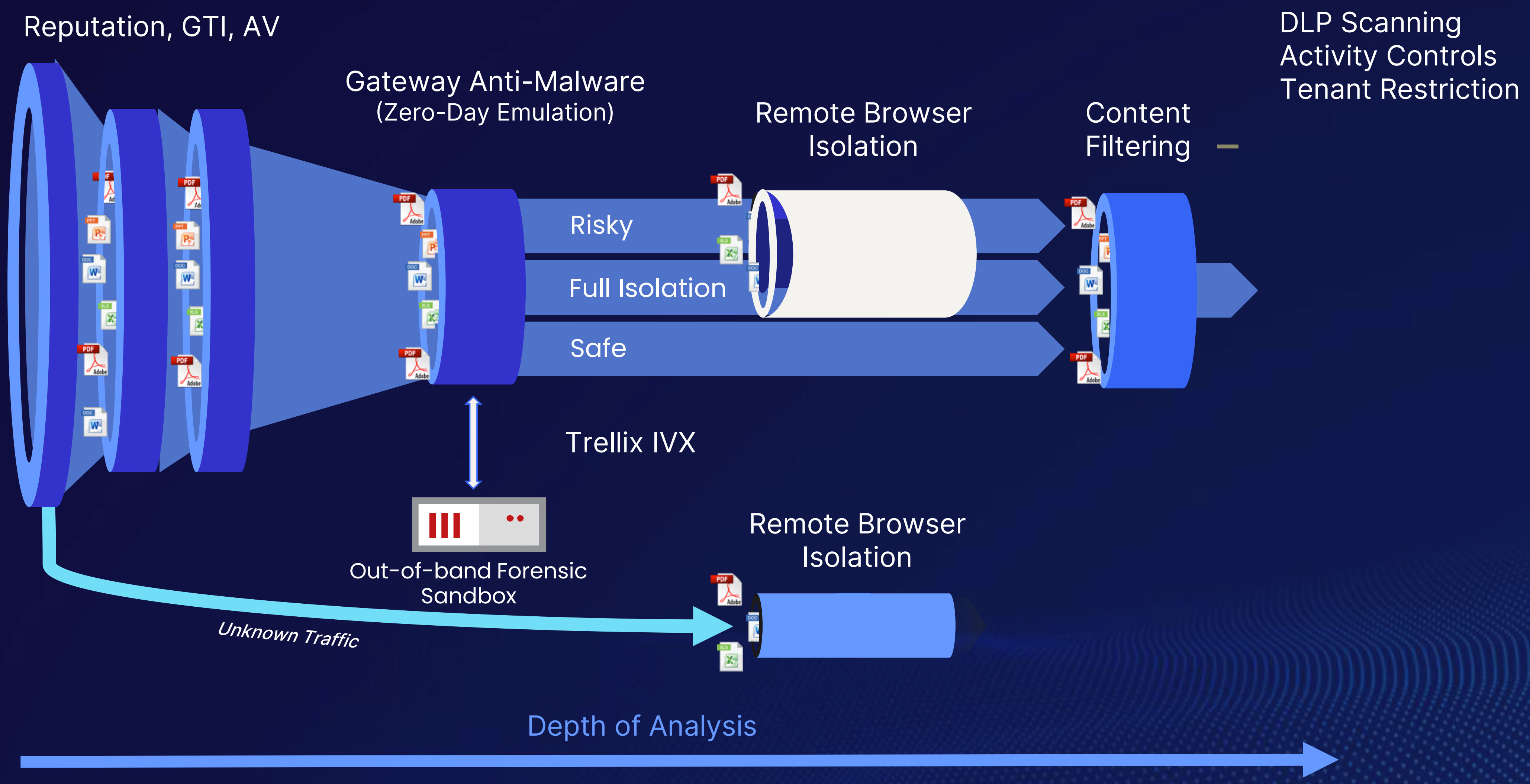
200 Supported File Types

Comprehensive, multi-layered detection

Verdict

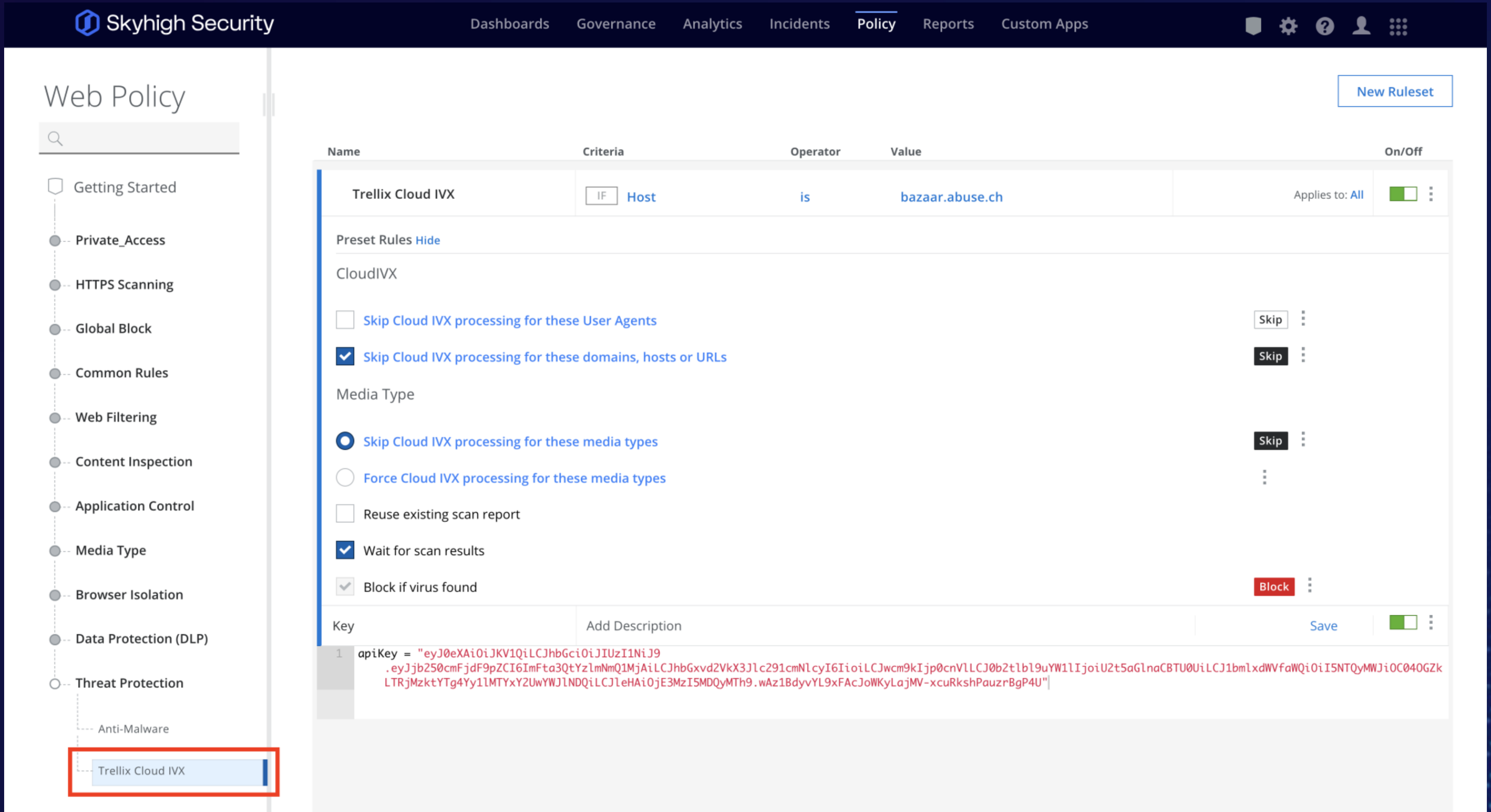


# Multi-Layered Inspection



# Skyhigh SSE - Trellix IVX Cloud Integration

Q2
2024



| Name | Criteria | Operator | Value | On/Off |
|---|---|---|---|---|
| Trellix Cloud IVX | IF Host | is | bazaar.abuse.ch | Applies to: All |

Preset Rules Hide

CloudIVX

- ☐ Skip Cloud IVX processing for these User Agents — Skip
- ☑ Skip Cloud IVX processing for these domains, hosts or URLs — Skip

