proofpoint.

SOLUTION BRIEF

Proofpoint Endpoint DLP and Proofpoint ITM

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

Products

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

Key Benefits

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

The modern, distributed workforce works from anywhere and everywhere. Employees, third parties and contractors have access to more data than ever—whether that data is on their laptop, email or in the cloud. The risk of data loss is thus at an all-time high. Data, however, doesn’t lose itself. People lose it.

Users who exfiltrate data can be categorized into three types: careless, malicious or compromised. Before you can put into place appropriate policies, you must first understand the context behind user behavior. This will also help you better determine the best response when an insider-led incident occurs.

Proofpoint Endpoint Data Loss Prevention (DLP) and Proofpoint Insider Threat Management (ITM) offer a people-centric approach to managing insider threats and preventing data loss at the endpoint.

They help IT and cybersecurity teams:

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

Proofpoint Endpoint DLP protects against data loss by everyday users. Proofpoint ITM includes the same protection, but also defends against threats from risky users by providing deep visibility into user activity. Both products are part of the Information Protection and Cloud Security platform. This is a comprehensive, contextualized, cloud-native platform that provides visibility and insights across channels. It lets you set up policies, triage alerts, hunt for threats and respond to incidents from a centralized console. The platform helps you stop data loss and investigate insider violations quickly and efficiently. And the faster an incident is resolved, the less damage it can do to your business, brand and bottom line.

Monitor Both Everyday and Risky Users

Flexibility with a single endpoint agent

In today's competitive environment, you must be able to manage insider threats and endpoint-based data loss. 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 of your users and all activities for the riskiest ones.

To meet this need, Proofpoint has developed a lightweight endpoint agent that protects against data loss and provides deep visibility into user activity. With a simple change to policy configuration, you can adjust the amount and types of data you collect for each user or group of users. This adaptive approach helps you investigate and respond to alerts more efficiently. And it doesn't require you to collect extreme amounts of data.

Everyday users are typically regular business users. And given their low risk, you can monitor them with Proofpoint Endpoint DLP to gain insights into data activities and user context. You can, for example, set up rules to generate alerts when a user tries to exfiltrate sensitive data by copying it to a USB drive or uploading it to a cloud sync folder.

Risky users need more attention. These users can include employees who are leaving or joining the company, third-party contractors, privileged account holders and targeted users, such as senior executives. You need deeper insights to understand their motivations and intentions. Monitoring them should be based on their behavior or circumstances. Proofpoint ITM collects in-depth data on the activities of these users. This data can provide contextual insight into their intentions before, during and after an event.

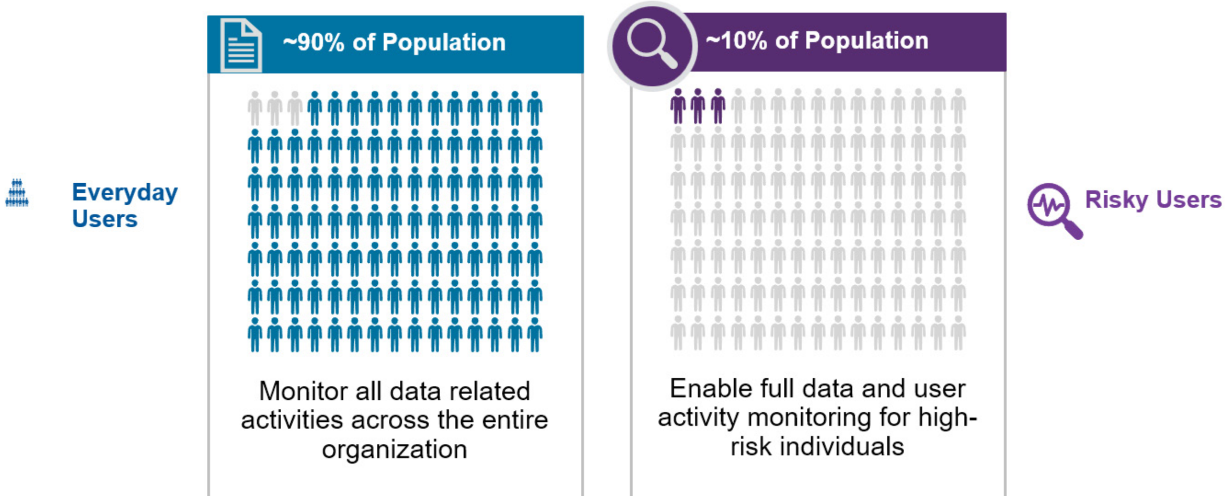

~90% of Population
Everyday Users
Monitor all data related activities across the entire organization
~10% of Population
Risky Users
Enable full data and user activity monitoring for high-risk individuals

Figure 1: A single lightweight endpoint agent provides flexibility to monitor both everyday and risky users.

