proofpoint.

SOLUTION BRIEF

# Proofpoint Endpoint Data Loss Prevention and Insider Threat Management

## People-Centric 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 programs

**Data doesn't lose itself. People lose it.**

That's why the Proofpoint Endpoint Data Loss Prevention and Insider Threat Management platform takes a people-centric approach to managing insider threats and preventing data loss at the endpoint. It helps modern IT and cybersecurity teams:

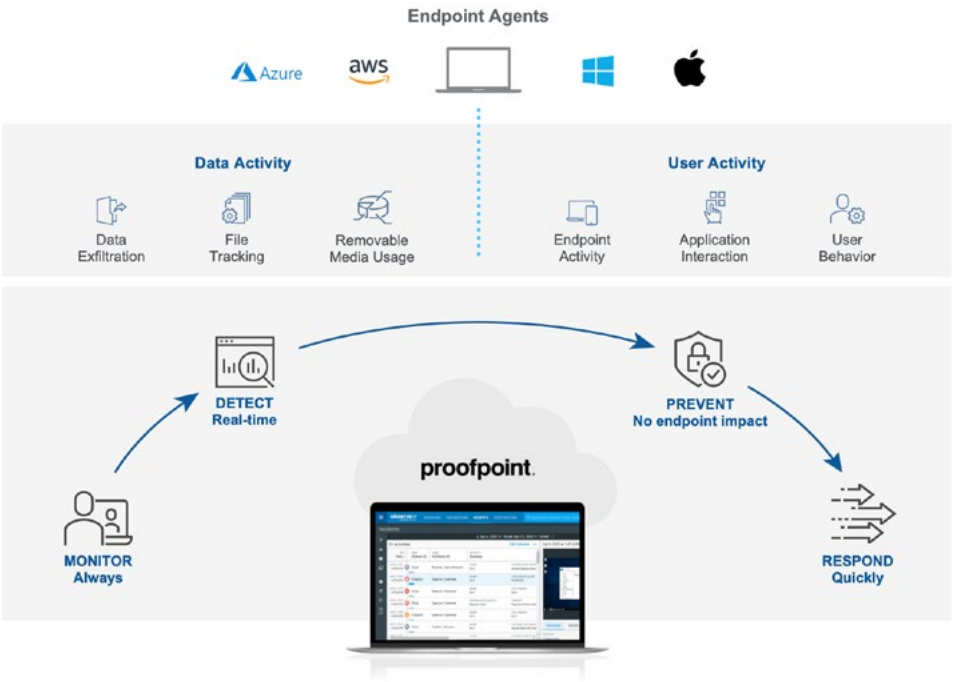
- Identify risky user behavior and data interaction
- Detect and prevent insider-led security incidents and data loss from endpoints
- Respond more quickly to user-caused incidents

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 and context are everything. Legacy data loss prevention (DLP) tools don't show the full picture of user-caused 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.

Our platform includes Proofpoint Insider Treat Management (ITM) and Proofpoint Endpoint DLP. With a shared modern, lightweight architecture, they help manage risky endpoint behavior by:

- Providing **visibility and context** into user and data activity
- **Detecting** and alerting on risky user behavior 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




*Proofpoint Endpoint DLP and ITM Platform*

## 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

The platform collects details about how users are interacting 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. Security teams can quickly see links between:

- 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 faster time to value and more real-time protection than traditional endpoint DLP tools, that rely on content inspection and classification first before providing any value. And they don't provide any visibility on data movement unless the action triggers an alert. You will miss out on data activity that seems benign on its own but, in context, offers critical clues to user intent.


*Context into file and data activity from origin to destination*

## 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 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 behavior occurs.

### Threat context

Visualizing the threat context around unique user groupings can help you better manage user risk. With our platform, 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

## Detect Risky User Behavior and Data Interaction in Real Time

### Alert library

Proofpoint ITM and Endpoint DLP include pre-built libraries of alerts for easy setup and faster time to value. Alert rules are based on threat templates created in partnership with academic and government experts and customer best practices. Both Endpoint DLP and ITM can alert you on risky data movement and interactions on the endpoint. In addition, ITM can alert you on a wider range of risky insider threat behavior.

