

The FORTINET logo is displayed in white, uppercase letters. The letter 'O' is replaced by a red square icon containing a white grid pattern.

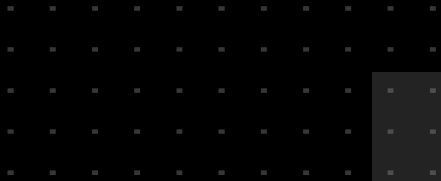
FORTINET

Anticipate and Prevent Data Theft

Introducing FortiDLP

The IntegraONE logo is shown in white text on an orange square background. The word 'Integra' is in a standard sans-serif font, and 'ONE' is in a larger, bold sans-serif font with a small cluster of white dots above the 'O'.

IntegraONE



Q325

Agenda

- Fortinet Intro
- Our New Currency - Data
- Introducing FortiDLP
- Use Case – Tracking Data from Origin
- Features
- Available Services
- Let's move forward?



Securing People, Devices and Data Everywhere

Est. 2000 – Sunnyvale CA

15,000+ employees

26 Support & Dev. Centers

170+ Global Cloud Locations

80% of Fortune 100

72% of Global 2000

20%+ Annual Growth
(\$6.4B)

**#1 Cybersecurity
Company in the World**

**Leading Every Evolution
of Cybersecurity**

- ✓ *Most Deployed*
- ✓ *Most Validated*
- ✓ *Most Patented*
- ✓ *Broadest Portfolio*

55+ Enterprise Products

1371+ patents issued

130+ Analyst Reports

12 Gartner Magic Quadrants

835,000+ WW Customers

#1 WW FW Market Share (52%)

Over 12.8m units shipped





The **Most Trusted** U.S.-Based Cybersecurity Company

Fortinet is ranked #7 in the Forbes Most Trusted Companies



#1 in Enterprise Networking & Security

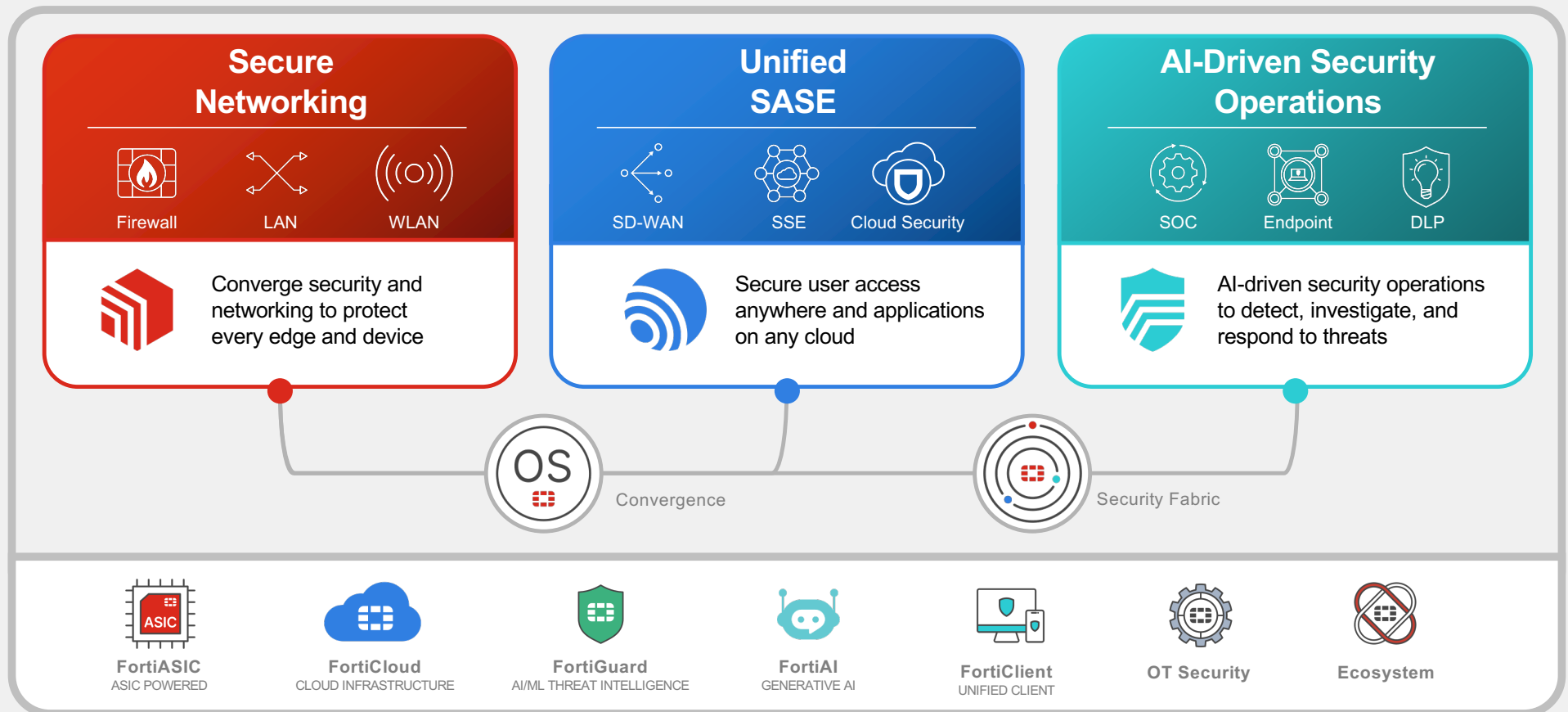
80% of Fortune 100 and **72%** of the Global 2000 depend on Fortinet to stay secure



Notes: Industry categories are based on 2024 billings from the G2000 list. G2000 - based off of the 2024 Forbes list; total number of accounts is 1,939 after factoring in M&A activity since publication. F100 - based off of the 2024 Fortune list; total number of accounts is 100 after factoring in M&A activity since publication.

© Fortinet Inc. All Rights Reserved.

