
FORTINET
COLOMBIA
& ECUADOR
XPERTS26

Ivonne Bastidas

Systems Engineer Colombia

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Shadow AI Track

Agenda

- Today’s Shadow AI Challenges
- Mitigating Shadow AI Risks
- Introducing FortiOS 8.0
- Introducing FortiDLP
- Introducing FortiCASB-SSPM
- Introducing FortiMail Browser Security

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Today’s GenAI Challenges

GenAI Tool Explosion - Today

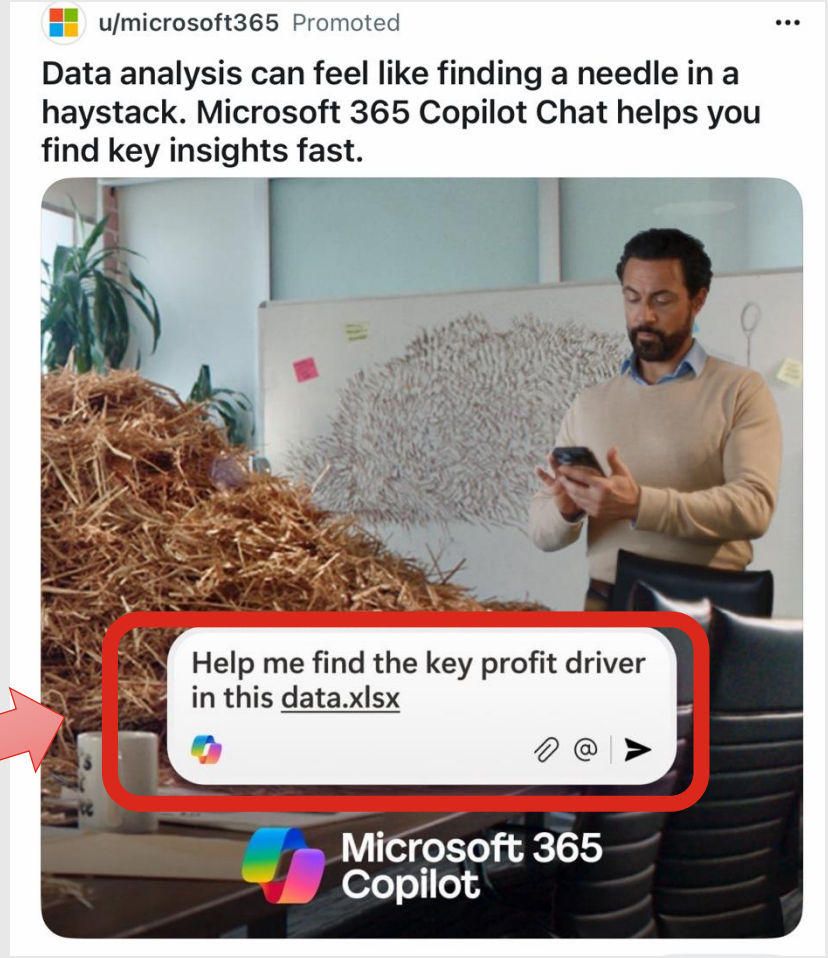
The Growing Problems of AI

"By 2025, generative AI usage among enterprise employees is near-universal, with over 90–98% of knowledge workers reporting some level of AI tool usage, and a majority using it regularly in daily workflows."

1. Alongside this growth came a rise in shadow AI. Today, over one-third (38%) of employees acknowledge sharing sensitive work information with AI tools without their employers' permission.

2. Shadow AI can expose companies to several risks including data leakage, fines for noncompliance and severe reputational damage:

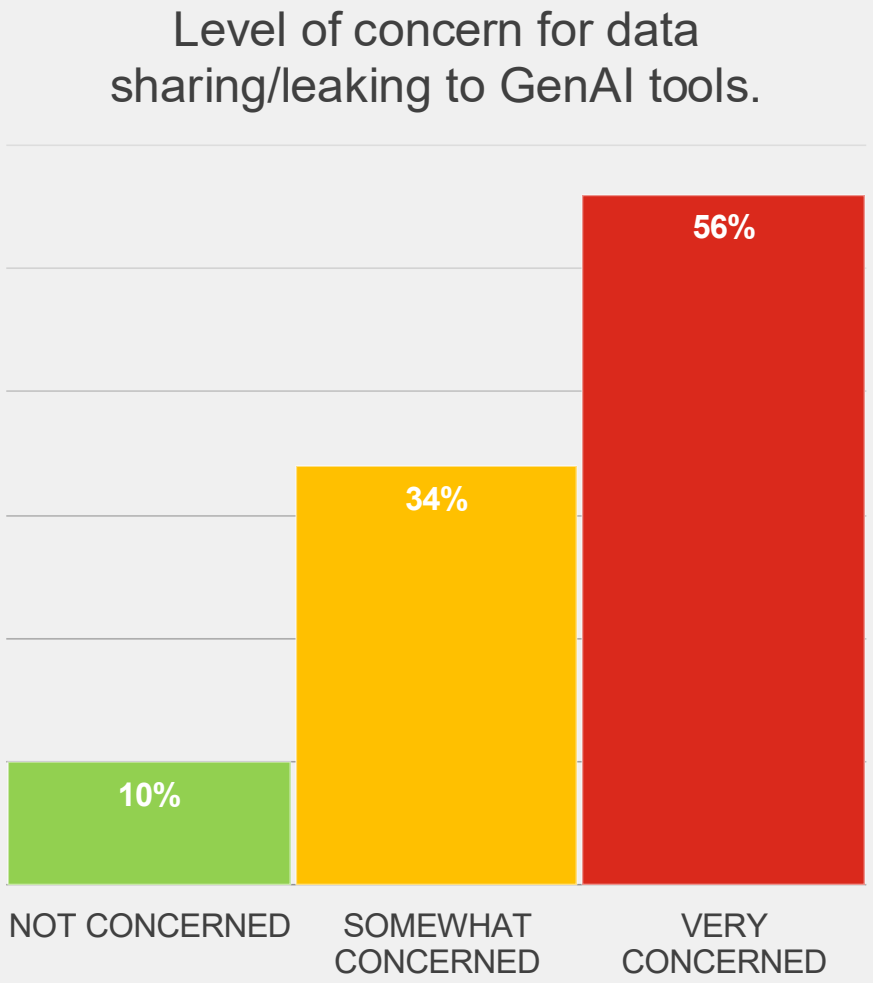
Your Data is very Welcome!!

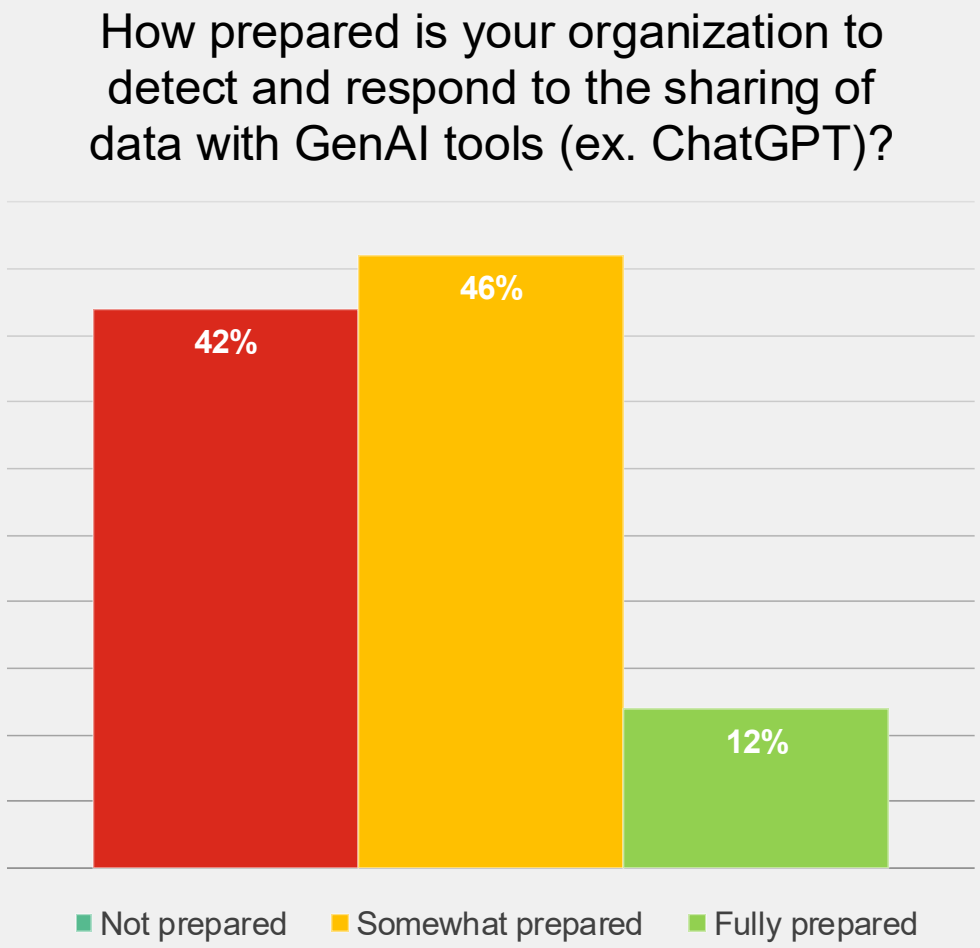


based on 2025 industry reports from firms like McKinsey, Gartner, and Microsoft Work Trend Index

Sentiments Regarding GenAI

2025 Data/Insider Risk Reports

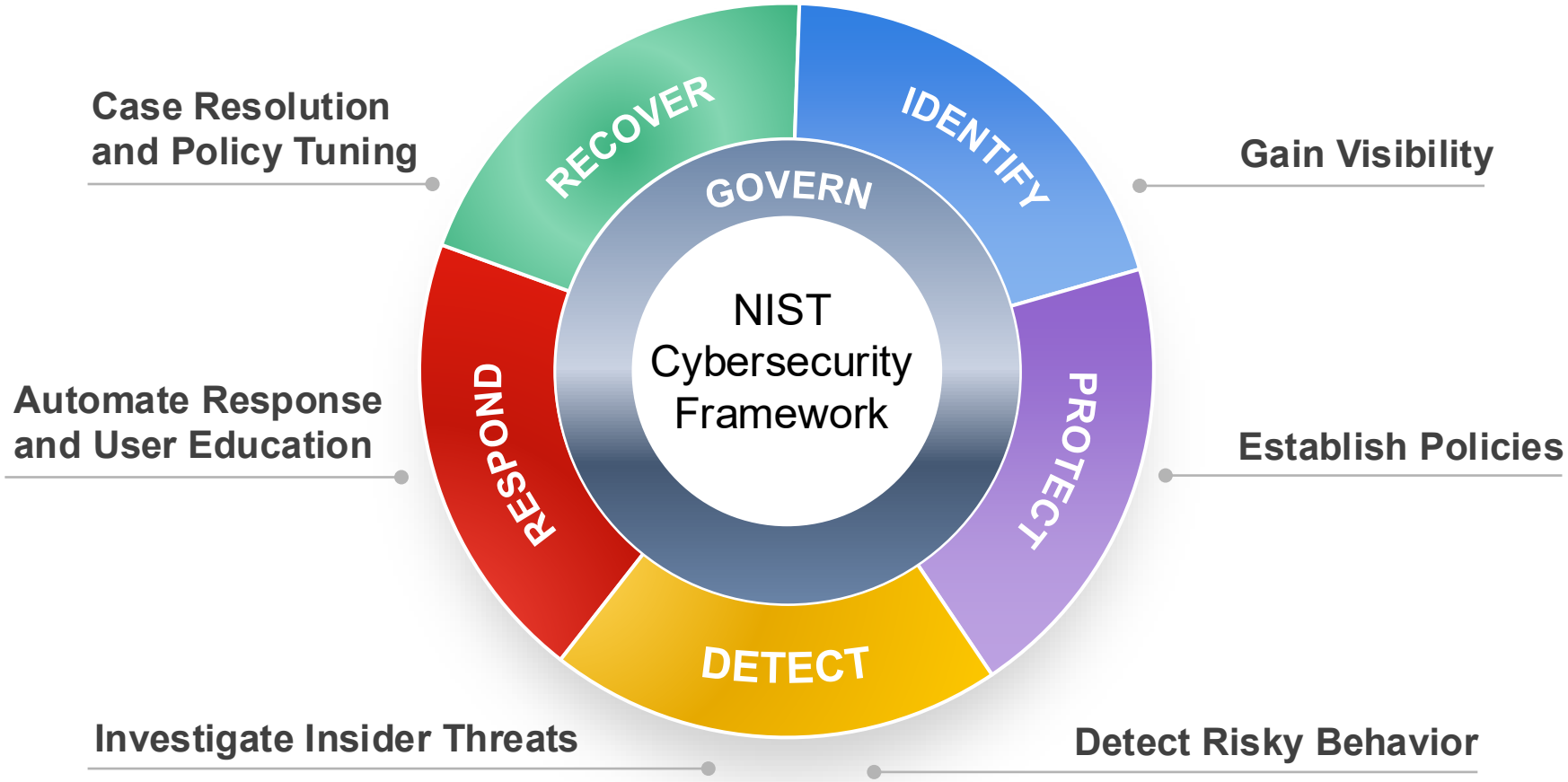




Mitigating Shadow AI Risk

Applying the NIST Framework to Mitigate GenAI Risk

Educate Users on Proper Data Handling Including GenAI Usage



Mitigating Shadow AI Risk

To get to a strong security posture with shadow AI, it's best to deploy the following combination of security solutions, configured for the anti-shadow AI use case. Here's why **Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) & SaaS Posture Management (SSPM)** are critical in this context.