## Endpoint DLP and ITM Alert Library

**Proofpoint Endpoint DLP**

### Data Activity

Data interaction and exfiltration related alerts including (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**

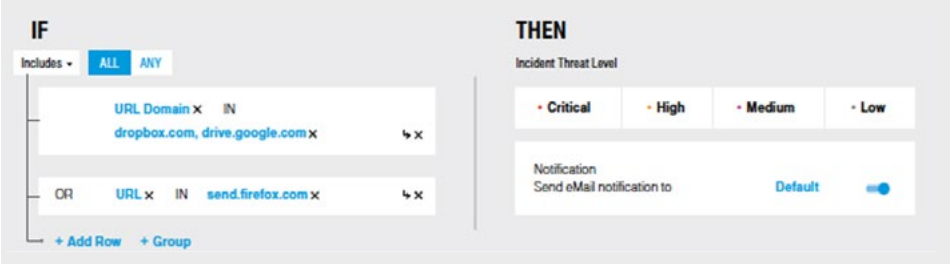
### User Activity

Alerts related to full range of endpoint user activity (100+ alerts):

- **Hiding information**
- **Unauthorized Access**
- **Bypassing Security Controls**
- **Careless Behavior**
- **Creating a Backdoor**
- **Copyright Infringement**
- **Unauthorized comm tools**
- **Unauthorized admin tasks**
- **Unauthorized DBA activity**
- **Preparing an attack**
- **IT Sabotage**
- **Privilege Elevation**
- **Identity Theft**
- **Suspicious GIT activity**
- **Unacceptable Use**

## Flexible rules engine

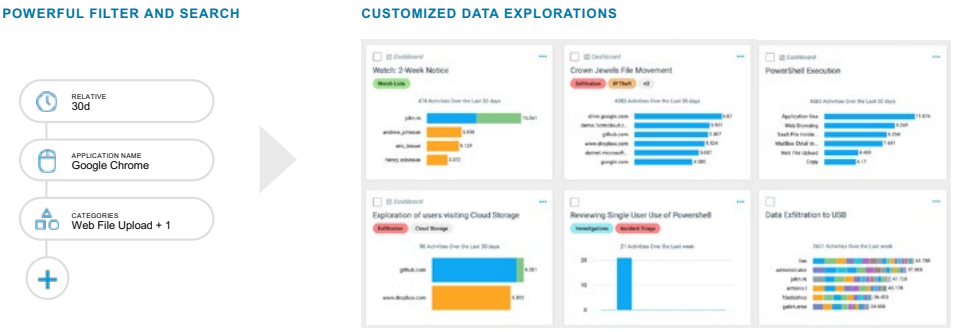
You can create rules and triggers tailored to your environment with our Boolean logic-based rules builder. Rules can be created from scratch or on top of our pre-built threat scenarios. Data loss rules can focus on sensitive data movement using Microsoft information protection labels. This reduces alert fatigue compared to anomaly-based detection systems.




*Setting up an alert with simple and flexible if-then statements*

## Point-and-click threat hunting

Our powerful filter and search features help you hunt for threats proactively with custom data explorations. You can search for risky behaviors and activities that apply to your organization or in response to new risks.




*Hunt for potentially risky or out of the ordinary behavior*

## Prevent Unauthorized Data Exfiltration From The Endpoint

Detecting risky user and data activity isn't always enough—you must also actively block it. With our platform, you can create rules that stop users from out-of-policy movement and interaction with sensitive data. These include:

- Transferring to USB devices
- Syncing files to other devices and the cloud
- File sharing
- Cut, copy and paste
- Web upload

And when you use Endpoint DLP with the rest of the Enterprise DLP suite, you can extend data loss prevention features to email and cloud applications.

