



# Anticipate and Prevent Data Theft

## Introducing FortiDLP

Klaidas Rimkus

Senior Systems Engineer - Baltics

# Data at Stake

Protect sensitive data from exfiltration or inadvertent disclosure.



## Intellectual Property

- Design Documents
- Project Plans
- Patent Applications
- Source Code
- Process Documentation
- Trade Secrets



## Corporate Data

- Financial Statements
- Employee Records
- Pricing Documents
- User Logins



## Customer Data

- End-user Logins
- Credit Card Numbers
- Social Security Numbers
- Medical Data

# Protecting Data Has Been an Uphill Battle

**\$4.88M**

Average Cost of a  
Data Breach

Increased Network  
Complexity

Insider-related Incidents  
On the Rise

Remote and Hybrid  
Workforces

Employee Actions Account  
for Most Data Disclosures

Ongoing Explosion  
in Data

Shadow SaaS and  
Shadow AI



Most organizations  
have DLP.  
They're not at all happy  
with their ROI.

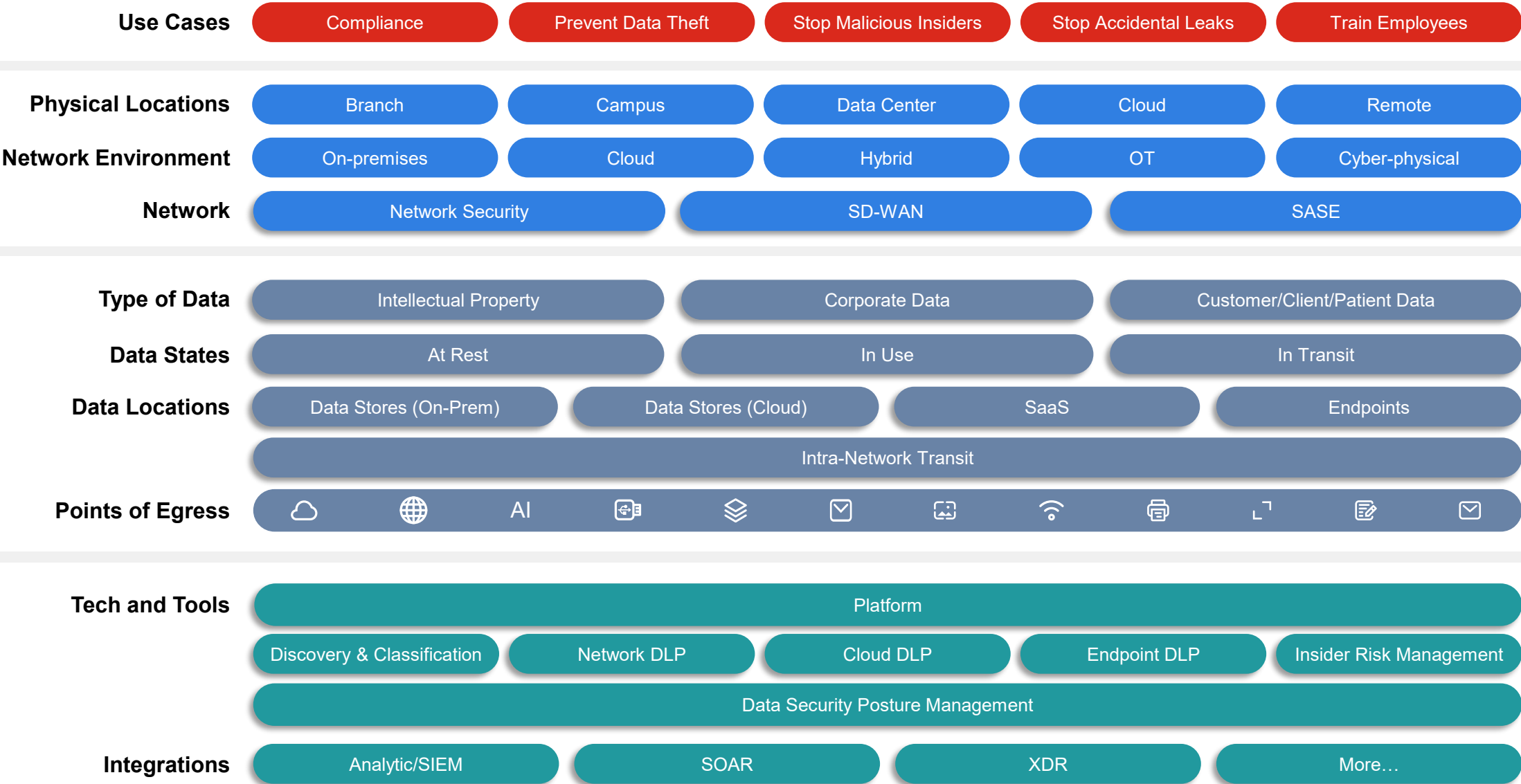
**55%**

Percent of incidents due  
to employee negligence

**\$8.8M**

Average annual cost to  
remediate these incidents

# Securing Data Is Complex



# Fortinet DLP Architecture 2025

## 1 Data in motion

- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

## 2 Data in use

- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT.
- Corporate sensitive data being accessed from anywhere

## 3 Data at rest

- FortiData enables the customer to discover and label sensitive data on cloud and on-premises data stores using modern AI machine learning technology. Integration with FortiGate brings additional context about the data for better automated enforcement





# Fortinet DLP Architecture 2025

## 1 Data in motion

- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

## 2 Data in use

- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT.
- Corporate sensitive data being accessed from anywhere

## 3 Data at rest

- FortiData enables the customer to discover and label sensitive data on cloud and on-premises data stores using modern AI machine learning technology. Integration with FortiGate brings additional context about the data for better automated enforcement



# Fortinet DLP Architecture 2025

## 1 Data in motion

- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

## 2 Data in use

- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT.
- Corporate sensitive data being accessed from anywhere

## 3 Data at rest

- FortiData enables the customer to discover and label sensitive data on cloud and on-premises data stores using modern AI machine learning technology. Integration with FortiGate brings additional context about the data for better automated enforcement



# Fortinet DLP Architecture 2025

## 1 Data in motion

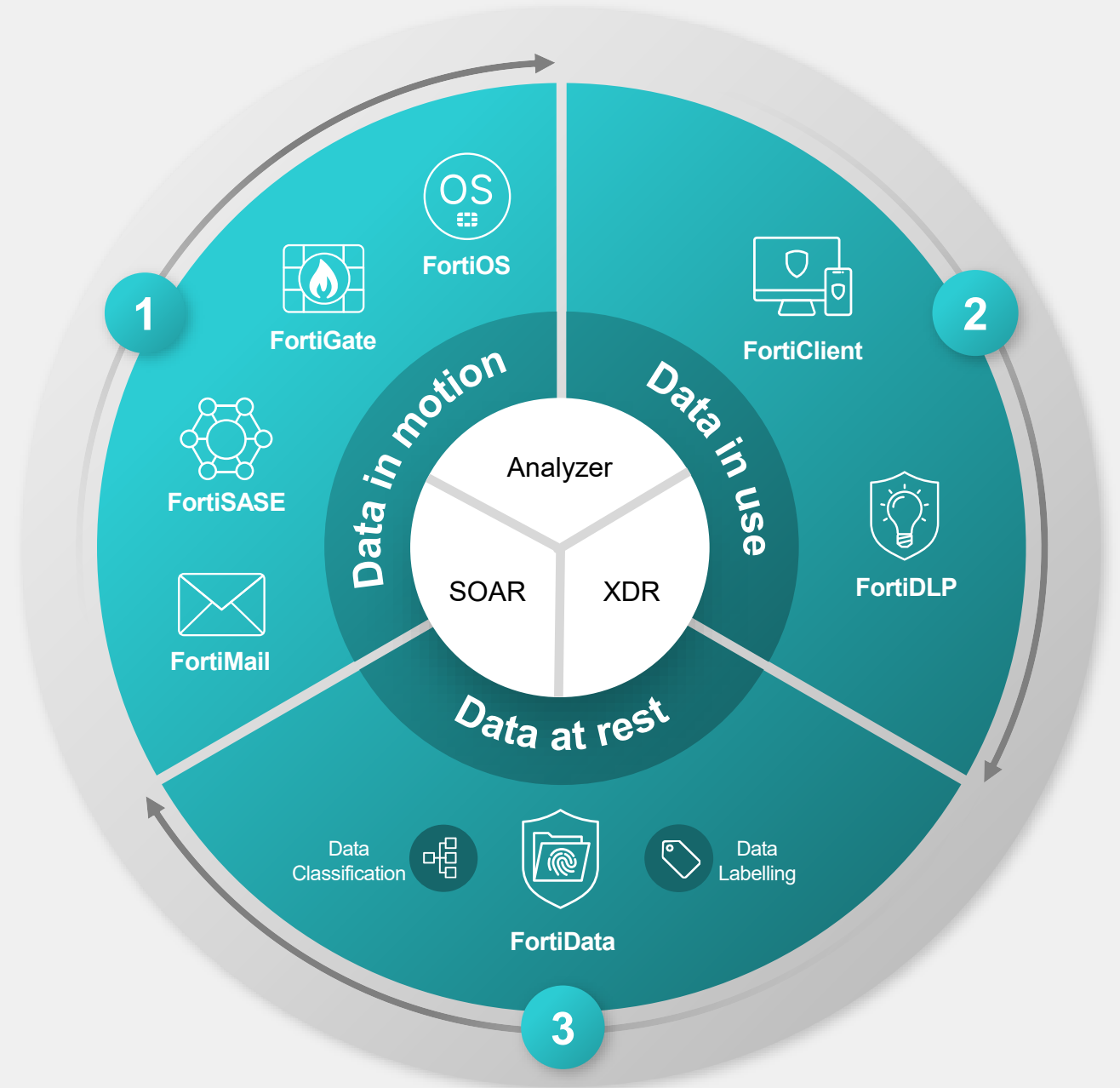
- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