The Most Advanced & Comprehensive Cybersecurity Platform

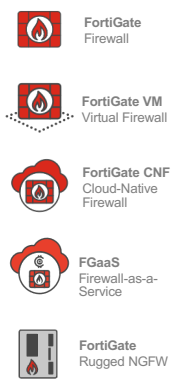


Fortinet Security Fabric Portfolio

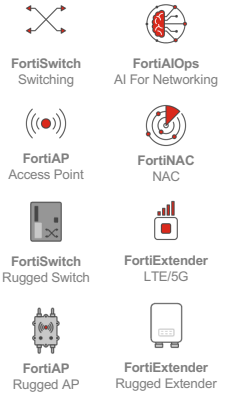
Secure Networking



Network Security



Enterprise Networking



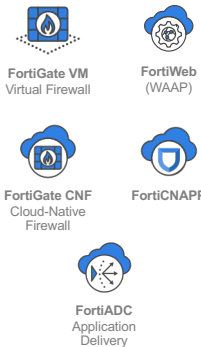
Unified SASE



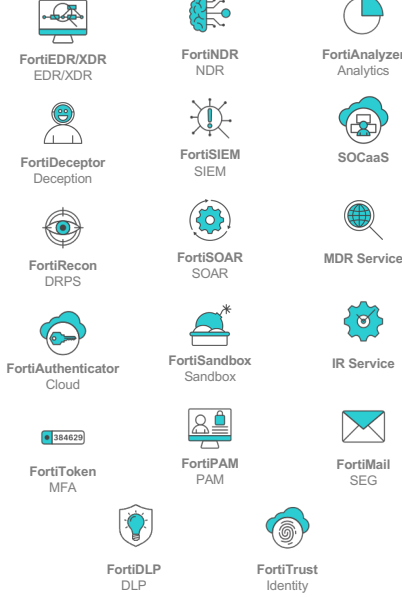
Secure Access



Cloud Security



Security Operations

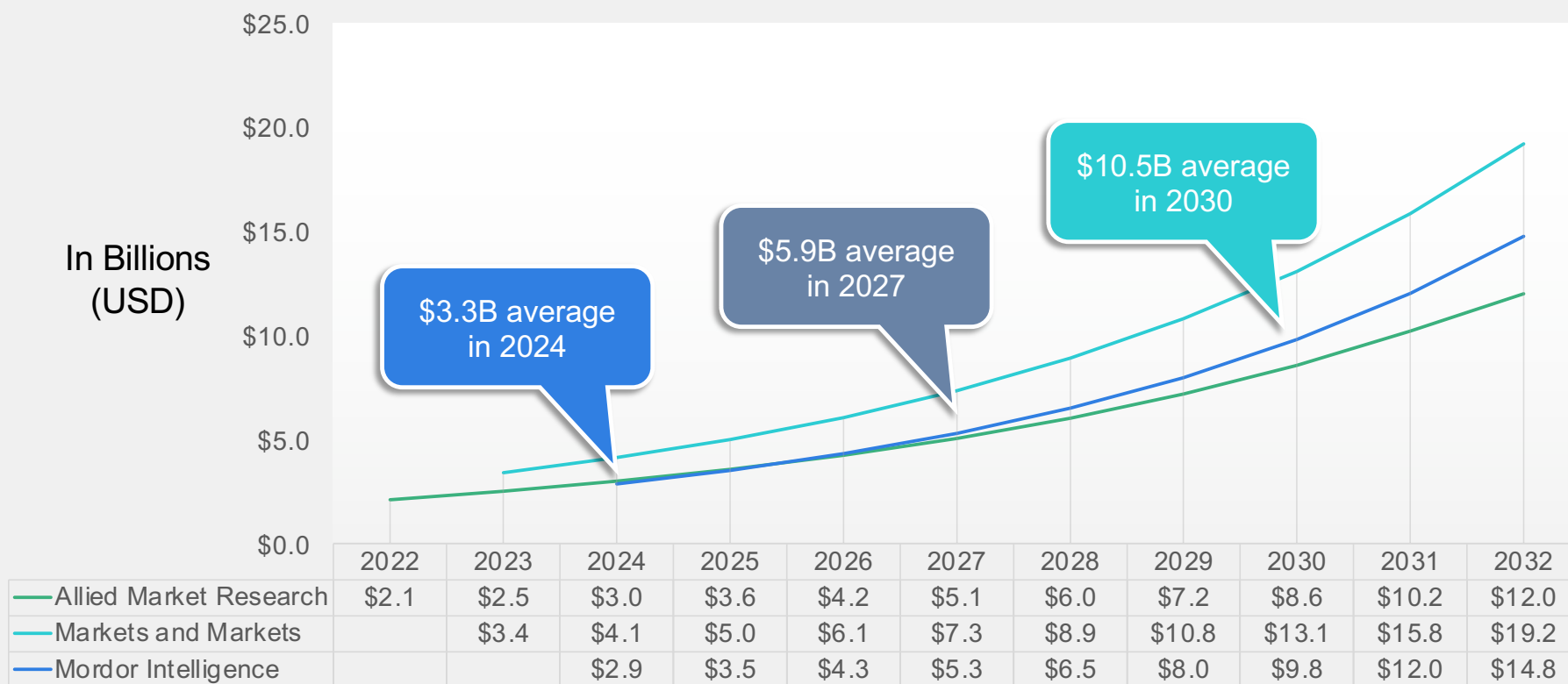




Our New Currency – Data



Data Loss Prevention Market Size



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

Source: Cost of a Data Breach Report 2024," Ponemon Institute - 2024
Source: "2025 Cost of Insider Risks: Global," Ponemon Institute - Spring 2025

Securing Data Is Complex

Use Cases

Compliance

Prevent Data Theft

Stop Malicious Insiders

Stop Accidental Leaks

Train Employees

Physical Locations

Branch

Campus

Data Center

Cloud

Remote

Network Environment

On-premises

Cloud

Hybrid

OT

Cyber-physical

Network

Network Security

SD-WAN

SASE

Type of Data

Intellectual Property

Corporate Data

Customer/Client/Patient Data

Data States

At Rest

In Use

In Transit

Data Locations

Data Stores (On-Prem)

Data Stores (Cloud)

SaaS

Endpoints

Intra-Network Transit

Points of Egress



AI



Tech and Tools

Platform

Discovery & Classification

Network DLP

Cloud DLP

Endpoint DLP

Insider Risk Management

Data Security Posture Management

Integrations

Analytic/SIEM

SOAR

XDR

More...



Introducing FortiDLP

Data Loss Prevention and Insider Risk Management



FortiDLP Global Customers

Across a Variety of Industry Verticals & Company Sizes

coinbase

 RIVIAN

dyson

 Versant
Health™

 Investec

 KARMA

 scansource®

 DrFirst.
Unite the Healthiverse™

 NORGES BANK
INVESTMENT MANAGEMENT

 tpi COMPOSITES

EnactSM

 CIG®
Capital Insurance Group

iCapital.
NETWORK

 LRMG

 Couchbase

MPS

Supporting Customers from 100 to 500,000 Endpoints.



Introducing FortiDLP



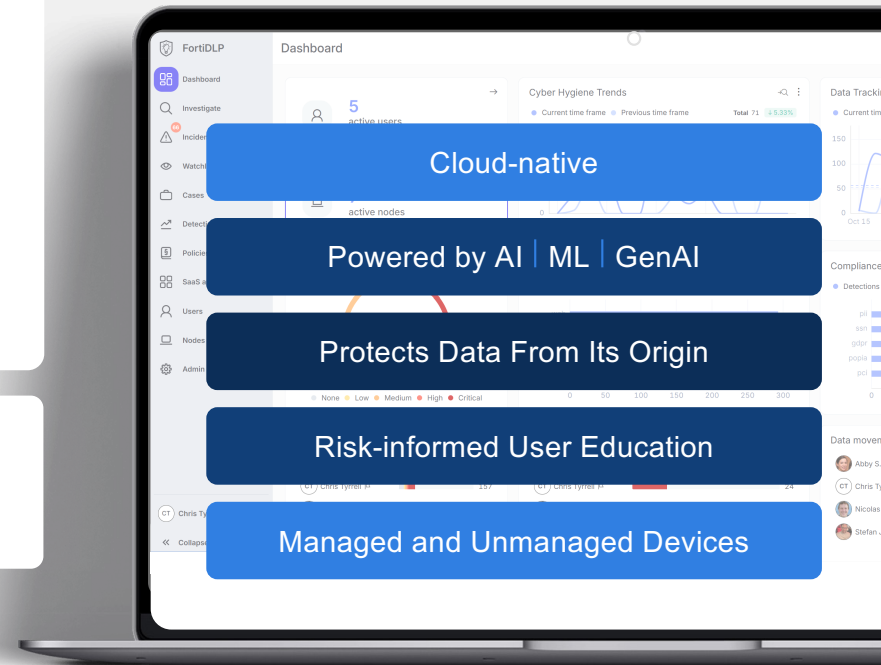
Next-Generation Endpoint DLP and Insider Risk Management Solution Anticipates and Prevents Data Theft

- Full visibility into data flows and risks
- Real-time context and content-level inspection
- Data protection across SaaS apps including Shadow AI
- Risk-informed user education at the point of data access

Data Loss
Prevention

Insider Risk
Management

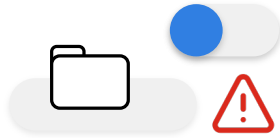
SaaS
Data Security



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



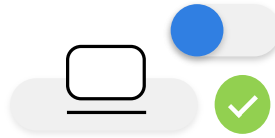
What is FortiDLP?



