proofpoint.

SOLUTION BRIEF

Proofpoint Endpoint DLP and Proofpoint ITM

Get people-centric data-loss and insider-threat protection at the endpoint

Key Benefits

- Reduce the risk of sensitive data loss and insider threats
- Simplify response for data-loss incidents and out-of-policy violations
- Accelerate time to value of insider threat and data loss prevention programmes

Data doesn't lose itself. People lose it. That's why the Proofpoint Endpoint Data Loss Prevention (DLP) and the Proofpoint Insider Threat Management (ITM) products take a people-centric approach to managing insider threats and preventing data loss at the endpoint.

It helps modern IT and cybersecurity teams:

- Identify risky user behaviour and sensitive data interaction
- Detect and prevent insider-led security incidents and data loss from endpoints
- Respond more quickly to user-caused incidents

When data loss or insider-led security incidents occur, you must quickly investigate and contain them. The faster an incident is resolved, the less damage it can do to your business, brand and bottom line.

When every second counts, visibility, detection, prevention and context are everything. Legacy DLP tools don't show the full picture of user-caused

Figure 1: The power of Proofpoint Endpoint DLP and Proofpoint ITM from the same shared endpoint sensors.

incidents. They miss critical signs of unapproved data exfiltration and other policy violations. And they don't provide the context of "who, what, where, when and why"—the details you need to tell what alerts and events are real from normal business activity.

Proofpoint Endpoint DLP and Proofpoint ITM extend the capabilities of the Proofpoint Information and Cloud Security platform to the endpoint. With a shared modern, lightweight architecture, these products help manage risky endpoint behaviour by:

- Providing visibility and context into user and data activity
- Identifying sensitive content that users moved from the endpoint
- Detecting and alerting on risky user behaviour and data interaction in real time.
- Preventing risky data exfiltration from the endpoint
- Speeding up incident response and investigations
- Simplifying deployment with a pure SaaS backend and lightweight endpoint agent architecture

Deliver Visibility and Context on User and Data Activity

Understanding the full context around users' digital activity is essential to assessing risk. But poring over log files can take too much time and often doesn't yield the insight your forensic analysts need to respond.

Visibility with Endpoint DLP

Proofpoint Endpoint DLP collects telemetry on user interactions with data on their endpoints. It doesn't just alert IT and security teams about risky data movement. It also provides context through a timeline that shows how users access, move and manipulate files and data. The telemetry focuses on:

- Sensitive data identification through content scanning at the endpoint and reading data classification labels (including from Microsoft Information Protection)

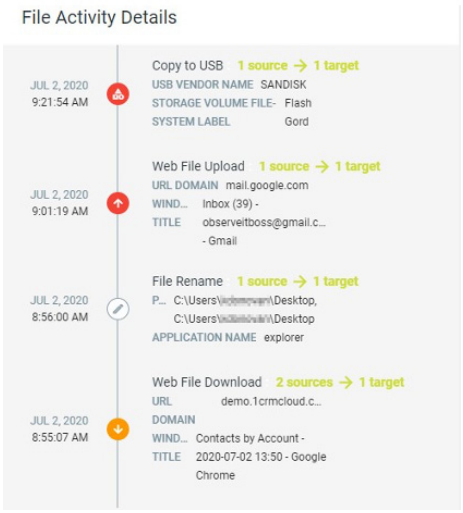

Figure 2: Context into file and data activity from origin to destination.

- User interaction with files or data (such as cut, copy, paste, rename, move)
- File name, extension and size
- Data classification label information (using Microsoft Information Protection labels)
- File and data tracking (including its origin, intermediate location and destination)
- Exfiltration channel (including domain name and URL if the data was moved through a web-based channel)
- Contents of data on the operating system's clipboard

This people-centric approach provides more granular visibility on your users' interaction with your sensitive data than the visibility you get from traditional endpoint DLP tools. Legacy DLP tools don't provide visibility into data movement unless the action triggers an alert. They also do not connect users to actions. Because of these omissions, you would have missed out on seemingly benign data activity that, in context, is part of broader risky behaviour.