- Visibility Into What AI Tools Are Actually Being Used
- Data Leakage Prevention
- Access & Permission Governance
- Compliance & Regulatory Risk
- Configuration & Security Posture of Approved AI Tools
- Policy Enforcement at Scale

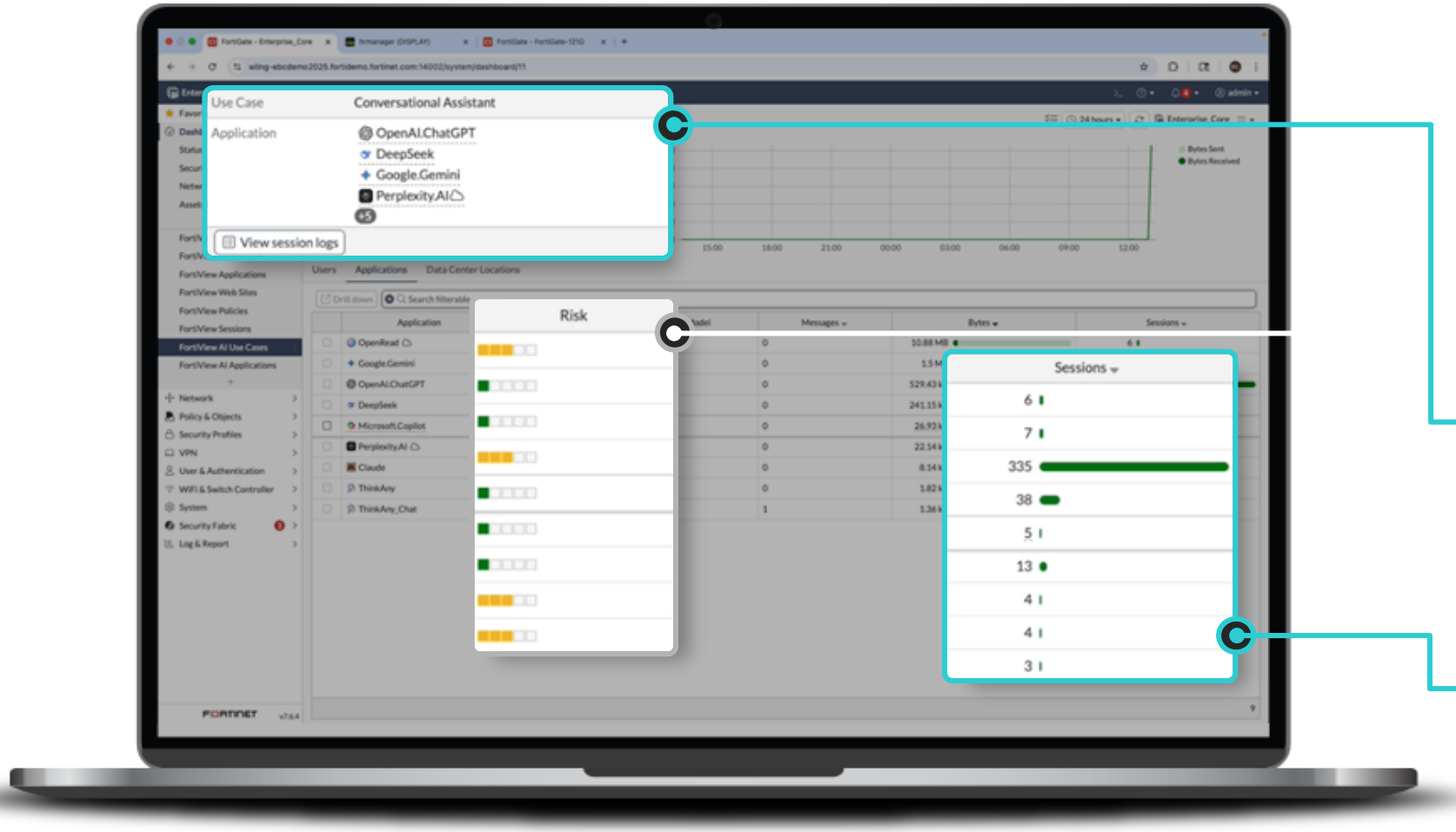
FORTINET | COLOMBIA & ECUADOR

XPERTS26

FortiOS 8.0

Assessing GenAI Risk

Granular visibility into risk and usage

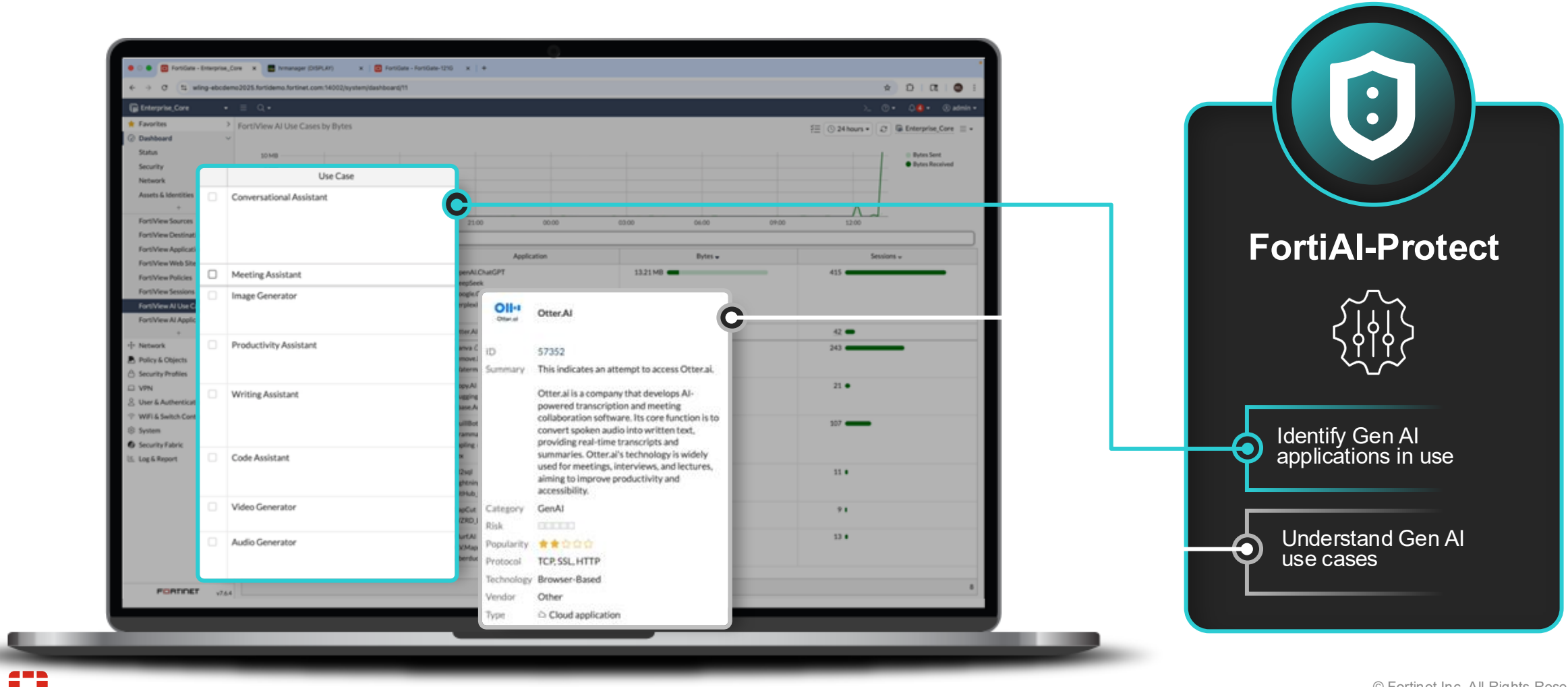


FortiAI-Protect

- Comprehensive Log Details
- Know risk level by Gen AI application
- Session Details

