A Unified Approach to Protecting Data, Users and AI Workflows

A descriptive overview of the core building blocks of Forcepoint Data Security Cloud

Forcepoint

February 25, 2026
Architectural Overview
Forcepoint Public

Table of Contents

Document Scope

This document presents an overview of Forcepoint Data Security Cloud and explains the key architectural components and how they fit together to deliver unified data security everywhere.

This document is intended for

- Enterprise Architects
- Security and Network Architects
- Solution Architects
- CISO and InfoSec Team
- CIO and CTOs

Note: It is not intended to be used as a deployment and troubleshooting guide.

Executive Summary

AI, cloud adoption, and distributed work have fundamentally changed how data is created, accessed, and exposed. Sensitive data now flows continuously across endpoints, SaaS applications, email, web channels, cloud data stores, and AI-driven workflows often outside the visibility and control of traditional security tools.

Traditional data security architectures were designed for a world of static data locations, predictable user behaviour, perimeter-based enforcement, and manually managed policies. Unfortunately, that world no longer exists.

Today, organizations face data sprawl across SaaS, IaaS, endpoints, and AI workflows. This increases insider risk and the chances of credential misuse. AI driven data ingestion and generation continue to grow rapidly. Hybrid environments are also evolving faster than traditional policies can keep up.

As a result, relying on standalone tools such as DLP, CASB, DSPM, email, or web security creates visibility gaps, inconsistent enforcement, and added operational complexity.

What is required is not more tools, but a unified data security architecture that delivers consistent visibility, classification, and protection across every user, device, application, and data flow.

Forcepoint Data Security Cloud introduces a next generation unified solution designed to secure data everywhere it lives and moves without slowing the business.

Built on a unified modern control plane, Forcepoint Data Security Cloud brings together data discovery, classification, prioritization, remediation and protection across cloud and on-prem environments, powered by AI and contextual intelligence.

This document presents the Forcepoint Data Security Cloud architectural overview and illustrates how it delivers a unified, adaptive approach to protecting sensitive data across the enterprise.

Forcepoint Data Security Everywhere

A framework solving for the most critical use cases

Forcepoint Data Security Cloud Architectural Overview

At its core, Forcepoint Data Security Cloud is asingle, cloud-native data security platform that unifies

Data Discovery

- Discovery of both structured and unstructured data across cloud and endpoint environments
- Continuous scanning to maintain a dynamic and always up to date data inventory
- Exposure mapping and posture insights including identification of blind spots
- File stubbing for visibility into unmanaged or abandoned data repositories

Data Detection and Response (DDR)

- Real time monitoring of sensitive data access, usage, and movement across cloud and endpoints
- Behavioral detection of risky data interactions
- Anomaly analysis across user and data activity
- Insider risk identification through contextual signals

Data Classification

- Highly accurate AI driven classification across enterprise data
- Explainable classification with transparent reasoning
- Coverage across structured and unstructured content
- Sensitivity identification and normalization at scale
- Consistent classification without performance throttling

Prioritize

- Contextual user risk scoring based on behavioral patterns
- Dynamic policy adjustments based on evolving risk posture
- Real time adaptive enforcement decisions
- Risk signal correlation across identity data and device posture

Remediate

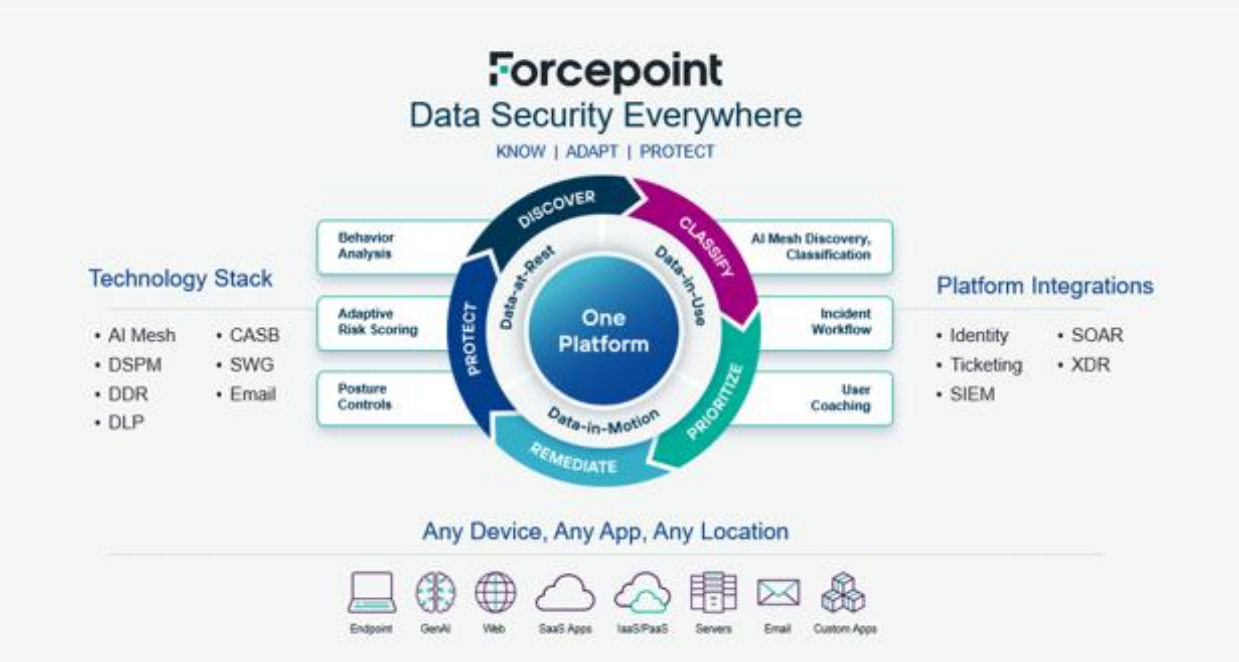
- Centralized incident management across all channels
- Cross channel forensics with activity timelines and evidence
- Alert triage and response workflows
- Policy refinement based on investigation insights

Protect

- Unified DLP Engine
- Risk adaptive enforcement across environments
- Application Security through CASB
- Web Security through SWG
- Email Security
- Remote Browser Isolation

Unified Policy and Intelligence Control Plane

- Centralized policy lifecycle management
- Integrated AI Assistant
- Insights analytics and reporting
- Identity and directory integrations
- API driven ecosystem integrations

