Forcepoint

Datasheet

Forcepoint ONE Data Security

Enterprise-class DLP, unified across all key channels and managed simply from the cloud.

Today, data security is a business-critical part of any company's strategy. But just when your organization feels like it has data security figured out, enter the latest security challenge; the safe use of GenAI applications. With data sprawled across devices, cloud environments, and now with the rise of GenAI applications, protecting sensitive data in an AI-world can seem like an impossible task.

Forcepoint ONE Data Security is a cloud-native DLP solution designed for the modern enterprise. This DLP SaaS solution protects sensitive information, prevents data breaches and enables compliance with privacy regulations worldwide. Providing rapid deployment and policy management, it streamlines data protection and delivers unified management across GenAI and cloud apps, web, email and endpoints. With Forcepoint Risk-Adaptive Protection, it offers real-time user risk insights. Experience reduced costs, risks and increased productivity with Forcepoint ONE Data Security.

Powerful enterprise DLP data identification across all channels

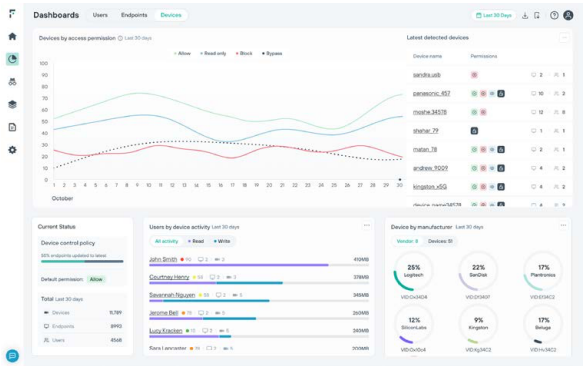
- → Over 1,700+ out-of-the-box predefined classifiers, templates and policies.
- → Natural Language Processing (NLP)
- → Advanced true file type detection covering over 900 file types.

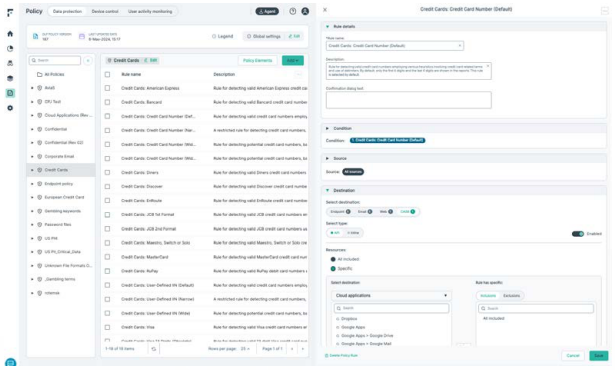
Safely use GenAI apps

Start your AI transformation journey today with Forcepoint. Boost productivity and efficiency with safe use of GenAI apps like ChatGPT, Copilot, Gemini, and many others. With Forcepoint ONE Data Security, you can coach users on how to use GenAI apps properly, inspect and block sensitive information in uploads and pasting – automatically, and log attempts to misuse sensitive data.

Unified management—"One policy to rule them all"

You can manage all Forcepoint ONE services seamlessly from the Forcepoint ONE Data Security interface. Exercise control over all channels (CASB, SWG, email and endpoint) through a single policy, ensuring uniformity across all key egress points. With a single click, deploy a new policy or apply an existing policy across all key channels. Conveniently monitor DLP incidents from a unified dashboard, acquiring a comprehensive view of data security across your organization.