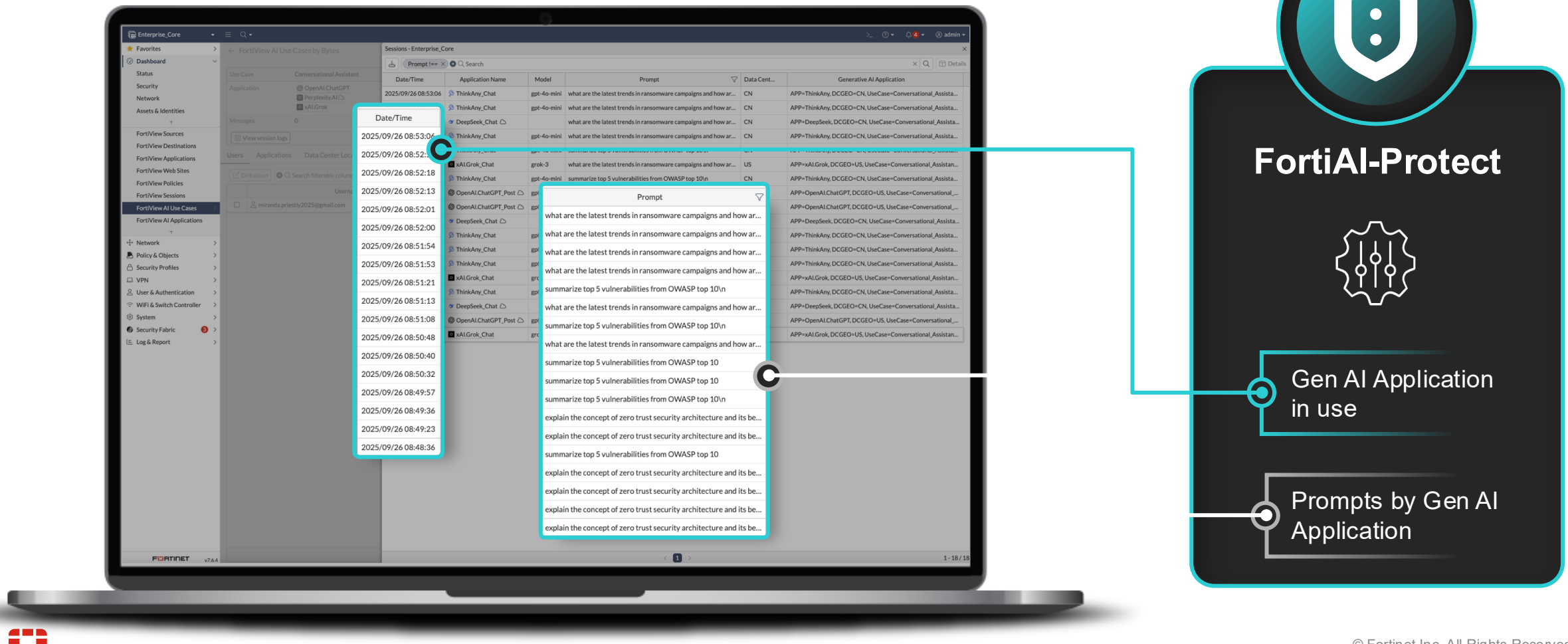
Assessing GenAI Risk

Know what is running by categories



Assessing GenAI Risk

Identify and Block unauthorized prompts by Gen AI Application



FORTINET | COLOMBIA & ECUADOR

XPERTS26

FortiDLP

Fortinet Solution

FortiAI-SecureAI
Secure LLM, AI Systems

Solution Specs

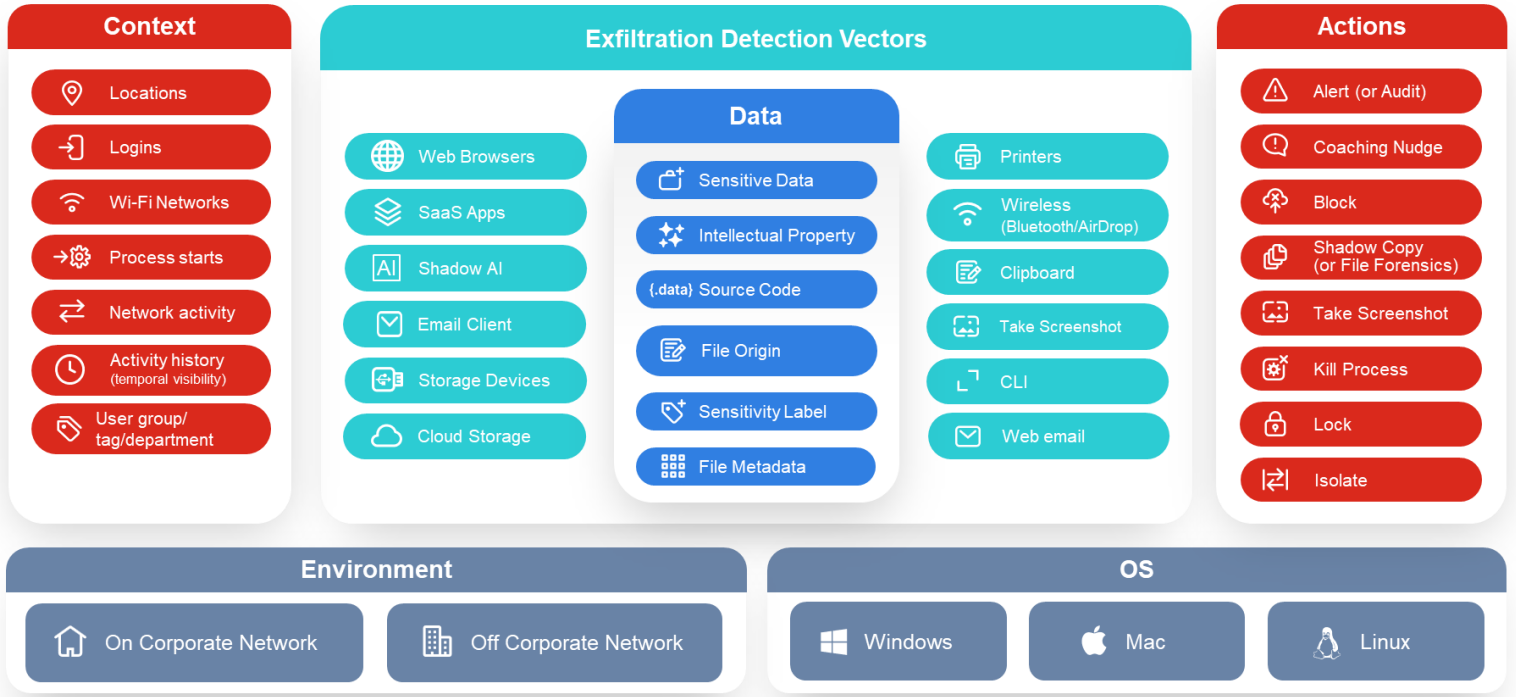
FortiDLP

Use Case:

Insider Risk Management +

Data Loss Prevention

- 4K Enterprise Licenses
- Best Practices Service



Visibility and Controls

Full visibility into business data flows combined with policy actions.

Stop Egress

Prevent exfil of IP/source code across multiple points. Experience with a prior incident.

Deep Forensics

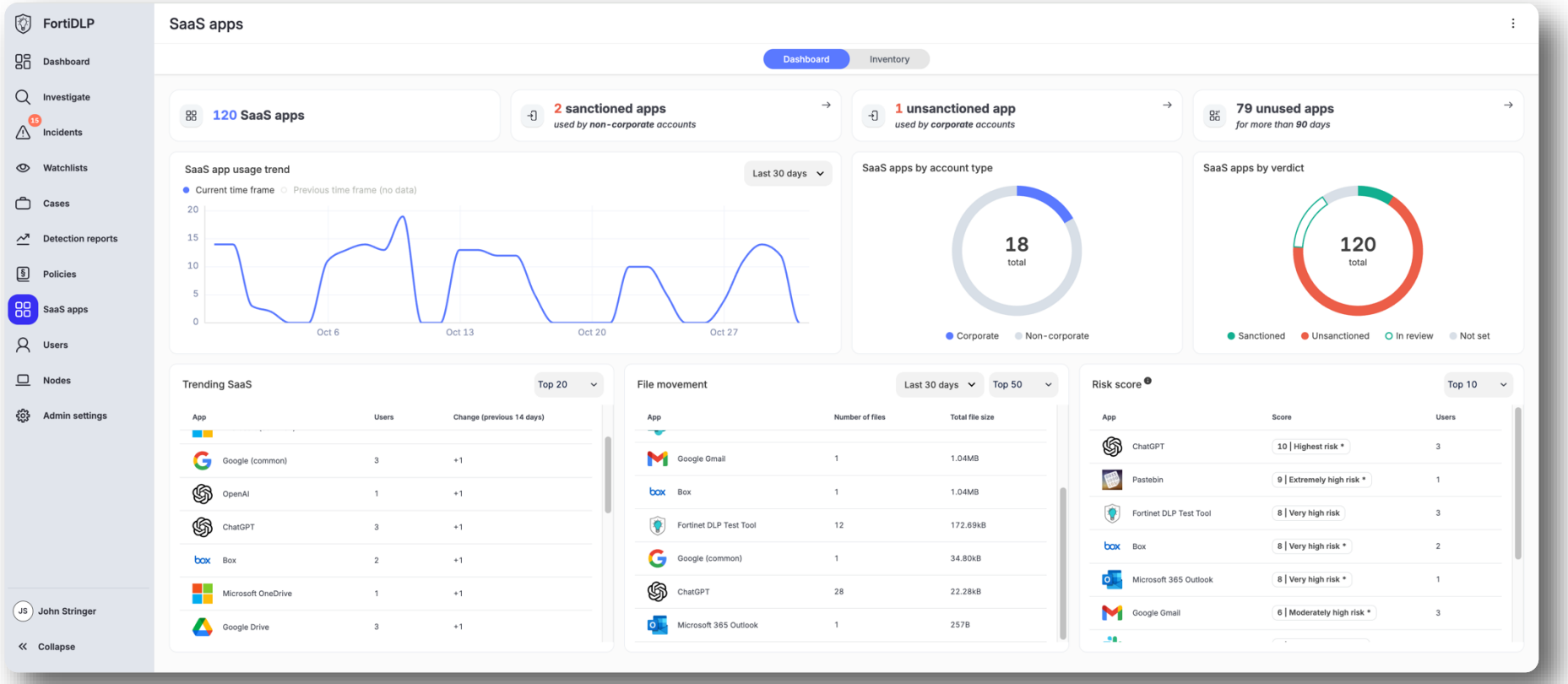
Enable forensics capture and investigation of potential insider threats and risks.

Gain Visibility into GenAI and SaaS App Usage

FortiAI-SecureAI
Secure LLM, AI Systems

IDENTIFY

Inventory and risk assessment of business data movement into GenAI and SaaS Apps



Automated GenAI and SaaS App Inventory

Classify Sanctioned vs. Unsanctioned Apps

Assess Risk Based on Data Movement

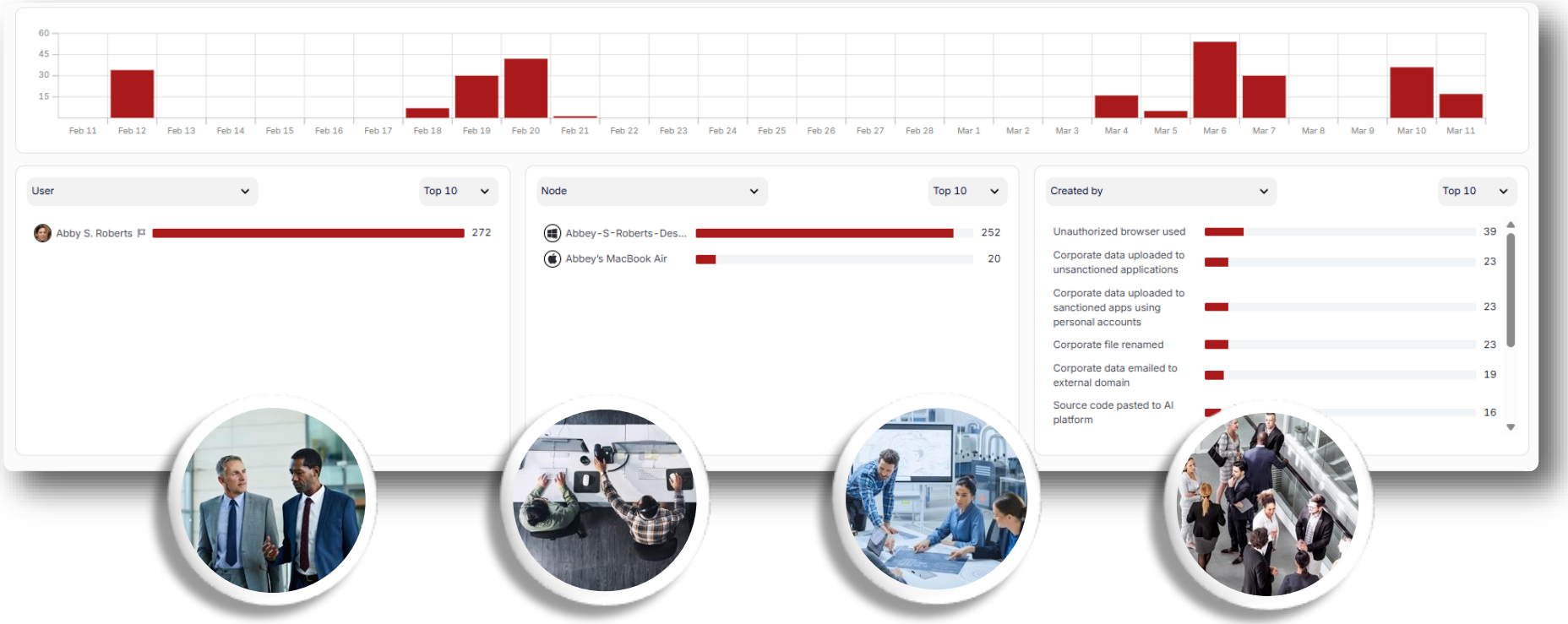
Prevent Data Loss to GenAI Apps

FortiAI-SecureAI
Secure LLM, AI Systems

PROTECT

Targeted policies prevent business data from being egressed via GenAI tools.

Allow authorized use.



Legal

Finance

Engineering

Sales

Automated GenAI and SaaS App Inventory

Classify Sanctioned vs. Unsanctioned Apps

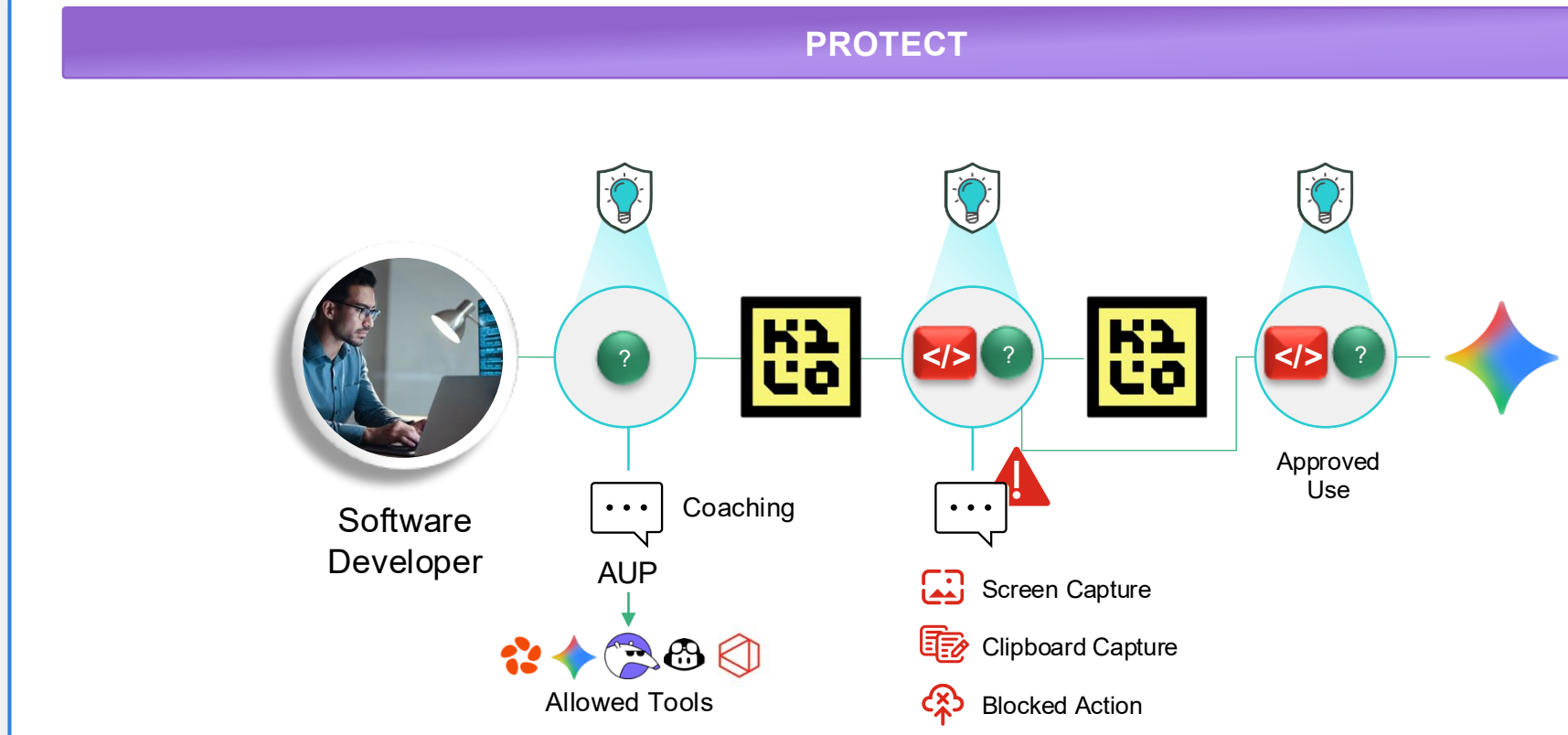
Assess Risk Based on Data Movement

Craft Policies Based on Usage and Business Inputs

FortiAI-SecureAI
Secure LLM, AI Systems

PROTECT

Create policies based on visibility and observed usage. Consult departments on specialized GenAI requirements.