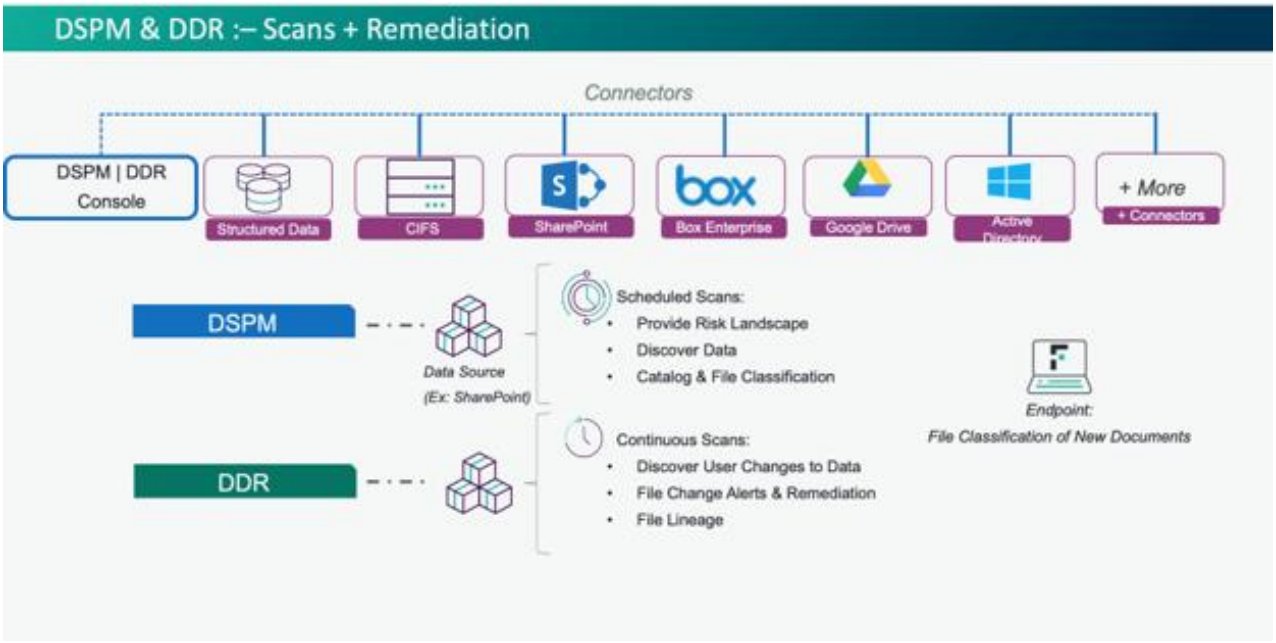


In the following sections, we will explore each key pillar of Forcepoint Data Security Cloud in greater detail to understand how these capabilities work together to deliver unified visibility, contextual prioritisation, and consistent data protection across users, devices, applications, and AI driven workflows.

Data Security Classification

Organizations cannot protect what they cannot see. **Forcepoint DSPM** provides continuous data discovery to deliver essential visibility into where sensitive data exists, how it is distributed, and who has access to it across cloud services, endpoints, on-premises systems, and AI workflows.

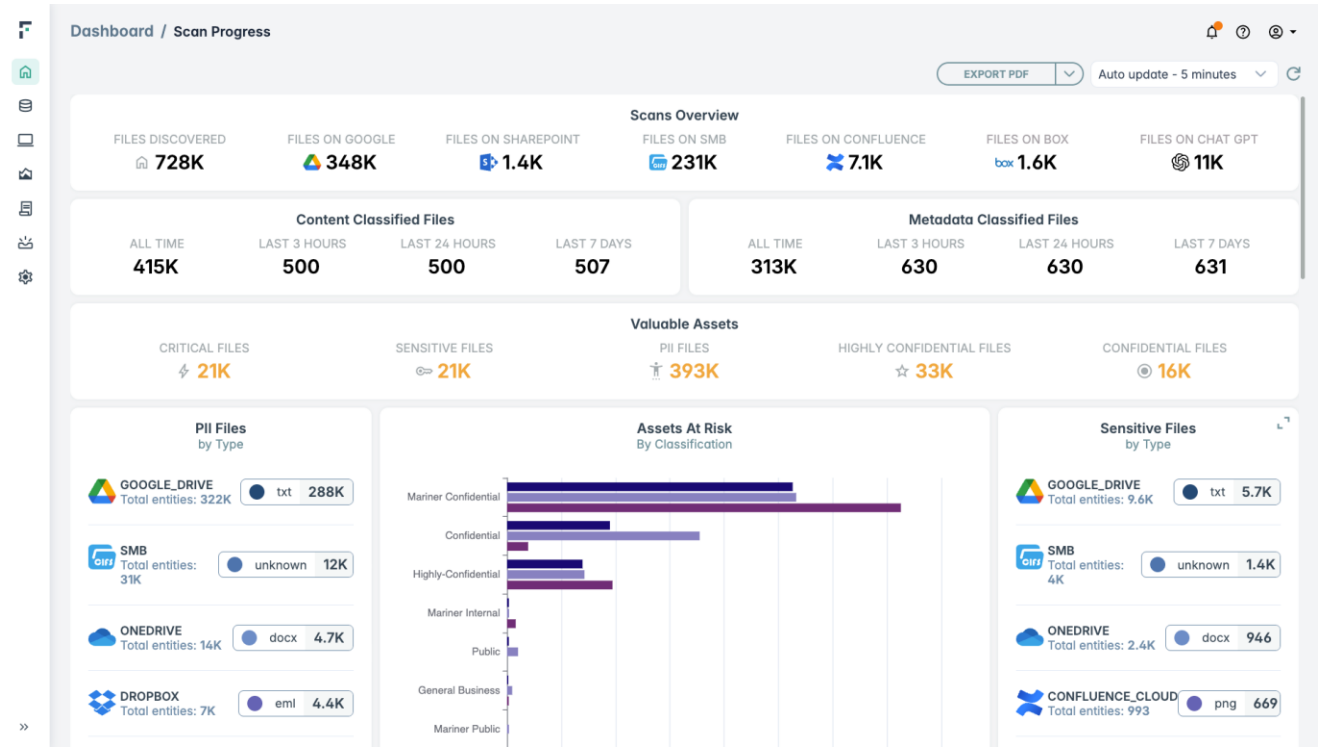
Forcepoint enables the discovery of both structured and unstructured data across cloud and endpoint environments, ensuring that sensitive information is not overlooked regardless of where it resides. Through continuous scanning, the platform maintains a dynamic and always up to date data inventory that reflects the evolving state of enterprise data.



This ongoing discovery also supports exposure mapping and posture insights, helping organizations identify risk prone data stores, overshared repositories, and potential blind spots across managed and unmanaged environments. In addition, file stubbing provides visibility into unmanaged or abandoned data repositories, ensuring that even orphaned or forgotten files also known as Redundant Obsolete Trivial (ROT) files are accounted for within the organization’s data security posture.

