Proofpoint Endpoint Data Loss Prevention

Protect from user-driven data loss

KEY BENEFITS

- Detect risky data activity and prevent data loss from the endpoint
- Simplify response to user-caused data loss incidents
- Accelerate time to value with highly scalable SaaS deployment powered by modern cloud-native backend
- Keep users productive with a lightweight endpoint agent

KEY ENDPOINT DLP USE CASES

- Regulated and sensitive data
- Removable media and USB usage
- Mergers and acquisitions
- Data loss incident response

Proofpoint Endpoint Data Loss Prevention (DLP) helps protect against data loss and brand damage from malicious, negligent and compromised users. Using a lightweight endpoint agent and modern cloud-based software-as-a-service (SaaS) architecture, it correlates risky data activity and user behaviour to help prevent, detect and respond to data loss incidents.

Unlike traditional endpoint tools for protecting sensitive and regulated data, Endpoint DLP is easy to roll out and does not slow users down. Our people-centric approach analyses users, data and threats in real time to detect risky behaviour, prevent data exfiltration and streamline incident response.

Detect, Prevent and Respond in Real Time

Correlate risky data movement with user activity as it happens—not just after data loss has occurred. Real-time visibility gives you powerful new ways to correlate, detect, prevent and resolve data loss incidents.

Data loss detection and analytics

Integrate Proofpoint Endpoint DLP data activity visibility into broader threat-hunting programmes. Our rules engine provides easily customisable, real-world indicators of data exfiltration and risky data movement including:

- Data exfiltration to web, USB device, cloud storage and email
- Copying and pasting files, folders and text
- File activities such as rename, copy, move and delete
- Data infiltration from web, email attachment and cloud
- Document printing

Data classification support

We integrate with Microsoft Information Protection (MIP). The Proofpoint Endpoint DLP agent reads sensitivity labels in real time as the user interacts with the file. You can set detection and prevention rules based on the file MIP sensitivity label, file origin, file type and file destination.

Data loss prevention

Endpoint DLP can prevent sensitive data exfiltration through common endpoint channels. That includes USB-connected devices such as local sync folders, network-attached storage, flash drives, multimedia devices and phones. It even works when the user is offline.

You can manage USB-based activities by user, groups and hosts as follows:

- Block data writing to USB
- Safelist some USB devices
- Block files that match filename patterns
- Block file types
- Block file sources
- Enforce global prevention rules

Users are advised when—and why—an action is blocked.

The Proofpoint Enterprise DLP suite can extend protection to email and cloud apps.

Irrefutable evidence of wrongdoing with Proofpoint Insider Threat Management (ITM)

With ITM on top of Endpoint DLP, you can capture screenshots of endpoint activity by suspected users. When set in context of the data timeline and PDF reports, these screenshots provide clear, irrefutable evidence of user intent.

Extend data risk visibility with Proofpoint Enterprise Data Loss Prevention

Endpoint DLP and ITM sit within a shared, modern SaaS backend under the broader Enterprise Data Loss Prevention platform. It's deployed as a pure SaaS offering with no on-premises infrastructure. That means it's scalable, secure and ready for enterprise-wide global deployments. With an attribute-based access control paradigm, Endpoint DLP can be configured to meet your unique needs. You can deploy fine-grained security and access policies to support data privacy and create workflows that fit your organisation.

Accelerate Time To Value

Legacy endpoint DLP tools are burdensome to deploy. They're hard to set up. And they provide little value to security teams until the data is properly classified—often a long, complex process. On top of all the upfront work, legacy endpoint DLP agents can slow systems to a crawl, while frustrating users.

Pure SaaS deployment

Proofpoint Endpoint DLP is a modern SaaS platform built for scale, analytics, security, privacy and extensibility. This reduces setup time and cost on the backend and simplifies ongoing management for security administrators across the organisation. This means instantaneous visibility on data activity.

Two problems, one lightweight solution

Proofpoint Endpoint DLP and ITM use a single, common, lightweight agent. When used together, Endpoint DLP protects from data loss risks among everyday users while ITM extends that protection to all risky behaviour by malicious and higher risk users.

LEARN MORE

For more information, visit proofpoint.com.