Data Loss Prevention (Endpoint)

Enhanced by AI/ML

-  Inspect context/content
-  Prevent data theft
-  Ensure compliance



Insider Risk Management

Enhanced by GenAI

-  Monitor user behavior
-  Identify risky actions
-  Mitigate risks



SaaS Data Security

Guardrail Data Access/Usage

-  Score risk across apps
-  Track data flows
-  Guardrail GenAI usage



Risk-Informed User Education



Prompt/nudge Users



Drive accountability



DLP Architecture & Security Challenge

1 Data in motion

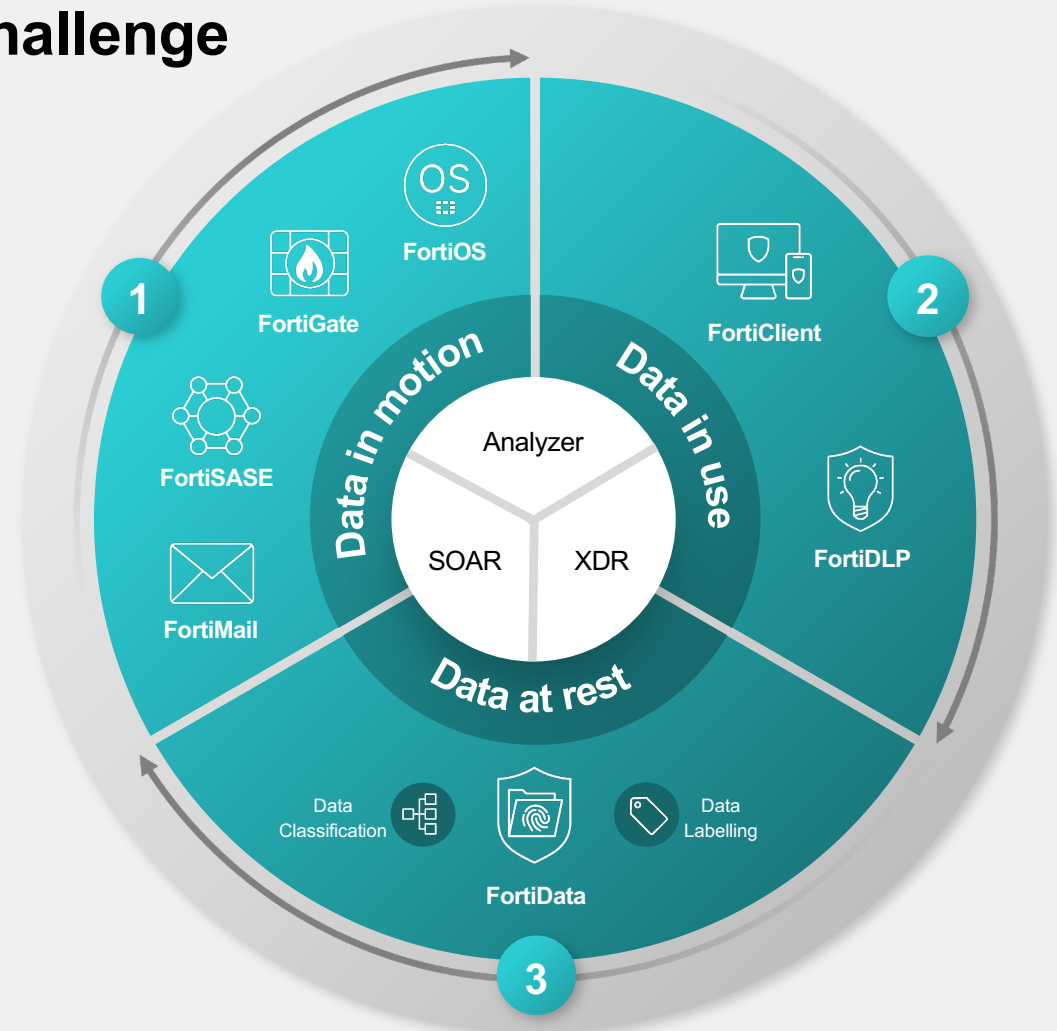
- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

2 Data in use

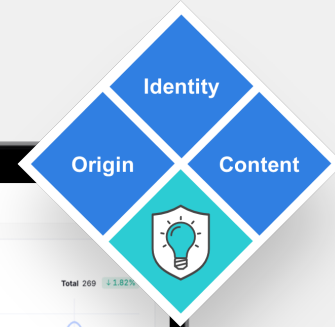
- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT. Corporate sensitive data being accessed from anywhere

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

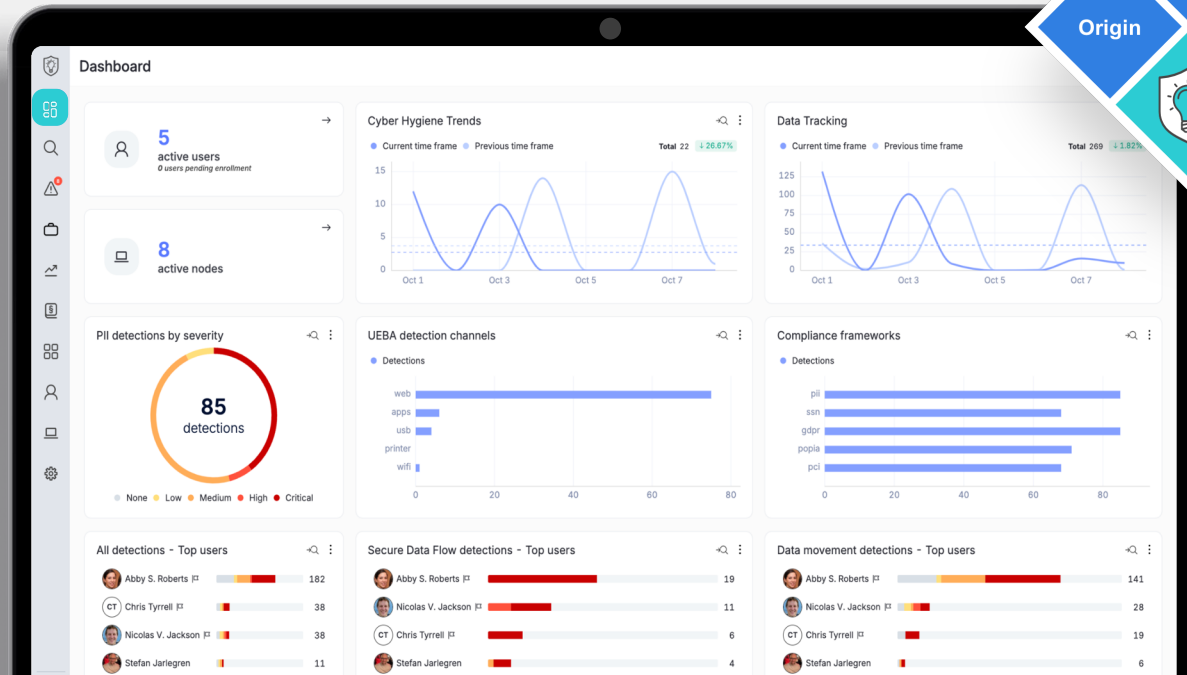


Data Loss Prevention: Differentiation



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

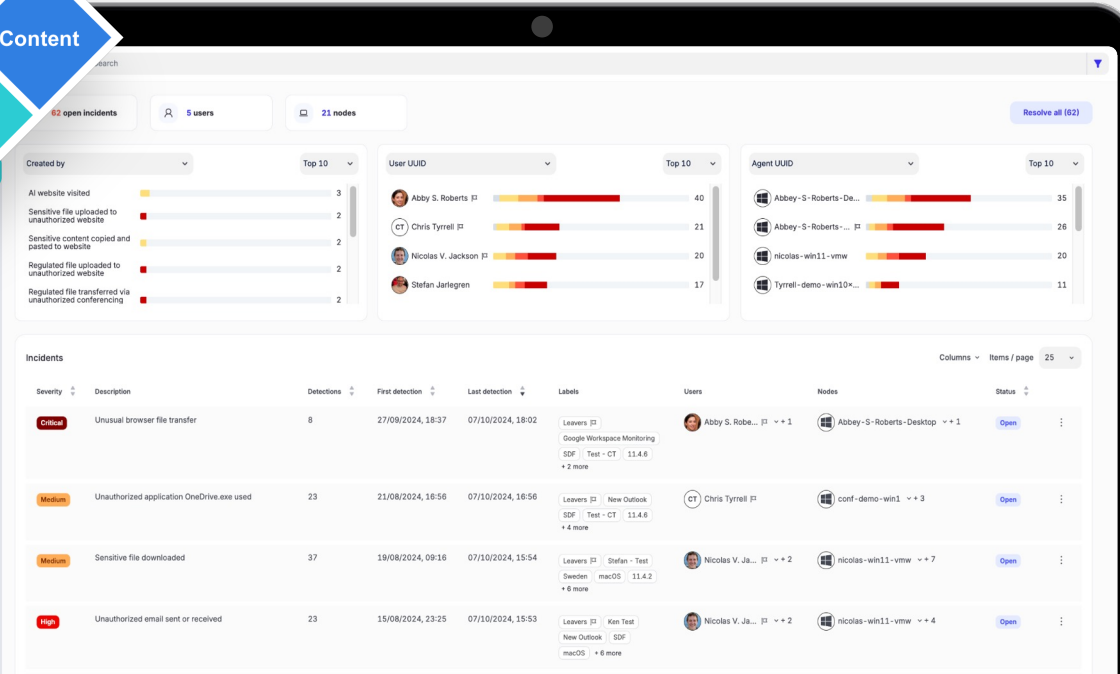
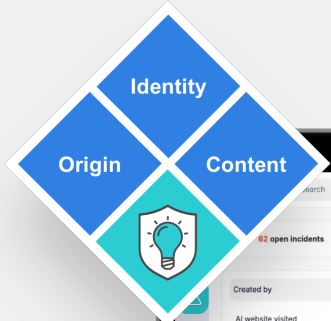
Instant Visibility