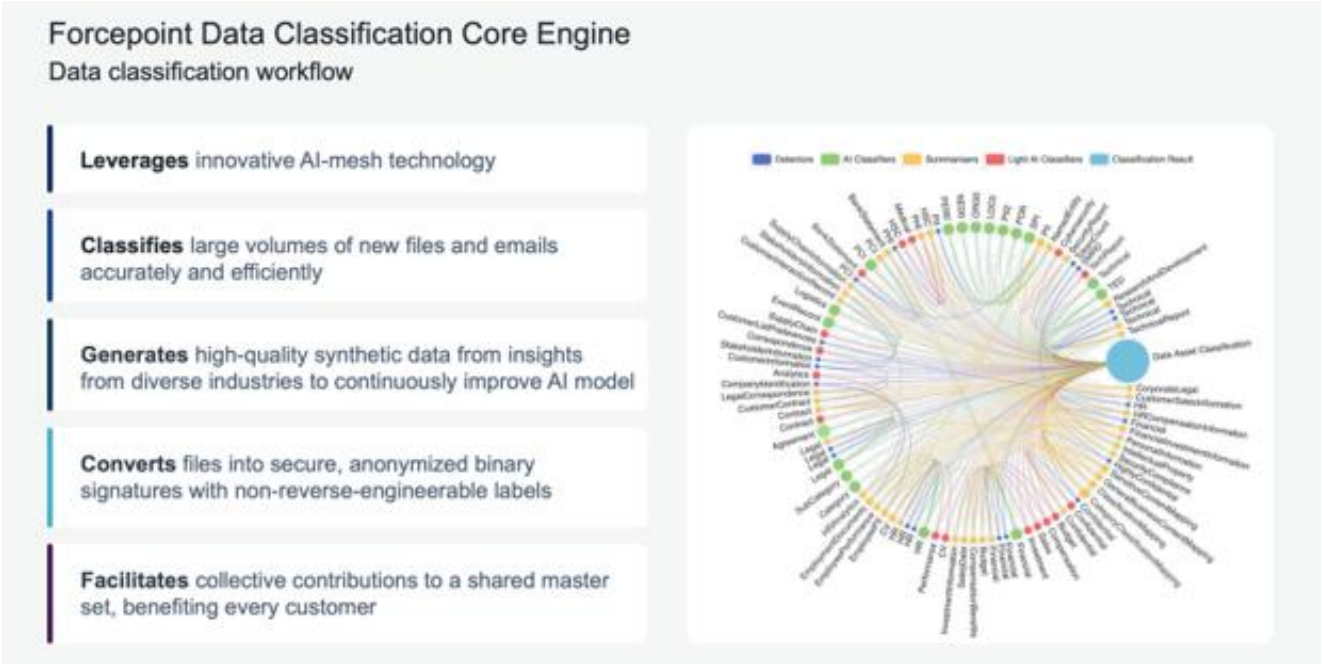
Forcepoint DSPM Redundant Obsolete Trivial (ROT) file's view highlighting redundant, obsolete, and trivial data that remains untouched

As data continues to sprawl across environments, these capabilities play a critical role in reducing risk by preventing sensitive data from remaining hidden in unknown locations or exposed through unintended access paths.



Forcepoint DSPM highlighting discovered and classified files across multiple data sources

Data discovery without context is noise. Forcepoint leverages its innovative AI Mesh technology to deliver highly accurate, context-rich classification of discovered SaaS data, transforming how organizations identify and manage sensitive information. Unlike traditional solutions that rely on static rules or basic automation, AI Mesh uses a networked architecture, including a generative AI Small Language Model (SLM), to intelligently analyze and classify vast volumes of files, emails, documents, and databases across SaaS environments.