## 2 Data in use

- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT.
- Corporate sensitive data being accessed from anywhere

## 3 Data at rest

- FortiData enables the customer to discover and label sensitive data on cloud and on-premises data stores using modern AI machine learning technology. Integration with FortiGate brings additional context about the data for better automated enforcement







# About FortiDLP



# Introducing FortiDLP



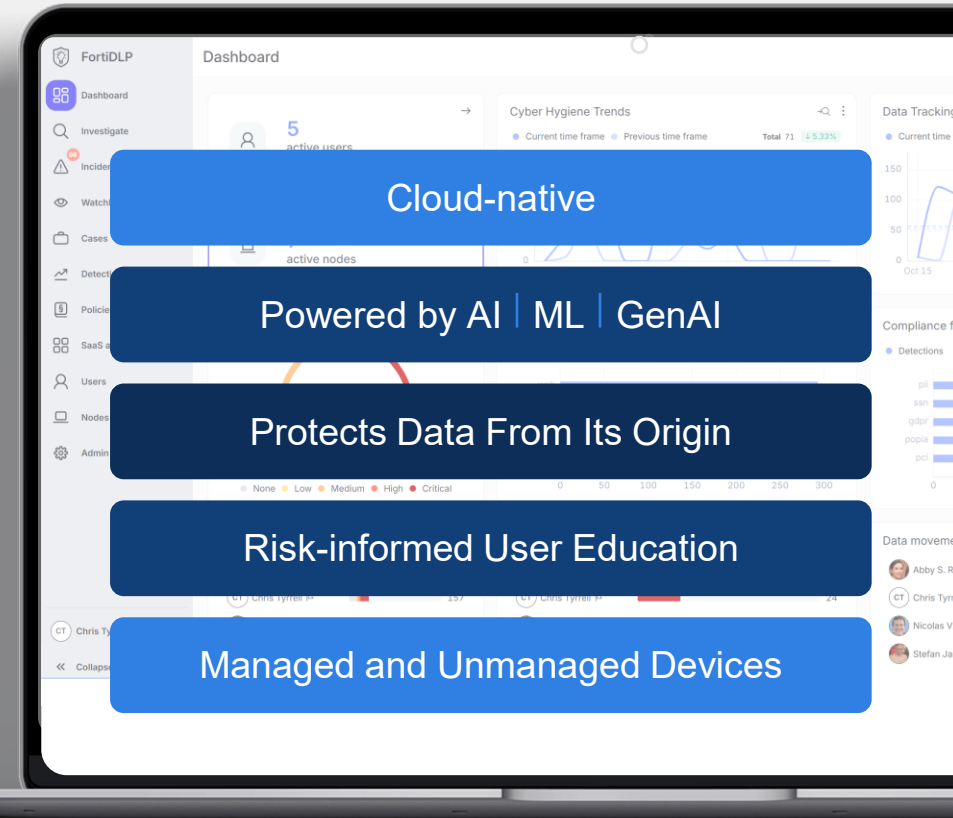
## Next-Generation Endpoint DLP and Insider Risk Management Solution Anticipates and Prevents Data Theft

- Immediate Data Risk Visibility Across Egress Channels
- Educate Employees on Safe Data Handling
- Protect IP and Sensitive Data using Origin and Content
- Detect and Investigate Insider Risk Data Exfiltration

Data Loss  
Prevention

Insider Risk  
Management

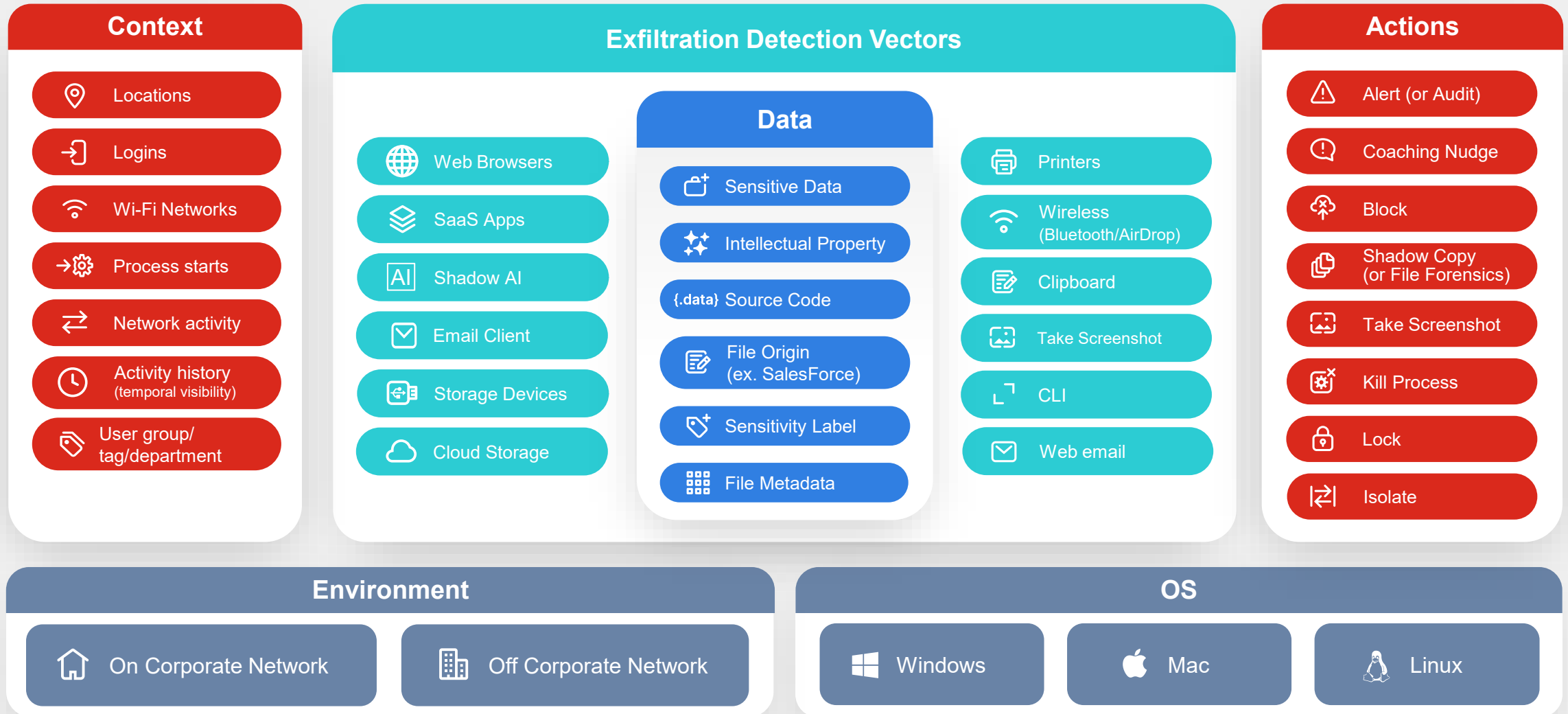
SaaS  
Data Security



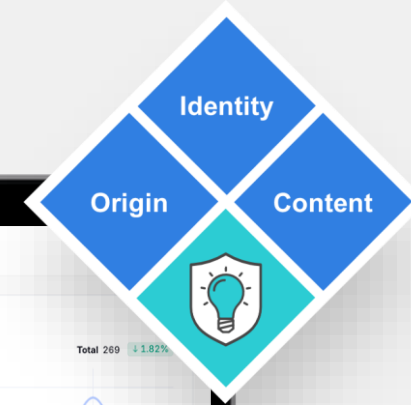
Automatically maps detections to MITRE ENGenuity™ Insider Threat TTP Knowledge Base.