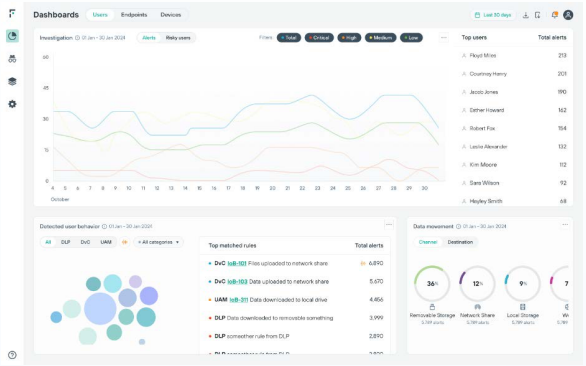
Simple policy configuration

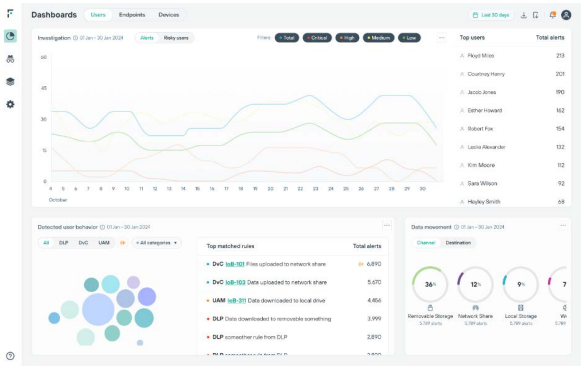
- → Streamline management by using over-the-air updates for the latest pre-defined policies, classifiers, and templates.
- → Create policies with just a few clicks and deploy in minutes instead of hours.
- → Gain out-of-the-box compliance policies for over 150 regions and 90 countries to ensure privacy regulation compliance in every major global region.

Easy incident and alerts management

Gain a complete view of all incidents and alerts in near real-time via the reporting dashboard. With integrated reporting, administrators gain a holistic view across cloud applications, web traffic, email, and endpoints. Native Device Control enhances data security and access control for removable media such as USB drives. Forcepoint ONE Data Security seamlessly integrates with Risk-Adaptive Protection, providing real-time context and understanding of user intent by focusing on behavior and data interaction. Forensics capabilities allow deeper insights into data movement, enabling effective investigation of security incidents to enhance policy enforcement and streamline compliance. All of this is managed through a single agent and UI.

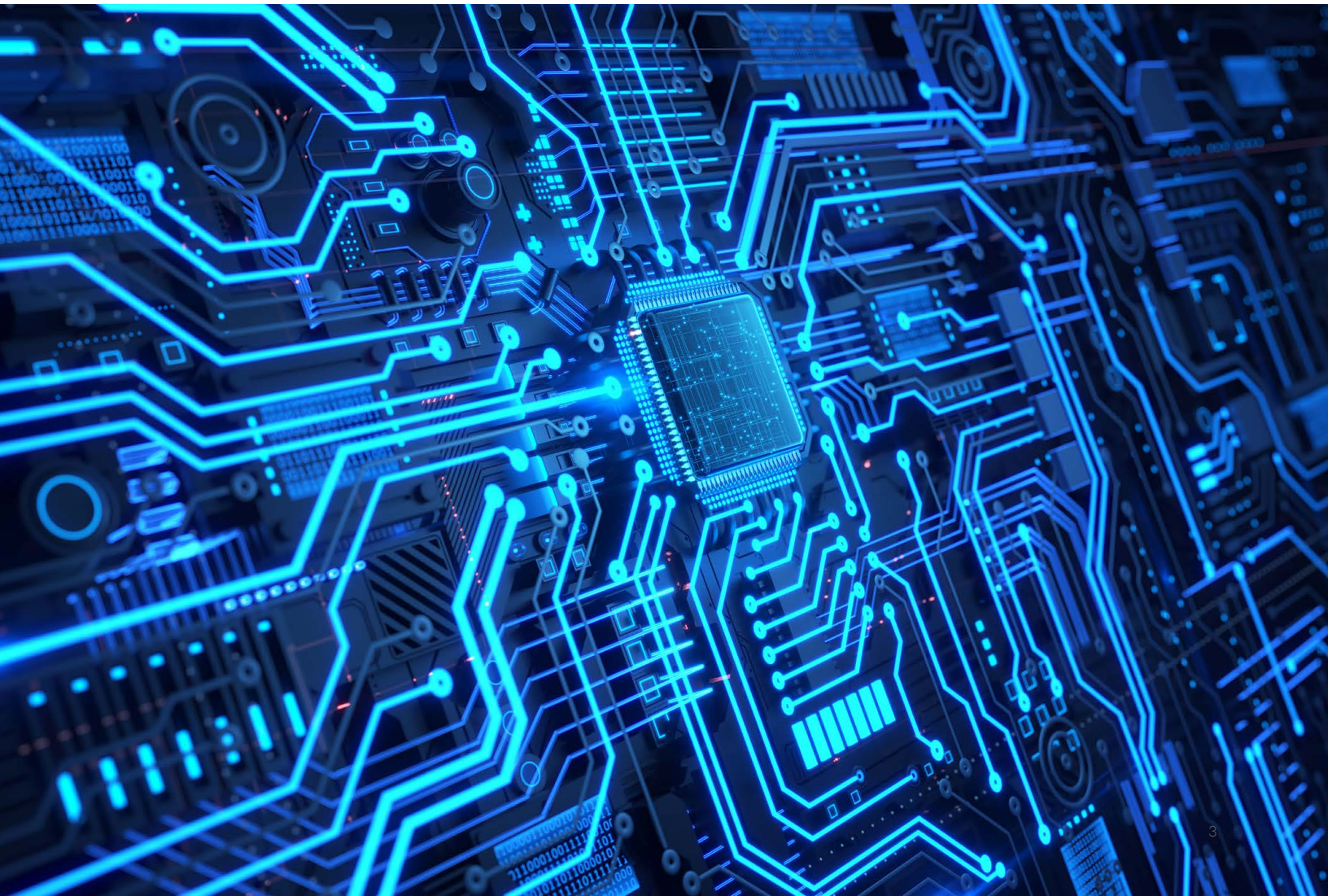
*Integration with Risk-Adaptive Protection (endpoint required for informing risk score) requires a separate SKU (add-on to Forcepoint ONE Data Security).