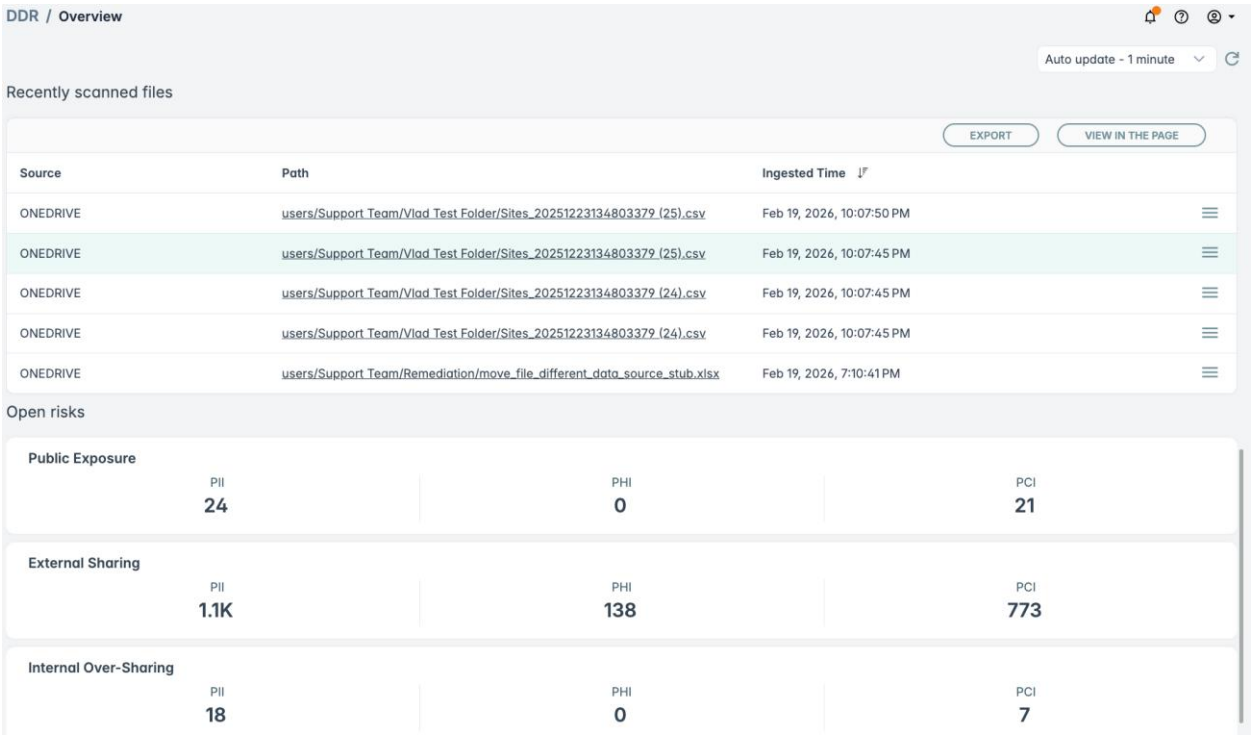


Data Detection and Response

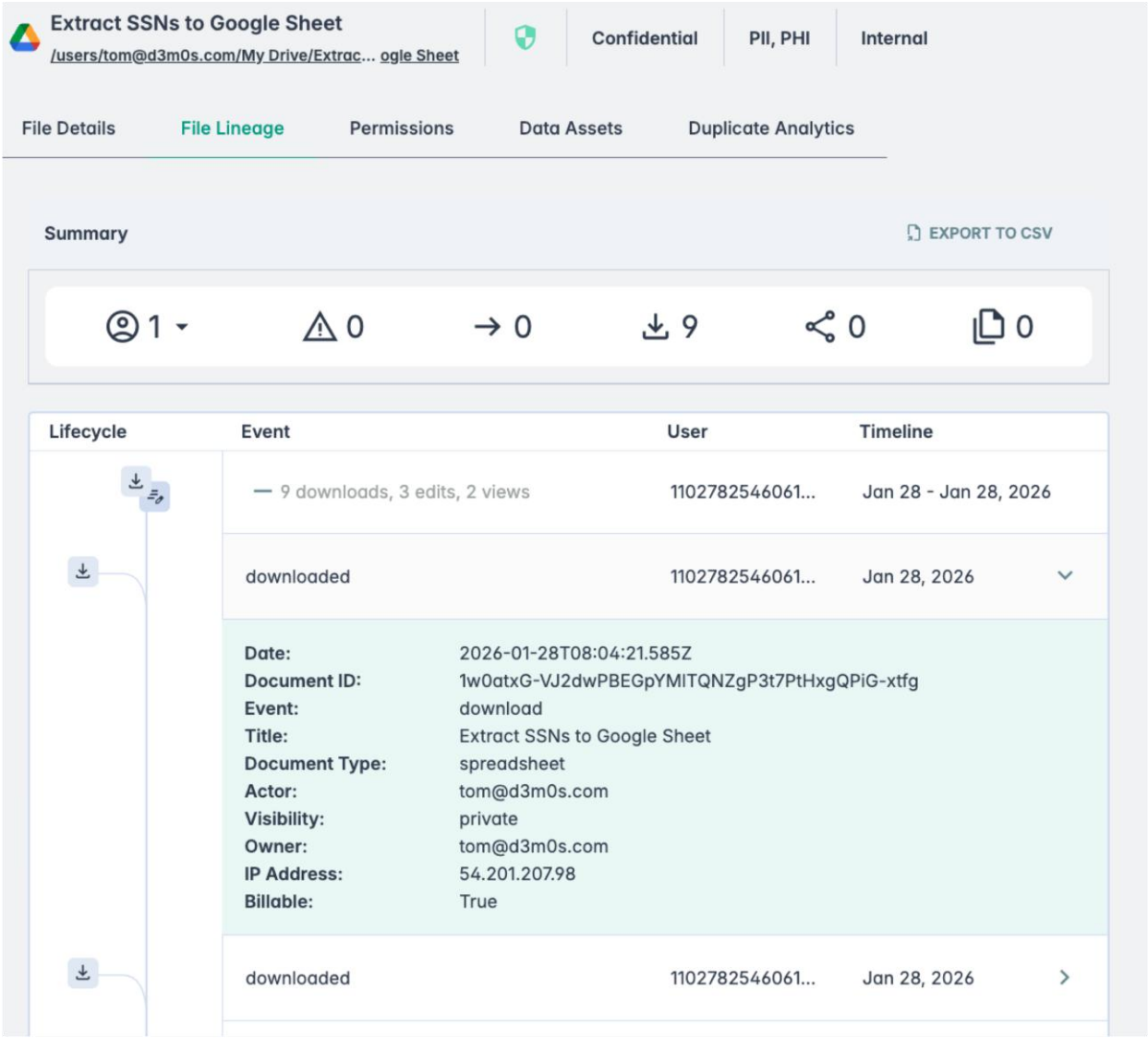
Forcepoint Data Detection and Response extends visibility beyond data at rest to monitor how sensitive data is actually being accessed, used, and moved across cloud and endpoint environments in real time. DDR continuously analyzes data interactions such as file access, sharing activity, permission changes, and abnormal movement patterns to detect behaviors that may indicate insider threats or compromised identities.

By correlating signals from data sensitivity, user activity, and access context, DDR enables organizations to identify risky actions as they occur and respond proactively before sensitive data leaves organizational control. This allows security teams to move from reactive alerting to behavior driven detection and response, reducing attacker dwell time and strengthening protection against data exfiltration.

By correlating signals from data sensitivity, user activity, and access context, DDR enables organizations to identify risky actions as they occur and respond proactively before sensitive data leaves organizational control. This allows security teams to move from reactive alerting to behavior driven detection and response, reducing attacker dwell time and strengthening protection against data exfiltration.



Forcepoint DDR dashboard showcasing real-time visibity into sensitive data activity and open risk indicatos



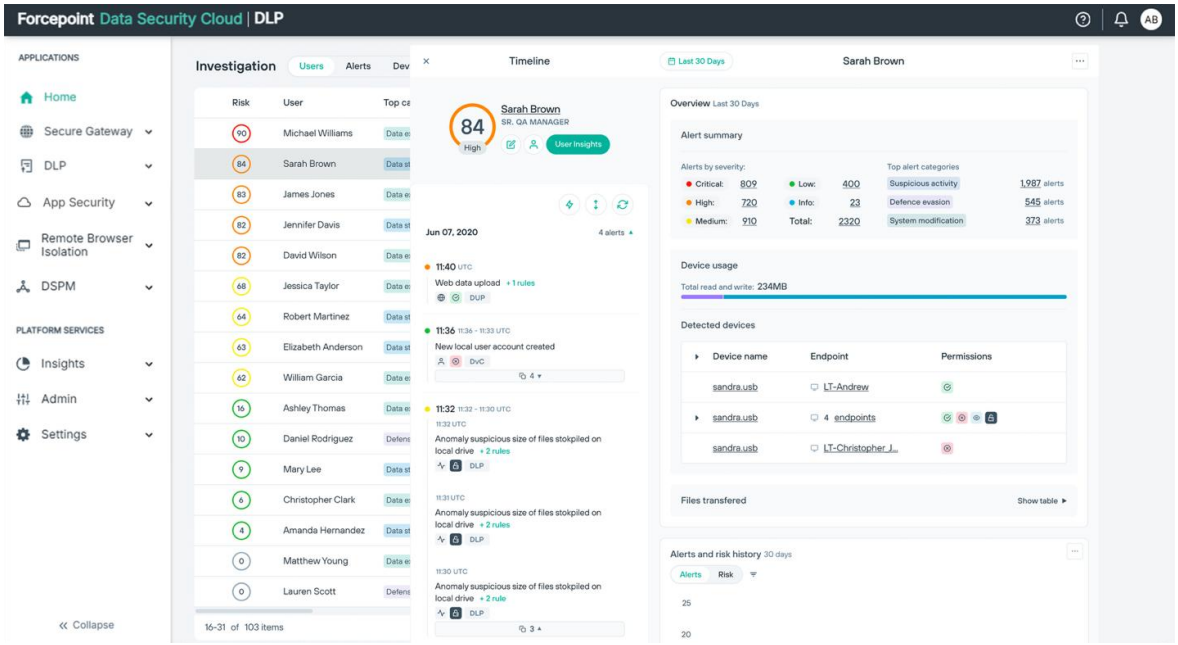
DDR File Lineage view illustrating users activities on a senseitive file present in Google Drive.

Prioritze

Forcepoint continuously evaluates user activity against established behavioral baselines to generate contextual risk scores through **Risk Adaptive Protection (RAP)**. By analyzing patterns such as unusual data access, excessive downloads, abnormal sharing activity, or interactions from unmanaged devices, the platform can detect deviations from normal user behavior that may indicate potential insider risk or compromised credentials.