User watch lists

Intelligent watch lists help you organize and prioritize users by risk tolerance based on their profile. These watch lists can be based on criteria such as the sensitivity of the user's role and data they access. They can also be based on the user's vulnerability to phishing and other social engineering threats. Criteria can also be based on the user's location, changes in their employment status and other HR and legal factors.

Deliver Visibility and Context on User and Data Activity

Visibility into everyday and risky users

Both Proofpoint Endpoint DLP and Proofpoint ITM provide visibility into how users interact with data. They differ, however, in the kinds and amount of data they collect.

Proofpoint Endpoint DLP collects telemetry on user interactions with data on the endpoint. This includes noting when users manipulate file types, such as changing the file extension, or when they rename files with sensitive data. It also includes noting when they try to move sensitive data, such as uploading to an unauthorized website or copying to a cloud sync folder.

Proofpoint ITM provides a more complete view of endpoint-based activity so you can monitor risky users. It captures the data interactions that Proofpoint Endpoint DLP captures, but also provides visibility into application use, screen captures of endpoint activity and other risky behavior. Such behavior may include installing and running unauthorized tools or conducting security admin activities. ITM's in-depth insights help answer the who, what, where and when around risky activity. With context and insight, you can better discern the user's intent when data loss or out-of-policy behavior occurs.

ITM's in-depth insights help answer the who, what, where and when around risky activity. With context and insight, you can better discern the user's intent when data loss or out-of-policy behavior occurs.

Proofpoint's people-centric approach provides more granular visibility into your users' interaction with sensitive data compared with traditional endpoint DLP tools. Legacy DLP tools don't provide visibility into data movement unless an action triggers an alert. They also do not connect users to actions. Because of these omissions, you could miss out on seemingly benign data activity that, in context, is part of broader risky behavior.

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.

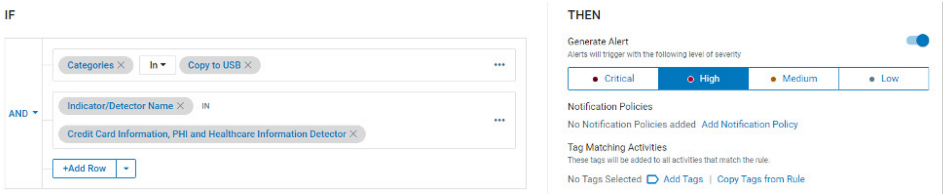
By leveraging your existing investments in data classification, you can identify sensitive business information, such as intellectual property, without creating a separate workflow for security teams and end users. In some cases, you might not be able to rely on data classification to identify regulated and customer data. But you can leverage best-in-class and proven content detectors from Proofpoint Cloud App Security Broker (CASB) and Proofpoint Email DLP. And Proofpoint Intelligent Classification and Protection (formerly Dathena) allows you to automatically discover and classify data in real-time with artificial intelligence.

You can set up content-scanning rules to detect and prevent risky behavior. An alert will be generated when behavior is out of policy, providing real-time actionable insights. Risky user activities trigger content scanning. These activities can include web upload or download, copy to USB, cloud share sync and document open.

Detect Risky User Behavior and Data Interaction in Real Time

Flexible rules engine

You can create rules and triggers from scratch that are tailored to your environment. Or you can adapt our prebuilt threat scenarios. You can modify scenarios by user groups, apps and date/time as well as data sensitivity, classification labels, sources and destinations, movement channels and types. To provide consistency and help you save time, the rules you set up for ITM can be applied to other channels, such as email, cloud and web, through the platform's unified policy orchestrator.



IF

AND

Categories In Copy to USB

Indicator/Detector Name IN Credit Card Information, PHI and Healthcare Information Detector

+Add Row

THEN

Generate Alert

Alerts will trigger with the following level of severity

○ Critical ● High ○ Medium ○ Low

Notification Policies

No Notification Policies added Add Notification Policy

Tag Matching Activities

These tags will be added to all activities that match the rule.

No Tags Selected Add Tags | Copy Tags from Rule

Figure 2: Set up alerts with simple if-then statements.

Alert library

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

Endpoint DLP and ITM Alert Library

DATA ACTIVITY	USER ACTIVITY (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 • File activities (rename, 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 • Unauthorized access • Bypassing security control • Careless behavior • Creating a backdoor • Copyright infringement • Unauthorized comm tools • Unauthorized admin task • Unauthorized database administrator (DBA) activity • Preparing an attack • IT sabotage • Privilege elevation • Identity theft • Suspicious GIT activity • Unacceptable use

Users often do not know that their behavior is risky. But you can enable notifications to educate them.