Secure Data Flow

Real-time User Education



Insider Risk Management: Differentiation



Insider Risk
Sequence Detection

Instant Visibility

File, Clipboard and
Screen Forensics

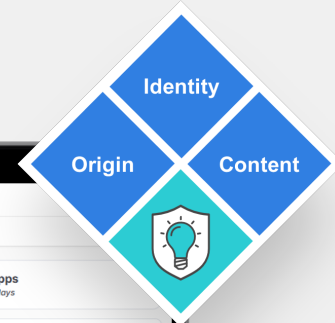
FortiAI
Analyst Insights

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

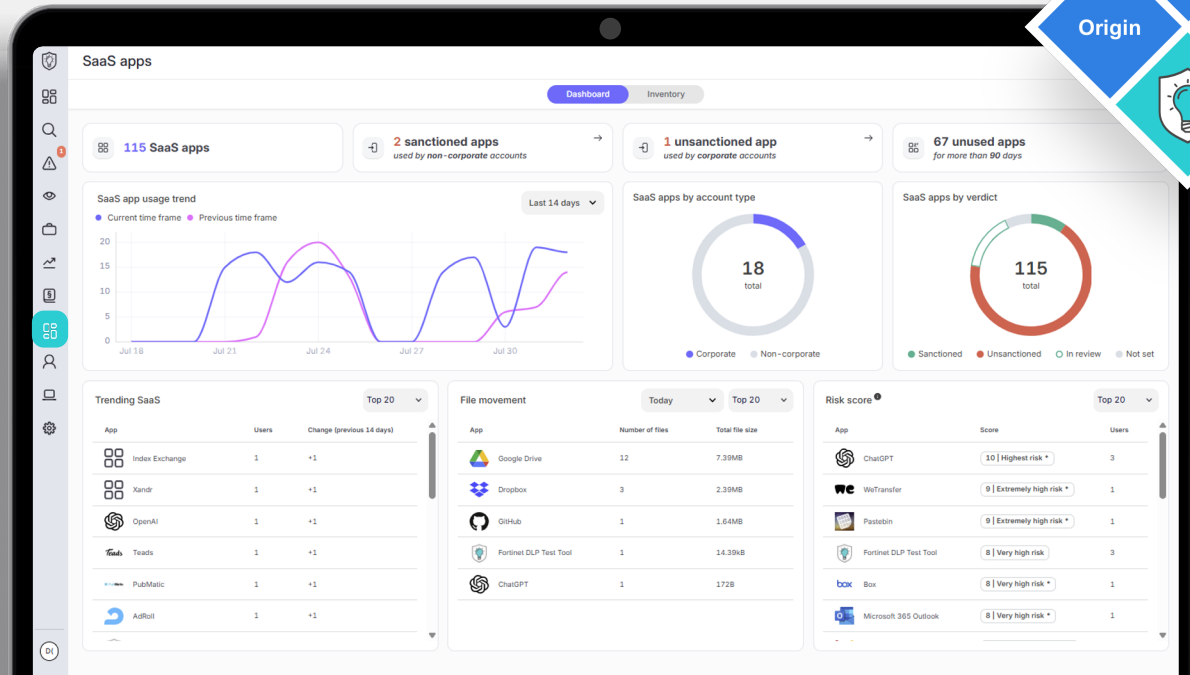


SaaS Data Security: Differentiation



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

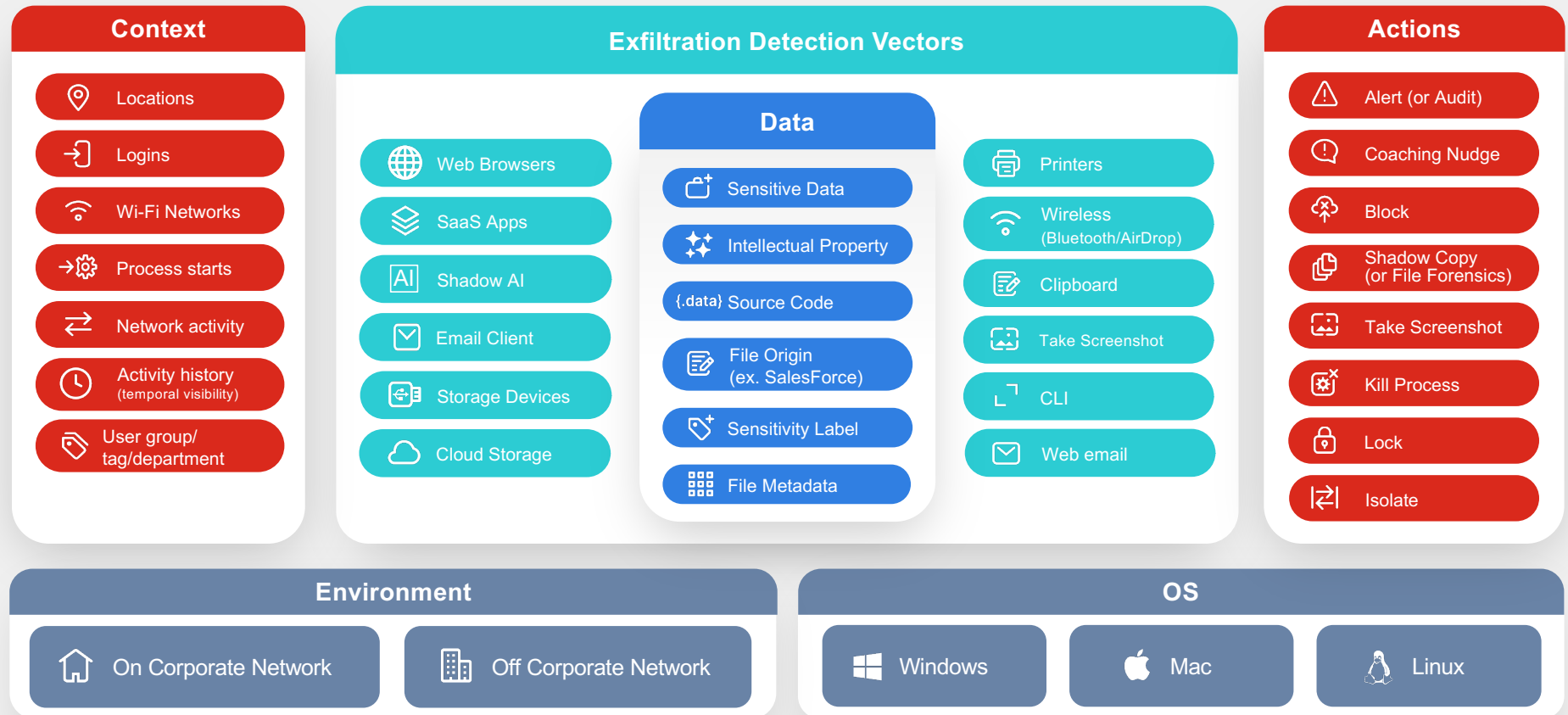


Education at the Point of Use of Sensitive Data

- 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



Deep and Broad Contextual Visibility is Required to Protect Data



Integrations: Endpoint



Windows



macOS



Linux

OS Support



Edge



Chrome



Firefox



Safari



Arc



Brave



Vivaldi

Browser Extensions



Google Drive



OneDrive



SharePoint



Outlook



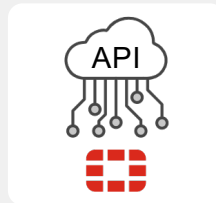
Outlook

Cloud Drive Connectors

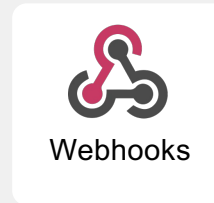
Add-ins



Integrations (Other Integrations)