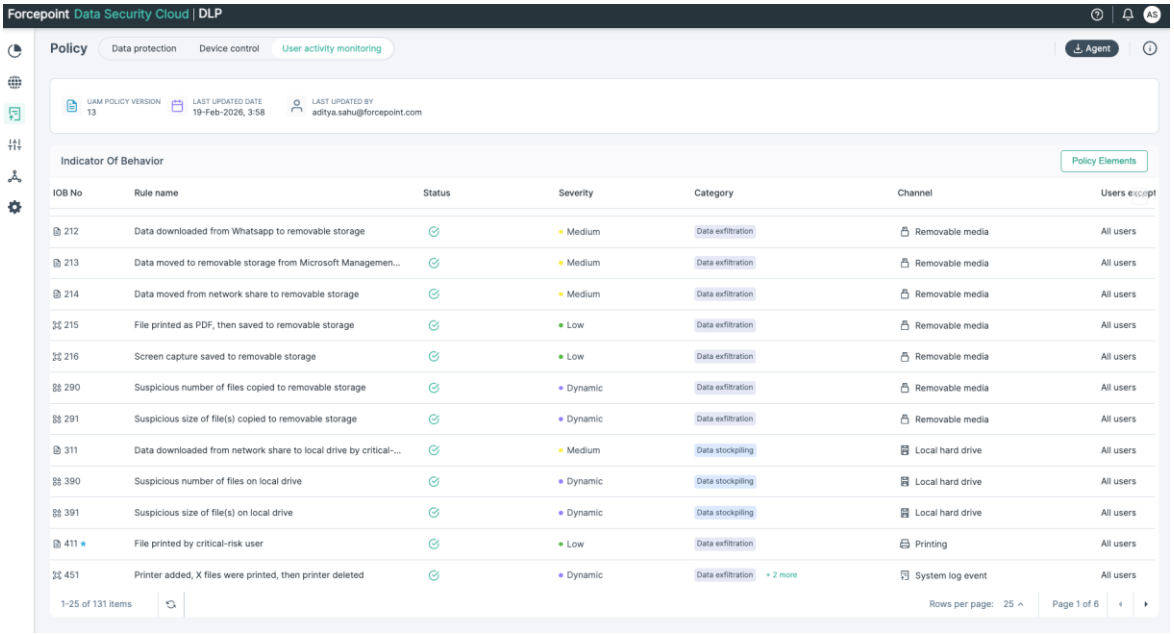
As user risk levels change over time, RAP automatically adapts data protection policies to reflect the current threat posture. This enables organizations to move beyond static enforcement and apply stricter or more permissive controls depending on the assessed level of risk, ensuring that security measures remain aligned with real time conditions.

Based on continuously updated RAP scores, Forcepoint can take immediate enforcement actions such as allowing, blocking, coaching, or restricting access to sensitive data. These decisions are made in real time to prevent potential misuse or exfiltration without unnecessarily disrupting legitimate business workflows.



Forcpeoint Data Security Cloud dashboard showcasing RAP scores across users along with detailed activity insights

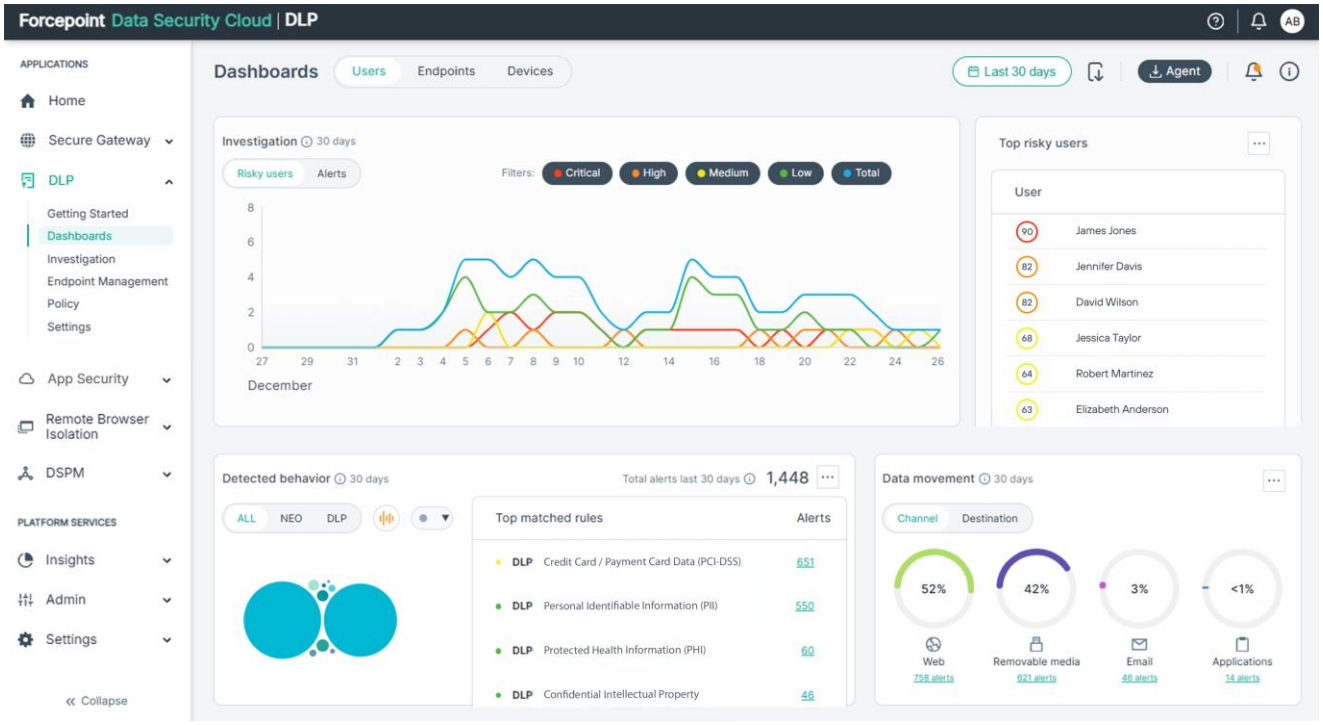
Forcepoint also correlates signals from multiple sources including user identity, device health, access context, data sensitivity and inbuilt Indicator of Behaviour (IOB). By combining identity attributes with device posture and behavioral analytics within RAP, the platform gains a comprehensive understanding of risk, enabling more accurate prioritization and targeted enforcement actions.



Indicator of Behavior from Forcepoint Data Security Cloud can be leveraged with rAP to enable dynamic, risk-based protection

Remediate

Forcepoint provides centralized incident management across all data channels, enabling security teams to investigate and respond to potential data risks from a unified console. Incidents generated across endpoints, cloud applications, web traffic, or email are aggregated into a single view, eliminating the need to pivot between multiple tools during an investigation.