Media Type

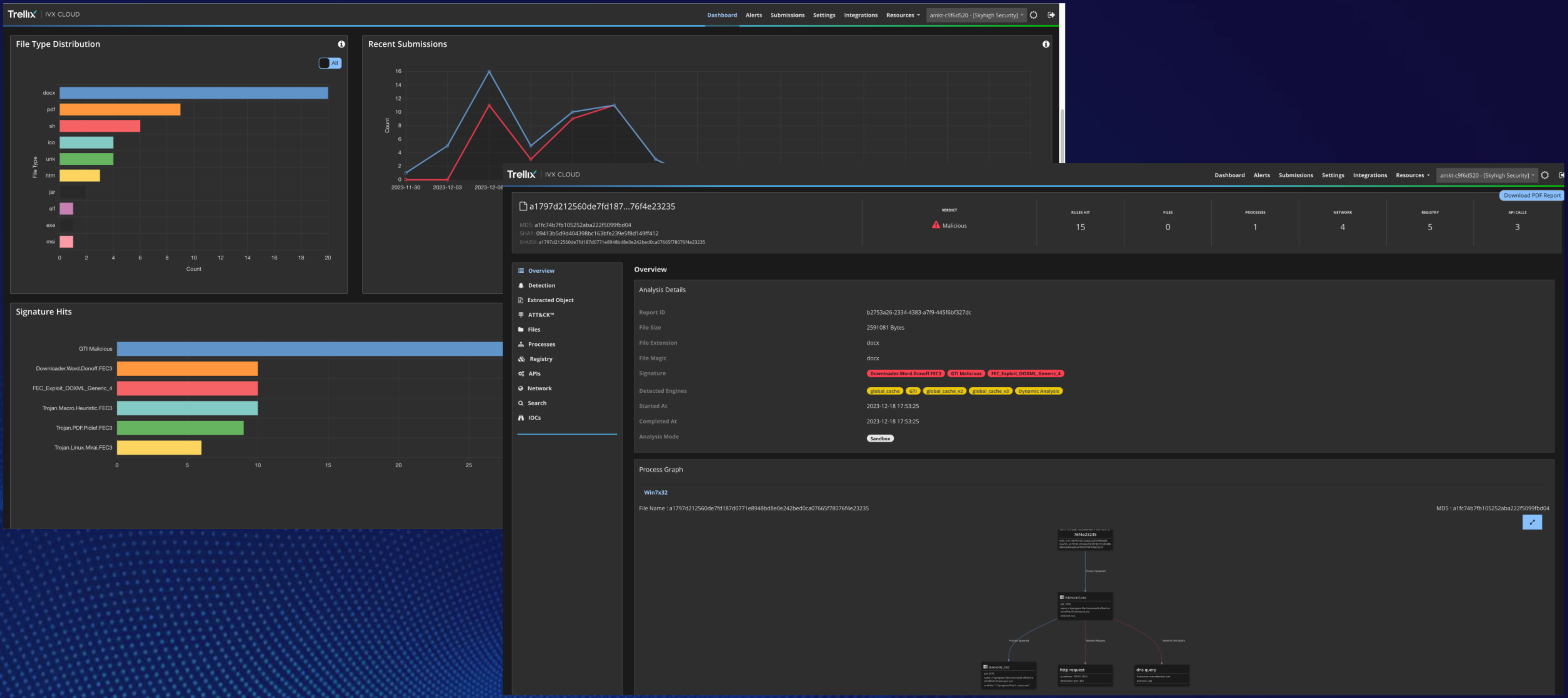
- ● Skip Cloud IVX processing for these media types — Skip
- ○ Force Cloud IVX processing for these media types
- ☐ Reuse existing scan report
- ☑ Wait for scan results
- ✓ Block if virus found — Block

Key — Add Description — Save

```
apiKey = "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
    .eyJjb250cmFjdF9pZCI6ImFta3QtYzlmNmQ1MjAiLCJhbGxvd2VkX3Jlc291cmNlcyI6IioiLCJwcm9kIjp0cnVlLCJ0b2tlbl9uYW1lIjoiU2t5aGlnaCBTU0UiLCJ1bmlxdWVfaWQiOiI5NTQyMWJiOC040GZk
    LTRjMzktYTg4Yy1lMTYxY2UwYWJlNDQiLCJleHAiOjE3MzI5MDQyMTh9.wAz1BdyvYL9xFAcJoWKyLajMV-xcuRkshPauzrBgP4U"
```