Open API



Webhooks



Azure
Sentinel

splunk>
a CISCO company

Splunk

panther

Panther



Tines

torq=

Torq



Microsoft
Entra ID



Google Cloud
Identity

okta

Okta

SIEM

SOAR

Identity



Microsoft
Entra ID



Google
Workspace



LDAP



Microsoft
Purview



Amazon S3



Azure Blob



Google



MinIO



Wasabi

Directories

Data Classification

Evidence Storage

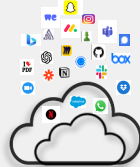


Secure Data Flow: Files downloaded from Web Apps

Track and control data originating from Web Apps

- Track file downloads from supported browsers
- Detect account used
- Detect file manipulation prior to egress
- Control egress using data origin and content

SaaS App Origin Configuration



File origin parameters (Windows and macOS only)

SaaS apps

Corporate accounts in Sacntioned Apps

Browser Download Tracking



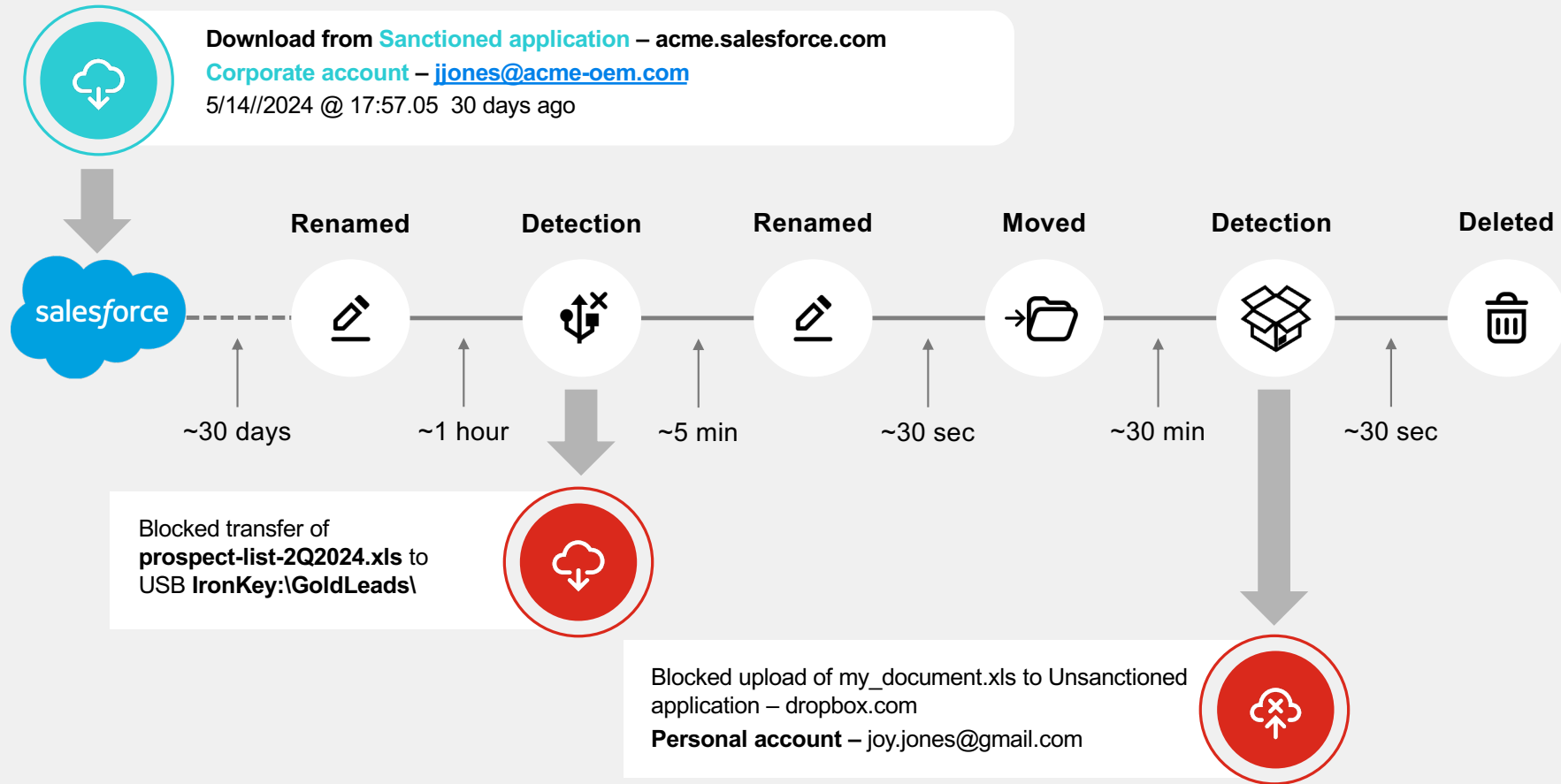
File Movement Tracking



Detections & Controls



Secure Data Flow: Origin Aware Data Protection



Investigation and Forensics

Forensics on Your Territory

FortiDLP

Dashboard

Investigate

Incidents

Watchlists

Cases

Detection reports

Policies

SaaS apps

Users

Nodes

Admin settings

← Cases

Legal Hold - Tyrrell Investigation Open Edit

Severity Critical

#ctyrrell

Created by Chris Tyrrell

Case summary

Case Summary

Reveal detected a series of suspicious activities involving an employee named Chris Tyrrell, who holds the position of Director of Sales Engineering. The activities suggest potential data exfiltration and misuse of sensitive information, including the handling of files containing US Social Security Numbers (SSN) and the use of unauthorized browsers and private browsing modes.

Event Details

The sequence of events began with Chris Tyrrell renaming a sensitive file from `employeeData.pdf` to `personal_medical_records.pdf`, which contained SSN information. Shortly after, the same file was compressed into a zip file

14 Events

Timestamp	Entities	Labels	Description	Pinned fields
10/07/2024, 09:53:14 AM	Nicolas V. Jackson nicolas - win11 - vmw	Leavers + 4	Critical File upload blocked to "drive.google.com" with personal account "nick.is.cool10011@gmail.com" from Google Chrome: my holiday photo.jpg with size 38.0KB from qush.my.salesforce.com (robbie.jakob - whitworth@qush.com) containing pattern email address with at least 3 matches.	Block Take s
09/27/2024, 12:39:15 PM	Chris Tyrrell Tyrrell - demo - win10x64	Leavers + 4	Critical Email blocked to ct2191977@gmail.com with 1 attachments: picnic.zip (30.4KB) containing patterns credit or debit card number, US Social Security Number (SSN) with at least 3 matches of each data identifier in the email body, subject, or attachments	Display Exfiltr
08/26/2024, 08:26:14 PM	Chris Tyrrell Tyrrell - demo - win10x64	Leavers + 5	Critical File upload blocked to "drive.google.com" from Brave: 085619_smart_pass_through_2635-10a-2.dwg with size 1.0MB from drive.usercontent.google.com (chris.tyrrell@gw.jazzdev.io).	Block
06/24/2024, 10:47:52 AM	Chris Tyrrell Tyrrell - demo - win10x64	Leavers + 4	Critical Unauthorized browser used: Brave	Display

CT Chris Tyrrell

← Collapse

aws
AWS

Azure Blob

Google

MinIO

Wasabi

Forensics Storage

Report on the MITRE ATT&CK indicators in this case.