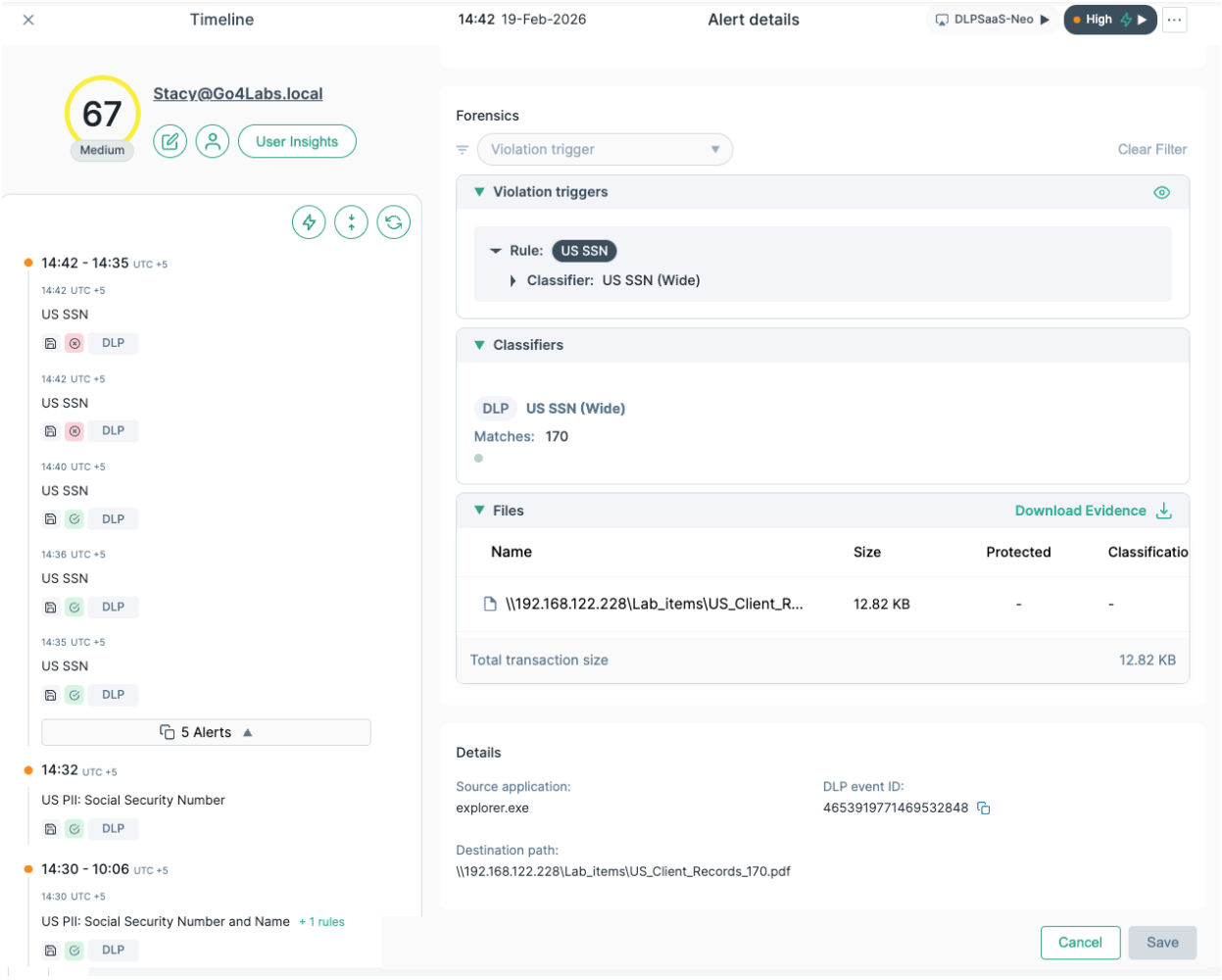


Forcpeoint Data Security Cloud dashboard illustrating risky user activities, top matched rules and data development across all channels

Through cross channel analytics, the platform captures detailed activity timelines along with supporting evidence such as file interactions, user actions, access patterns, and data movement across environments. This enables analysts to reconstruct the sequence of events and understand the full scope and impact of an incident.

Forensics

Forcepoint Data Security Cloud provides deep cross channel forensics that enable security teams to investigate data incidents with full contextual awareness. When a policy violation or risky activity is detected, the platform captures detailed evidence including user actions, file interactions, access patterns, sharing behavior, and data movement across endpoints, SaaS, web, and email channels.



Forensic view offering detailed information about incident

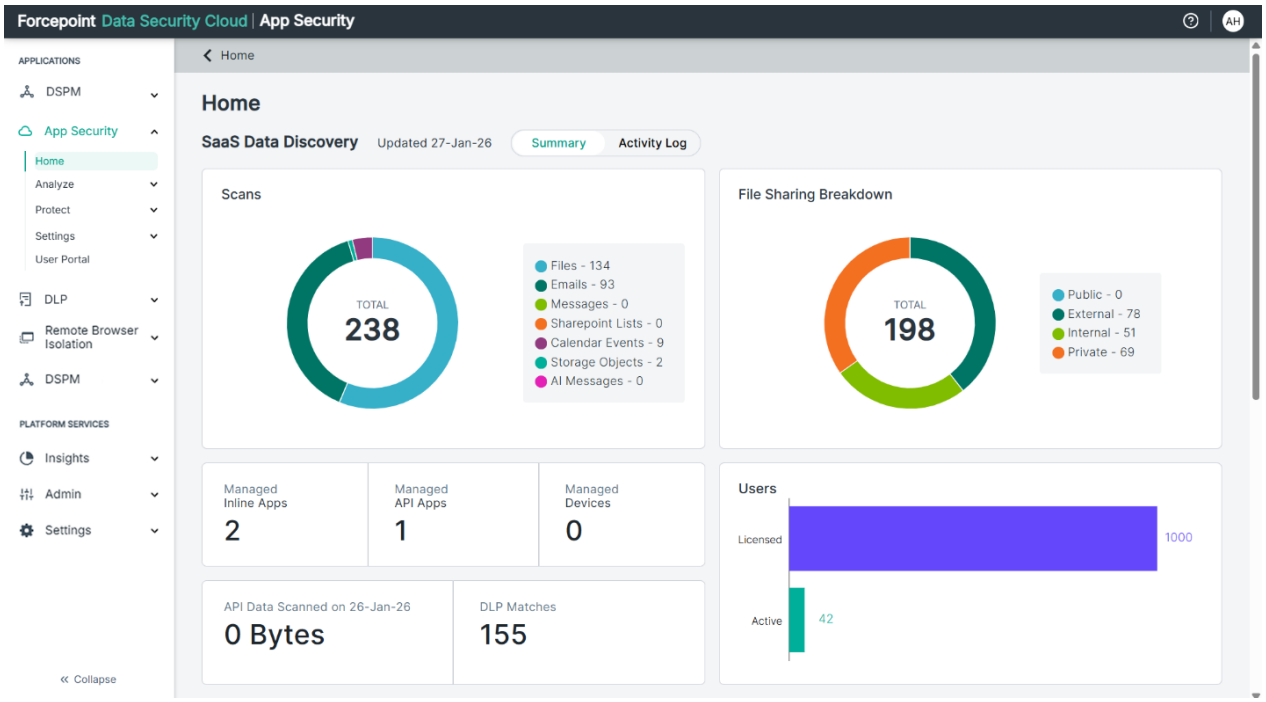
Security teams can review a unified activity timeline to reconstruct events and understand how sensitive data was accessed, modified, or shared over time. This forensic context, enriched by classification insights and RAP risk signals, helps analysts quickly determine intent, assess impact, and initiate targeted remediation actions such as restricting access, revoking sharing permissions, or safely relocating data.

Protect

Forcepoint Data Security Cloud delivers a modern contextual driven DLP engine that enables consistent data protection policies to be applied across endpoints, cloud applications, web traffic, and email channels from a single control plane. This ensures that sensitive data is governed by the same set of policies regardless of where it resides or how it is accessed.

Through risk adaptive enforcement across environments, the platform dynamically adjusts protection actions based on user behavior, device posture, and contextual risk signals. This allows organizations to apply stricter controls in high-risk scenarios while minimizing disruption for legitimate business activity.