Trellix | Skyhigh Security

# Skyhigh SSE - Trellix IVX Cloud Integration



a1797d212560de7fd187...76f4e23235

MD5: a1fc74b7fb105252aba222f5099fbd04
SHA1: 09413b5d9d404398bc163bfe239e5f8d149ff412
SHA256: a1797d212560de7fd187d0771e8948bd8e0e242bed0ca07665f78076f4e23235

| VERDICT | RULES HIT | FILES | PROCESSES | NETWORK | REGISTRY | API CALLS |
|---|---|---|---|---|---|---|
| Malicious | 15 | 0 | 1 | 4 | 5 | 3 |

Overview

Analysis Details

| | |
|---|---|
| Report ID | b2753a26-2334-4383-a7f9-445f6bf327dc |
| File Size | 2591081 Bytes |
| File Extension | docx |
| File Magic | docx |
| Signature | Downloader.Word.Donoff.FEC3 GTI Malicious FEC_Exploit_OOXML_Generic_4 |
| Detected Engines | global_cache GTI global_cache_v2 global_cache_v3 Dynamic Analysis |
| Started At | 2023-12-18 17:53:25 |
| Completed At | 2023-12-18 17:53:25 |
| Analysis Mode | Sandbox |

Process Graph

Win7x32

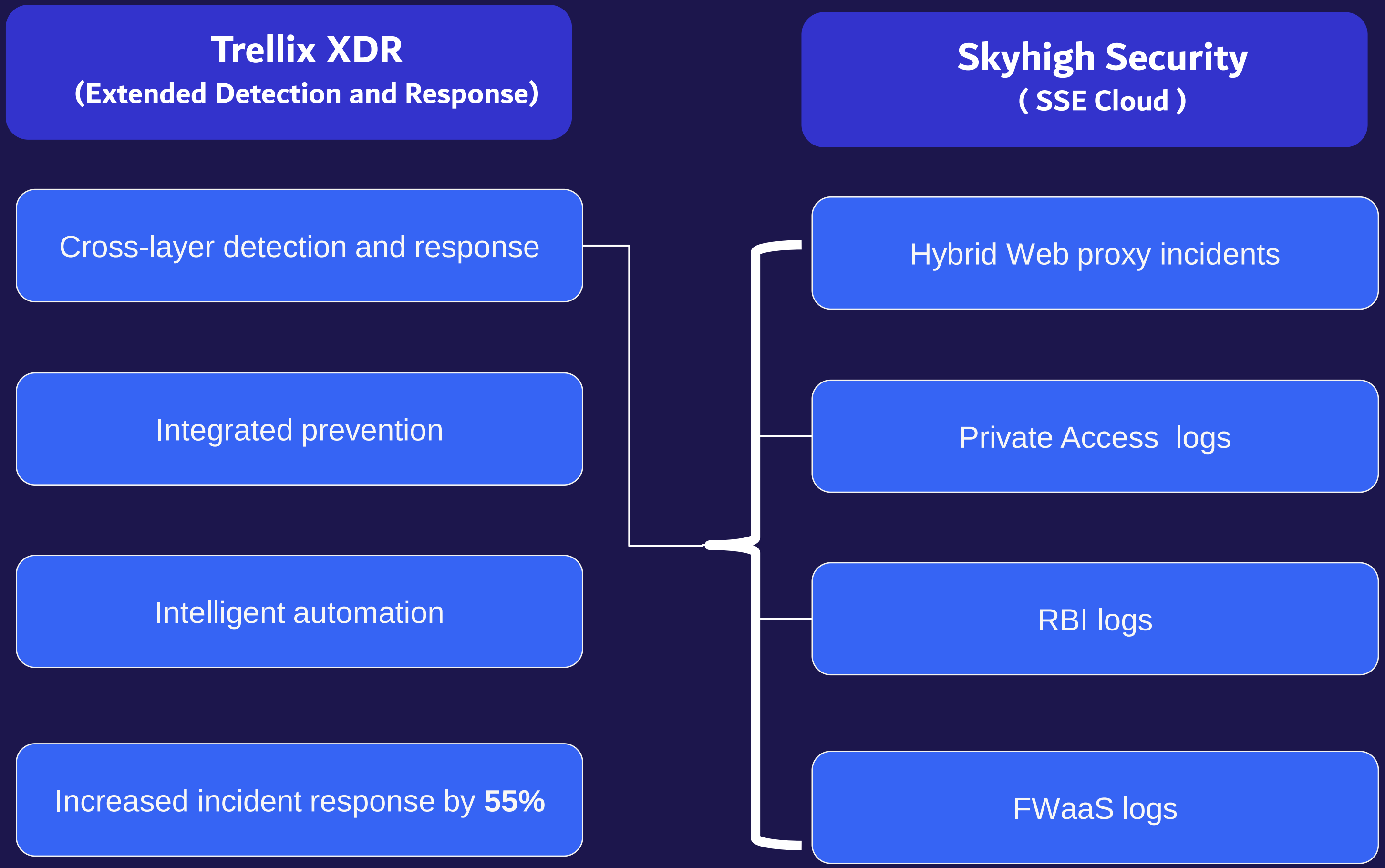
File Name : a1797d212560de7fd187d0771e8948bd8e0e242bed0ca07665f78076f4e23235