XTND less than 1 minute ago

Case Summary

Chris Tyrrell, the Director of Sales Engineering at JazzDemoCloud, engaged in multiple suspicious activities involving sensitive data. These activities included unauthorized browser usage, downloading and renaming sensitive files, attempting to upload these files to personal cloud storage, and ultimately writing sensitive data to a USB device. Reveal detected and blocked several of these actions, but some activities were successfully executed, posing significant risks to the organization's data security.

Event Details

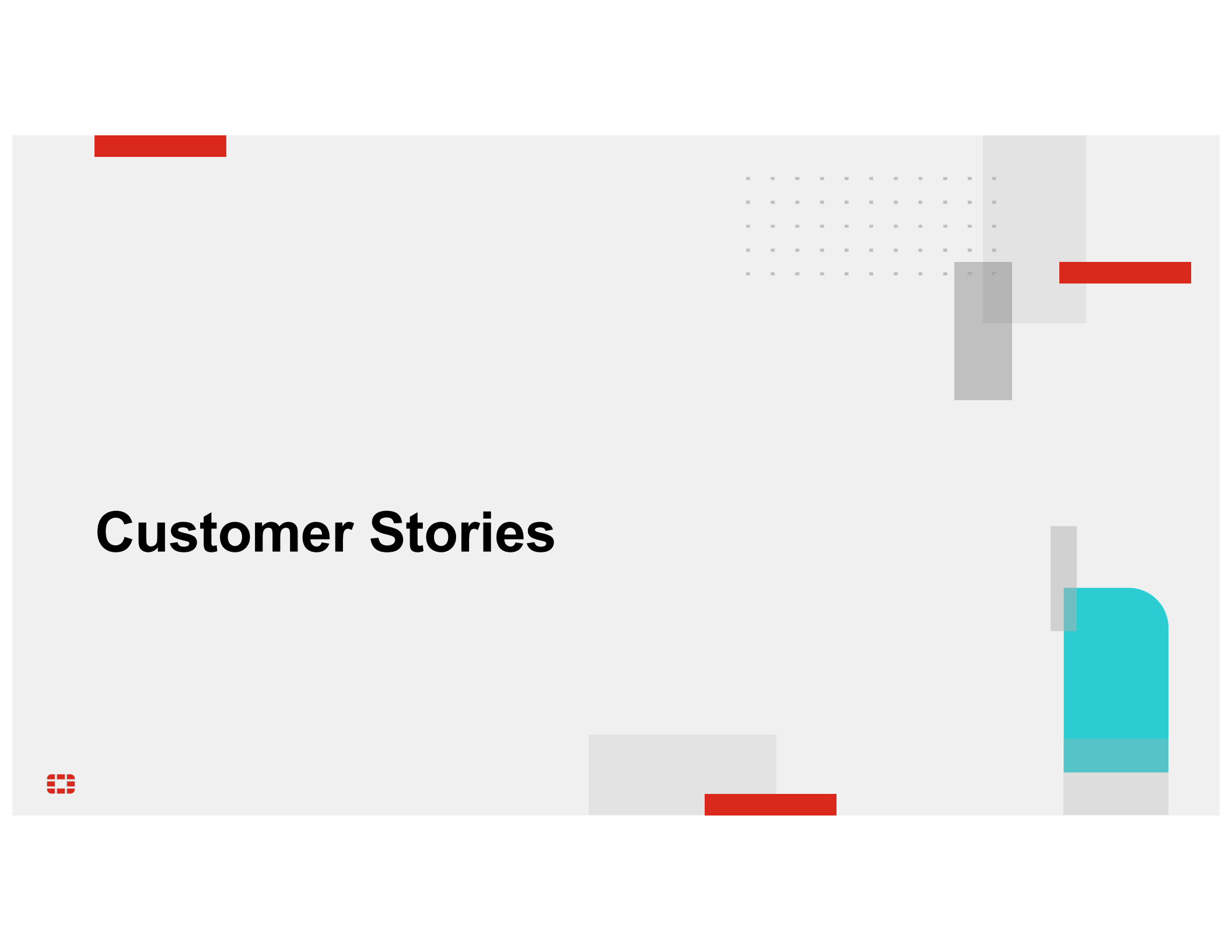
TA0009 (Collection)

- T1213 (Data from Information Repositories):** Chris Tyrrell downloaded a file named `EmployeeData.xlsx` containing US Social Security Numbers from Google Drive using Google Chrome.
- T1530 (Data from Cloud Storage):** The same file was accessed from Google Drive, indicating the use of cloud storage

Prompts for: This case

- Summarize the events in this case.
- Contextualize the websites in this case.
- Contextualize the processes in this case.
- Contextualize the content patterns in this case.
- Contextualize the policy violations in this case.





Customer Stories



Bridging compliance gaps

The challenge

An online gaming company must be **PCI compliant** to access credit card information and adhere to ISO 27001. **As part of their audit, they need visibility of who accesses credit card data.** The risk management and data loss prevention products they tested previously required too much **CPU, slowing down their developers' computers.** Also, **the company wants to shift from focusing on incidents recorded for the ISO 27001 audit to proactive work to ensure compliance.**

The solution

With FortiDLP, the company **uses policies that provide content inspection on file, USB, browser, and process activities.** In turn, they can **see and control access to files containing credit card information.**

Benefits

The company goes from **medium to low risk.** By **gaining visibility of the users accessing credit card information, they identify and address compliance gaps before their audit starts.** They also detect and block more incidents, which drive updates to company policies. Further, they train and assess their developers on compliance at CPU usage below 3%.



Securing the remote workforce

The challenge

A **municipality** is struggling to keep their **endpoints secure with the current perimeter and system-centric security tools**. With an increasing number of people working remotely, both part time and full time, they are **losing the visibility needed to secure their employees and organization**.

The solution

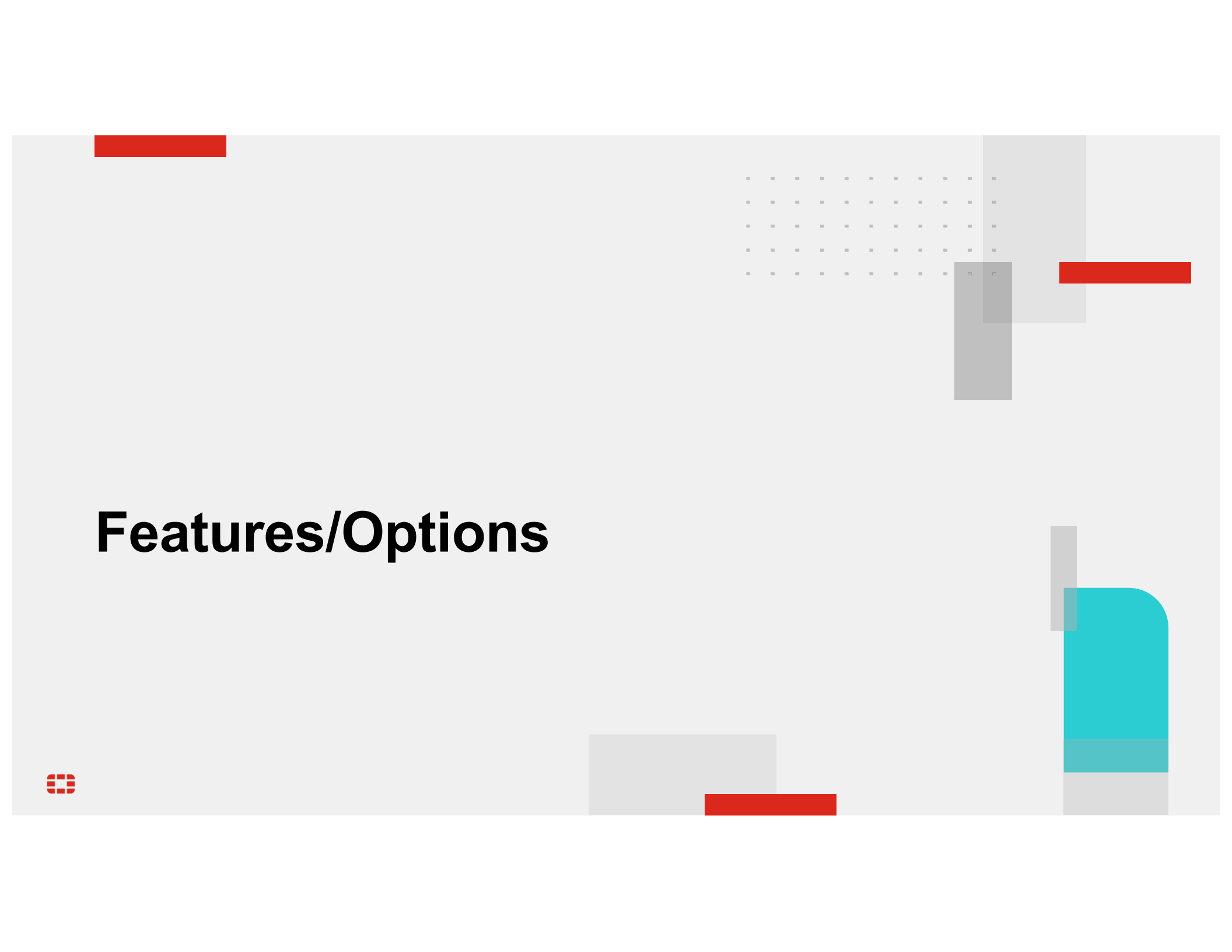
With FortiDLP, the municipality **gets visibility of their data and endpoints outside of the office**. Working remotely breeds new behaviors, where organization-owned computers are used for both work and personal use. **FortiDLP notifies the municipality of unsecure Wi-Fi configurations, unapproved applications, unsanctioned cloud storage, USB storage device usage, unwanted file activities, and more.**