Cloud-native SaaS solution

- → Lower overall costs.
- → No on-prem hardware and software setup costs.
- → Cloud-native solution offers greater and more efficient scalability .
- → Simple data security management with continuous updates with new features, bug fixes and security patches.
- → Automated over-the-air updates for endpoint.
- → Deployed on AWS globally with 99.99% uptime with no scheduled downtime.
- → Built on AWS IoT to easily scale to hundreds of thousands of endpoints.



Forcepoint ONE Data security delivers a comprehensive solution for managing global policies across all channels, including GenAI and cloud apps, web, email, and endpoints. With an extensive array of pre-defined templates, policies and classifiers, we simplify your workload, enabling streamlined incident management and allowing you to prioritize critical tasks.

FEATURES	BENEFITS
Over 1,700 out-of-the-box predefined classifiers, templates and policies	Streamline DLP initial deployment and ongoing policy management with prebuilt policies/ templates/classifiers
Natural Language Processing (NLP)	Unsurpassed accuracy recognizing common data types (PII, PHI, PCI) based on described content using 300+ predefined natural language scripts
Advanced true file type detection	ID over 900 file types regardless of whether they are renamed to avoid detection, including OCR and text in images
Unified policy control across CASB, SWG, email and endpoints	Manage all channels from within a single policy. Write once, deploy across all egress channels
Unified reporting across CASB, SWG, email and endpoints	Unified reporting across CASB, SWG, email and endpoints
Compliance policies for over 150 regions globally out of the box, 90 countries	Policies available out of the box to enable privacy regulation compliance in every major region globally
Automated updates	Simplify data security management with automated updates of the most up-to-date pre-defined policies, classifiers and templates
Fast access to alerts in reporting dashboard (cloud portal)	See all incidents and alerts in near real-time from an efficient, organized dashboard
Integrated reporting	See all reporting across DLP, Device Control and Risk-Adaptive Protection in an integrated user interface
Incident prioritization	View top ten actions that require immediate attention in the incident interface. Combined with Risk-Adaptive Protection scoring, can include number of incidents and risk severity of users to prioritize workflow
Forensics	Provides visibility into data movement to investigate security incidents, understand the cause of data breaches, conduct detailed incident investigations, enhance policy effectiveness, and supports legal/compliance needs.
Over-the-air upgrades	Removes need to interact with IT on agent updates, decreases time to publish updates
Agent management visibility	Gain visibility into your endpoint deployment status and quickly find issues with agents
Network connection not required for endpoint enforcement	No need to be connected to the network for endpoints to have visibility into security violations. Data is always protected regardless of network connectivity
Integration with device control	Extends data security and access control for removable media into single agent and UI
Integration with Risk-Adaptive Protection	Real-time, context-sensitive automated policy enforcement as well as incident management from single agent/UI Requires a separate SKU forRisk-Adaptive Protection (add-on to Forcepoint ONE Data Security)
99.99% uptime with no scheduled downtime	Deployed on AWS globally with 99.99% uptime