# Deep and Broad Contextual Visibility is Required to Protect Data

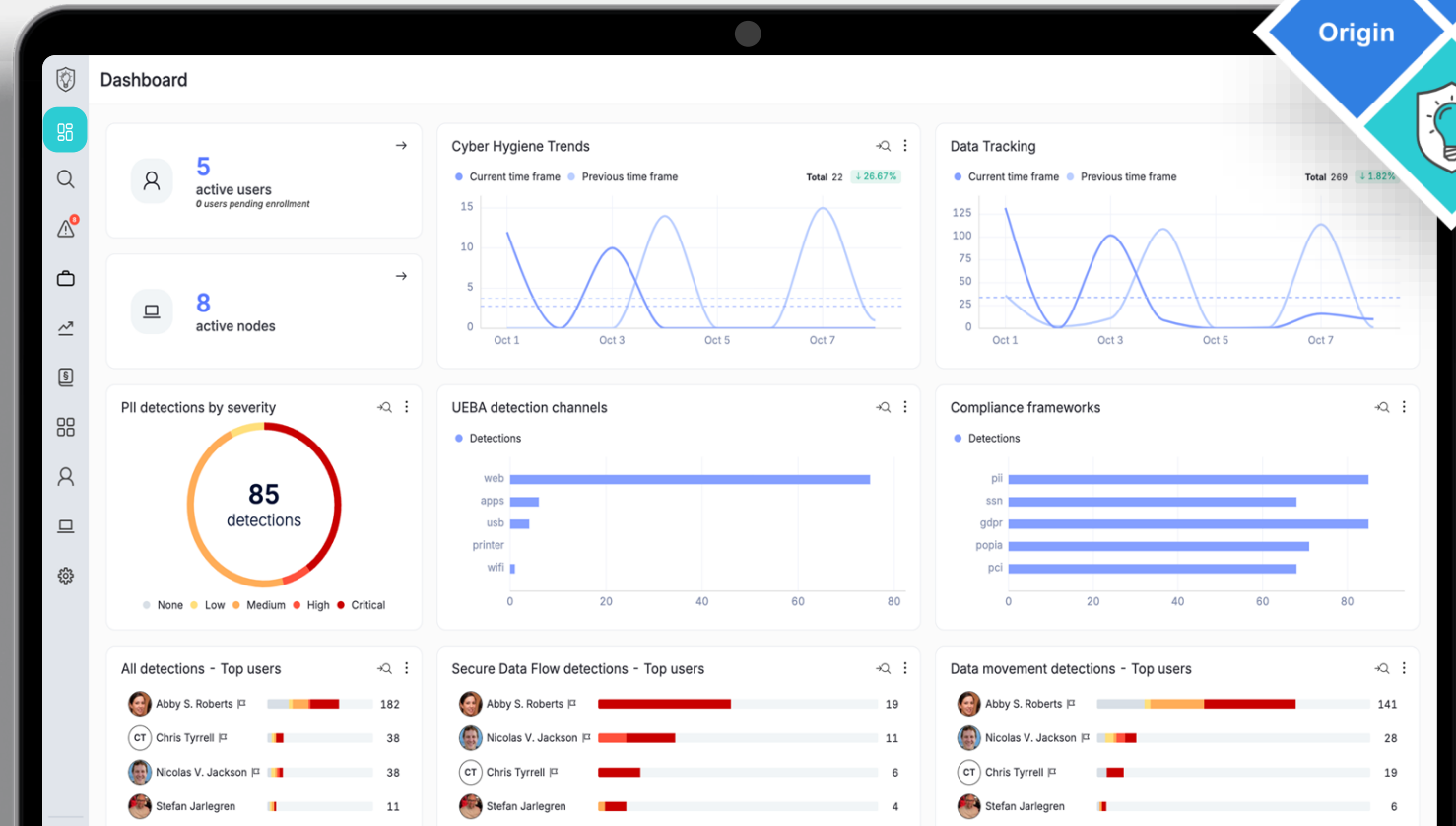


# Data Loss Prevention: Differentiation



## Next-Generation DLP

- Cloud-native SaaS solution
- Demonstrates data risk on day one
- Protects data based on content and data source (e.g. Salesforce) and sensitivity labels
- Out-of-the-box coverage for major compliance, security and privacy frameworks/regulations
- Security fabric integrations (Including FortiClient and FortiEDR)



Multi-OS

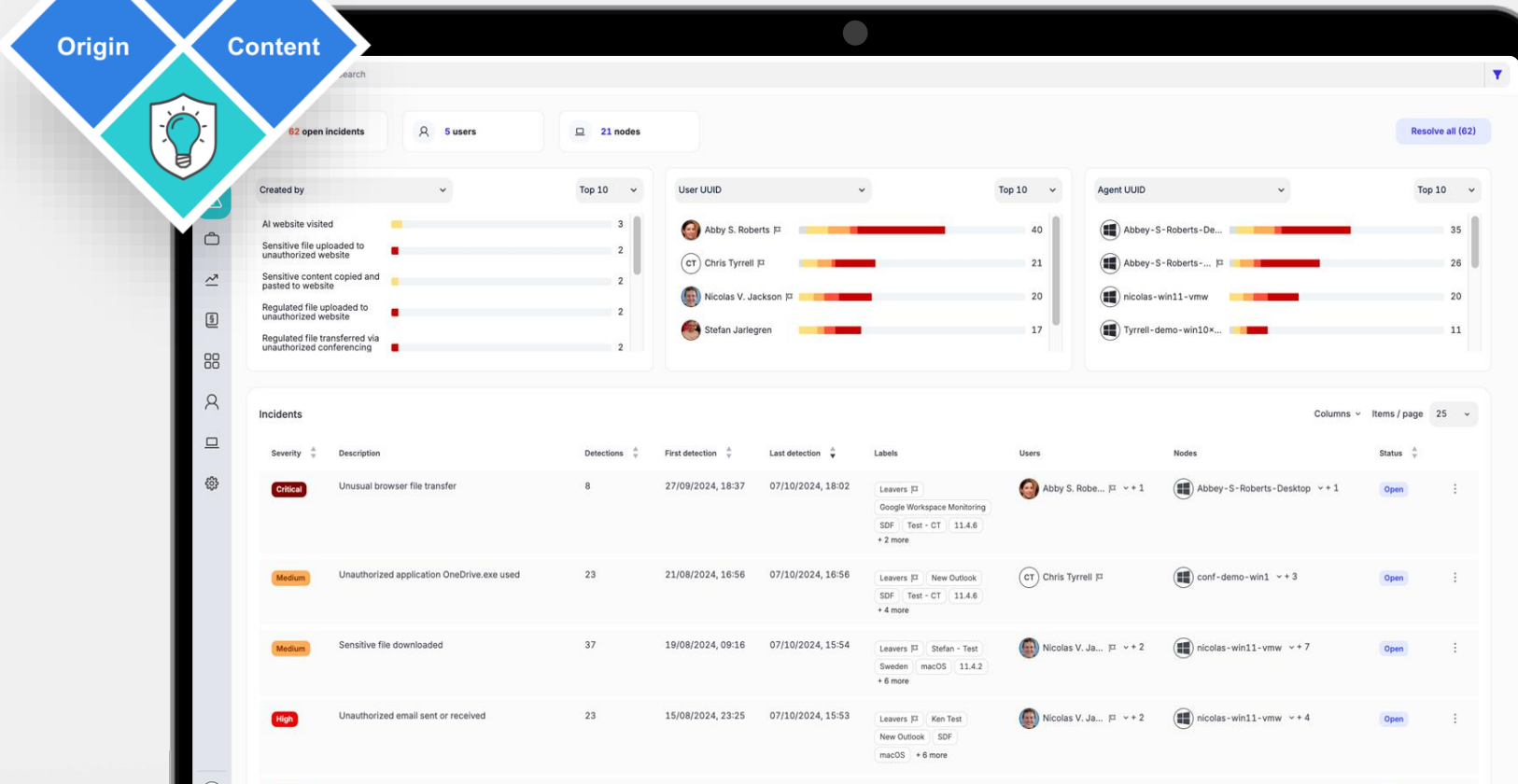
Instant Visibility

Secure Data Flow

Real-time User Education



# Insider Risk Management: Differentiation



Insider Risk  
Sequence Detection

Instant Visibility

File, Clipboard and  
Screen Forensics

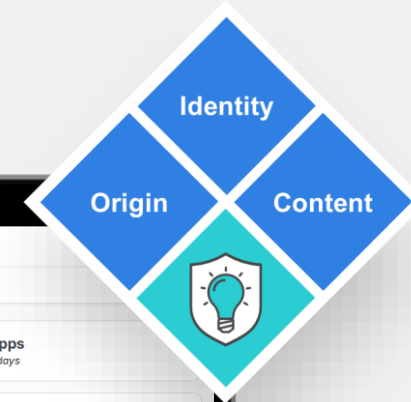
FortAI  
Analyst Insights

## Insider Threat: Detection and Response

- Deep insights into user, endpoint and cloud drive activity
- ML-UBA baselines user activity
- Insider Risk Sequence Detection
- Incident and case management with anonymization for privacy
- Forensics file and screen evidence
- FortiAI case reports (BETA)