Benefits

The municipality and employees **improve cyber hygiene**, keeping data and endpoints secure, regardless of location.



Government



Features/Options



Feature Options

	STANDARD	ENTERPRISE	MANAGED
Features			
DLP			
Device Control	•	•	•
Inline DLP Web, Email, Cloud Drive, and Connected Media	•	•	•
Real-time Content Inspection (On and Off Network)	•	•	•
- Prevention of Data Loss Based on Data Source (e.g., Salesforce and Github)	•	•	•
GenAI and SaaS Application Risk Inventory and Data Flow Analytics	•	•	•
Customized Employee Coaching with Response Telemetry	•	•	•
Data Privacy and Regulatory Compliance Global Policy Library	•	•	•
Microsoft Purview Sensitivity Label Support	•	•	•
Evidence Store Support for File and Clipboard Forensics	•	•	•
Incident Management and DLP Activity Timeline	•	•	•
Dynamic Risk Adaptive Policies	•	•	•



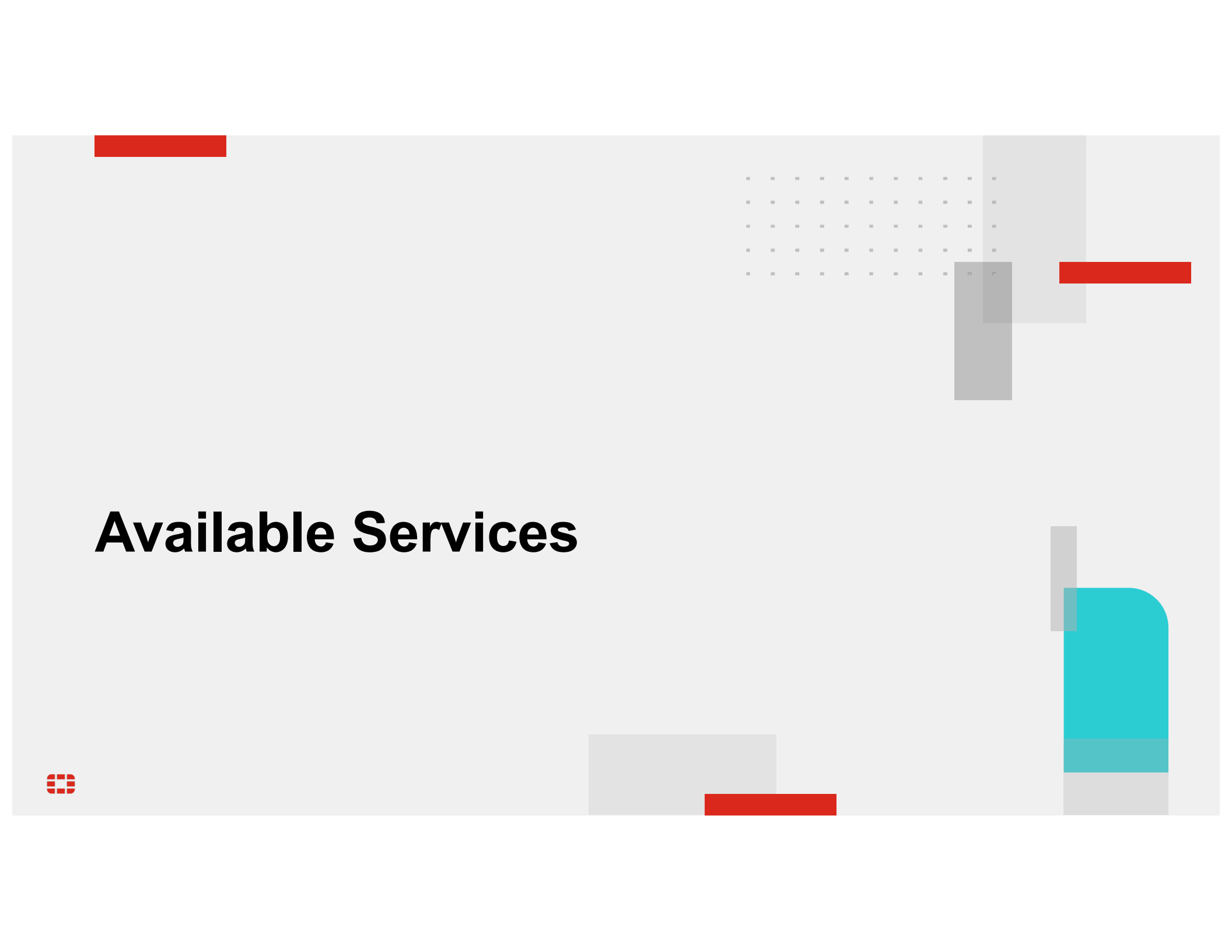
Feature Options (Continued)

	STANDARD	ENTERPRISE	MANAGED
Features			
Insider Risk			
Immediate Visibility into User and Data Risks Across Endpoint and Enterprise Cloud Drive		•	•
Machine Learning-Powered Behavior Analytics		•	•
Data Lineage Tracking with File Manipulation Detection		•	•
Endpoint Isolate and Real-time Lock		•	•
MITRE ATT&CK®-mapped Insider Threat Detection Library		•	•
Insider Threat Data Exfiltration Sequence Detection Incidents		•	•
Case Management		•	•
Cloud Drive Integration			
Google Workspace Connector		•	•
Microsoft Office 365 Connector		•	•
Box Drive Connector		•	•
Real-time Employee Coaching via Slack and Teams Messaging		•	•
Support for M365 (Purview), Google, and Box Classification Labels		•	•
File Sharing Controls		•	•



Feature Options (Continued)

	STANDARD	ENTERPRISE	MANAGED
Features			
Managed Service			
Product Configuration and Provisioning			•
Monthly Data Reports and Security Analyst Reviews			•
DLP Policy Optimization			•
Incident Monitoring Assistance			•
Product Change Management			•

The background is a light gray with several abstract geometric elements. In the top left, there is a solid red horizontal bar. In the top right, there is a dotted grid pattern, a solid red horizontal bar, and a vertical gray bar. In the bottom left, there is a small red icon consisting of a 3x3 grid of squares. In the bottom center, there is a solid red horizontal bar. In the bottom right, there is a vertical gray bar and a cyan-colored shape with a rounded top. The text "Available Services" is centered on the left side of the page.