Visibility with ITM

Understanding the full context around user-driven incidents requires seeing the full spectrum of user activity, including data movement. That's why our ITM features provide a more complete view of endpoint-based activity. Along with data interactions captured by Endpoint DLP, ITM shows you:

- How users access and use web apps, removable media, servers, virtual applications and desktops
- Mouse and keyboard usage on the endpoint
- Screen captures of endpoint activity

Together, these elements help answer the who, what, where, when and why around risky activity. With context and insight, you can better discern the user's intent when data loss or out-of-policy behaviour occurs.

Threat context

Visualising the threat context around unique user groupings can help you better manage user risk. With our our endpoint products, you can build user watchlists based on criteria such as:

- The sensitivity of user's role and data they interact with
- User's vulnerability to phishing and other social engineering
- Location of user
- Changes in user's employment
- Other HR and legal factors

Content Scanning and Data Classification

You can identify sensitive data in motion, when it is most at risk. This is made possible through scanning content in motion and reading data classification labels, such as from Microsoft Information Protection.

By leveraging your existing investments in data classification, you can identify sensitive business information such as intellectual property without creating a separate workflow for security teams and end users.

For cases when data classification cannot be relied on to identify regulated data and customer data, you can leverage best-in-class and proven content detectors from CASB and Email DLP. You can scan content while users move it through the web, USB devices and cloud sync folders.

Detect Risky User Behaviour and Data Interaction in Real Time

Alert library

Proofpoint Endpoint DLP and Proofpoint ITM include out-of-the-box libraries of alerts for easy setup and faster time to value. Both Endpoint DLP and ITM can alert you on risky data movement and interactions on the endpoint. In addition, ITM can alert you to a wider range of risky insider threat behaviour.

Endpoint DLP and ITM Alert Library

DATA ACTIVITY	USER ACITVITY (ITM ONLY)
Data interaction and exfiltration related alerts, including (more than 40 alerts): • File upload to web • File copy to USB • File copy to local cloud sync • File printing • Copy/paste of file/folder/text • File activities (rename, copy, move, delete) • File Tracking (web to USB, web to web, etc.) • File download from web • File sent as email attachment • File downloaded from Email/Endpoint	Alerts related to full range of endpoint user activity (more than 100 alerts): • Hiding information • Unauthorised access • Bypassing security control • Careless behaviour • Creating a backdoor • Copyright infringement • Unauthorised comm tools • Unauthorised admin task • Unauthorised DBA activity • Preparing an attack • IT dabotage • Privilege relevation • Identity theft • Suspicious GIT activity • Unacceptable use

Flexible rules engine

You can create rules and triggers tailored to your environment from scratch or you can adapt our prebuilt threat scenarios. You can modify scenarios by user groups, apps, date/time, website categories, data sensitivity, data classification labels, data sources and destinations, data movement channels and data types.

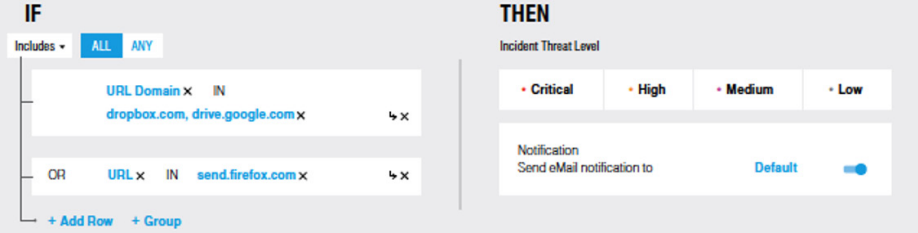

Figure 3: Set up alerts with simple if-then statements.

Point-and-click threat hunting

Our powerful search and filter features help you hunt for threats proactively with custom data explorations. You can search for risky behaviours and activities that apply to your organisation or in response to new risks. Similar to our detection capabilities, you can adapt one of the out-of-the-box threat exploration templates or build your own template.