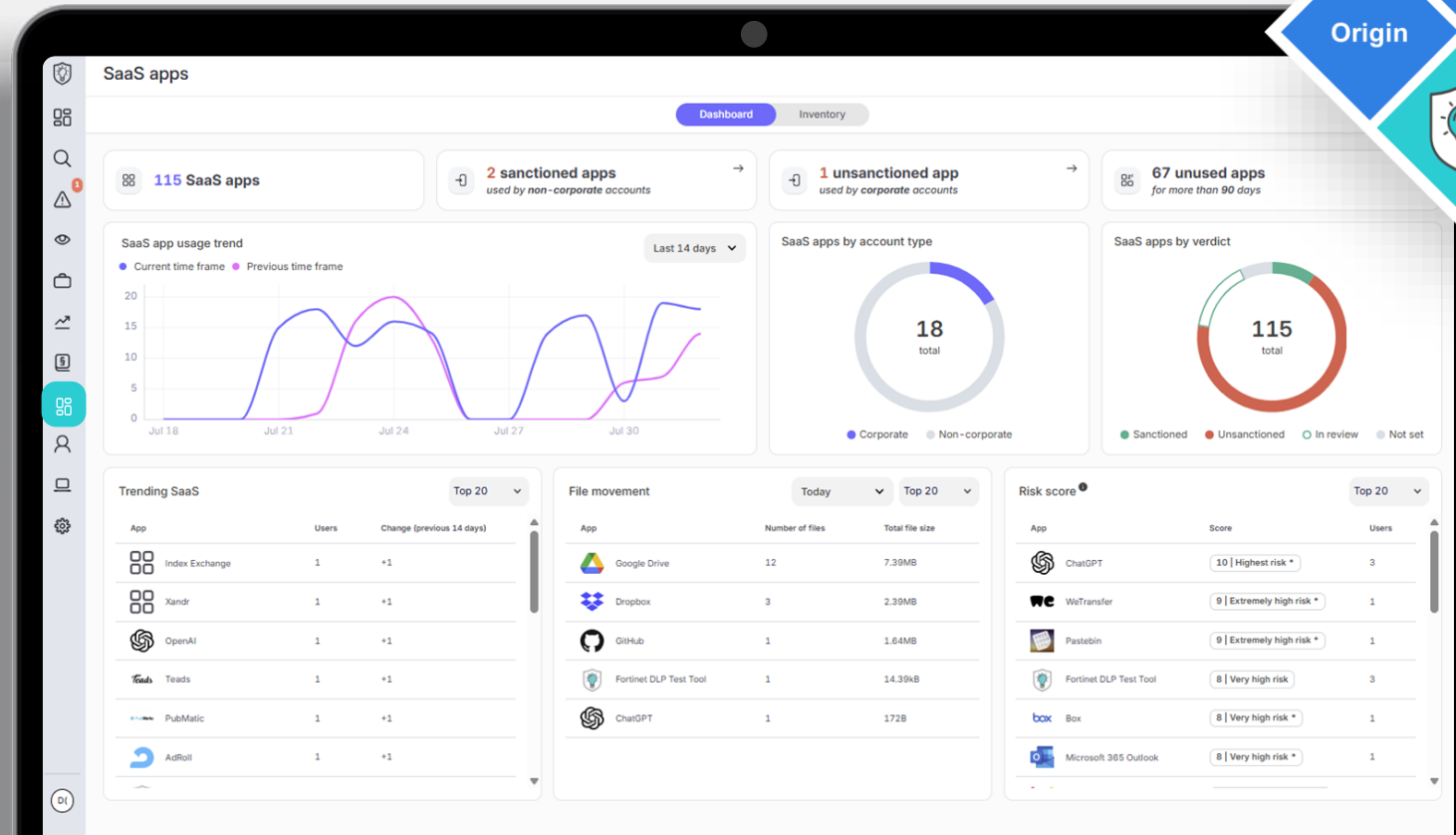


# SaaS Data Security: Differentiation



## Full visibility into SaaS apps including Shadow AI

- Track, categorize, and score risk across sanctioned and unsanctioned apps
- Insights into GenAI usage
- Ingress/egress visibility into sensitive data flows and risks
- Expose unauthorized usage
- Identify use of unsanctioned SaaS apps and insecure personal credentials



SaaS Inventory  
and Risk Scoring

Data Flow and  
Identity Insights

Data Protection  
for Shadow AI

Real-time User  
Education





# Insider Risk Management: Differentiation



## Education at the Point of Use of Sensitive Data

- Increases employee awareness while enforcing accountability
- Nudges employees with proper data handling practices when accessing sensitive data
- Applies expansive range of policy actions based on sensitivity of data (context and content)
- Nudges employees whether remote or working offline

Risk-based  
Actioning

Nudges

Customizable  
Messaging

Education +  
Forensics Capture





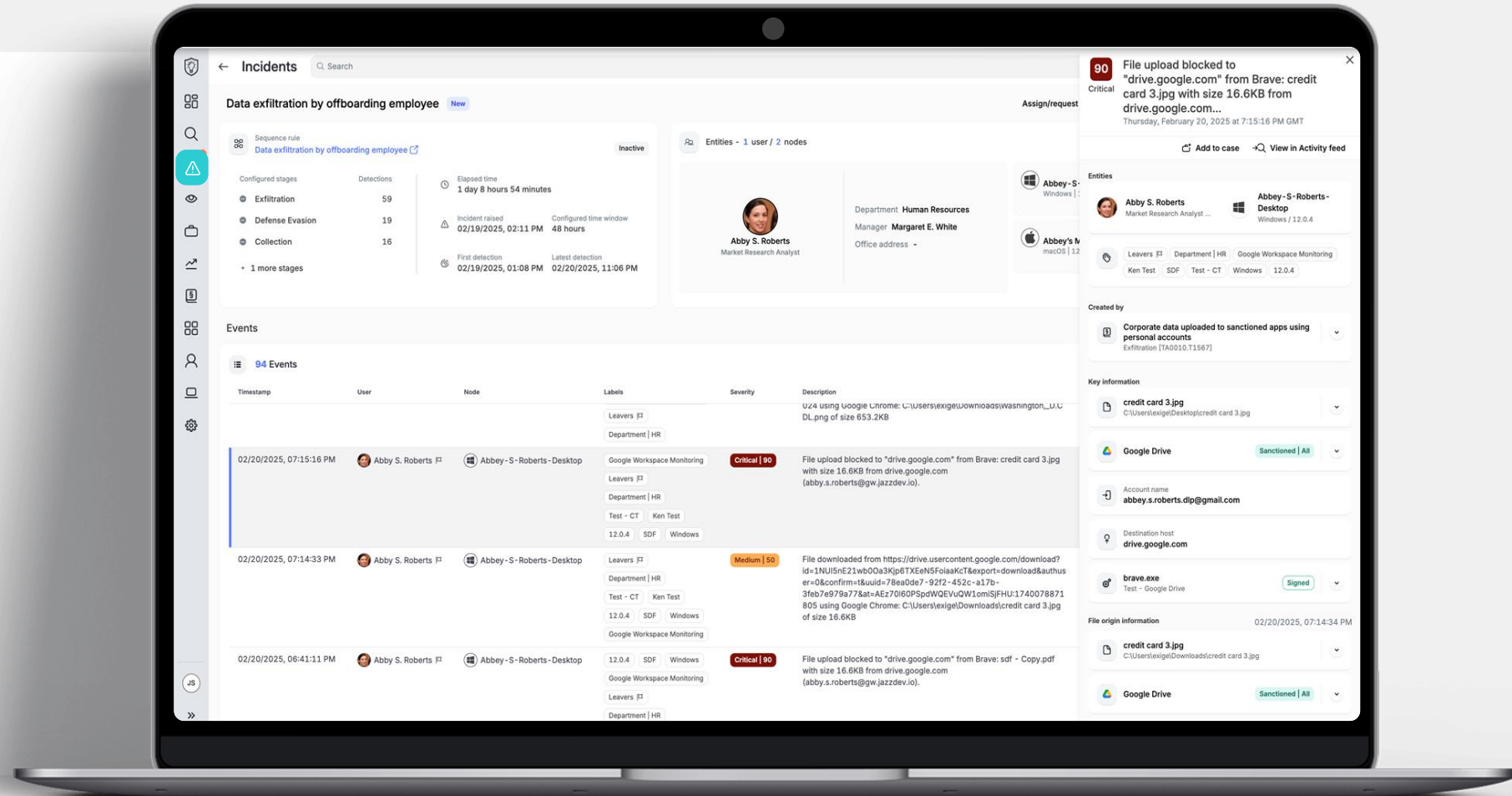
# Use Case: Content Classification



# Realtime Content Classification of Data

## Content Inspection and Classification

- Data Privacy regulations e.g. GDPR and PDPA
- Financial regulations
- National PII and PHI identifiers
- Sensitivity labels
- Realtime content scanning at the point of creation/access





# Use Case: Tracking Data from Origin

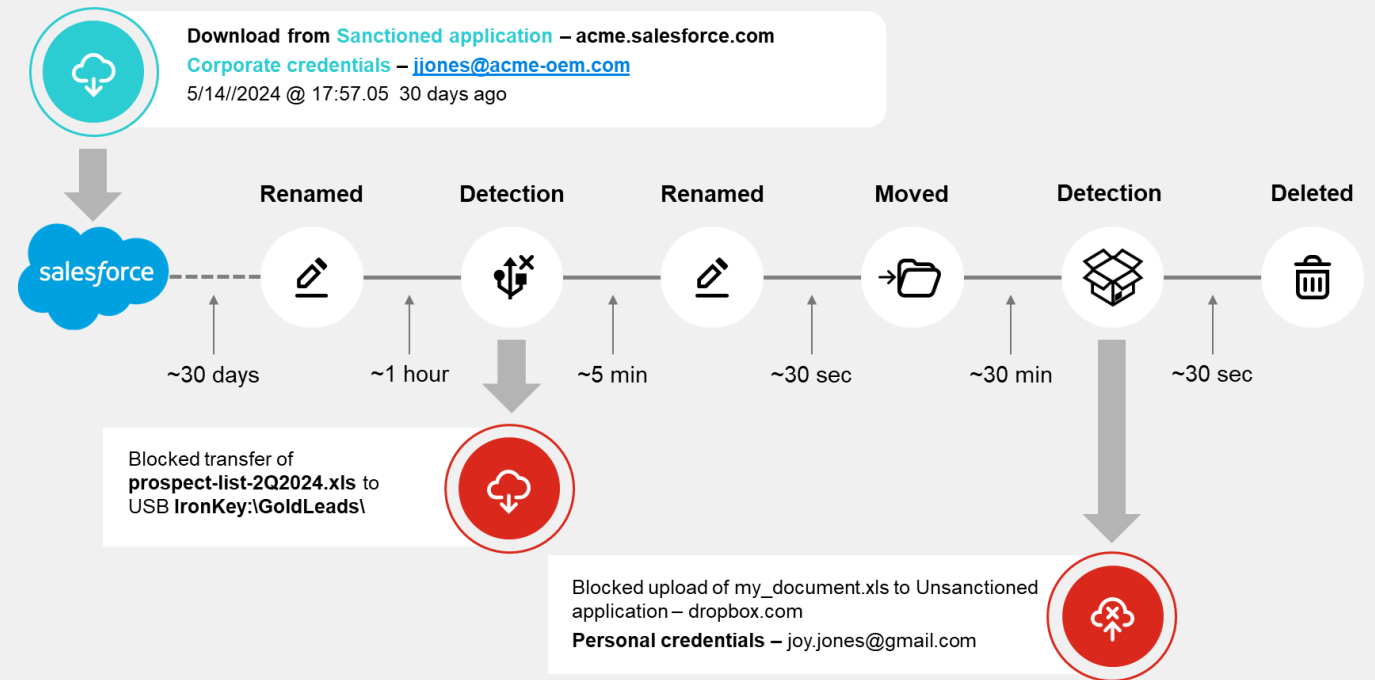


# Secure Data Flow: Protect Data From Its Origin

Protect and Track Data Based on its Source (Origin)

## Track from Origin to Attempted Egress

- Identify IP and sensitive data based on its origin
- Detect file manipulations and obfuscations
- Prevent egress based on file origin and content
- Differentiate between corporate and non-corporate accounts on SaaS Apps (e.g. Google Drive)
- View file tracking and lineage in DLP alerts



# Secure Data Flow: Analyst Experience

## Summary

- Roadmap exfiltrated by an off-boarding employee to their personal cloud drive
- Employee has attempted to cover their tracks by renaming the file prior to exfiltration.