Define Usage and Organizational Requirements

Establish Guardrails for Usage

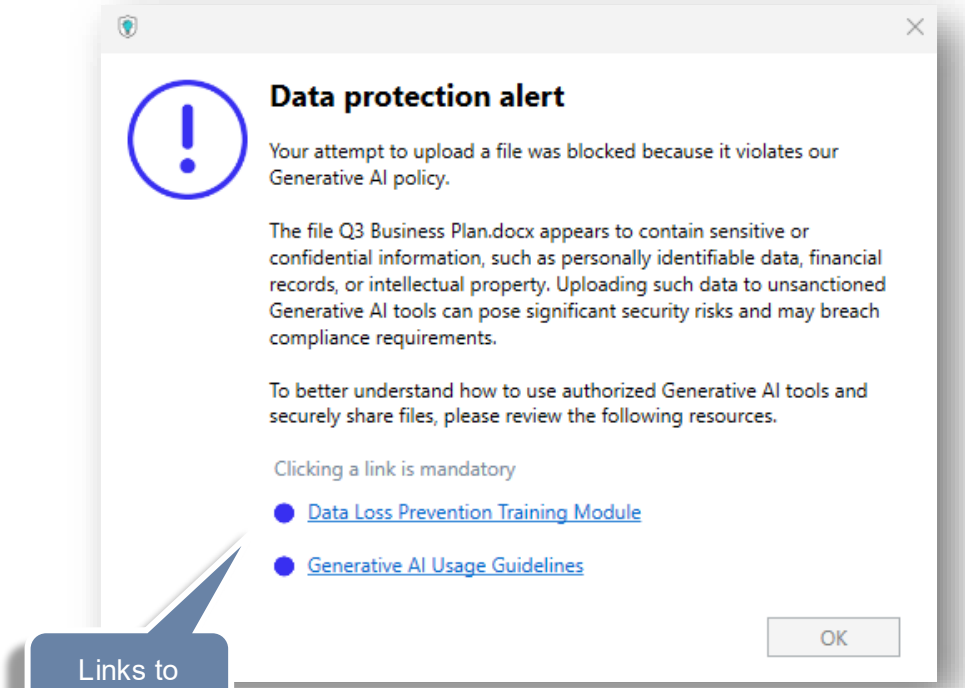
Automate Response Actions for Violations

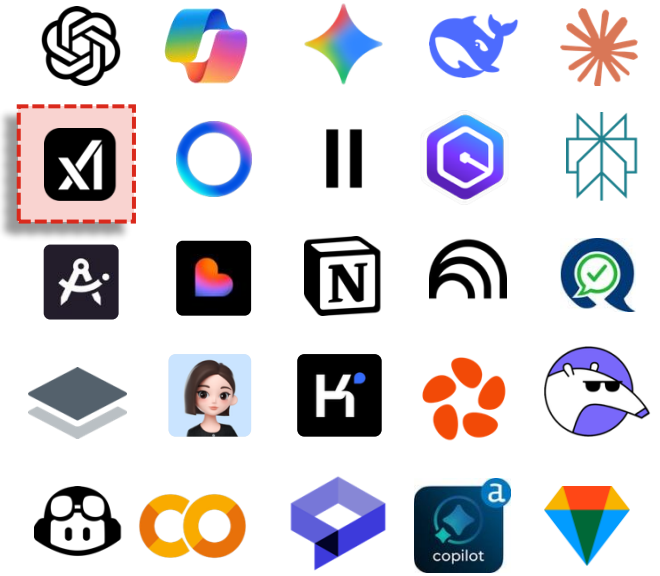
Educate Employees to Mitigate GenAI Data Loss Risk

FortiAI-SecureAI
Secure LLM, AI Systems

DETECT

Implement real-time risk-informed employee coaching with interactive response workflows.





Customizable Realtime Coaching

Interactive Response Workflow

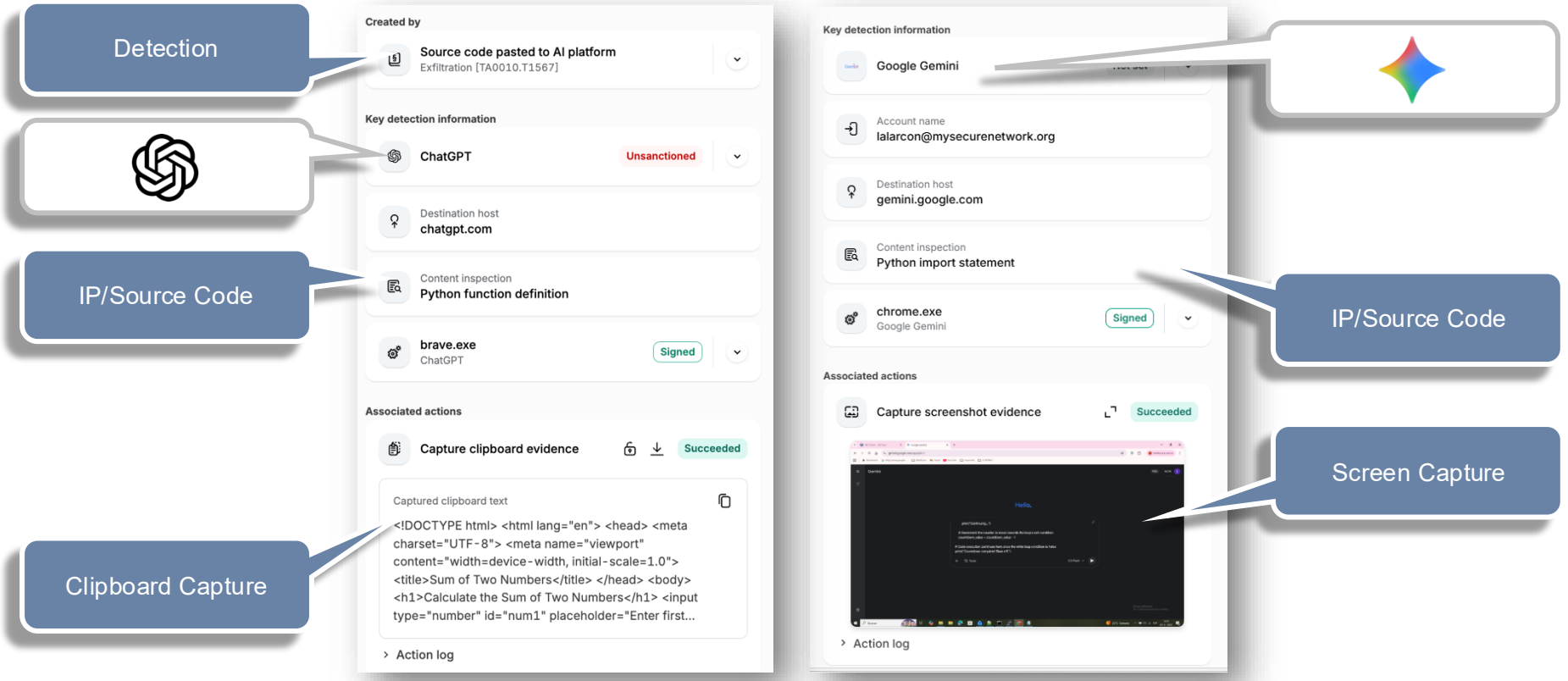
Endpoint, Teams and Slack

Capture Evidence to Accelerate Investigations

FortiAI-SecureAI
Secure LLM, AI Systems

RESPOND

The investigator can access rich evidence data sets securely stored in the customer's object storage solution.



Evidence Capture for File, Screen, and Clipboard

GenAI Prompt Capture [coming soon]

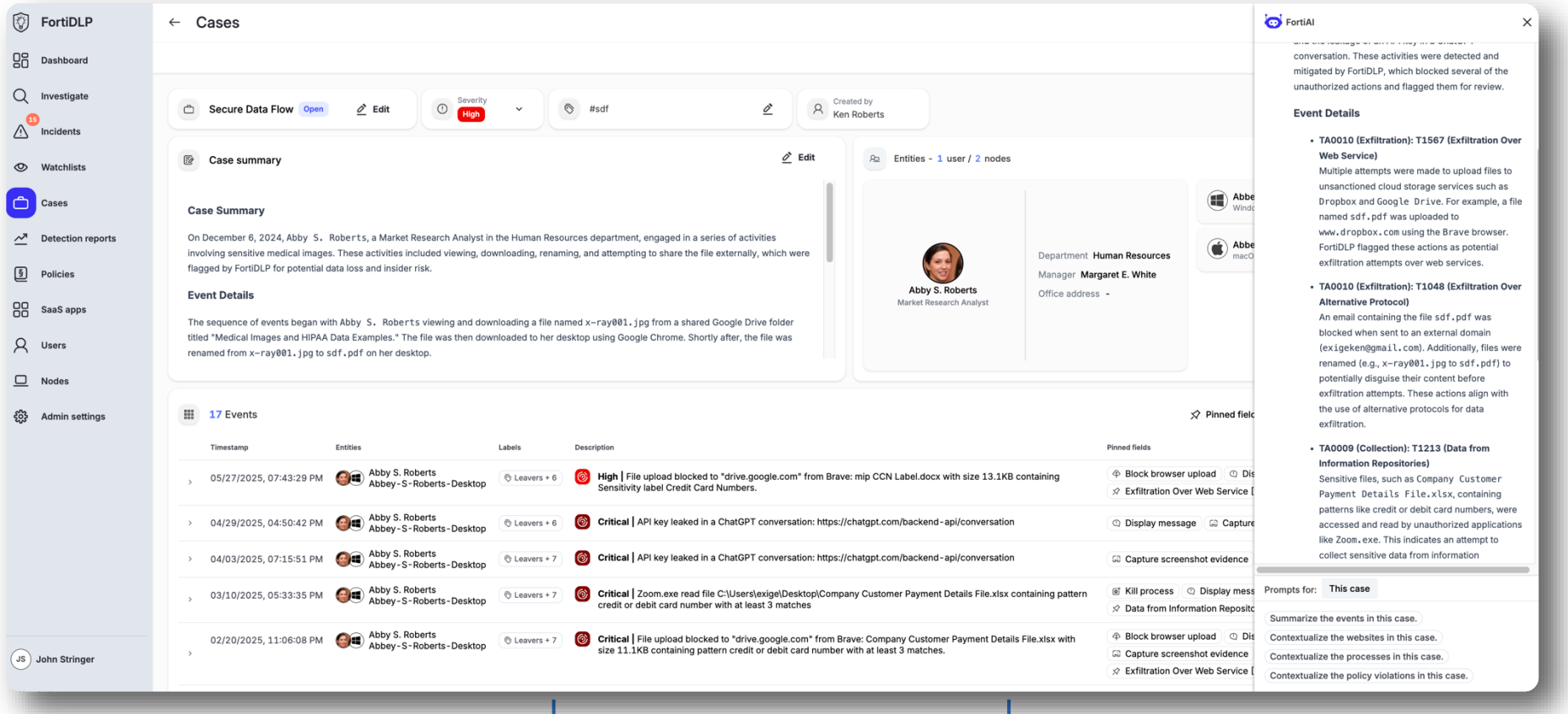
Enterprise Grade Privacy Controls

FortiAI Assist Summarizes and Contextualizes Cases

FortiAI-SecureAI
Secure LLM, AI Systems

RESPOND

Leverage FortiAI Assist to summarize and contextualize observed high-risk user activity.