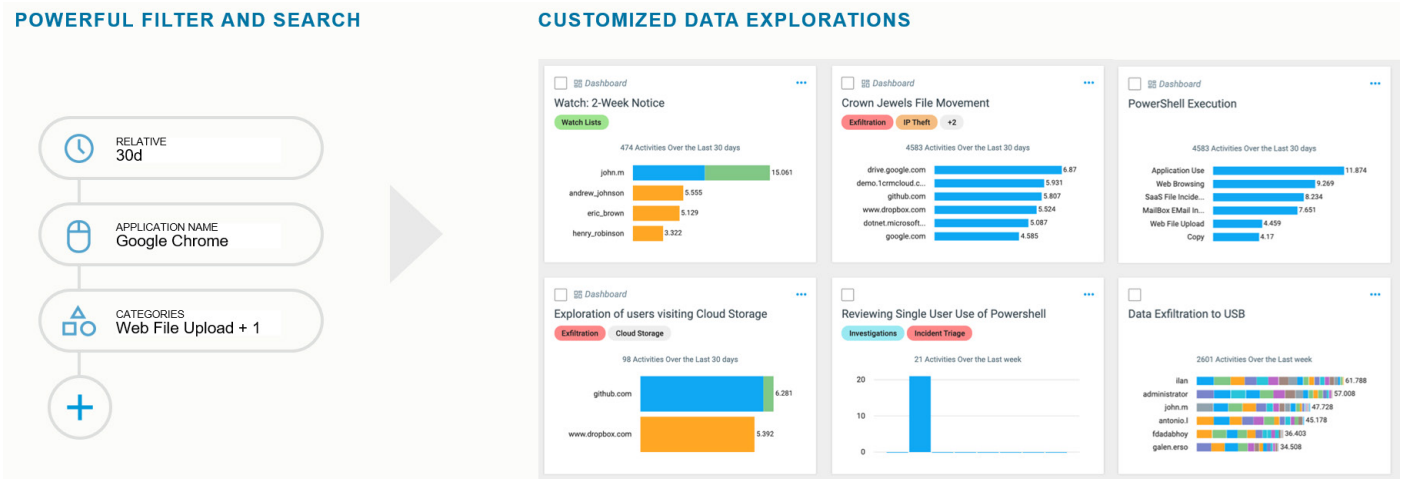

Figure 4: Hunt for potentially risky or out-of-the-ordinary behaviour.

Prevent Unauthorised Data Exfiltration From The Endpoint

Detecting risky user and data activity isn't always enough—you must also actively block data leakage in real time. With our platform, you can prevent users from out-of-policy interaction with sensitive data. These include:

- Transferring to and from USB devices
- Syncing files to other devices and the cloud

Customise your prevention based on users, user groups, endpoint groups, process names, USE device, USB serial number, USB vendor, data classification labels, source URL and content-scan match. You can extend DLP features to email, cloud and web applications with the rest of our Information and Cloud Security platform.

Support Incident Response and Investigations

Investigating and resolving insider-caused security alerts can be a long, costly process. And it often involves non-technical departments such as HR, compliance, legal and line-of-business managers.

Proopoint Endpoint DLP and Proofpoint ITM rely on our powerful Information and Cloud Security platform to help you streamline incident response and investigations of user-caused incidents.

Three powerful capabilities underlie:

- Contextual data visualisations that anyone can understand
- Export and share with HR for smoother workflows
- Optional screen captures that show exactly what the user did (only with ITM)

Screen capture (ITM Only)

In security and data loss investigations, a picture can be worth a thousand words. ITM can capture screen shots of the user's activity. Having clear, irrefutable evidence of malicious or negligent behaviour can help inform decisions by HR, legal and managers.