## Action


- Secure Data Flow identifies data being downloaded from corporate SaaS app
- Files are tracked by the FortiDLP agent and file manipulation activity is audited.
- At the point of egress, the file is controlled based on data origin and destination, i.e. a corporate cloud drive to personal cloud drive.

80  
High

File from sensitive corporate Google Workspace location uploaded to Google Drive associated with an unapproved/non-corporate account  
Wednesday, 22 November 2023 at 14:30:32 GMT+01:00

Add to case ▾ Export ⌵

JC  
Juan Christianos  
UX designer

  
DESKTOP-ABC1234  
WINDOWS 11

Labels

Windows | Department | Automated | All | bot | 7.6.1 | Country | UK

File from corporate Google Workspace uploaded to unsanctioned web app

Policy group: My test DLP policies  
#dlp #exfiltration #usb #block

Data lineage

File downloaded

20/11/2023 at 10:20:30 GMT+01:00

File name (original)  
Q4 Product Roadmap (NDA).png  
More details ▾

Web app (source)  
Google Drive  
More details ▾

Associated account  
juan.christianos@nextdlp.com

File uploaded (blocked)

20/11/2023 at 10:22:57 GMT+01:00

File name (current)  
cute\_cat.png  
More details ▾

Web app (destination)  
Google Drive  
More details ▾

Associated account  
j.m.christianos@gmail.com

Block upload

Succeeded

Display message - config

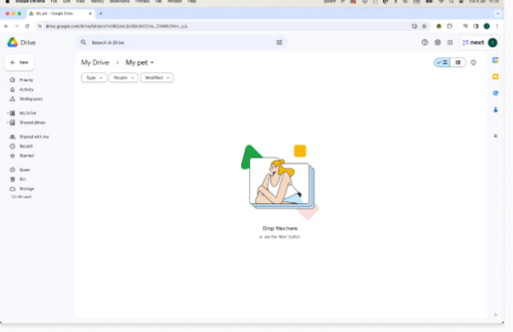
Succeeded

Header  
Upload blocked

Body  
According to the company's acceptable use policy, uploading sensitive files to non-corporate Web apps is prohibited. Please visit the corporate policy on how to handle sensitive data below

Screenshot

Succeeded



All event details

key	value_value.val	key	value_value.val
key	value_value.val	key	value_value.val





# Secure Data Flow - Data Lineage

## Summary

Data lineage provides analysts with insights into the origin of egressed data, tracks data movement across the endpoint and identifies data manipulation prior to egress.



## FortiDLP Solution



- 1 The FortiDLP agent identifies data being downloaded from corporate and private SaaS applications.
- 2 The agent tracks data movement and any manipulation of the data e.g., file rename, move, copy.
- 3 The origin and data lineage information is presented in a DLP detection to enable analysts to quickly understand risk.

## Value and Impact



An analyst can quickly identify where the detected data originated from and if it was manipulated before detection.

Original file name and source information


 **Q4 Report.pdf**  
C:\Downloads Lineage 

 **Google Drive**  
john.doe@company.com Sanctioned 

Data lineage


 **Data lineage** 

17.May 2024 - 18:00

 Downloaded **Q4 Results.pdf** from Google Drive as **joe.doe@company.com**


---

17.May 2024 - 18:01

 Renamed **Q4 Results.pdf** to **cute\_cat.png**


---

17.May 2024 - 18:03

 Moved **cute\_cat.png** to **C:\Users\Joe\Pictures**


---

17.May 2024 - 23:55

 Attached **cute\_cat.png** to an email in **Outlook.exe**




---

17.May 2024 - 23:57

 **Critical | 100**

Blocked email with attachment "cute\_cat.png" from a sensitive origin "Google Drive" sent to unauthorized recipient "joe@external.com"

Associated detections

 **4 associated detections**  
Related to the same original file  





# Use Case: Monitoring GenAI Usage

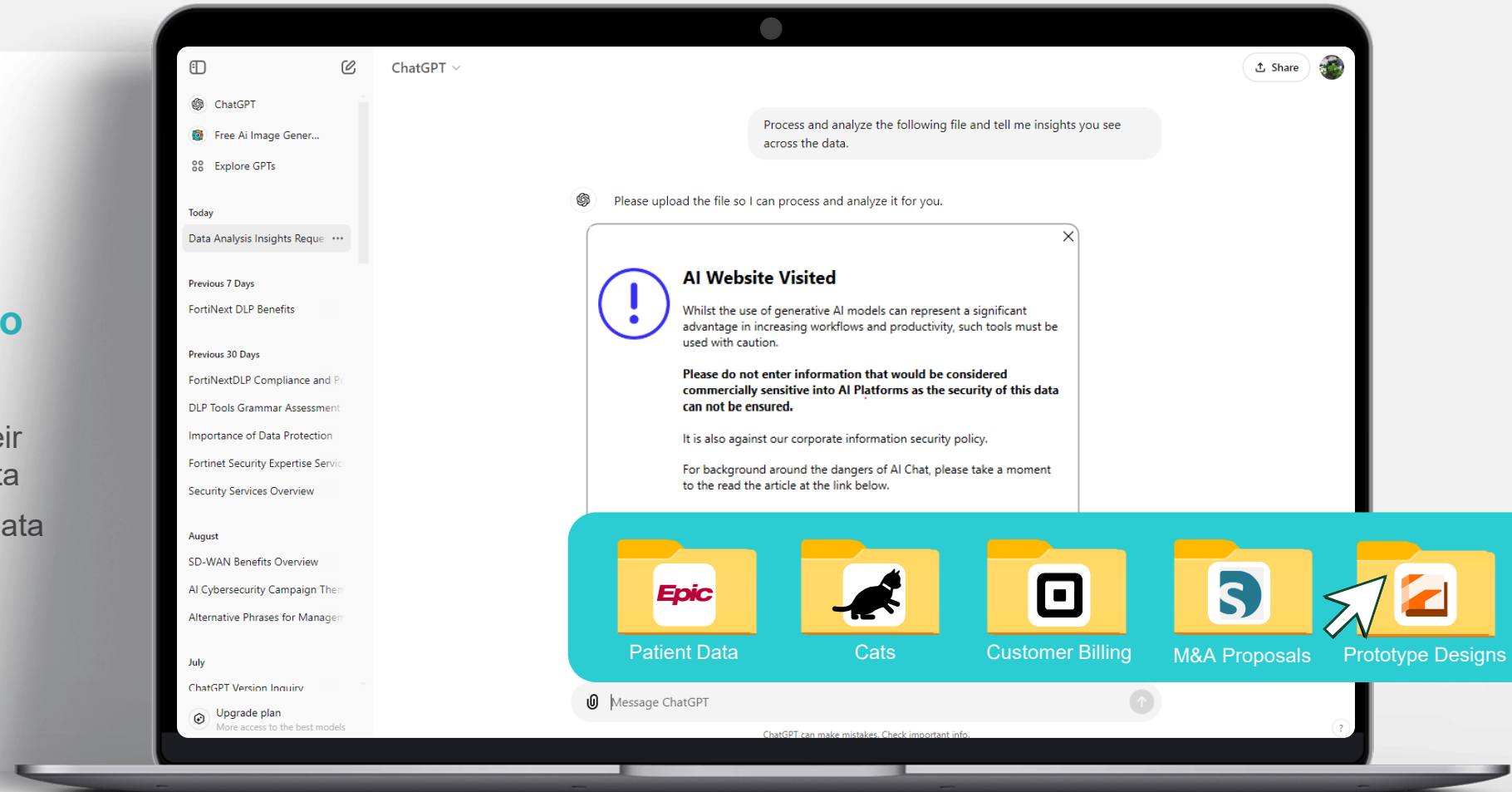


# Protect Against Sharing of Sensitive Data with AI Tools

Protect data without impacting productivity when employees use popular unapproved GenAI tools.