Prevent unauthorized data exfiltration from the endpoint

Detecting risky users 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.

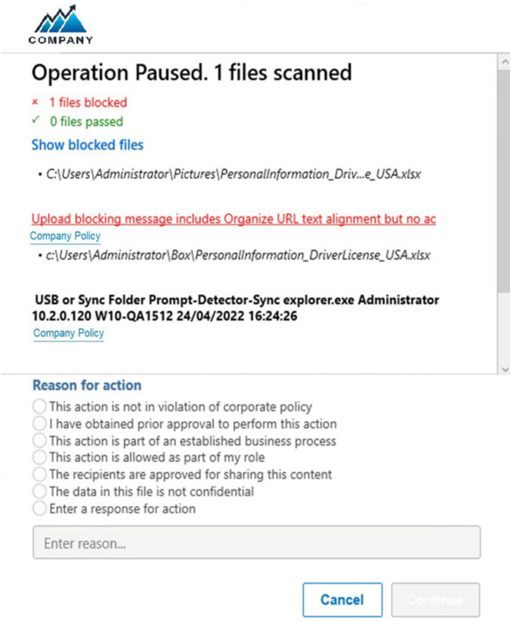
These kinds of interactions include:

- Transferring to and from USB devices
- Syncing files to cloud folders
- Uploading to unauthorized websites
- File printing

Customize your prevention based on users, user groups, endpoint groups, process names, USB 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 Protection and Cloud Security platform.

Educate users on risky behavior

Users often do not know that their behavior is risky. But you can enable notifications to educate them. For example, when users try to move sensitive files, they will be notified that the action violates corporate policy. And they will then be asked for a justification. A link to the company policy can be added to the notification. Notifying employees about their behavior helps keep them productive while reinforcing security controls. Notifications can be customized based on a user's risk, function or location.



Operation Paused. 1 files scanned

× 1 files blocked

✓ 0 files passed

Show blocked files

• C:\Users\Administrator\Pictures\PersonalInformation_Driv...e_USA.xlsx

Upload blocking message includes Organize URL text alignment but no ac

Company Policy

• c:\Users\Administrator\Box\PersonalInformation_DriverLicense_USA.xlsx

USB or Sync Folder Prompt-Detector-Sync explorer.exe Administrator 10.2.0.120 W10-QA1512 24/04/2022 16:24:26

Company Policy

Reason for action

○ This action is not in violation of corporate policy
○ I have obtained prior approval to perform this action
○ This action is part of an established business process
○ This action is allowed as part of my role
○ The recipients are approved for sharing this content
○ The data in this file is not confidential
○ Enter a response for action

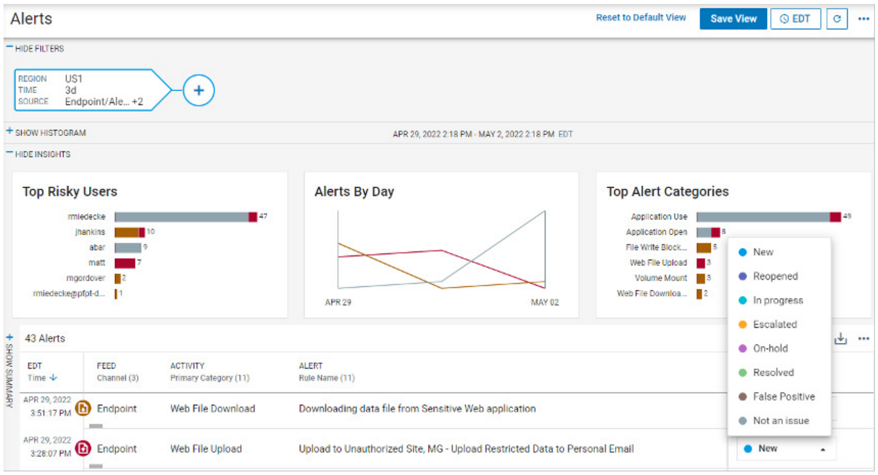
Enter reason...

Figure 3: Notify end users of their risky behavior and ask for justification.

Accelerate Incident Investigations and Response

Unified console

Proofpoint Endpoint DLP and Proofpoint ITM leverage the Information Protection and Cloud Security platform. This helps you to streamline insider-led investigations and response. The platform gathers telemetry from endpoints, email and cloud to provide multichannel visibility in one place. Its unified console provides intuitive visualizations to help you monitor activity, correlate alerts, manage investigations, hunt for threats and coordinate incident response.