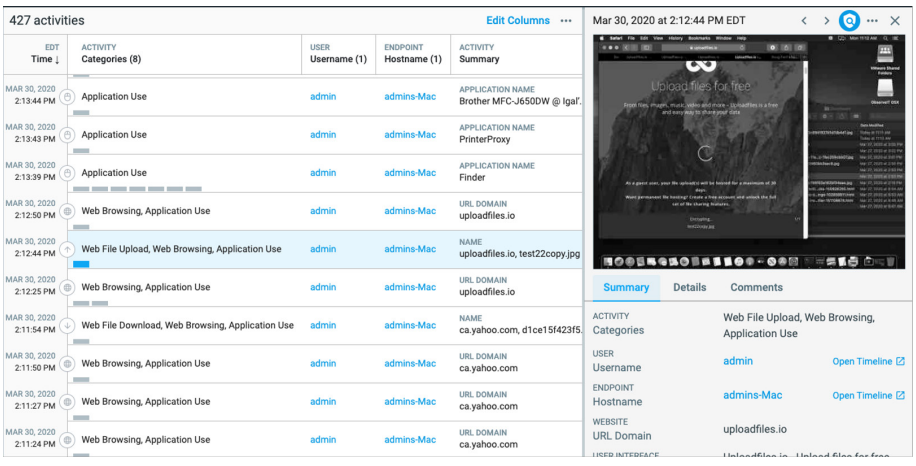

Figure 5: Timeline view of user activities with screen capture of user endpoint.

Alert triage

The data visualisations from the Information and Cloud Security platform provide context around user-driven events in a way that even non-technical teams can understand. Timeline-based views contextualise alerts within a larger incident and a powerful search function helps teams pull in relevant data quickly. Security teams can quickly see which events they need to investigate further and which ones they can close out right away.

Investigation workflow

Basic workflow and information-sharing features within the Information and Cloud Security platform streamline cross- functional collaboration. You can export records of risky activity across multiple events as common file formats, including PDF. With the ITM product, these PDF exports from the platform include screenshot evidence and related context.

Simplify Deployment with Pure Saas Delivery and Lightweight Endpoint Agent Architecture

Proofpoint Endpoint DLP and Proofpoint ITM rely on shared endpoint agents and our modern, cloud-native Information and Cloud Security platform. For Endpoint DLP, the agent collects data activity. For ITM, the agent collects both data and user activity.

Lightweight agent architecture

Endpoint DLP and ITM rely on shared, lightweight endpoint agents that collect most telemetry in user mode. In other words, they're side by side with the endpoint transaction, without interfering with it. The products only intercept endpoint transactions during data loss prevention actions. The agent doesn't get in users' productivity or clash with other kernel-level security tools. This also provides an app-agnostic view into the users' activity on their endpoints.

Easy to integrate into complex security environments

The Information and Cloud Security platform architecture is driven by microservices. Webhooks into our platform make it easy for your SIEM, SOAR tools to ingest Endpoint DLP and ITM alerts, helping you to identify and triage incidents faster.

Those with a complex security infrastructure may need to maintain a single source of truth across systems. We make that easy with automatic exports of Endpoint DLP and ITM data to your owned and operated AWS S3 storage.

Understanding Endpoint DLP and ITM

Managing insider threats and endpoint-based data loss is critical in today's competitive environment. But most organisations don't need to, and arguably shouldn't, collect endpoint telemetry around all activities for all users all the time.

Instead, we recommend a more adaptive, risk-based approach. That means getting insight into some activities for all users and all activities for some users—namely, those who pose a higher risk. These users might include employees on a watch list, high-privilege users, contractors and targeted users such as executives.

The products give you that flexibility. Using a single set of policy rules and the same endpoint agent, you can:

- Limit collection to sensitive data-related activity with Endpoint DLP
- Include user-related context for higher-risk users through ITM

With a simple policy configuration change, you can adjust how much and what type of data you collect for each user or group of users. This adaptive approach helps you investigate and respond to alerts more efficiently and without collecting an arduous amount of data.

LEARN MORE

For more information, visit **proofpoint.com**.