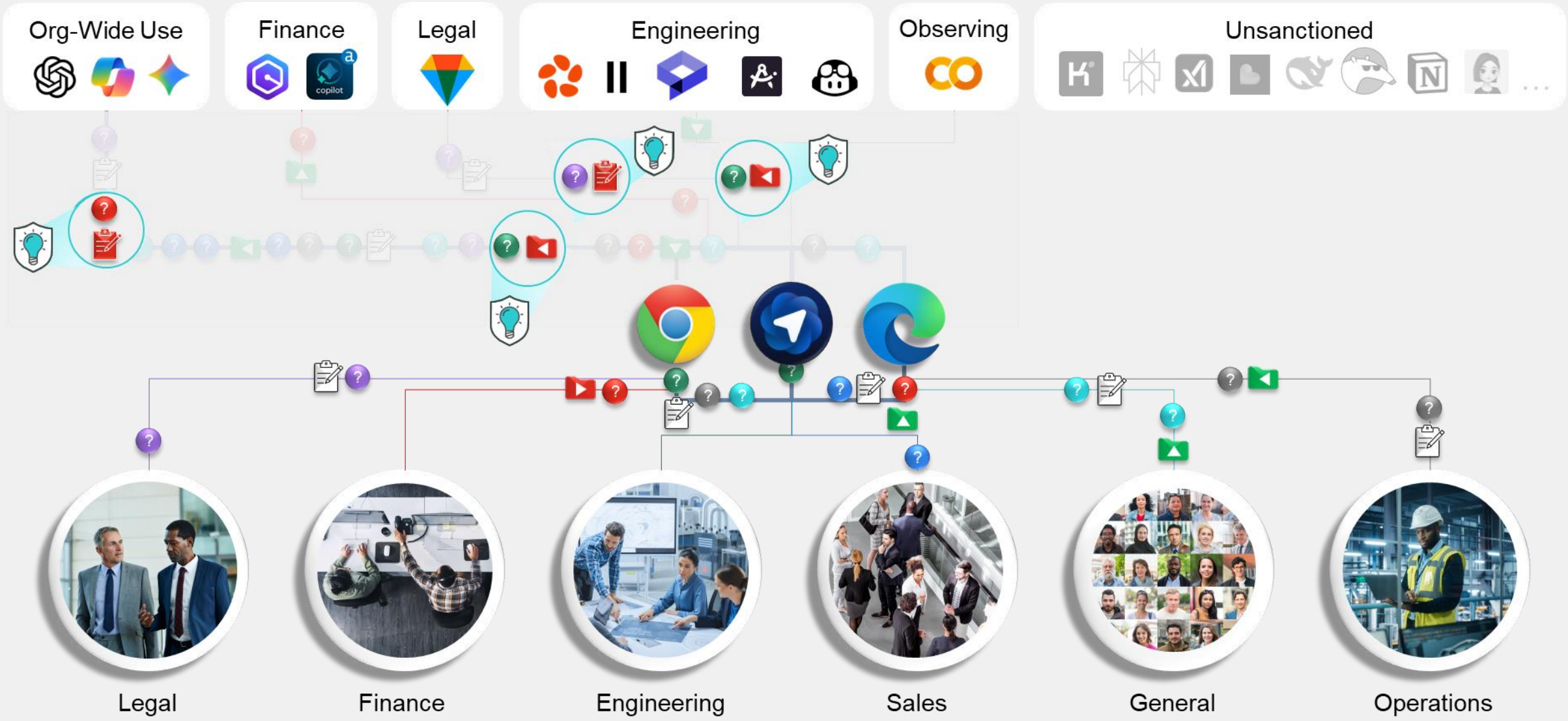
Automated Insider Sequence Detection

MITRE ATT&CK® Mapped Detections

Integrated FortiAI Assistant

GenAI – What Managing Risk Can Look Like

FortiAI-SecureAI
Secure LLM, AI Systems



FORTINET | COLOMBIA & ECUADOR
XPERTS26

Workshop Time

AI Hands-on Labs

- **ESPAÑOL**
  https://latam.amerintlxperts.com/ai/ai-colombia/index.html
- **INGLES:**
  https://latam.amerintlxperts.com/ai/ai-colombia/Shadow-AI/index.html
  - User: amerintlxperts
  - Password: xPerts2026!

El usuario y contraseña para todo:

Username: fortiadmin

Password: XpertsLab-2026

Jorge Portilla

Systems Engineer Ecuador

FORTINET | COLOMBIA & ECUADOR

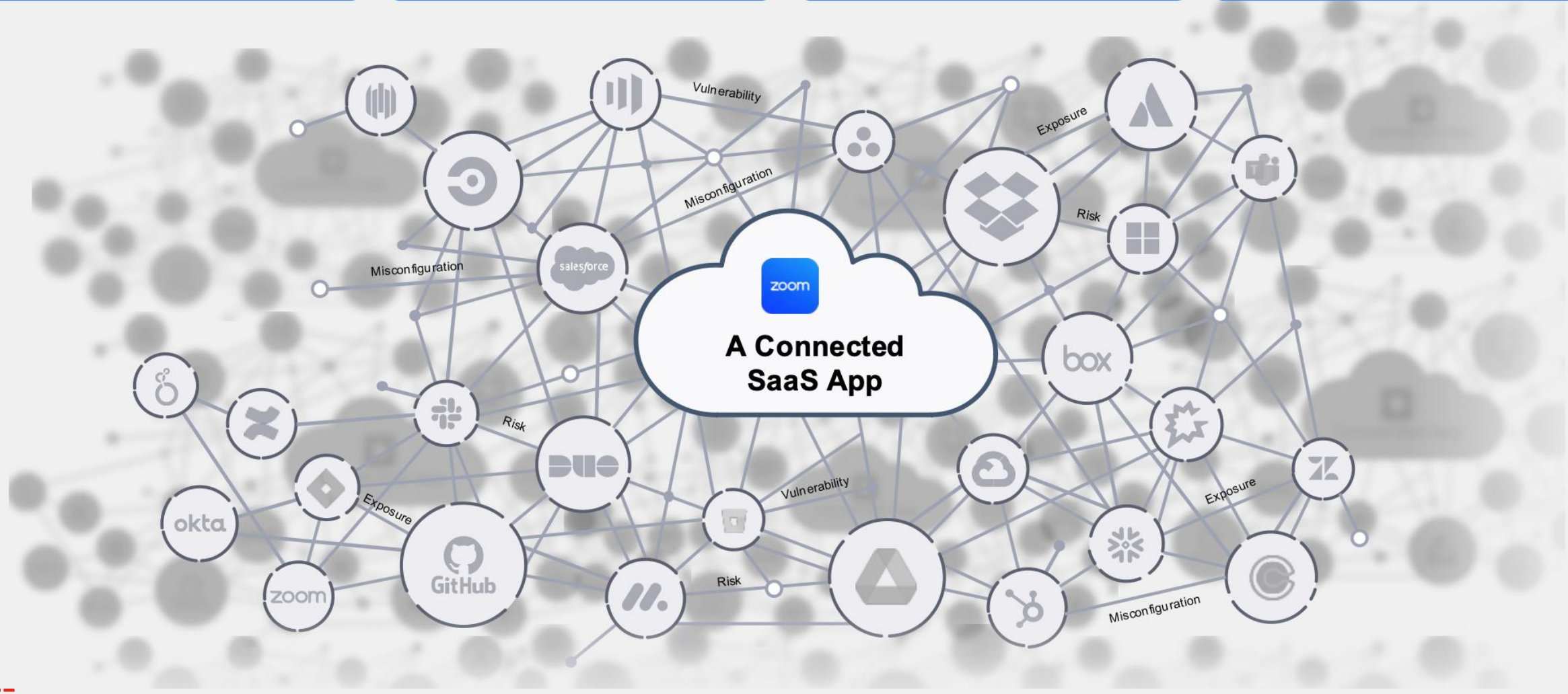
XPERTS26

FortiCASB-SSPM

SaaS and Third-Party Security Challenges

FortiAI-SecureAI
Secure LLM, AI Systems

Identify the Entire SaaS Stack	Detect and Respond to Suspicious Third Parties	Control Identities	Automate Remediation



FortiCASB-SSPM | Key Use Cases

Shadow and Third-Party Discovery and Visibility

Discover unknown SaaS apps that didn’t go through Security / IT

SaaS Misconfiguration Management (SSPM)

Automatically identify misconfigurations across enterprise SaaS apps

Identity Posture Management

Gain visibility into identities across SaaS apps

Gen-AI Applications Management

Control the use of Generative AI apps

Data Security Posture Management

Identify and protect sensitive data across SaaS applications

Remediation and Workflows

Create workflows to automate responses and take actions

FortiCASB-SSPM

FortiAI-SecureAI
Secure LLM, AI Systems

Non-intrusive and agentless data collection methods from over 100 sources

SaaS Network Building

Running our AI engine to map the interconnectivities and build the SaaS graph

Risks Identification

Identifying exposures, misconfigurations, vulnerabilities, and risks

Prioritization

The correlation engine connects the dots and provides context, not just creating overhead

Workflows

Implementing protection and compliance

The Platform

An agentless solution that identifies and prevents the next SaaS originated breach

Shadow and Third-Party Discovery and Visibility

FortiAI-SecureAI
Secure LLM, AI Systems

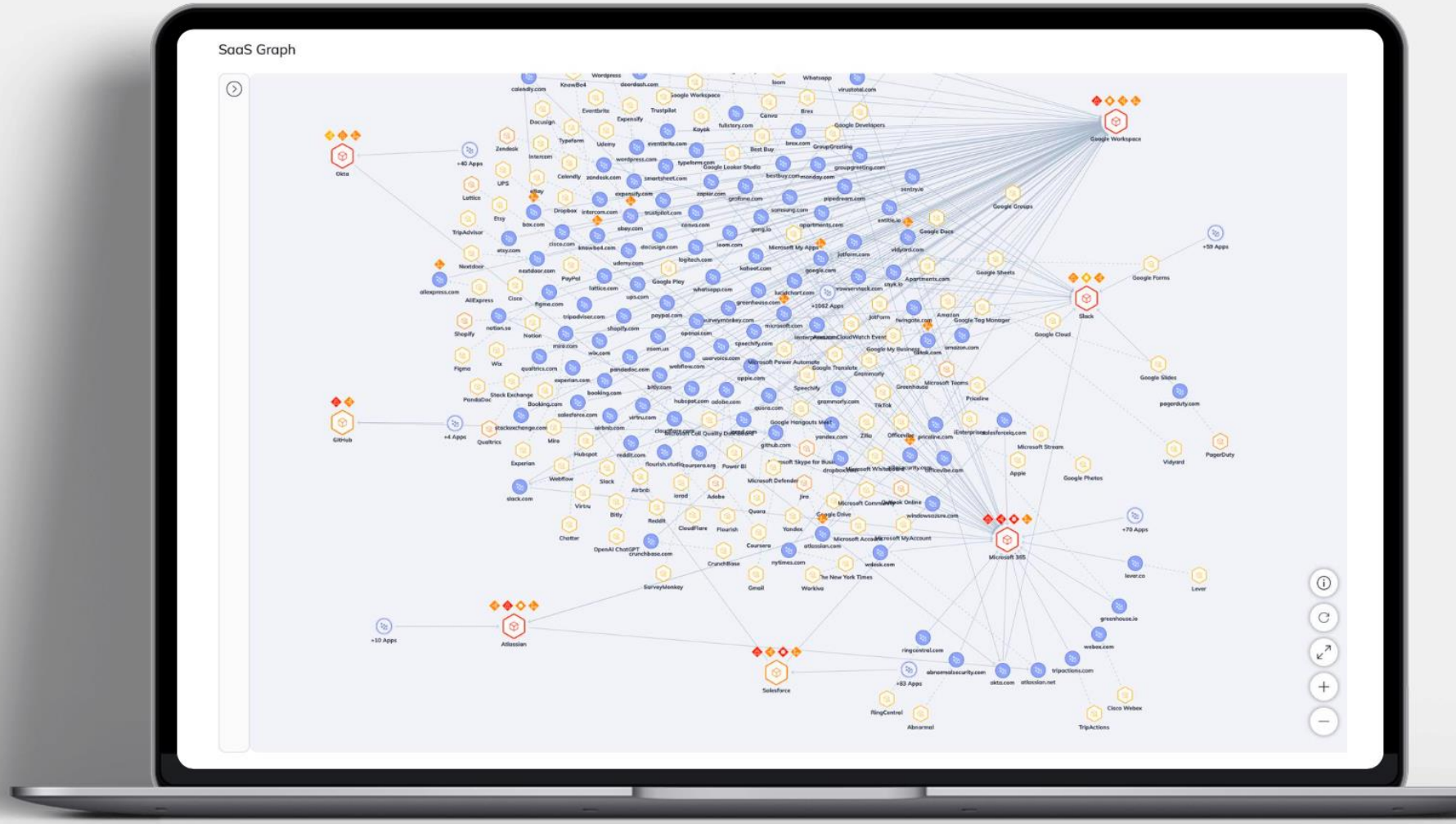
Enhanced Visibility
Uncover suspicious connections

