Defend Against Insider Threats

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

Key Benefits

- Protect against financial and brand damage with visibility into risky behavior
- Accelerate investigations with irrefutable evidence
- Achieve rapid time to value with ease of deployment and a lightweight endpoint agent

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 and insider threats is thus at an all-time high.

Insider threats can be categorized into three types: careless, malicious or compromised. To proactively defend against insider threats, you must understand the context behind user behavior. This will also help you determine the best response when an insider-led incident occurs.

Proofpoint protects against data loss by everyday users and defends against threats from risky users by providing deep visibility into user activity and behavior. Proofpoint provides a comprehensive, contextualized, cloud-native solution 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. We help 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 your users and all activities for the riskiest ones.

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.

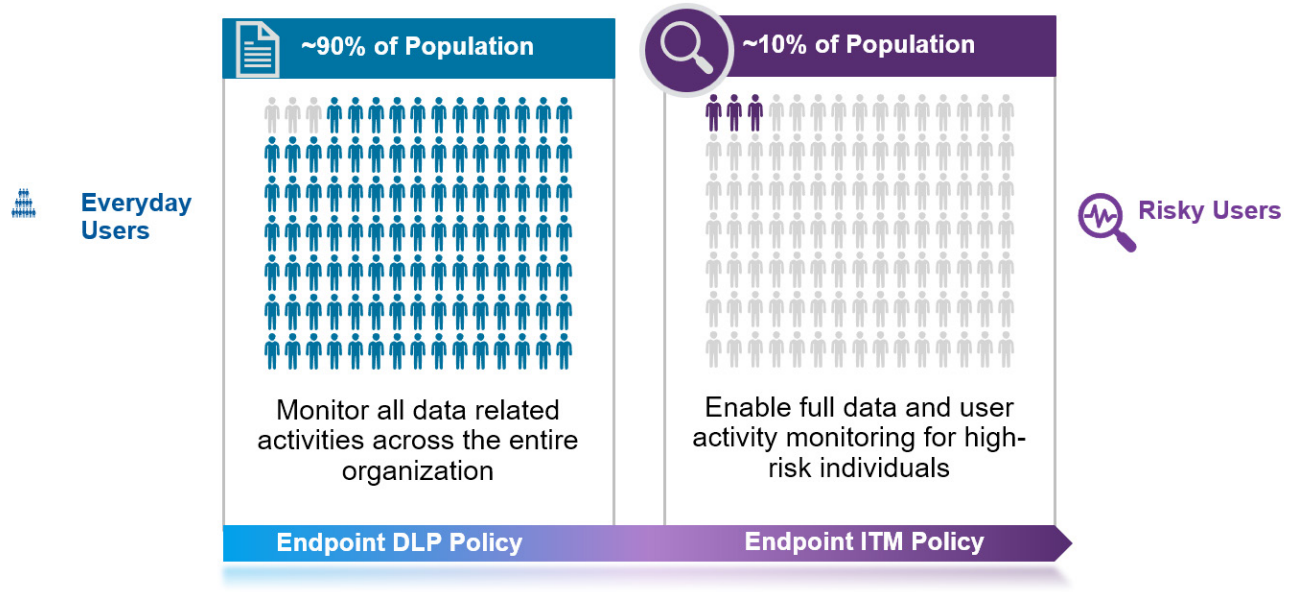

Figure 1: A single lightweight endpoint agent provides flexibility to monitor both everyday and risky users.

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 to gain insights into data activities and user context.

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.

Deliver Visibility and Context on User and Data Activity

Visibility into everyday and risky users

Proofpoint 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 provides a more complete view of endpoint-based activity so you can monitor risky users. It captures the data interactions, 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. Proofpoint provides in-depth insights to help you 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.

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 DLP and Proofpoint Email DLP.

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.

Alert library

Proofpoint includes out-of-the-box libraries of alerts. These allow for easy setup and faster time to value. They can alert you to risky data movement and interactions on the endpoint. And we can also alert you to a wider range of risky insider threat behavior.

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, such as transferring to and from USB devices or syncing files to cloud folders.

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.

Accelerate Incident Investigations and Response

Unified console

Proofpoint helps you to streamline insider-led investigations and response. You can gather telemetry from endpoints, email and cloud to gain multichannel visibility in one place. The unified console provides intuitive visualizations to help you monitor activity, correlate alerts, manage investigations, hunt for threats and coordinate incident response.

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 Proofpoint, you can dive deep into each alert. You can 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.

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

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, these PDF exports 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 can capture screenshots of the user's activity. Having clear, irrefutable evidence of malicious or careless behavior can help inform decisions by HR, legal and managers.

Easy to integrate into complex security environments
Webhooks make it easy for your SIEM and SOAR tools to ingest alerts. This helps you 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 Proofpoint 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. 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.

Address privacy with attribute-based access controls

You need flexibility and control over data access to address privacy requirements. With Proofpoint, you can easily manage access to make sure that security analysts only see data on a need-to-know basis. 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

Proofpoint takes a human-centric approach to content, behavior and threats to stop data loss and insider 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 can also dive deep into the metadata of alerts. This helps you to understand what happened before, during and after an event. And Proofpoint is a cloud-native solution that can be deployed rapidly, which will help you achieve quick time to value.

LEARN MORE

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