## 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.

Our platform streamlines these cross-team efforts with three powerful capabilities:

- Intuitive data visualizations that anyone can understand
- Screen captures that show exactly what the user did
- Easy report exports and sharing for smoother workflows

### Screen Capture

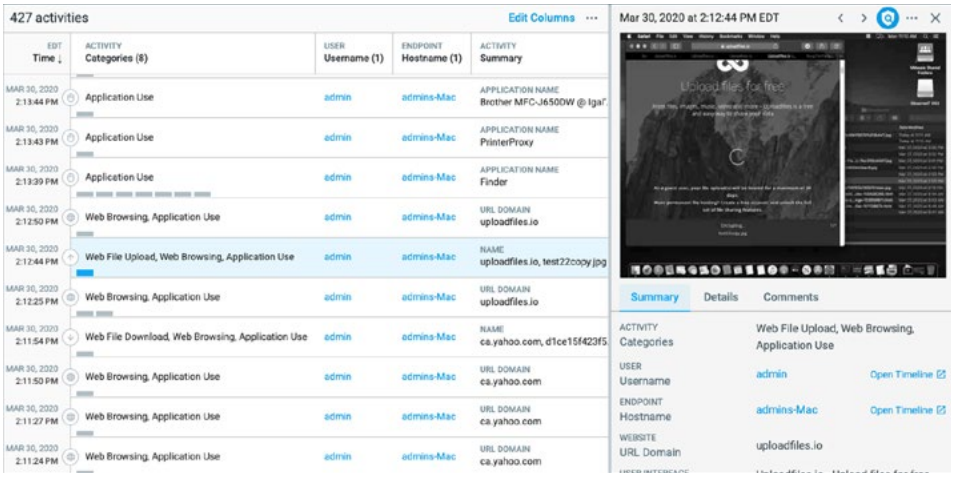
In security and data loss investigations, a picture can be worth a thousand words. ITM can capture screen shots of the user's activity. Having clear, irrefutable evidence of malicious or negligent behavior can help inform decisions by HR, legal and managers.

### Alert Triage

Our data visualizations provide context around user-driven events in a way that even non-technical teams can understand. Timelines tag alerts to incidents and a powerful search function helps teams pull in relevant data quickly. With our platform, 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 platform streamline cross-functional collaboration. You can export records of risky activity across multiple events as common file formats, including PDF. These reports include screenshot evidence and related context.




*Timeline view of user's activities with screen capture of user endpoint*

## Simplify Deployment with Pure Saas Delivery and Lightweight Endpoint Agent Architecture

Our modern, cloud-native architecture is built for scale, ease of use, security and extensibility. For Endpoint DLP, the agent collects data activity. For ITM, the agent collects both data and user activity.

### Global enterprise scale

The platform is built on public cloud infrastructure that is highly redundant and scalable. You're supported whether you're monitoring thousands of users or hundreds of thousands.

### Security and privacy by design

You can authenticate platform users using their credentials from Microsoft Office 365, Okta Identity Cloud, Google Cloud IAM and other providers with our SAML and OAUTH integrations.

- User
- Resource
- Activity to view
- Environment

The platform includes SAML and OAUTH integrations that work with most single-sign-on and multifactor authentication providers. That includes Okta Identity Cloud, Microsoft Office 365, Google Cloud Identity and Access Management (IAM) and more.

Privacy is also crucial to any ITM program. With advanced policy management, you can set monitoring policies, data-exclusion lists and user-exclusion lists. You can organize groups by users, applications, files and endpoints. These include common groupings such as:

- Geography (to comply with regional data-protection mandates)
- Business units (to separate remote facilities, such as retail stores, from corporate offices)

### Lightweight agent architecture

Our platform relies on a lightweight endpoint agent that intercepts only endpoint transactions for a prevent rule. Otherwise, most telemetry is collected in user mode. The agent doesn't get in users' way or clash with other kernel-level security tools. With our agent, you get an app-agnostic view into the user's activity on the endpoint.

### Easy to integrate into complex security environments

Our API-first 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 organizations 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.

Our platform gives 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 Insider Threat Management

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**