Manage sanctioned apps and enforce security checks

Offboard unsanctioned and inactive apps by eliminating access

Identify all connected plug-ins, add-ons and third-party APIs and tokens

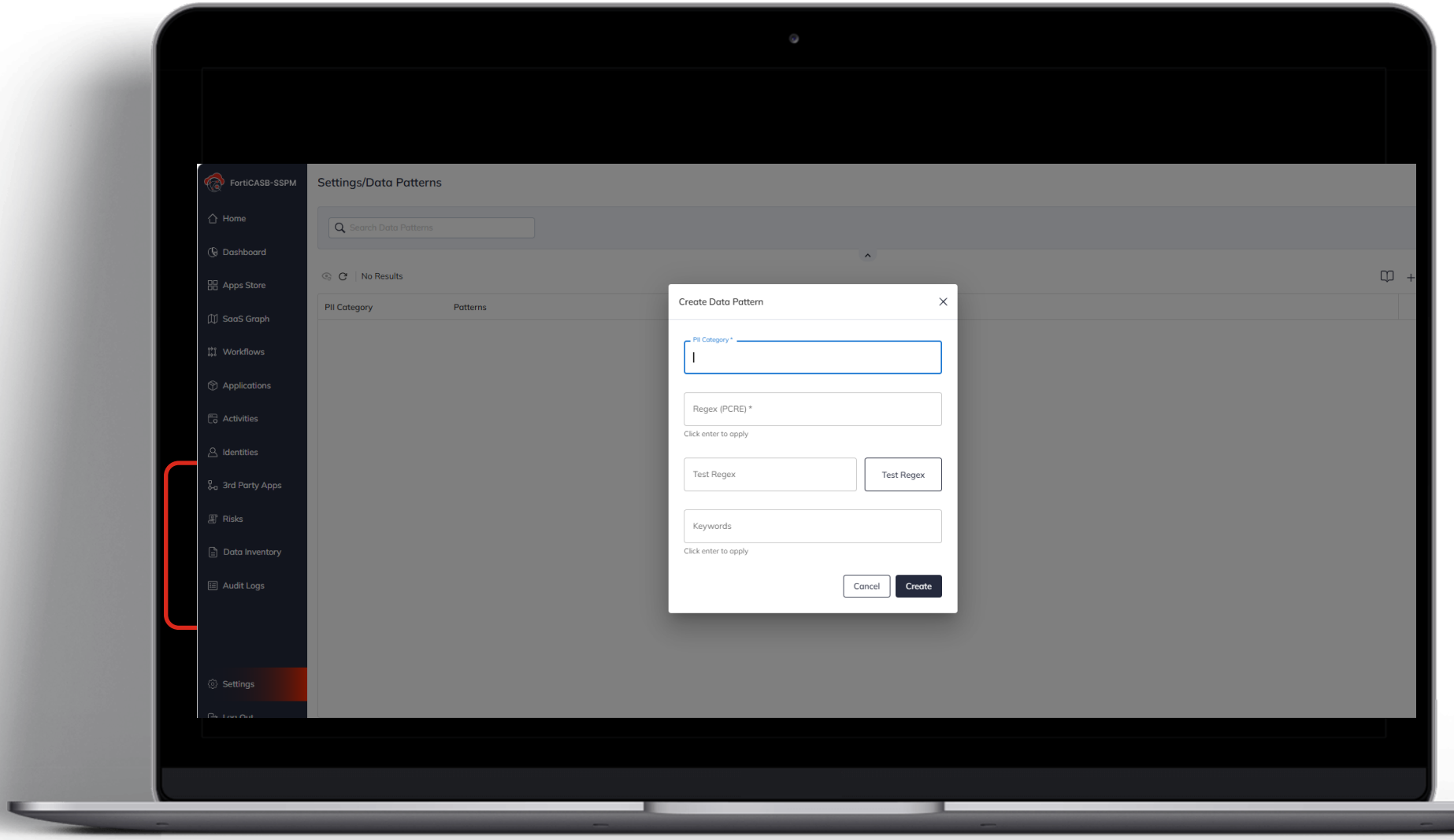
Uncover third-party permissions, data, usage, and compliance risks



FortiCASB-SSPM Data Confidencial

The Integration

- FortiCASB SSPM (SaaS Security Posture Management) con búsqueda de patrones permite identificar y clasificar información sensible almacenada en aplicaciones SaaS mediante el uso de expresiones regulares (regex), palabras clave, diccionarios y patrones predefinidos. Esta capacidad ayuda a las organizaciones a descubrir datos confidenciales expuestos en plataformas como Microsoft 365, OneDrive, SharePoint, Google Workspace, Box, Dropbox y otras aplicaciones en la nube.



GenAI Applications Management

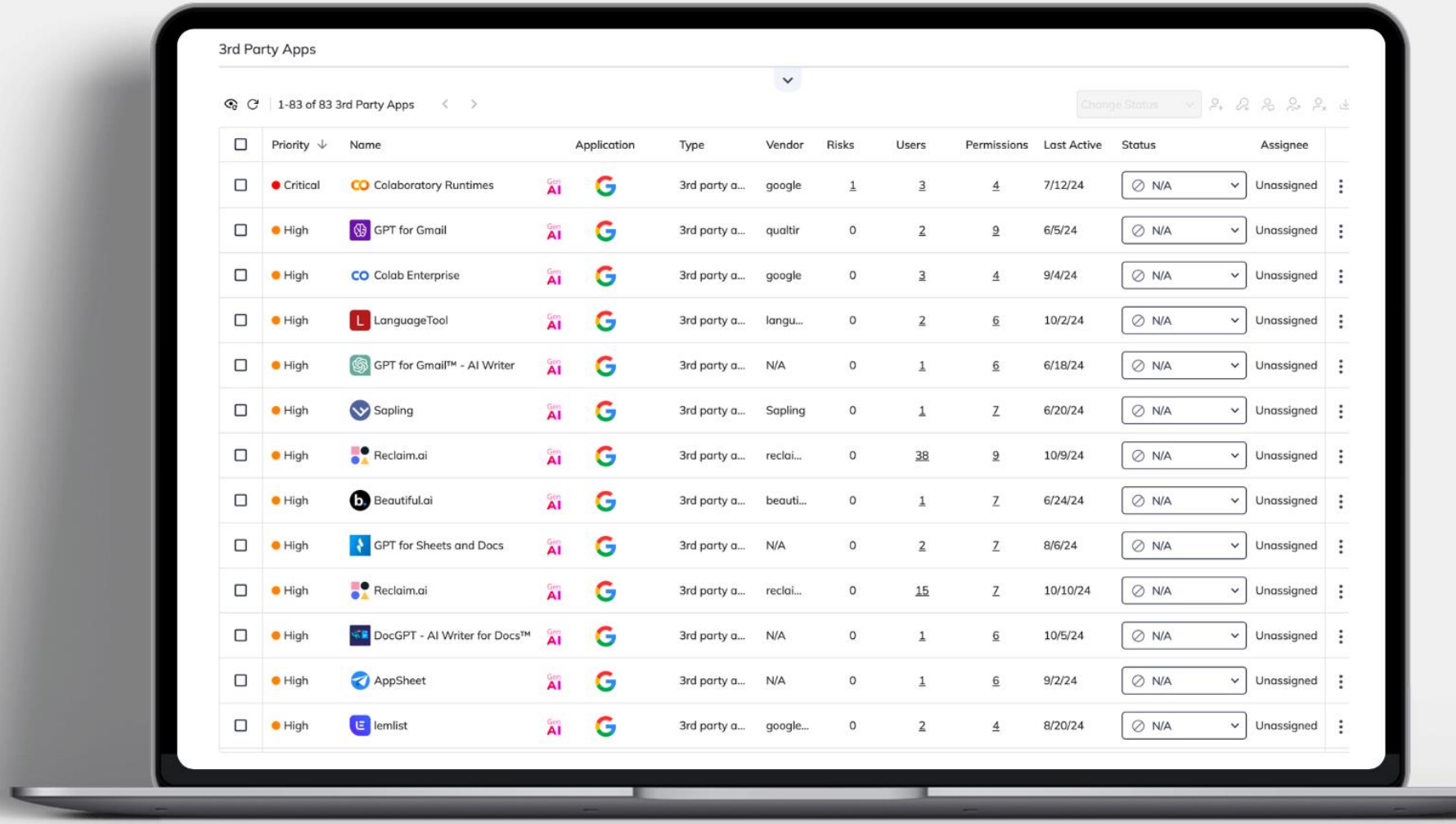
FortiAI-SecureAI
Secure LLM, AI Systems

Manage GenAI Apps

Control the use of GenAI applications across the enterprise

Revoke access to unauthorized third-party apps

Use no-code workflows, automate the security analysis and control of GenAI tools



Priority	Name	Application	Type	Vendor	Risks	Users	Permissions	Last Active	Status	Assignee
Critical	Colaboratory Runtimes		3rd party a...	google	1	3	4	7/12/24	N/A	Unassigned
High	GPT for Gmail		3rd party a...	qualtir	0	2	9	6/5/24	N/A	Unassigned
High	Colab Enterprise		3rd party a...	google	0	3	4	9/4/24	N/A	Unassigned
High	LanguageTool		3rd party a...	langu...	0	2	6	10/2/24	N/A	Unassigned
High	GPT for Gmail™ - AI Writer		3rd party a...	N/A	0	1	6	6/18/24	N/A	Unassigned
High	Sapling		3rd party a...	Sapling	0	1	7	6/20/24	N/A	Unassigned
High	Reclaim.ai		3rd party a...	reclai...	0	38	9	10/9/24	N/A	Unassigned
High	Beautiful.ai		3rd party a...	beauti...	0	1	7	6/24/24	N/A	Unassigned
High	GPT for Sheets and Docs		3rd party a...	N/A	0	2	7	8/6/24	N/A	Unassigned
High	Reclaim.ai		3rd party a...	reclai...	0	15	7	10/10/24	N/A	Unassigned
High	DocGPT - AI Writer for Docs™		3rd party a...	N/A	0	1	6	10/5/24	N/A	Unassigned
High	AppSheet		3rd party a...	N/A	0	1	6	9/2/24	N/A	Unassigned
High	lemlist		3rd party a...	google...	0	2	4	8/20/24	N/A	Unassigned