Application security is enforced through **Forcepoint CASB**, which provides both inline and API based visibility and control over data interactions within sanctioned SaaS applications. It continuously scans these environments to identify sensitive data, monitor sharing behavior, and assess exposure risks such as oversharing or publicly accessible links.

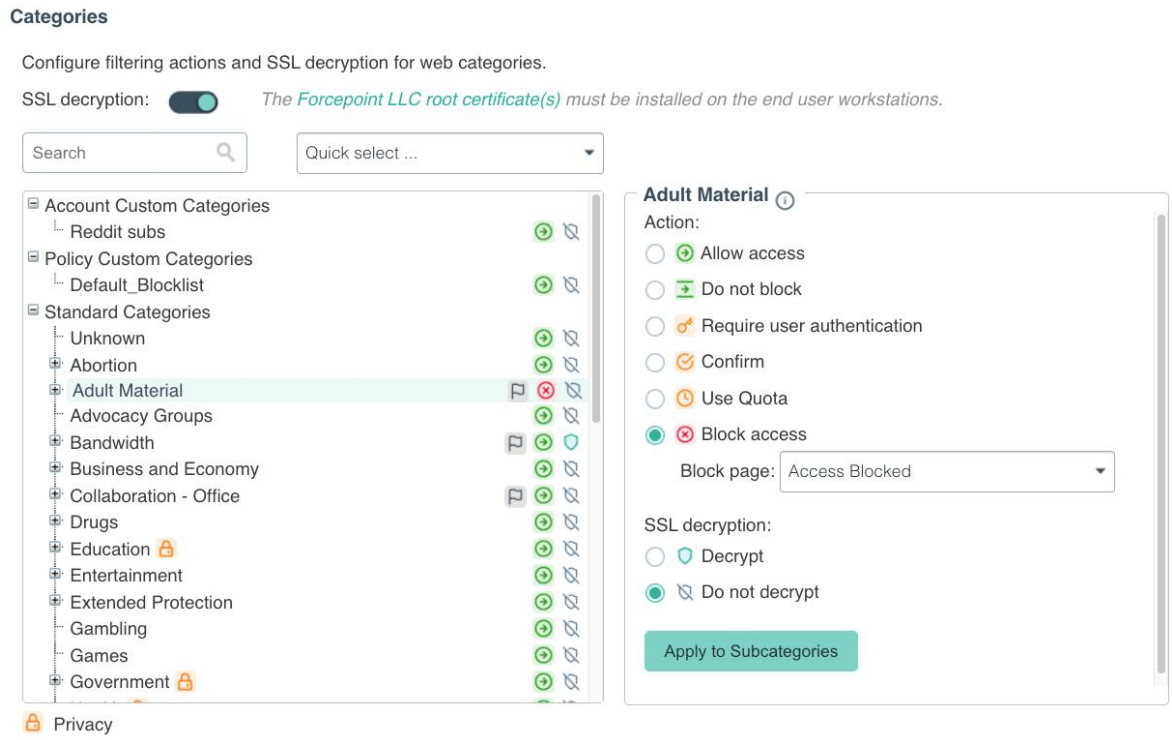


Forcpeoint CASB showcasing dashboard with SaaS data discovery and file sharing insights

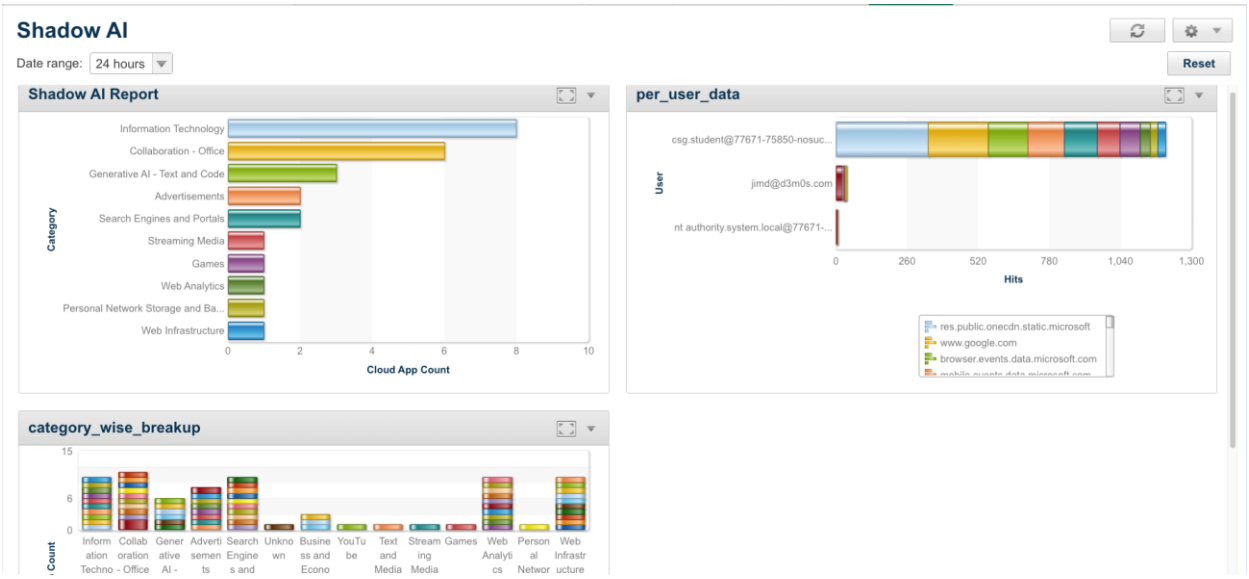
With API-driven inspection, CASB enables discovery of data at rest along with automated, policy-based remediation, such as revoking public links or restricting risky access. Inline controls extend protection to data in motion, allowing Forcepoint to prevent unauthorized uploads, downloads, or sharing of sensitive information in real time, ensuring that data remains protected across cloud applications.

Web security is delivered through **SWG**, enabling inline inspection of data in motion across web traffic to prevent unauthorized uploads or downloads of sensitive information.

Forcepoint Secure Web Gateway enables organizations to monitor and control how sensitive data moves across web traffic by inspecting user interactions with websites, cloud applications, and AI tools in real time. It provides deep inline visibility into web sessions, helping security teams detect and prevent unauthorized sharing of sensitive information over the web channel.



Forcpeoint SWG category selection interface for defining web access and security controls



Forcpeoint SWG dashboard providing visibility into overall web usage and traffic patterns

By applying unified DLP policies across web sessions, SWG ensures that sensitive data remains protected even when users interact with external platforms such as personal email, file sharing sites, or unsanctioned applications. The platform can dynamically allow, block, or coach user actions based on data sensitivity, user risk, and device posture, enabling secure web usage without disrupting legitimate business activity.

Integrated with Risk Adaptive Protection, SWG aligns enforcement decisions with real time contextual risk signals, helping organizations prevent data exfiltration while maintaining productivity across managed and unmanaged environments. Additionally, Remote Browser Isolation provides a secure environment for accessing potentially risky web content, preventing data exposure by isolating user sessions from the endpoint.