MD5 : a1fc74b7fb105252aba222f5099fbd04

Trellix | Skyhigh Security

# Skyhigh SSE – Trellix Hellix  (XDR) integration

# Skyhigh Security and Trellix XDR



**Trellix XDR**
**(Extended Detection and Response)**

Cross-layer detection and response

Integrated prevention

Intelligent automation

Increased incident response by **55%**

**Skyhigh Security**
**( SSE Cloud )**

Hybrid Web proxy incidents

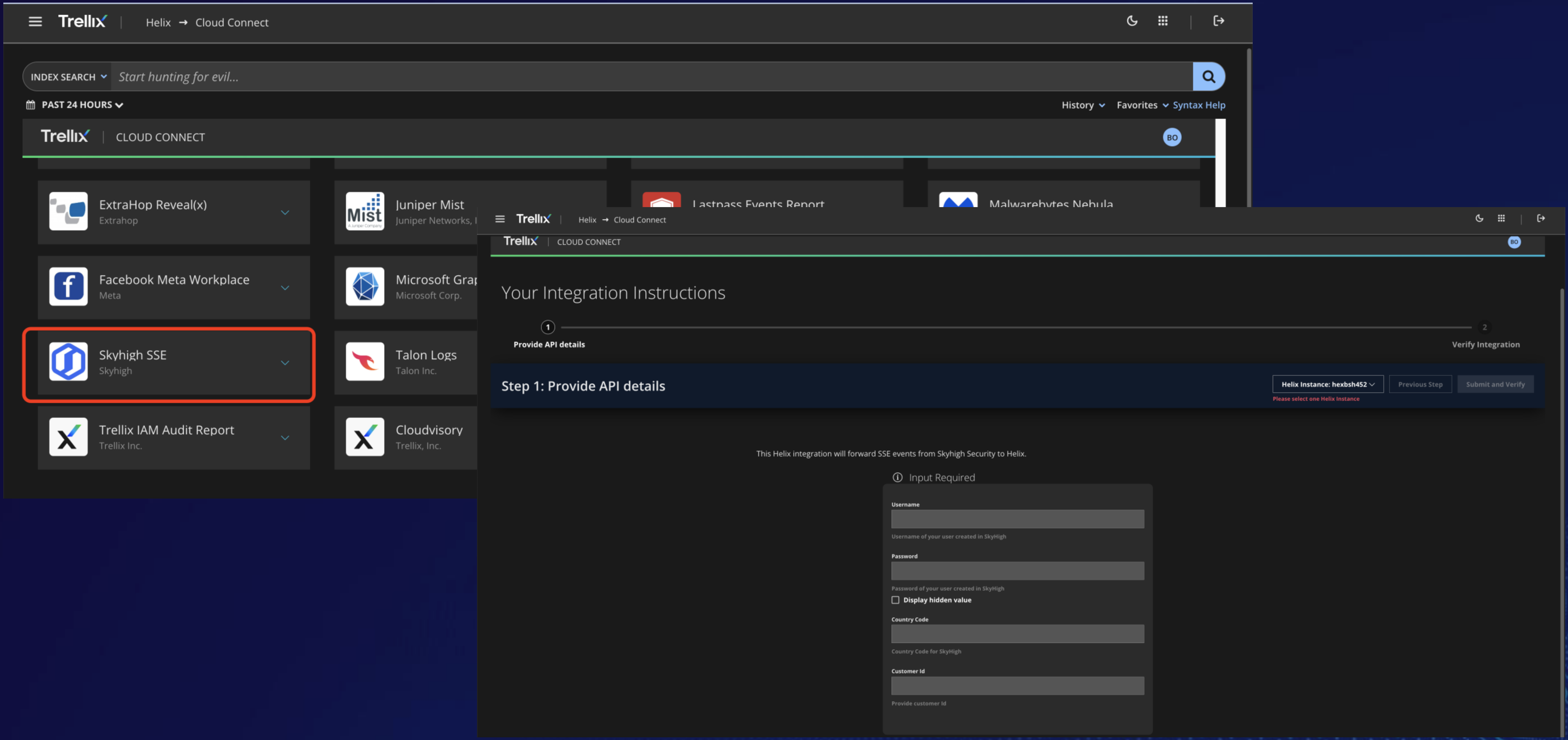
Private Access logs

RBI logs

FWaaS logs

Trellix | Skyhigh Security

# Native API Integration



Your Integration Instructions

1 Provide API details

2 Verify Integration

Step 1: Provide API details

Please select one Helix Instance

This Helix integration will forward SSE events from Skyhigh Security to Helix.