Remediation and Workflows

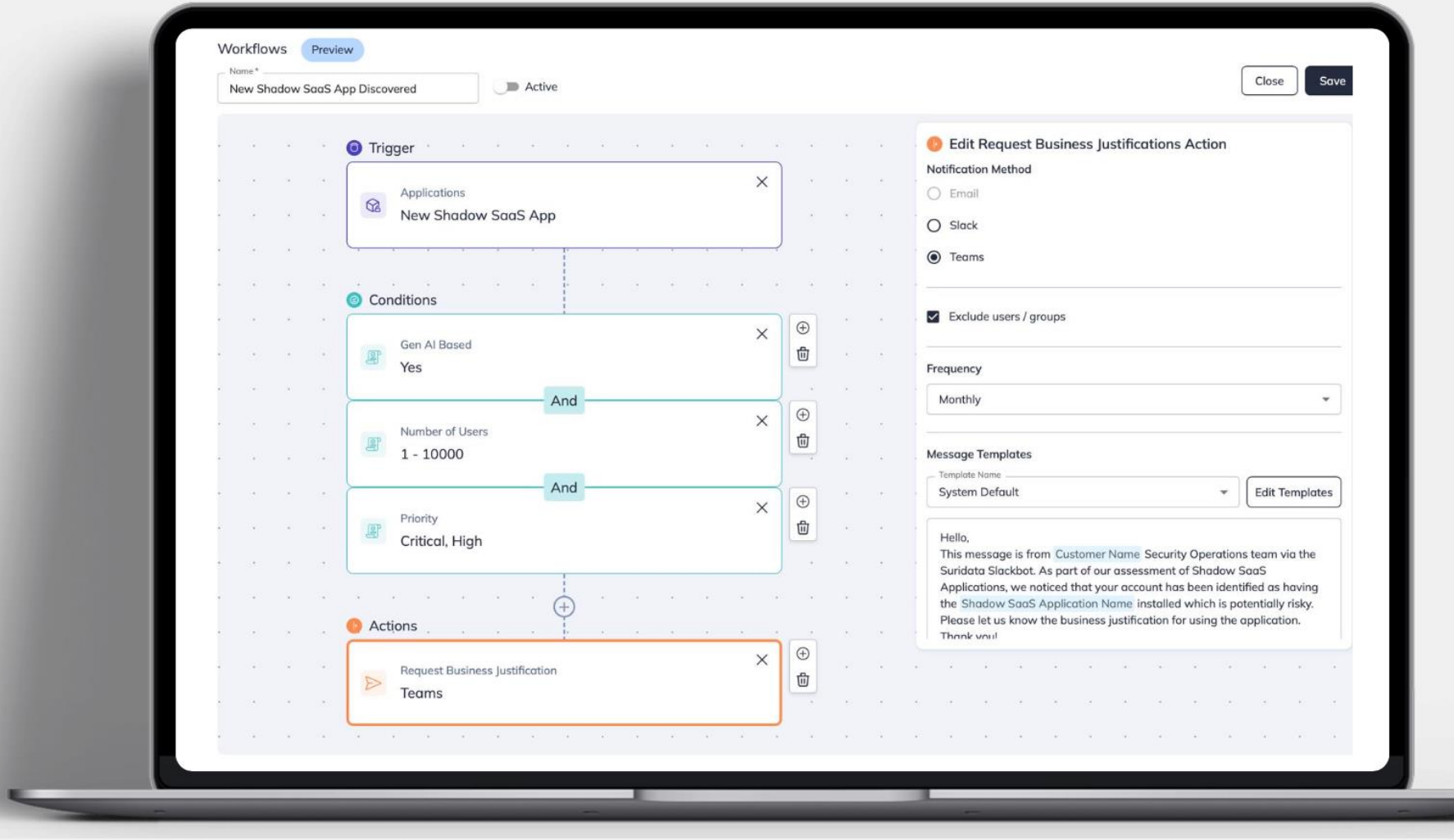
FortiAI-SecureAI
Secure LLM, AI Systems

Automation Workflows

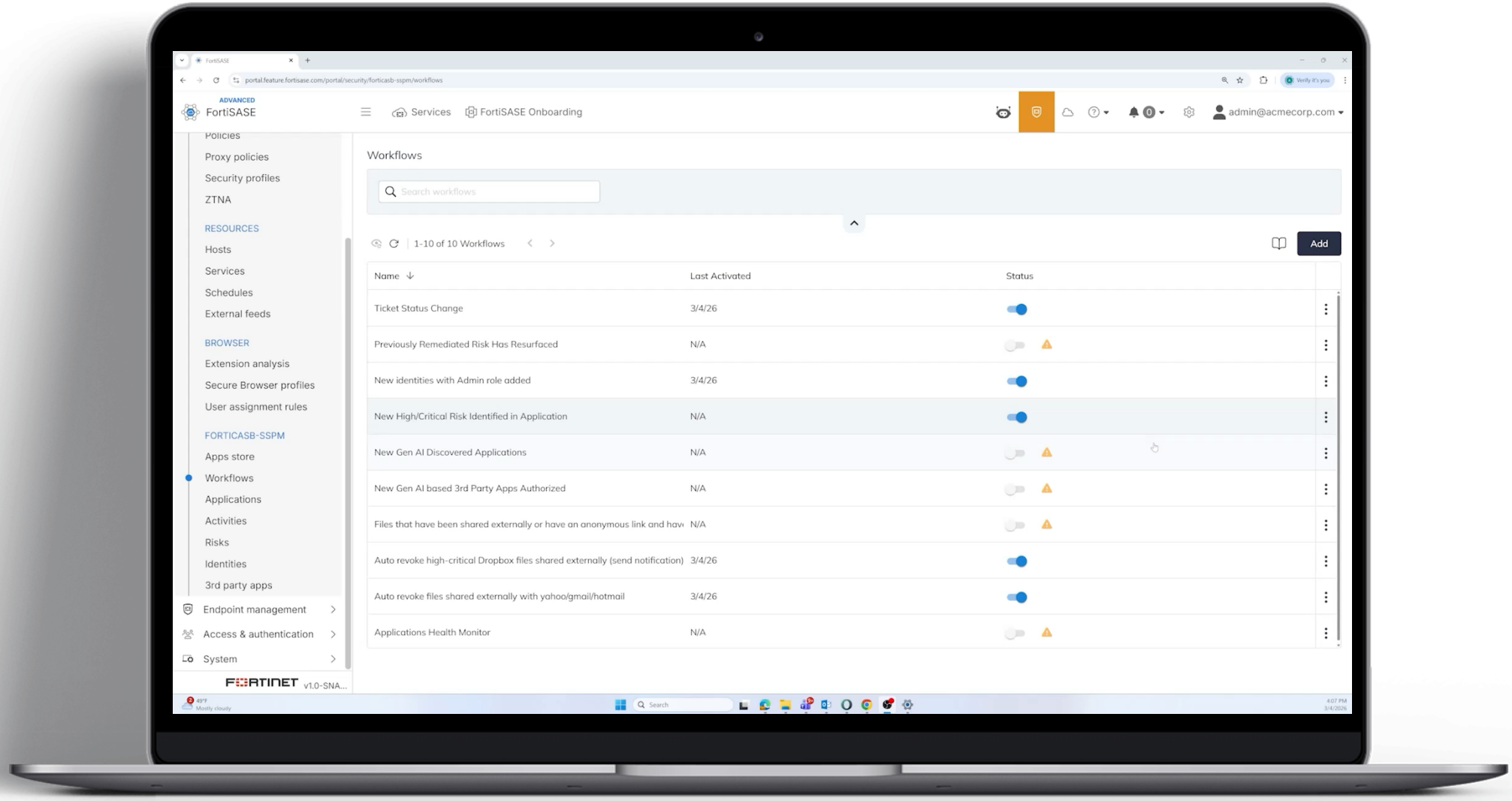
Request business justification from business owners and authorized users

Automate ticketing, notifications, and risk assignment across business, security, and IT teams

Revoke access and offboard users efficiently



Demo – CASB/SSPM



FortiCASB-SSPM

FortiAI-SecureAI
Secure LLM, AI Systems

Non-intrusive and agentless data collection methods from over 100 sources

SaaS Network Building

Running our AI engine to map the interconnectivities and build the SaaS graph

Risks Identification

Identifying exposures, misconfigurations, vulnerabilities, and risks

Prioritization

The correlation engine connects the dots and provides context, not just creating overhead

Workflows

Implementing protection and compliance

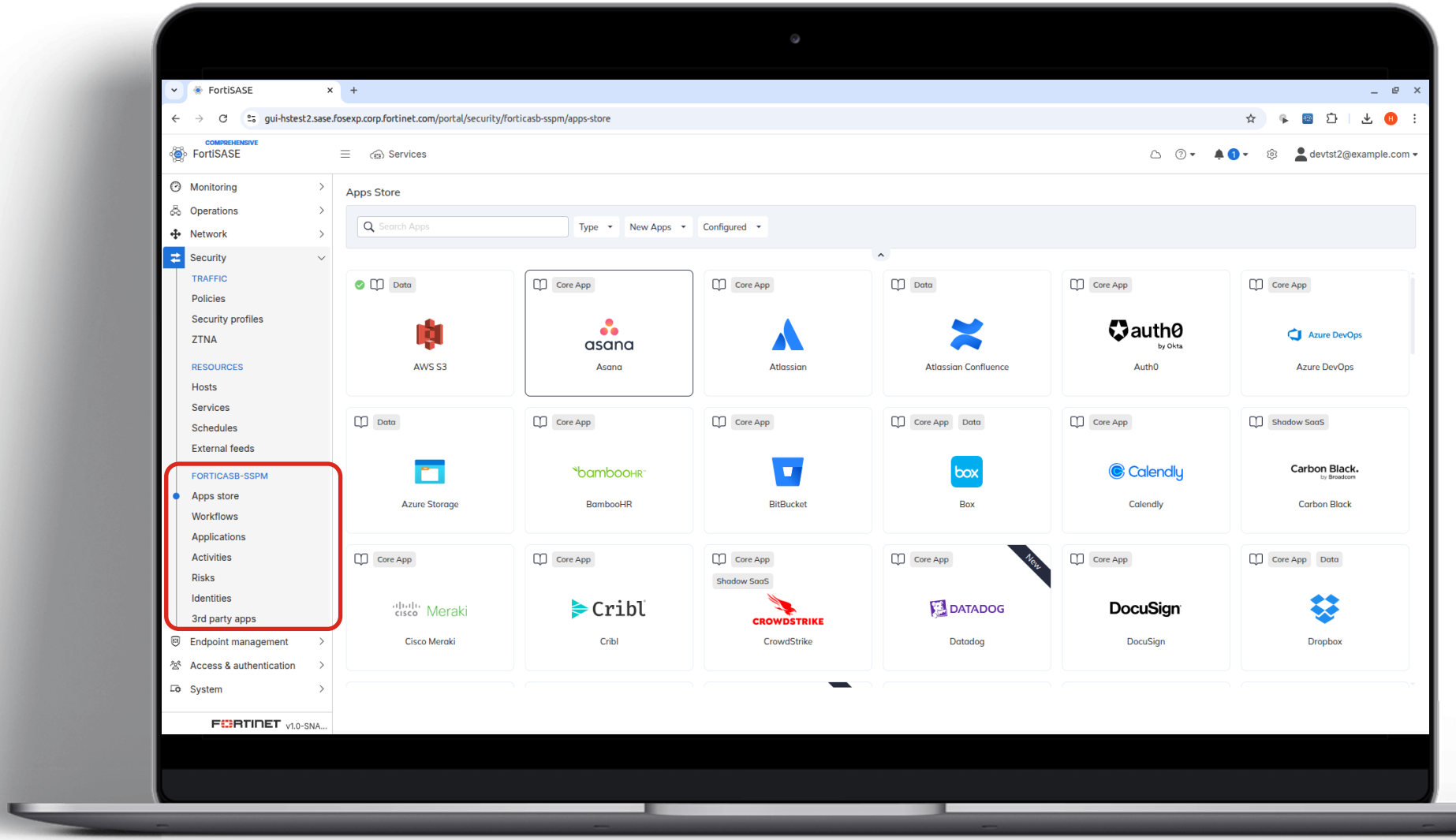
The Platform

An agentless solution that identifies and prevents the next SaaS originated breach

FortiCASB-SSPM integration with FortiSASE

The Integration

- Release scheduled for 26.2.1 (beginning of June)
- Full integration of FortiCASB-SSPM in FortiSASE GUI
- All features available in FortiCASB-SSPM will be available in FortiSASE
- Current API-BASED CASB Menu will be removed from FortiSASE



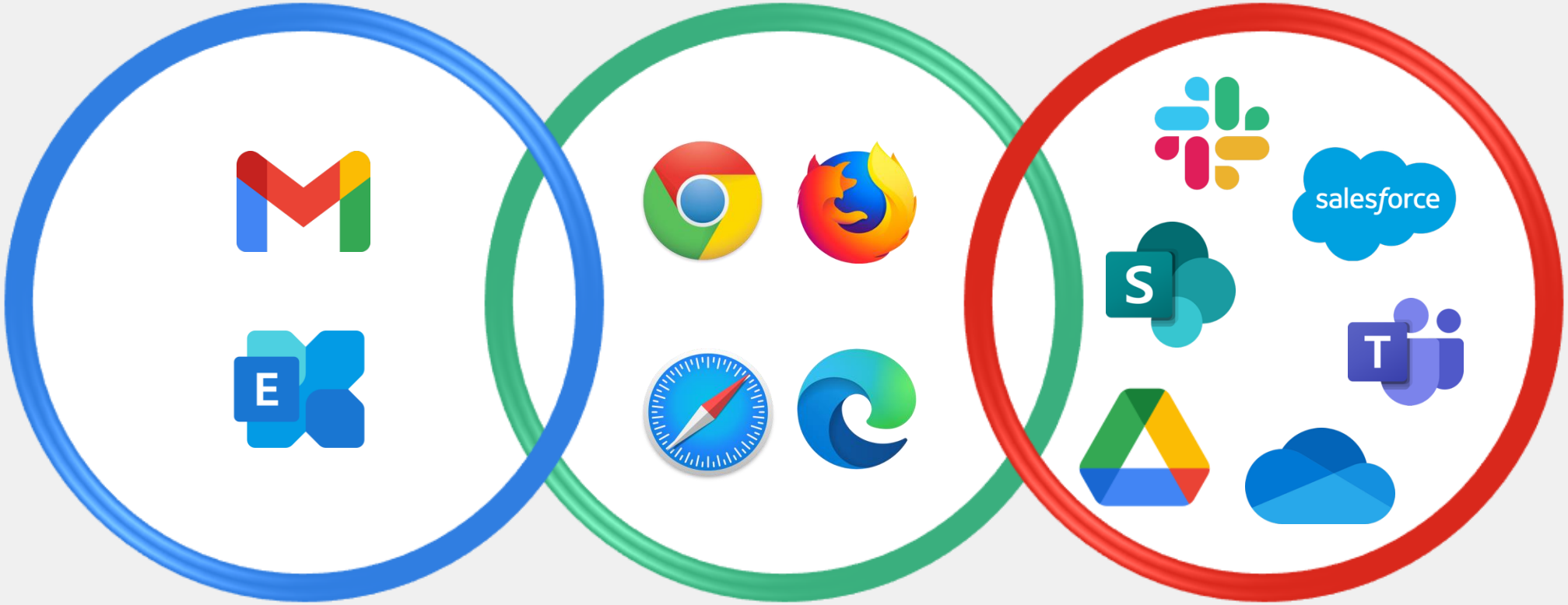
FORTINET | COLOMBIA & ECUADOR

XPERTS26

FortiMail BrowserSecuirty

Fortimail Workspace Security

FortiAI-SecureAI
Secure LLM, AI Systems



Email
Keep email safe and productive with real-time prevention.