## Guard against employees uploading sensitive data to GenAI and other AI tools

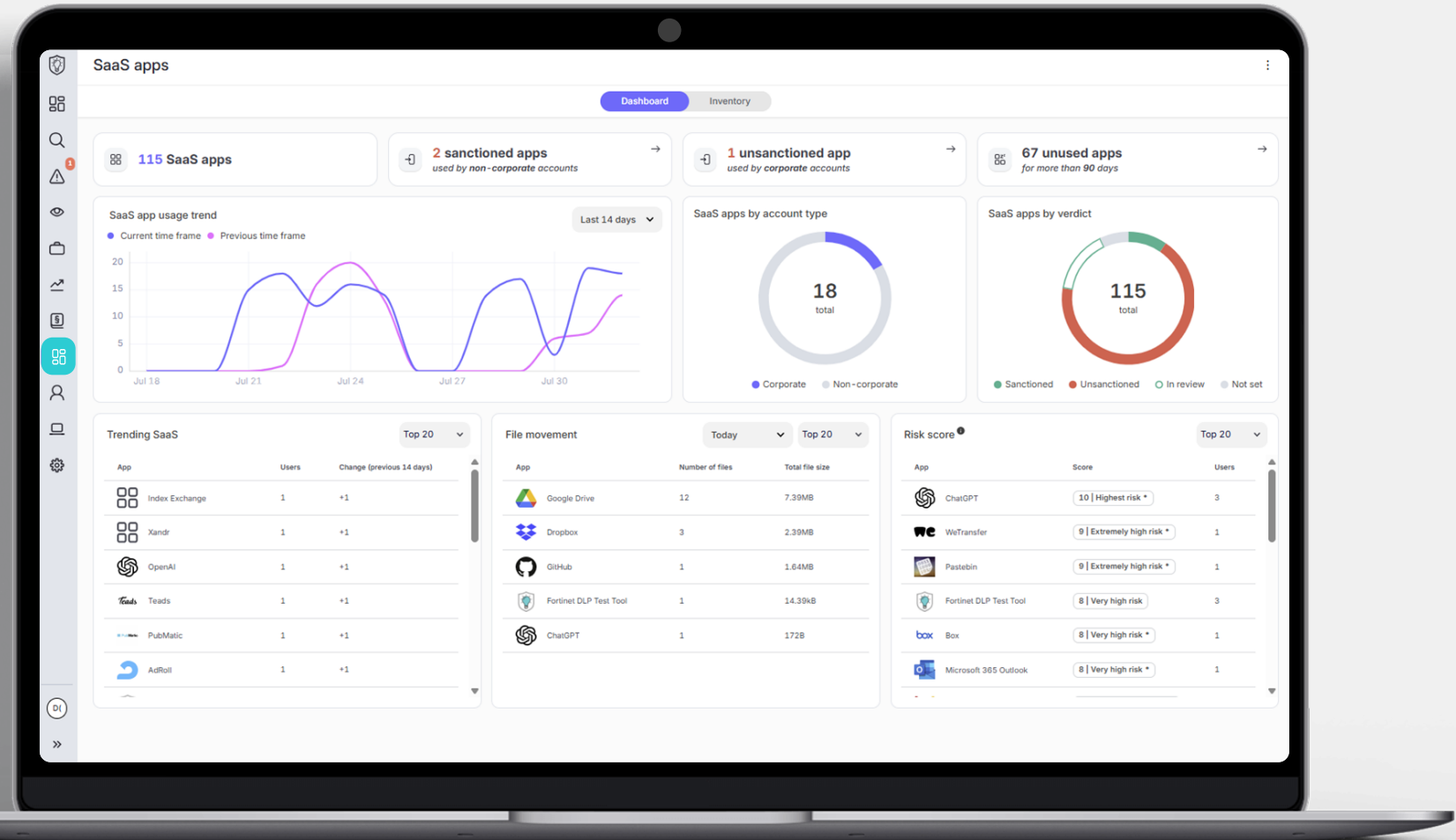
- Alerts employees/users when their actions may expose sensitive data
- Drives accountability for proper data handling by employees



# Report & Educate Employees on Safe GenAI Usage

## Full visibility into SaaS apps including GenAI tools

- Identify employees visiting sanctioned and unsanctioned GenAI apps
- Audit the types of data being pasted and uploaded / download from GenAI tools



deepseek



Grok





# Use Case: Forensics + Case Management



# Report & Educate Employees on Safe GenAI Usage



## Accelerated Investigations through FortiAI

- Analyst activates FortiAI (AI Assistant)
- Requests a summarization of insider threat activity referencing MITRE ENGENUITY™ Insider Threat TTP indicators
- FortiAI reasons on the incident data set and provides a detailed summary

**Insider risk & DLP sequence** [Open](#)

Severity: 75 | High | Case created by: Insider risk & DLP sequence | First detection: 4/14/23, 5:25 PM | Last detection: 4/14/23, 5:33 PM | ~8 min

**Sequence**

Initial Access (TA0001) → Defense Evasion (TA0005) → Collection (TA0009) → Exfiltration (TA0010)

Initial Access: 1 x Low | Defense Evasion: 1 x Medium, 2 x Low | Collection: 1 x Medium, 2 x Low | Exfiltration: 1 x High

**Entities**

Joy James (Developer) | Manager: Liz Brown | Department: Engineering | Office: London - UK | Labels: Leaver, +5 more

**6 Events**

Timestamp	Description	Policy
4/14/23, 5:33 PM	File upload blocked to "www.dropbox.com" with personal account "joy.james@gmail.com" from Google Chrome: Archive.zip with size 1.4KB containing uninspected content.	Sensitive file uploaded to personal file share website
4/14/23, 5:29 PM	Finder creating compressed file at /Users/joy.james/Downloads/Archive.zip, containing 2 files including trading_algorithm.py, price_estimator.py	Compressed file created
4/14/23, 5:29 PM	This node connected to Wi-Fi network called "Huckletree Guest". However, based on the Wi-Fi landscape and historical connections, the node is expected to connect to the network called "jasa"	Connection made to unauthorized Wi-Fi network
4/14/23, 5:29 PM	File downloaded from git.acmecorp.com using Google Chrome: /Users/joy.james/Downloads/trading_algorithm.py of size 27B containing Source code with at least 1 match	Sensitive file downloaded from company domain
4/14/23, 5:29 PM	File downloaded from git.acmecorp.com using Google Chrome: /Users/joy.james/Downloads/price_estimator.py of size 27B containing Source code with at least 1 match	Sensitive file downloaded from company domain
4/14/23, 5:25 PM	User Joy James logged in outside expected working hours at Tue April 4 17:25:50 GMT 2023	Login outside office hours

**FortiAI: AI-based Assistance**

Isaac Kennedy Just now  
Create a summary of this case

**XTND Just now**  
**Defense Evasion (TA0005)**  
The user, Joy James, logged in outside of expected working hours, which could be an attempt to avoid detection (T1078). Additionally, the user connected to an unexpected Wi-Fi network, "Huckletree Guest", instead of the expected "jasa" network, which could be another evasion tactic (T1562.006). The creation of a compressed file containing sensitive source code files is also indicative of evasion (T1027).

**Collection (TA0009)**  
Joy James downloaded two files containing source code from git.acmecorp.com, namely "price\_estimator.py" and "trading\_algorithm.py" (T1530, T1213.003). This action falls under the collection tactic as the user is gathering information that could be used for malicious purposes.

**Exfiltration (TA0010)**  
An attempt was made to upload a compressed file containing the previously downloaded source code files to Dropbox using a personal account (T1567.002). This action was blocked, indicating an attempt at data exfiltration.















**Conclusion**  
The sequence of events suggests that the user, Joy James, attempted to exfiltrate sensitive data from the company. The user employed evasion tactics, such as logging in outside of normal working hours and connecting to an unexpected Wi-Fi network. They collected sensitive source code files and attempted to exfiltrate this data by uploading it to a personal Dropbox account. This sequence of events aligns with several tactics in the MITRE ATT&CK Framework, including Defense Evasion, Collection, and Exfiltration.

[Copy](#) [Provide feedback](#)




# Investigation and Forensics

Your Business Data, Your Cloud Data Storage



Cases

 Tyrrell Suspicious Activity Investigation Open Edit

Severity

Critical

Add tags to the case

Created by

Chris Tyrrell

Case summary

Edit

Case Summary

Chris Tyrrell, the Director of Sales Engineering, exhibited suspicious behavior indicative of potential data exfiltration and insider threat activities. The sequence of events includes web searches related to quitting his job, renaming and uploading corporate files, copying regulated content, and downloading sensitive data from unauthorized sources. These actions align with various MITRE ATT&CK tactics and techniques, suggesting a deliberate attempt to exfiltrate sensitive information.

Event Details TA0043 (Reconnaissance)


- Chris Tyrrell performed a web search using the term "how do I quit my job without notice?" on Google Chrome. This indicates potential reconnaissance activity as he may be planning to leave the organization abruptly.

Entities

Department -

Manager -

Office address -



Tyrrell-demo-win10x64













Microsoft Windows 10 Pro


OS Windows


Agent version 12.0.5


13 Events


Pinned fields Default Columns Items / page 50


Timestamp	Entities	Labels	Description
> 01/22/2025, 07:07:36 PM	 Tyrrell-demo-win10x64	 Leavers + 5	 Critical C:\Use Secur
> 01/22/2025, 07:07:15 PM	 Tyrrell-demo-win10x64	 Leavers + 5	 Printe
> 01/22/2025, 07:06:49 PM	 Tyrrell-demo-win10x64	 Leavers + 5	 Critical agent
> 01/22/2025, 07:06:36 PM	 Tyrrell-demo-win10x64	 Leavers + 5	 Critical Secur mail.gc

AWS

Azure Blob

Google

MinIO

Wasabi

Forensics Storage



# Additional Features



# Feature: Cloud Drive Policies and Detections

SaaS Data Security

Standard | Enterprise

## Summary















- Employees access, share, and download files via Enterprise Cloud Drives on managed and unmanaged devices.
- FortiDLP now provides visibility and detection policies across OneDrive/SharePoint, Google Workspace, and Box.