Available Services

FortiCare Premium Service

Technical support for your FortiDLP solution

- **"Break-fix" technical support**
- **24x7 telephone support**
- **24x7 web support**
- **1-hour critical issue response time**
- **Software updates**
- **Asset Management Portal**



FortiDLP Best Practices Service

Essential guidance for your FortiDLP solution

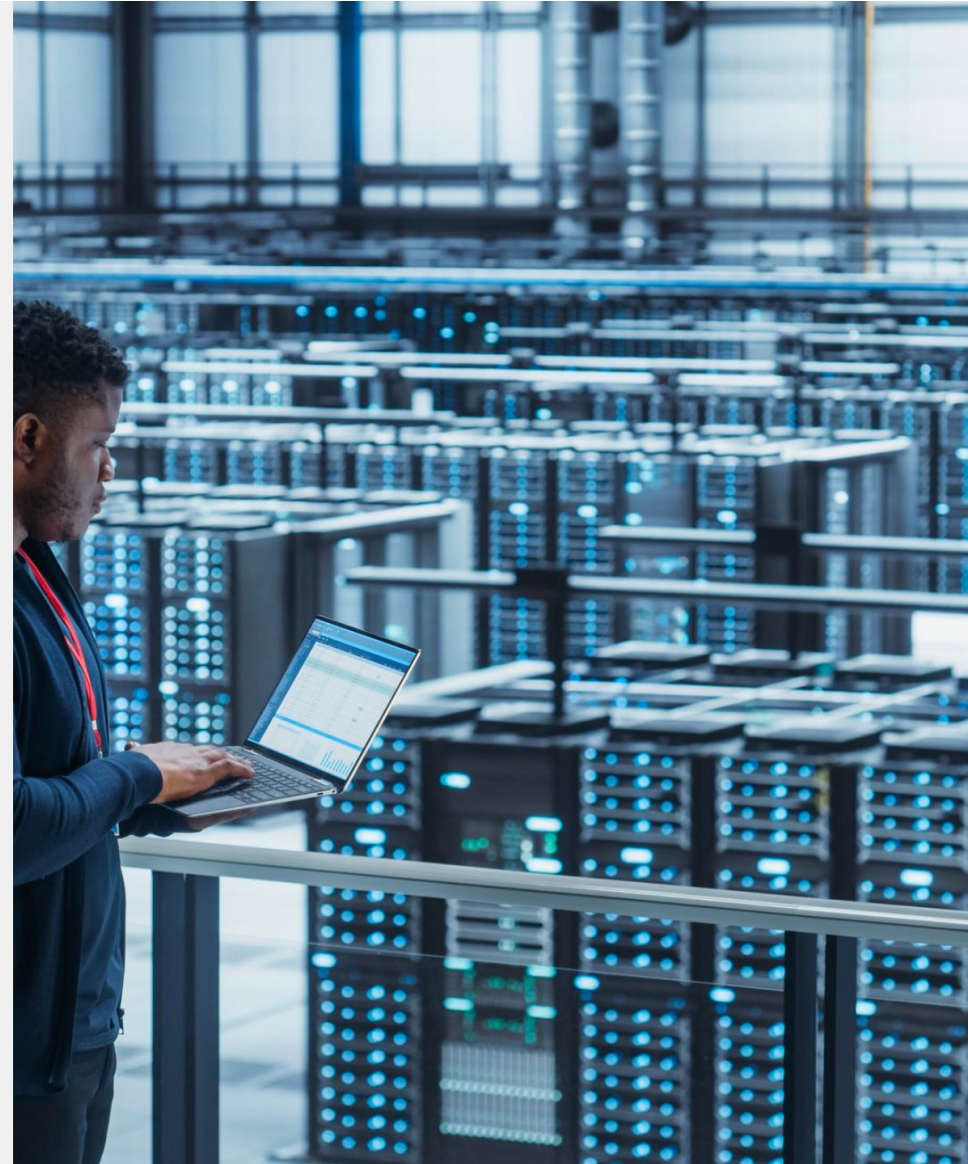
- **Designated expert FortiDLP resource**
 - Providing best practice advice to assist customers with solution management
- **"High touch" Setup phase**
 - For new business or additional business unit onboarding
 - Weekly meetings with expert for deployment guidance
- **On-demand best practice advice and guidance**
 - "How to" answers provided throughout the subscription
- **Quarterly FortiDLP deployment status reviews**
 - Q&A with the designated expert familiar with the deployment
 - Product configuration recommendations for evolving business needs



FortiDLP Managed Service

Helping you manage your FortiDLP solution

- **Managed service provided by designated expert resource**
 - Reducing the load on resource-stretched customer teams
 - Full cloud configuration service
- **Best Practices Service features included**
 - Setup service for new or additional unit onboarding
 - "How to" answers provided throughout the subscription
- **Monthly data reports and reviews**
 - DLP data forensics assistance from security analyst
- **Significant incidents monitoring**
 - Helping customer teams react promptly to DLP incidents
- **Annual product configuration and policy review**
 - Solution optimization
 - Ongoing solution alignment with business requirements





Resources



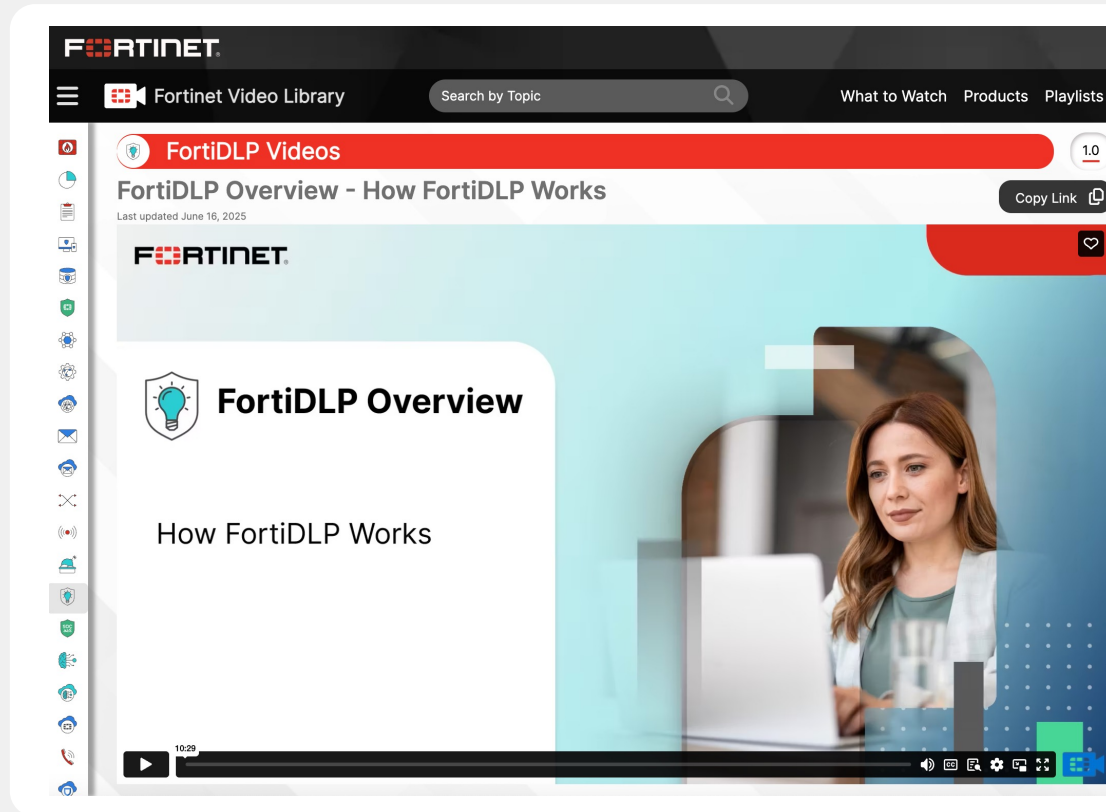
Resources - Fortinet.com

Key Resources

- Data Sheet
- Solution Brief
- White Paper – Shadow SaaS and Shadow AI
- White Paper – DLP Checklist
- POV – Addressing Legacy DLP Challenges
- Ordering Guide
- Demo Videos



<https://video.fortinet.com/products/fortidlp>



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.

FortiDLP: Ready to move forward?

Ready to move forward?

- Schedule a demonstration?
- Kick off a POC?





IntegraONE

FORTINET

Thank you!