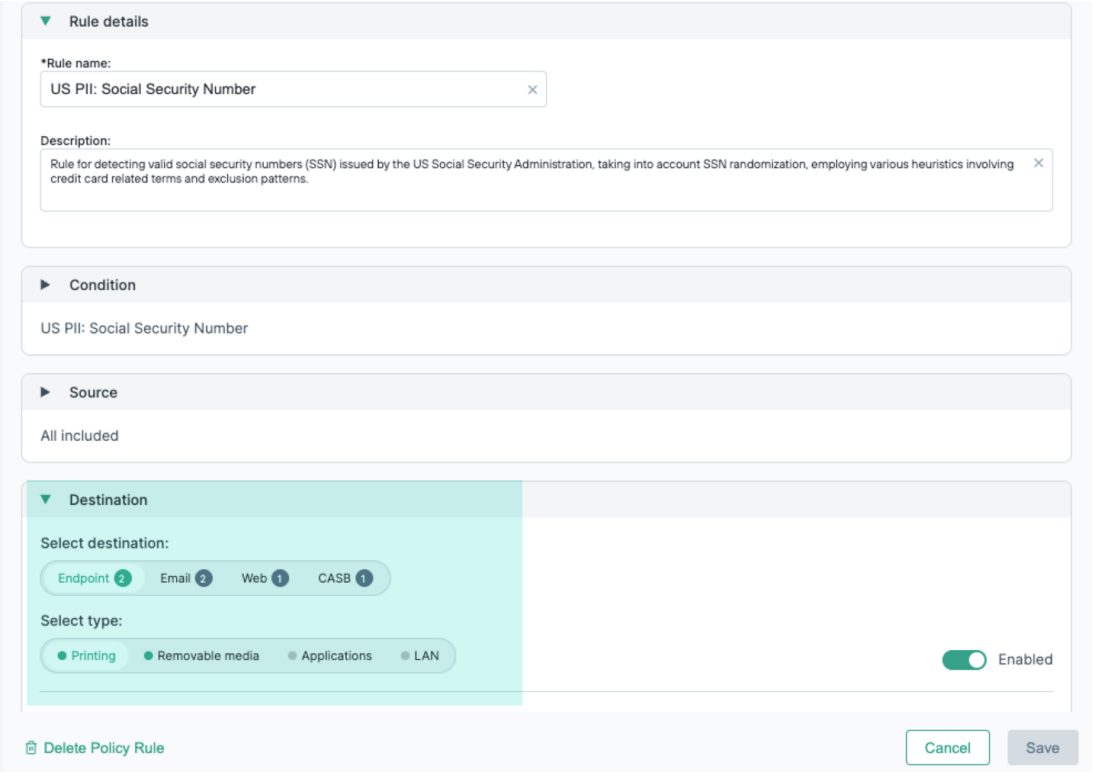
Email security extends DLP controls to outbound communications, ensuring that sensitive content is not inadvertently shared through email channels.

Together, these capabilities enable organizations to enforce data protection policies consistently across all channels without hindering productivity.

Unified Policy and Intelligence Control Plane

Forcepoint Data Security Cloud provides a unified data loss policy management framework that enables organizations to define, manage, and enforce data protection policies consistently across all users, devices, applications, and data channels.

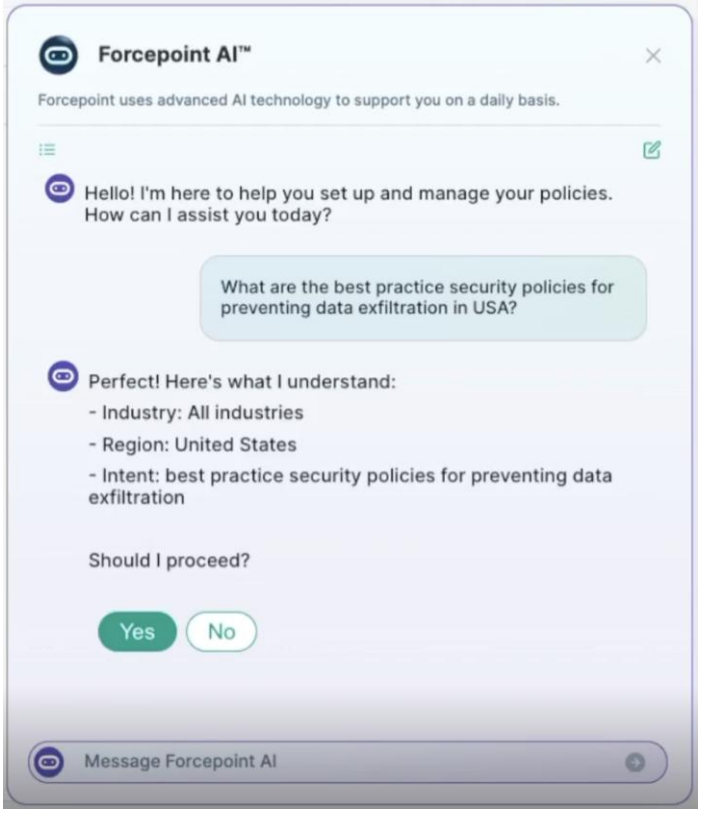
Security teams can create data loss prevention policies once and apply them everywhere, leveraging a common classification and context engine to ensure sensitive data is protected the same way whether it is accessed in SaaS, IaaS, endpoints, on premises systems, web traffic, or AI workflows.



Forcpeoint DLP policy view illustrating consistent US PII protection across all channels

Policy management is identity aware, and context driven, incorporating user identity, group membership, device posture, data sensitivity, application type, and activity context. This enables precise, risk-based controls rather than broad, disruptive restrictions.

An integrated AI Assistant simplifies policy creation and tuning by providing intelligent recommendations based on observed data usage and evolving risk patterns. With natural language understanding capabilities, it can recommend new policies or policy modifications and deploy them directly from the user interface.



Forcpeoint AI suggestinog a security policy

Conclusion

Modern data security requires more than isolated controls across endpoints, cloud, web, and AI-driven workflows. As sensitive data moves dynamically across users, devices, applications, and generative AI applications, fragmented point solutions introduce visibility gaps, inconsistent enforcement, and delayed response.

Forcepoint Data Security Cloud delivers a unified, cloud native architecture that brings together continuous data discovery, AI driven classification, behavioral prioritisation through Risk Adaptive Protection, cross channel investigation, and consistent policy enforcement across all data interactions.

By correlating signals from data sensitivity, user behavior, identity, and device posture, the platform enables real-time adaptive controls that evolve with changing risk conditions. This allows organizations to move from static, policy driven protection to dynamic, context aware data security that proactively mitigates insider threats, credential misuse, and AI driven data exposure.

The result is a single, intelligence driven control plane that secures data everywhere it lives and moves, while enabling secure collaboration, cloud adoption, and AI innovation without compromising productivity or compliance.

Forcepoint Data Security Cloud transforms data protection from a reactive control mechanism into a continuous, risk-aware security strategy aligned with how modern enterprises create and use data today.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real-time, and protect at scale with a unified, single-policy framework. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, LinkedIn, Instagram and YouTube.

[FDSC Architecture Overview] 26 Feb. 26