REGION US1
TIME 3d
SOURCE Endpoint/Ale... +2

APR 29, 2022 2:18 PM - MAY 2, 2022 2:18 PM EDT

43 Alerts

EDT Time ↓	FEED Channel (3)	ACTIVITY Primary Category (11)	ALERT Rule Name (11)	
APR 29, 2022 3:51:17 PM	Endpoint	Web File Download	Downloading data file from Sensitive Web application	
APR 29, 2022 3:28:07 PM	Endpoint	Web File Upload	Upload to Unauthorized Site, MG - Upload Restricted Data to Personal Email	● New

Figure 4: View all events and alerts in a unified console.

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 behaviors and activities that apply to your organization or in response to new risks. Like our detection capabilities, you can adapt one of the out-of-the-box threat exploration templates or you can build your own template.

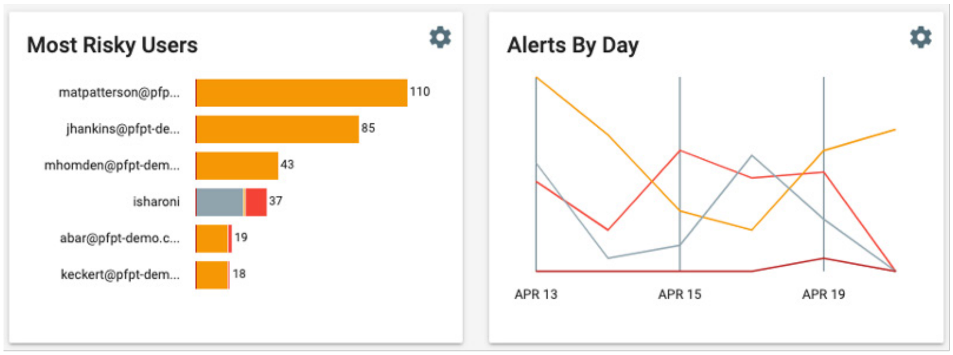
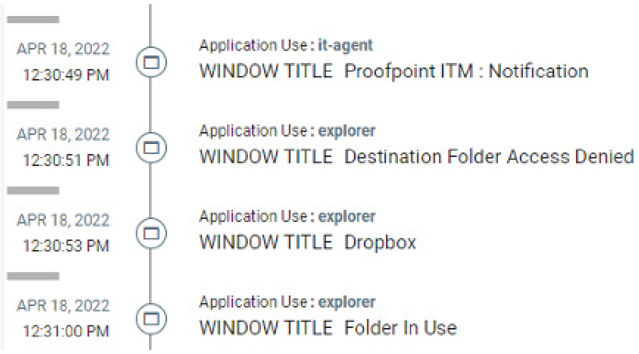


Figure 5: Hunt for potentially risky or out-of-the-ordinary behavior.



APR 18, 2022 12:30:49 PM	Application Use : **it-agent** WINDOW TITLE Proofpoint ITM : Notification
APR 18, 2022 12:30:51 PM	Application Use : **explorer** WINDOW TITLE Destination Folder Access Denied
APR 18, 2022 12:30:53 PM	Application Use : **explorer** WINDOW TITLE Dropbox
APR 18, 2022 12:31:00 PM	Application Use : **explorer** WINDOW TITLE Folder In Use

Figure 6: Easy-to-view timeline provides history of user data interaction.

Alert triage

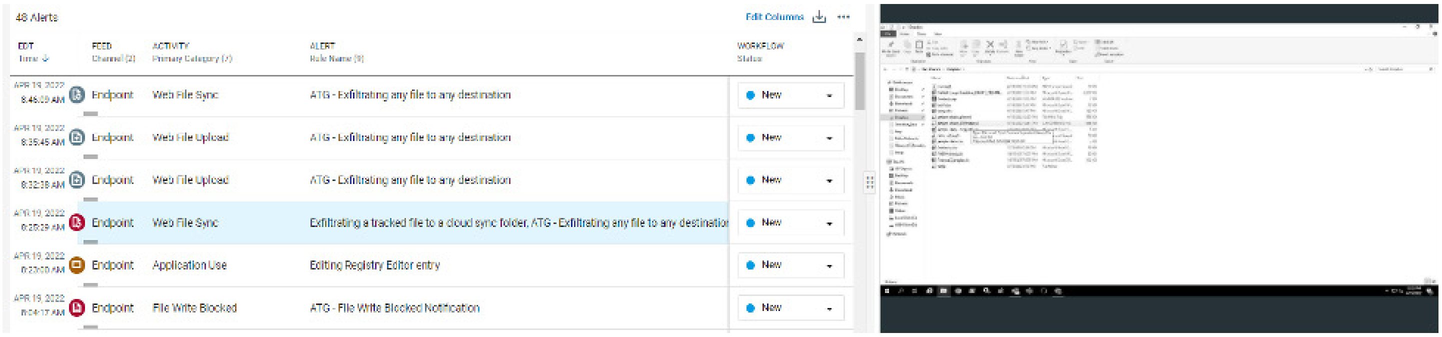
Investigating and resolving insider-caused security alerts is not always easy. It can be a long, costly process. And it often involves non-technical departments such as HR, compliance, legal and line-of-business managers.