Input Required

Username

Username of your user created in SkyHigh

Password

Password of your user created in SkyHigh

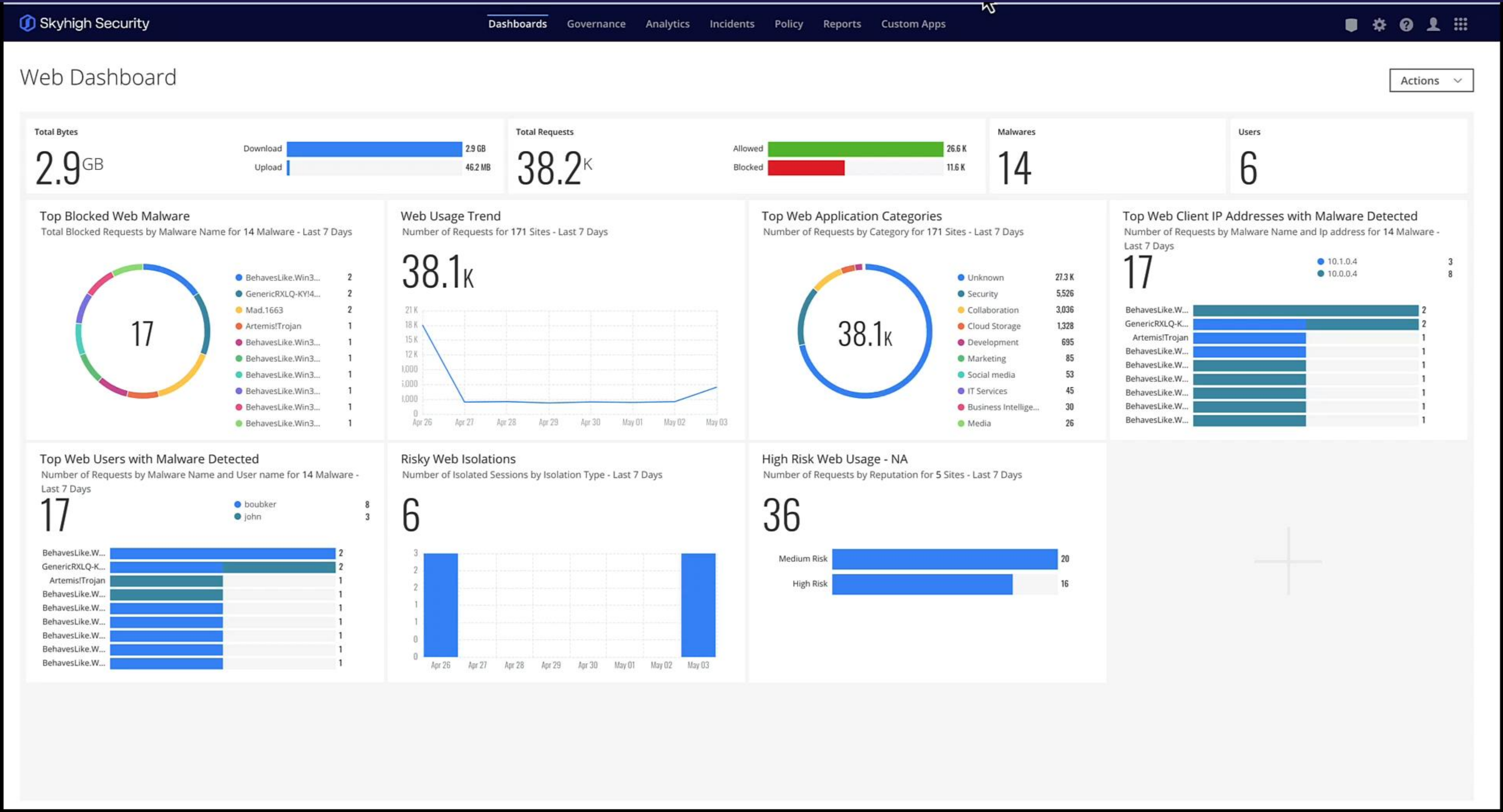
□ Display hidden value

Country Code

Country Code for SkyHigh

Customer Id

Provide customer Id



# Web Dashboard

| Total Bytes | | |
|---|---|---|
| 2.9GB | Download | 2.9 GB |
| | Upload | 46.2 MB |

| Total Requests | | |
|---|---|---|
| 38.2K | Allowed | 26.6 K |
| | Blocked | 11.6 K |

Malwares

14

Users

6

## Top Blocked Web Malware

Total Blocked Requests by Malware Name for 14 Malware - Last 7 Days

17

| | |
|---|---|
| BehavesLike.Win3... | 2 |
| GenericRXLQ-KY!4... | 2 |
| Mad.1663 | 2 |
| Artemis!Trojan | 1 |
| BehavesLike.Win3... | 1 |
| BehavesLike.Win3... | 1 |
| BehavesLike.Win3... | 1 |
| BehavesLike.Win3... | 1 |
| BehavesLike.Win3... | 1 |
| BehavesLike.Win3... | 1 |

## Web Usage Trend

Number of Requests for 171 Sites - Last 7 Days

38.1K

## Top Web Application Categories

Number of Requests by Category for 171 Sites - Last 7 Days

38.1K

| | |
|---|---|
| Unknown | 27.3 K |
| Security | 5,526 |
| Collaboration | 3,036 |
| Cloud Storage | 1,328 |
| Development | 695 |
| Marketing | 85 |
| Social media | 53 |
| IT Services | 45 |
| Business Intellige... | 30 |
| Media | 26 |