## FortiDLP Solution

- Visibility into user and data movement across OneDrive, SharePoint, Google Drive, and Box, including file sharing and downloads across managed and unmanaged devices.
- Policies for detecting file sharing, downloading, and movement activities across supported enterprise cloud drives.
- Integration with each platform's data classification solution to ensure data sensitivity and value is factored into policy logic.

## Customer value and impact

- Comprehensive visibility into cloud drive activity and protection against data exposure in corporate cloud drives, regardless of device type or location.

User	Device	Severity	Description
 Joy Jones		Critical	Downloads <b>vacation-plan.csv</b> from <b>Acme Corp   OneDrive</b>
 Joy Jones		Info	Login outside of usual working hours
 Joy Jones		Low	Uploaded <b>vacation-plan.csv</b> to <b>Acme Corp   OneDrive</b>
 Joy Jones		High	Renamed <b>sales-contacts.csv</b> to <b>vacation-plan.csv</b>
 Joy Jones		High	Downloaded <b>sales-contacts.csv</b> from <b>Salesforce</b>
 Joy Jones		Info	Login outside of usual working hours
 Joy Jones		Info	Connected to <b>HOME_SWEET_JONES</b>



# Feature: Slack and Teams Employee Coaching

SaaS Data Security

Standard

Enterprise

## Summary

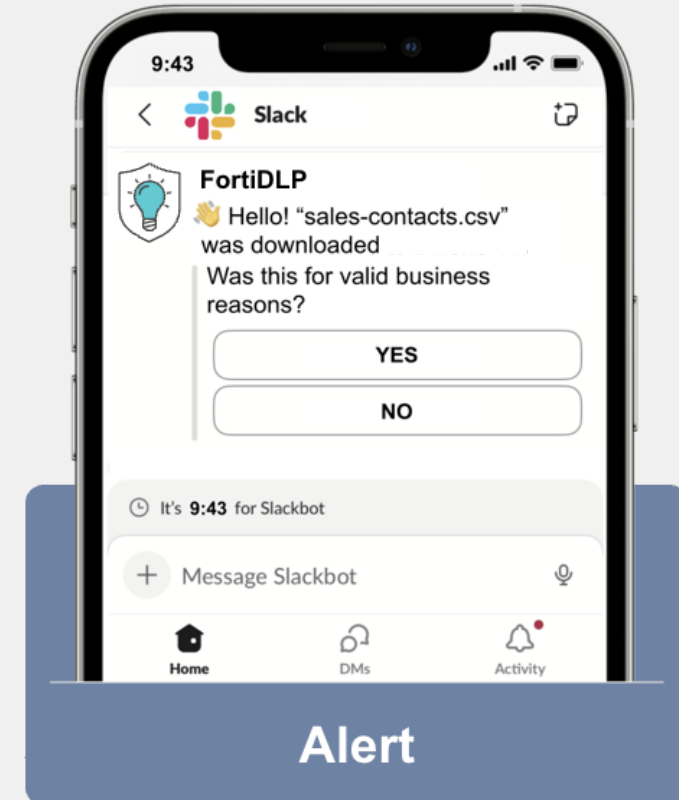
- Exposure of data within enterprise cloud drives can occur on both corporate and personal devices, so employee coaching needs to adapt to address managed and unmanaged devices.

## FortiDLP Solution

- Provide immediate feedback and training to users on any device when they violate cloud drive policies, notifying them of unauthorized activities such as file uploads, downloads, or sharing.
- Initiate automated or user-driven remediation, including:
  - Notification of automated remediation workflow (e.g., file sharing permissions altered to mitigate risk).
  - User-driven remediation via one-click actions.

## Customer value and impact

- Strengthen user awareness and accountability by delivering timely, in-context guidance that reinforces data protection policies during everyday workflows.



# Data Exfiltration from Cloud Drive to Device Prevented With Alert





# How It Works





# How FortiDLP Works: Overview

## SIEM



splunk>  
a cisco company



panther

## IAM



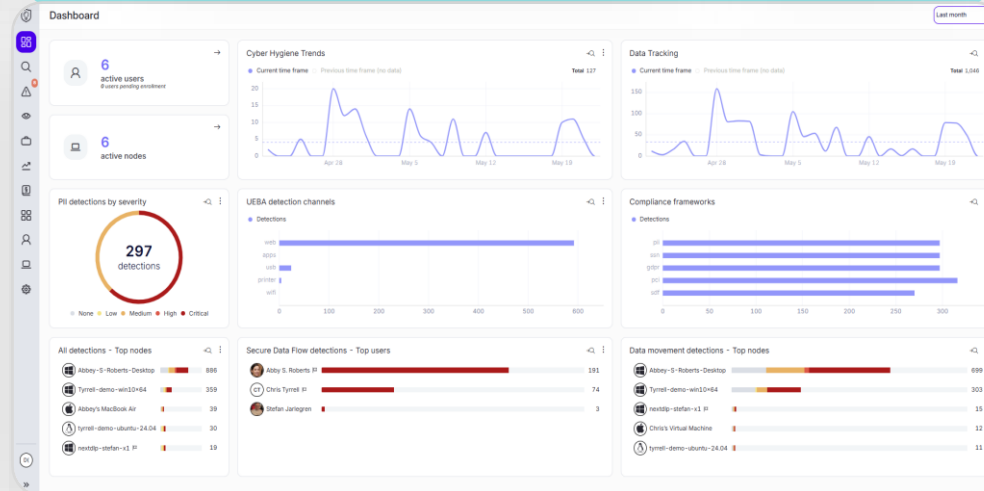
okta

## XDR



## Evidence Store

aws



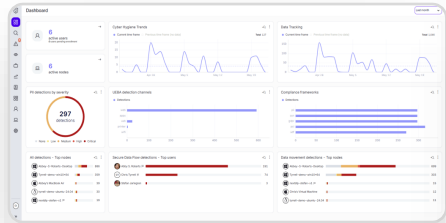
## OS Integrations



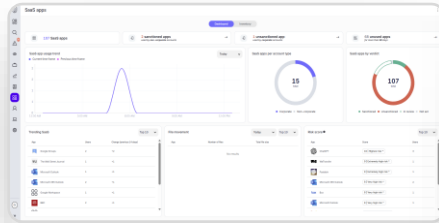
## Connectors



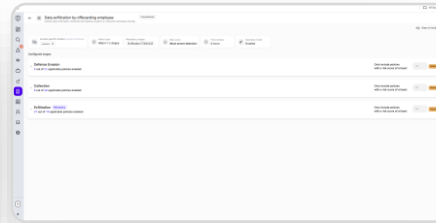
# How FortiDLP Works: Management Portal



Dashboard



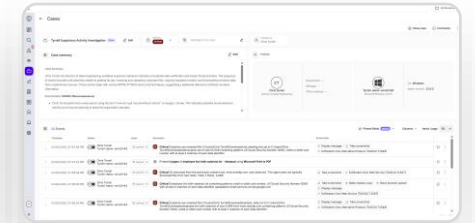
SaaS Visibility



Sequence Detection



Activity Feed



Case Management



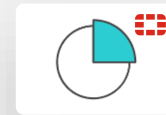
Directories



Open API



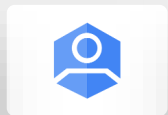
Web Hooks



Analytics



Evidence Storage



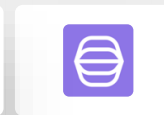
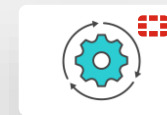
Identity