Browser
Protect users easily while they use their browser of choice.

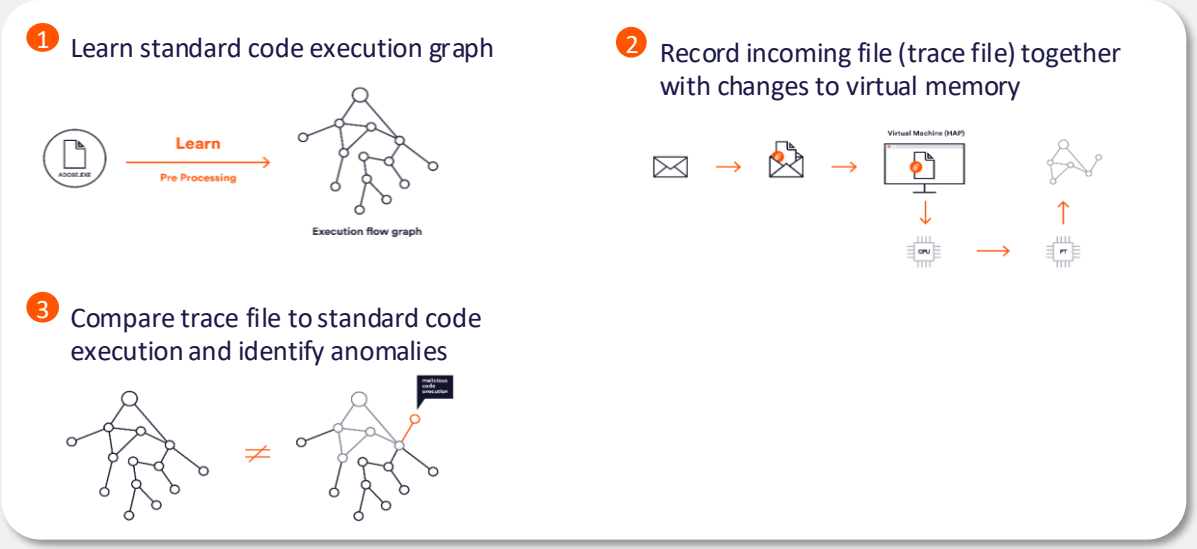
Collaboration
Give collaboration tools the security solution they natively lack.

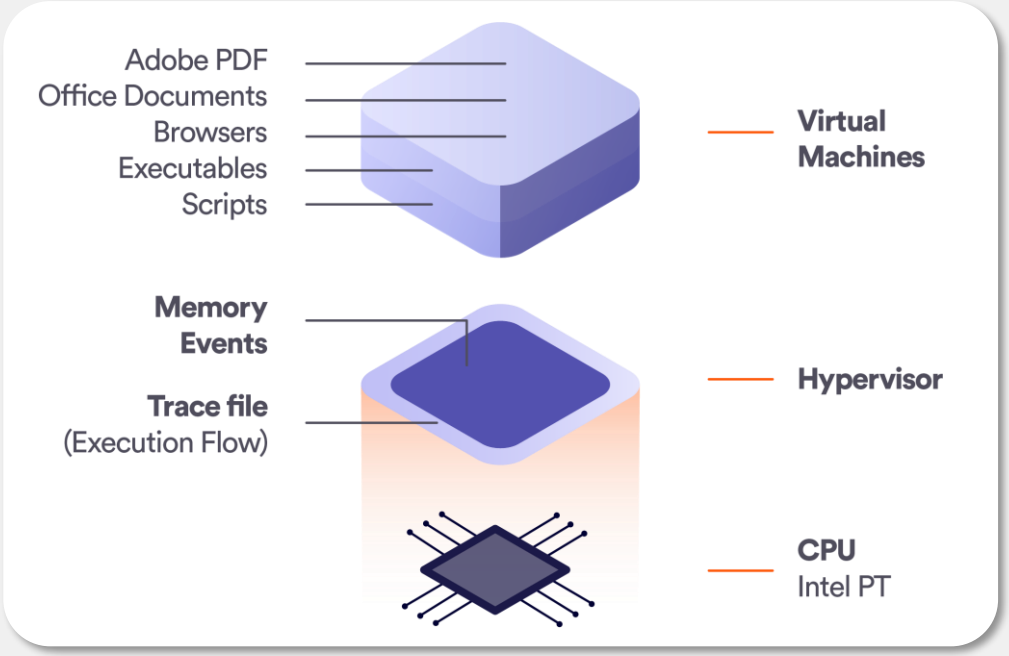
The HAP

Next Gen Dynamic Sandbox

KEY GOAL

- Provides real-time prevention by intercepting malicious files and URLs that leverage:
  - Zero-Day vulnerabilities
  - N-day targeting unpatched vulnerabilities
  - Malicious code execution in scripts
  - Malicious code in executable files





HOW IT WORKS

- Software algorithms use CPU level data to access the entire execution flow, right from the processor
- Deterministically intercepts exploit techniques pre-malware release
- Includes mechanisms to bypass evasion techniques

Advanced Browser Security

Browser Security and Control

Adds AI-powered threat detection, DLP, and browser-level governance to any standard browser

Provides dynamic protection with zero impact on user experience or browsing quality

Includes a 24/7 managed incident response service and leverages cross-channel context

Instantly and centrally deployed via a lightweight browser extension for Chrome/Edge/Safari/Firefox, etc

Advanced Browser Security

Feature Highlights

Safe Browsing
Blocks advanced phishing, malware, and browser exploits

- Anti-evasion, by design
- Deep recursive file unpacking
- 0-day file exploit detection (HAP)
- Anti-phishing (ML, image-based)
- Web exploits (e.g., XSS)
- Detect malicious extensions
- Password reuse alerts

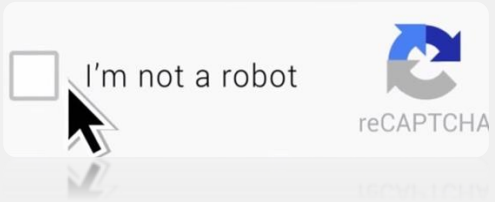
Data Loss Prevention
Protects data from insider and 3rd party/contractor threats

- Clipboard controls
- Printing controls
- Download/upload restrictions
- Watermarking
- Shoulder surfing protection
- Monitor user logins/shadow IT
- Data exfiltration alerts

Browser Governance
Control browser/web policies and enhance visibility

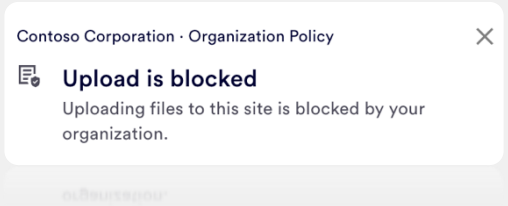
- Restrict website categories
- Safe Generative AI usage
- Restrict downloads by file type
- Auto-block extensions by risk
- Anti-tampering protection
- Conditional access
- Browser version visibility

Browser Security – The Workspace Value



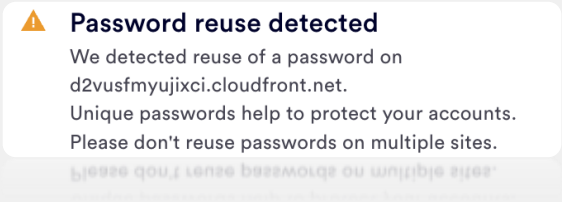
Next-Gen URL Anti-Evasion

Detects phishing attacks even if they apply CAPTCHAs, Geofencing, or Time-based evasions



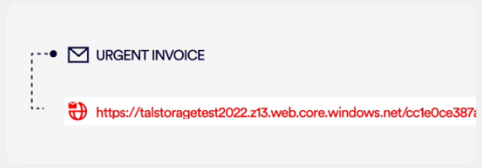
Browser-Based DLP

Detects users uploading/downloading sensitive content in any web app (GenAI, email, etc.)



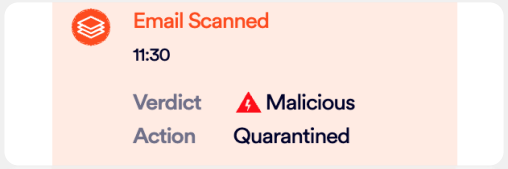
User Security Awareness

Warns users against bad practices, such as password reuse and potential data loss on 3rd party sites



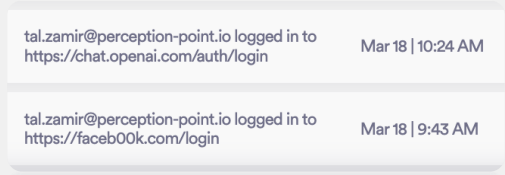
Correlating Browser & Email Events

URLs opened in the browser are automatically correlated to the originating email for investigation



Cross-App Remediation

Quarantines emails/files across protected apps (e.g., quarantining all emails with browser-detected URL)



Post-Breach Impact Analysis

Gains visibility into user login events to identify phished users and perform remediation actions

Return

PERCEPTION POINT™

Perception Point Demos

This is a catalog of sample threats, including advanced phishing, malware, evasion techniques, etc.
The catalog is provided for educational purposes only. Do not enter any personal information.

Phishing Websites

Attempts to steal credentials (e.g. username, password, and 2FA code) or payment method information (e.g. credit card numbers).

Credential Phishing

Credential phishing is a type of phishing attack that targets login credentials.

Google BiTB

A Google browser-in-the-browser attack faking a "Sign in with Google" window.

Microsoft BiTB

A Microsoft browser-in-the-browser attack faking a "Sign in with Microsoft" movable window.

Password Reuse Alerts

Alerts that notify users when they reuse passwords across different websites.

Clickjacking

A clickjacking attack that tricks users into clicking on a hidden element.

Web Evasion Techniques

Various techniques and tactics used by attackers to avoid being detected by scanning services.

Evasion by Delay

Phishing attacks that delay loading of malicious elements to evade detection.

Evasion by Input (Clicks)

Phishing attacks that require user interaction (clicks/keystrokes) to evade detection.

Evasion by Input (Move)

Phishing attacks that require user interaction (mouse movement) to evade detection.

Return

Gmail Images Sign in

Google

888.com

888.com
888.com **poker**
888.com **live**
888.com **download**
888.com **zambia**
888.com **slot**
888.com **register**
888.com **phone number**
888.com **logo**
888.com **share price**

Google Search I'm Feeling Lucky

Report inappropriate predictions

About Advertising Business How Search works Our third decade of climate action: join us Privacy Terms Settings

FORTINET | COLOMBIA & ECUADOR
XPERTS26

Workshop Time

AI Hands-on Labs

- **ESPAÑOL**
  https://latam.amerintlxperts.com/ai/ai-colombia/index.html
- **INGLES:**
  https://latam.amerintlxperts.com/ai/ai-colombia/Shadow-AI/index.html
  - User: amerintlxperts
  - Password: xPerts2026!

El usuario y contraseña para todo:

Username: fortiadmin

Password: XpertsLab-2026

FORTINET | COLOMBIA & ECUADOR

XPERTS26

Gracias!