## Top Web Client IP Addresses with Malware Detected

Number of Requests by Malware Name and Ip address for 14 Malware - Last 7 Days

17

| | |
|---|---|
| 10.1.0.4 | 3 |
| 10.0.0.4 | 8 |

| | |
|---|---|
| BehavesLike.W... | 2 |
| GenericRXLQ-K... | 2 |
| Artemis!Trojan | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |

## Top Web Users with Malware Detected

Number of Requests by Malware Name and User name for 14 Malware - Last 7 Days

17

| | |
|---|---|
| boubker | 8 |
| john | 3 |

| | |
|---|---|
| BehavesLike.W... | 2 |
| GenericRXLQ-K... | 2 |
| Artemis!Trojan | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |
| BehavesLike.W... | 1 |

## Risky Web Isolations

Number of Isolated Sessions by Isolation Type - Last 7 Days

6

## High Risk Web Usage - NA

Number of Requests by Reputation for 5 Sites - Last 7 Days

36

| | |
|---|---|
| Medium Risk | 20 |
| High Risk | 16 |

# Skyhigh Security Value

## Secure Web Gateway + Cloud Access Security Broker + Zero Trust Network Access

- Secure access to the web, cloud services, and private applications
- Extend protection and data visibility into enterprise sanctioned applications
- Identify and protect data in use, in motion, and at rest to achieve compliance
- Protect from malware and identify compromised accounts and insider threats
- Enable a hybrid workforce
- Apply Zero Trust principles