Data Classification



SIEM



SOAR



Dashboard



Investigate



Incidents



FortiAI



Cases



Users



SaaS Apps



Endpoints



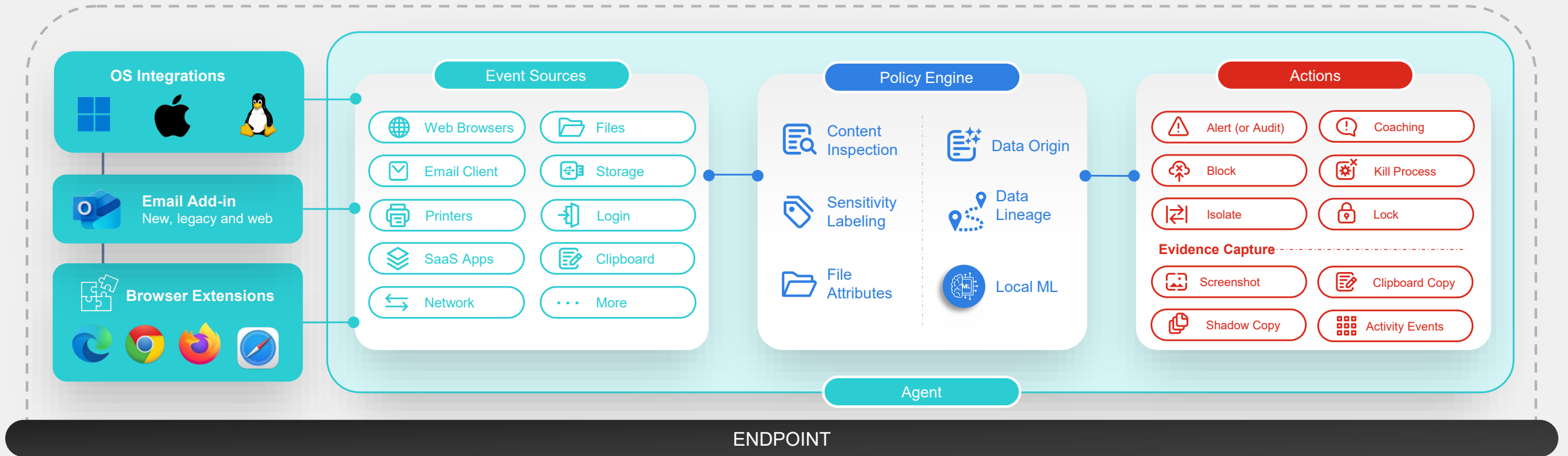
Policies



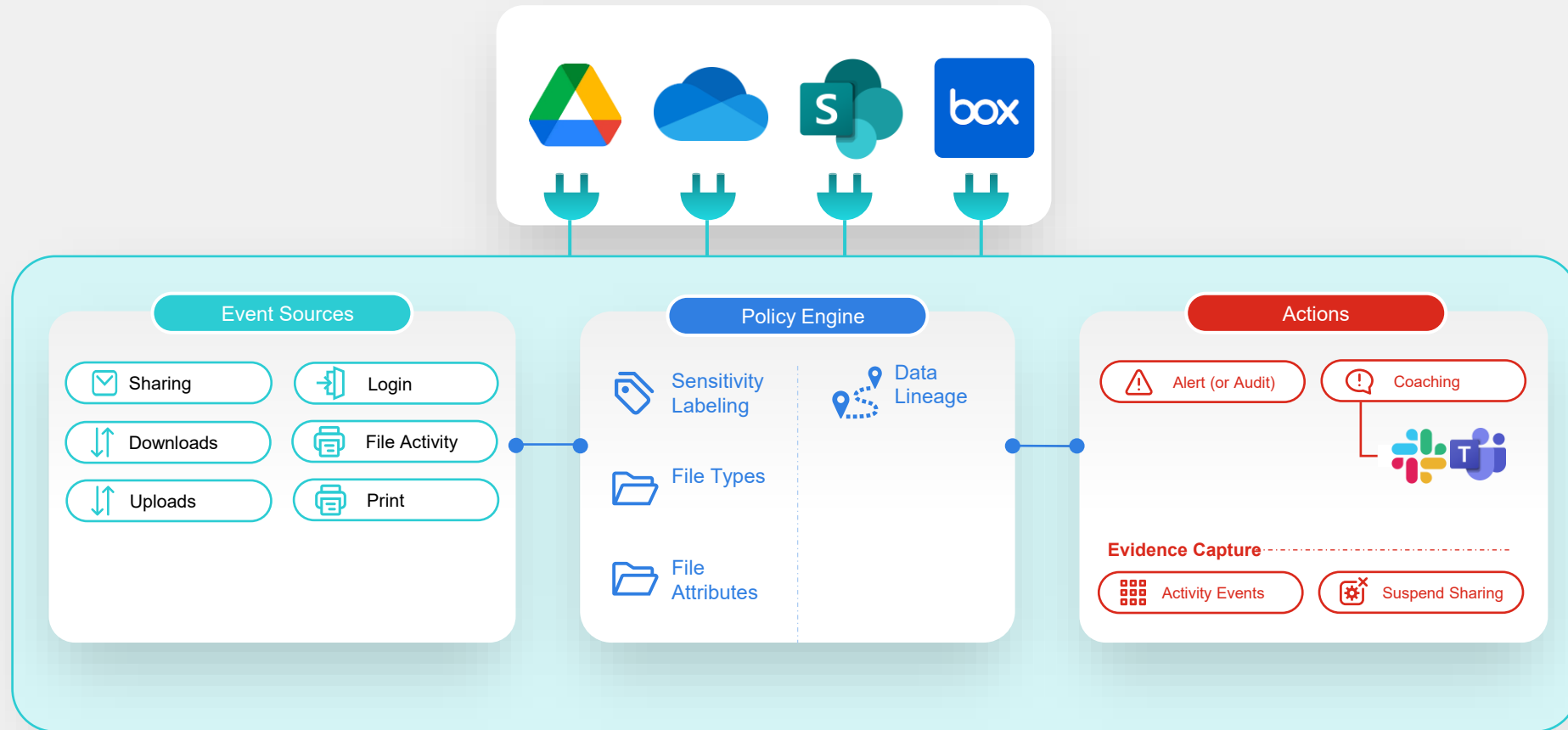
Reports



# How FortiDLP Works: Endpoint View



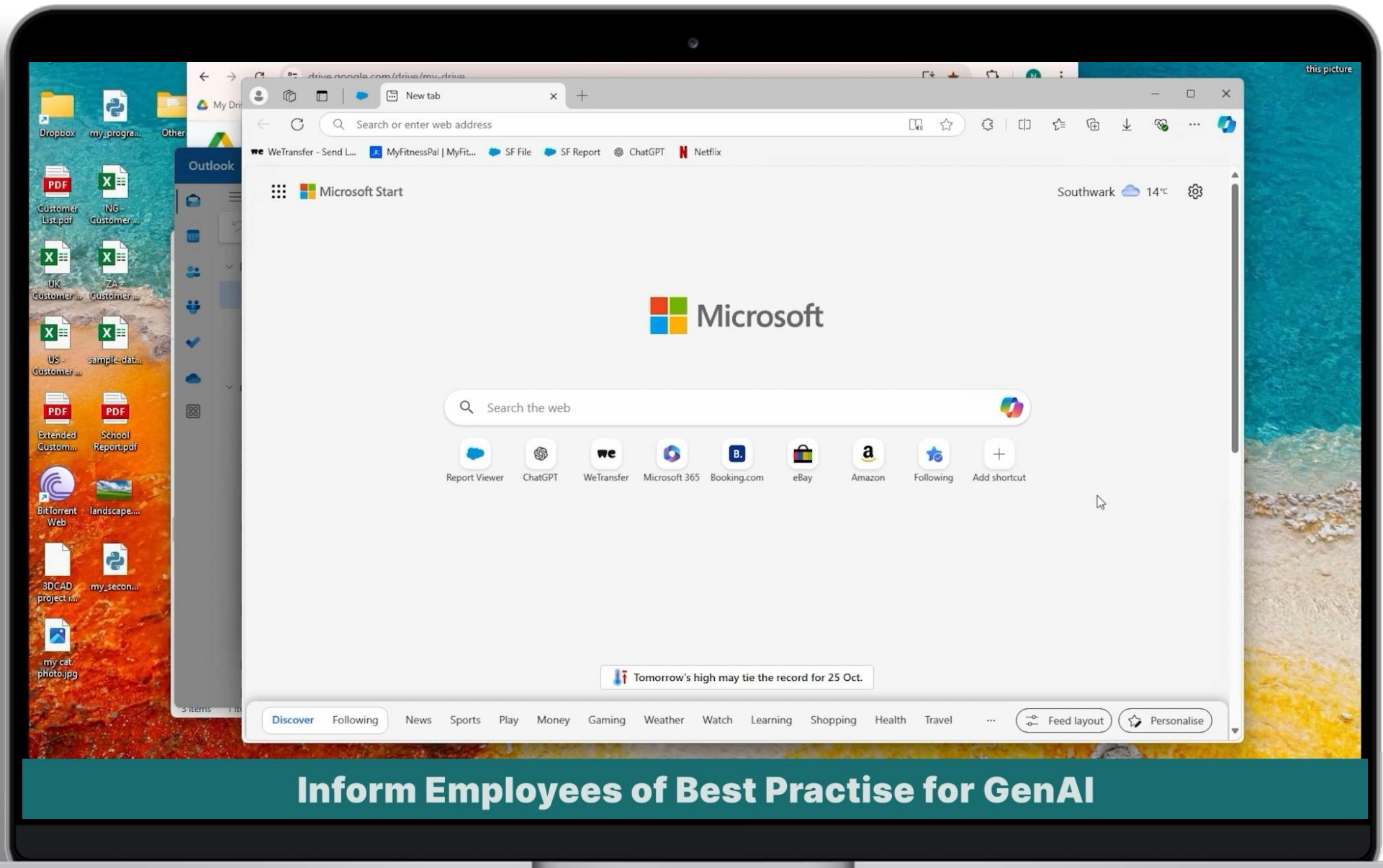
# How FortiDLP Works: Cloud Connectors





# Demo





**Inform Employees of Best Practise for GenAI**





# Why FortiDLP

FortiDLP delivers the optimal balance of risk insights and endpoint data loss prevention.



## Complete Visibility

Cloud, system, user, data, and network telemetry, plus organizational and origin context.



## Rapid Time-to-Value

Instant-on endpoint and cloud sensors; visibility without policy. Get protection from day one.



## Cross-Platform Protection

Data protection with dynamic responses, from ingress to egress, on managed and unmanaged devices.



## Accelerated Investigation

AI-enhanced detection of insider threat activity, plus workflows that reduce time to contain and respond. FortiAI (AI Assistant) ups the game for security operations.



The background features a dark gray grid of squares, some of which are semi-circular at the top or bottom. Several solid red horizontal bars are positioned at various heights. In the bottom right, there is a light gray grid of dots and a vertical gray bar. The word "FORTINET" is centered in a bold, white, sans-serif font, with the "O" replaced by a red square with a white grid pattern.

**FORTINET**