With Endpoint DLP and Proofpoint ITM, you can dive deep into each alert. They allow you to see the metadata and gain contextualized insights with timeline-based views. Security teams can quickly see which events they need to investigate further and which ones they can close out right away. Tags can be used to group and classify alerts. This helps facilitate coordination.

Basic workflow and information-sharing features streamline cross-functional collaboration. You can export records of risky activity across multiple events as common file formats, including PDF. With Proofpoint ITM, these PDF exports from the platform include screenshot evidence and related context. This can help non-technical teams such as HR and legal easily interpret the data for forensic investigations.

Screen capture for risky users

A picture can be worth a thousand words. Proofpoint ITM can capture screen shots of the user's activity. Having clear, irrefutable evidence of malicious or careless behavior can help inform decisions by HR, legal and managers.



48 Alerts

EDT Time	FEED Channel (2)	ACTIVITY Primary Category (7)	ALERT Rule Name (9)	WORKFLOW Status
APR 19, 2022 8:46:09 AM	Endpoint	Web File Sync	ATG - Exfiltrating any file to any destination	New
APR 19, 2022 8:35:45 AM	Endpoint	Web File Upload	ATG - Exfiltrating any file to any destination	New
APR 19, 2022 8:32:38 AM	Endpoint	Web File Upload	ATG - Exfiltrating any file to any destination	New
APR 19, 2022 8:28:29 AM	Endpoint	Web File Sync	Exfiltrating a tracked file to a cloud sync folder, ATG - Exfiltrating any file to any destinatio	New
APR 19, 2022 8:23:00 AM	Endpoint	Application Use	Editing Registry Editor entry	New
APR 19, 2022 8:04:17 AM	Endpoint	File Write Blocked	ATG - File Write Blocked Notification	New

Figure 7: Timeline view of user activities with screen capture of user endpoint.

Easy to integrate into complex security environments

Microservices drive the Information Protection and Cloud Security platform. Webhooks into our platform make it easy for your SIEM and SOAR tools to ingest Endpoint DLP and ITM alerts. This helps you to identify and triage incidents quickly.

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

Address Privacy and Compliance Needs

Manage data residency and storage

We provide multiregion data-center support for the Information Protection and Cloud Security platform. This can help you meet data privacy and data residency requirements. We currently have data centers in the United States, Europe, Australia and Japan.

You can control endpoint data storage through a grouping of endpoints. Each grouping, or realm, can map to a data center for storage. This lets customers easily separate data geographically. For example, US endpoint data can be managed by a US realm, which is sent to the US data center.

Address privacy with attribute-based access controls

You need flexibility and control over data access to address privacy requirements. With Endpoint DLP and Proofpoint ITM, you can easily manage access to make sure that security analysts only see data on a need-to-know basis. For example, you can write granular policies and assign access so that a security analyst based in Europe can only see European data, not data in the United States or the Asia-Pacific region. You have the flexibility to give an analyst access only to a specific user’s data or to limit how long they have access to that data.

Gain Multichannel Visibility and Context

Endpoint DLP and Proofpoint ITM leverage the full power of the Information Protection and Cloud Security platform. They take a people-centric approach to content, behavior and threats to stop data loss and investigate threats. Through a unified console, you can gain visibility and contextualized insights across multiple channels, including endpoints, cloud, email and web.

You can work from one console to set up policies, hunt threats and investigate and respond to alerts, regardless of the channel. You do not need to pivot from tool to tool to undertake each activity. You can also dive deep into the metadata of alerts. This helps you to understand what happened before, during and after an event. The cloud-native solution can also be deployed rapidly, which will help you achieve quick time to value.

Work more efficiently, save valuable time and minimize business disruption from data loss and insider threats with the visibility and context that the Information Protection and Cloud Security platform provides.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

proofpoint.