# Next Steps

## Executive Briefing

Vision

Roadmap

Exec Peering

## Cloud Security Assessment

Current Posture

Recommendations

## Security Workshop

Digital Workplace

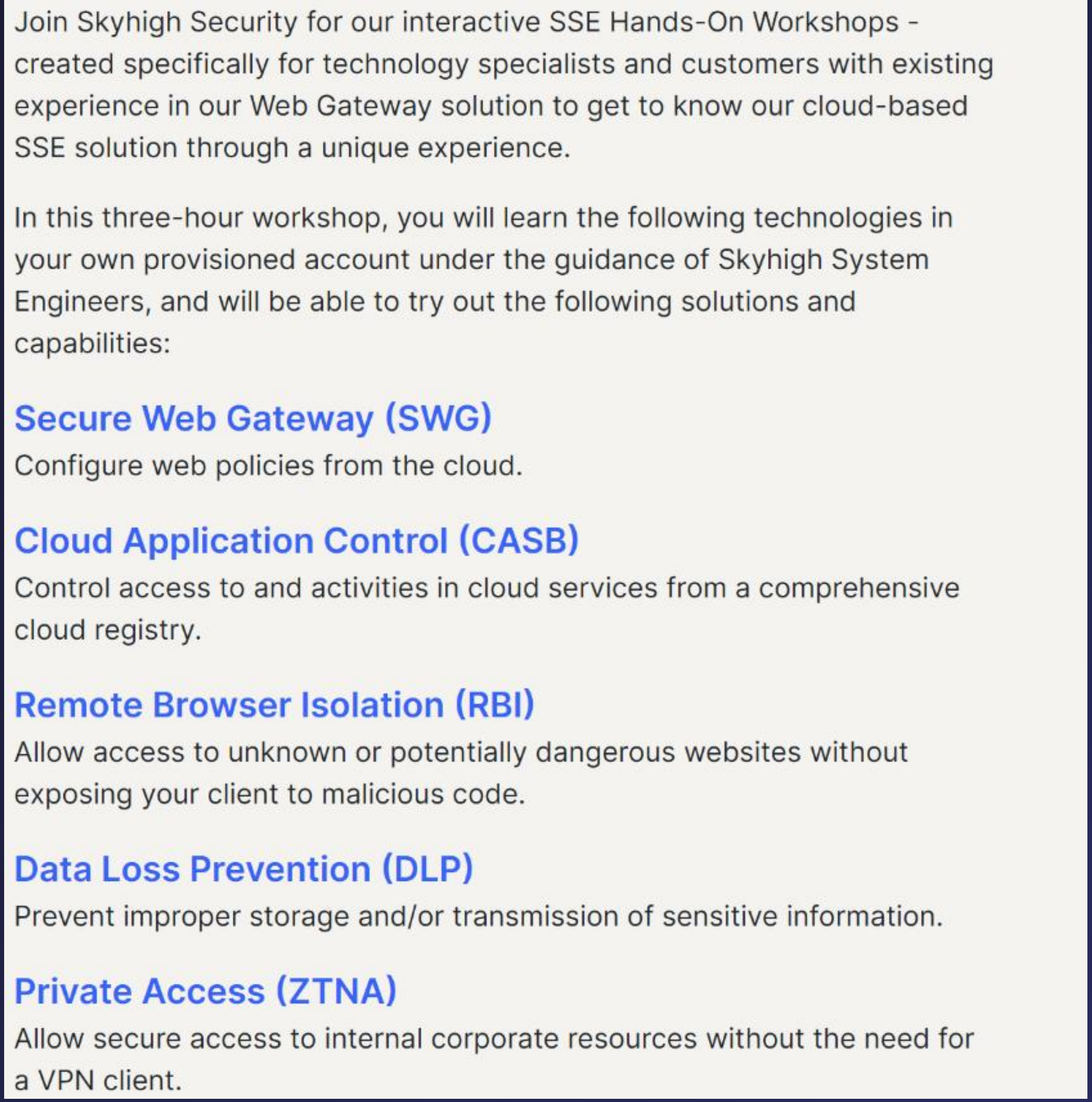
Cloud Architecture

Data Protection

Hands-on Labs

DLP/SSE/Hybrid

# Skyhigh SSE Hands-On Workshop



Join Skyhigh Security for our interactive SSE Hands-On Workshops - created specifically for technology specialists and customers with existing experience in our Web Gateway solution to get to know our cloud-based SSE solution through a unique experience.

In this three-hour workshop, you will learn the following technologies in your own provisioned account under the guidance of Skyhigh System Engineers, and will be able to try out the following solutions and capabilities:

### Secure Web Gateway (SWG)

Configure web policies from the cloud.

### Cloud Application Control (CASB)

Control access to and activities in cloud services from a comprehensive cloud registry.

### Remote Browser Isolation (RBI)

Allow access to unknown or potentially dangerous websites without exposing your client to malicious code.

### Data Loss Prevention (DLP)

Prevent improper storage and/or transmission of sensitive information.

### Private Access (ZTNA)

Allow secure access to internal corporate resources without the need for a VPN client.

Join us for our next SSE Hands-On Workshop to try out Skyhigh SSE yourself

Register here: https://www.skyhighsecurity.com/sse-virtual-workshop

# Thank You!

Trellix | Skyhigh Security