proofpoint.

SOLUTION BRIEF

Proofpoint Insider Threat Management

Protect your organization from risky insiders

Key benefits

- Defend against financial and brand damage caused by careless, malicious and compromised insiders
- Proactively detect risky behavior with granular visibility of behavioral indicators
- Accelerate investigations with irrefutable evidence
- Collaborate effectively with HR, legal, and other stakeholders
- Protect end-user privacy and ensure objectivity during investigations
- Achieve rapid time to value with ease of deployment and a lightweight endpoint agent

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

Modern, distributed workforces operate from anywhere and everywhere. Employees, third parties and contractors have access to more data than ever—whether that data is on devices, email or in the cloud. Organizational changes, such as mergers and acquisitions, divestitures and restructuring, cause uncertainty that can trigger insider threats. And geopolitical and economic tensions promote insider-led cyber-espionage.

These dynamics heighten the risk of insider threats that might lead to theft of trade secrets and intellectual property, fraud, espionage and system sabotage. All of these outcomes can inflict material financial, reputational and strategic damage on an organization. To effectively address insider risk, security teams need contextual insight into risky behavior.

Proofpoint Insider Threat Management (ITM) delivers comprehensive visibility into careless, malicious and compromised insiders. It helps security teams identify risky behavior and investigate insider-led incidents efficiently. ITM enables a human-centric approach by providing granular insights into user behavior and intentions. It lets you set up policies, triage alerts, hunt for threats and respond to incidents from a centralized console. With forensics evidence, you can investigate insider violations quickly and efficiently. The faster an incident is resolved, the less damage it can do to your business, brand and bottom line.

Proactively reduce security risk

Comprehensive view of human risk

Insider threats can come from anywhere at any time. This makes them one of the top cybersecurity concerns for Chief Information Security Officers (CISOs) globally. Using Proofpoint Human Risk Explorer (HRE) with ITM, you can view correlated risk signal scoring to proactively uncover and mitigate emerging risks. HRE provides a comprehensive understanding of human risk by analyzing multiple dimensions all in one place. These include individual employee vulnerabilities, behaviors, exposure to attacks, handling of sensitive data, security awareness, and identity.

HRE also uses data-driven insights to make recommendations. For example, if a user shows risky behavior, such as downloading large volumes of sensitive information, you can take immediate action. This might include enforcing stricter security controls, assigning targeted training, or elevating monitoring. By addressing high-risk users first, you can significantly reduce the likelihood of incidents and improve your overall risk posture.

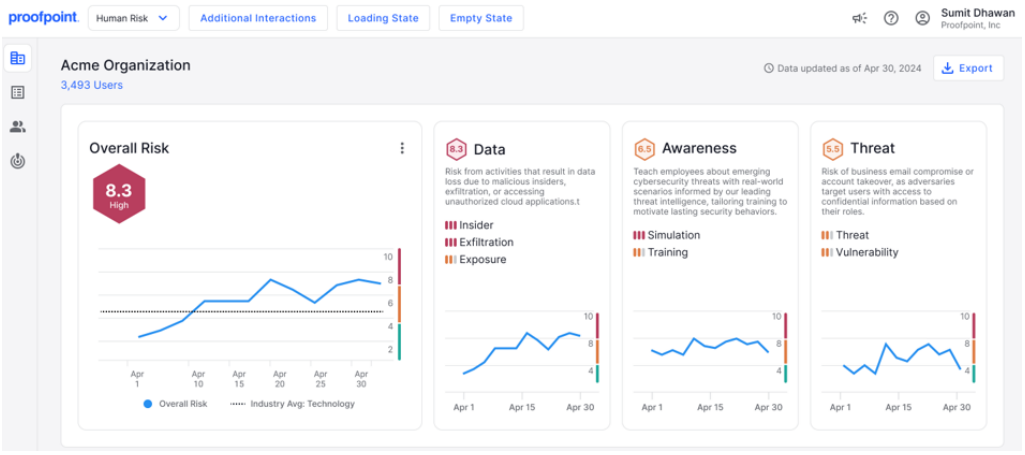


Figure 1: Using Human Risk Explorer, you can easily understand the overall risk for your organization and how it compares to the industry. Diving deeper, you can gain insights into risks associated with insiders, data exfiltration and data exposure.

Adaptive, risk-based approach

To mitigate insider risk, most organizations identify common risk groups. These are individuals or teams whose roles, behaviors, or circumstances mean they might pose an increased risk to the integrity of systems and data. Common risk groups include departing employees, new employees, users with privileged access, executives, contractors, clickers and more.

But what about unknown risky users? Most organizations don't need to—and arguably shouldn't—collect endpoint telemetry around all activities for all users all the time. Instead, Proofpoint facilitates an adaptive, risk-driven approach. That means a shift from static, manual policies to ones that automatically adjust in real time, based on user behavior.

In an adaptive approach, dynamic policies adjust user monitoring based on behaviors, not on predetermined risk characteristics. For example, consider a user who is not part of any risk group. When that user starts to copy sensitive data to a USB drive, ITM generates an alert, triggering elevated monitoring. The elevated monitoring policy captures detailed metadata and screenshots for a specified amount of time. Monitoring occurs only when there is a need. This helps ensure privacy and streamlines alerts for security analysts. With an adaptive, risk-based approach, you save time and enhance detection accuracy.

Highly stable, flexible endpoint agent

To enable an adaptive, risk-based approach, Proofpoint uses a single, lightweight endpoint agent that protects against data loss and provides deep insight into user behavior. You can adjust the amount and types of data collected for each user or group of users. This helps you detect threats early and investigate and respond to alerts efficiently, with less processing and storage costs. The Proofpoint user-mode agent does not conflict with other solutions or require heavy processing, ensuring stability, user productivity and performance.

Get real-time insights into risky behavior

Granular visibility into risky users

To help you detect risky behavior, Proofpoint provides a detailed view of endpoint data activity. This includes users trying to move sensitive data, such as uploading to unauthorized websites or copying to cloud sync folders. It also includes users manipulating file types (for example, changing file extensions) or renaming files with sensitive data. These activities might indicate users hiding their tracks. Coupled with additional context, such as an employee giving their notice and leaving for a competitor, these activities might highlight a high-risk user that needs further investigation.

Proofpoint also provides visibility of application use and web browsing. Risky behavioral signals include installing and running unauthorized tools, conducting security admin activities, tampering with security controls, or downloading malicious software. 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 user intent when unusual behavior occurs.

Content scanning and data classification

Sensitive data is most exposed when shared or transferred. Proofpoint scans data in motion and interprets classification labels—such as Microsoft Information Protection (MIP)—to ensure the right policies are applied.

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. However, in some cases, you might not be able to rely on data classification to identify regulated and customer data. In these situations, you can leverage Proofpoint's best-in-class detectors, including Exact Data Matching (EDM) for structured data and Indexed Document Matching (IDM) for unstructured content such as intellectual property. These advanced methods improve detection accuracy and safeguard your most critical information.

Flexible rules engine and alert library

With ITM, you can create new rules and triggers tailored to your environment. Or, you can adapt our prebuilt threat scenarios. You can modify these scenarios by user groups, apps, and dates and times. You can also modify them based on data sensitivity, classification labels, sources and destinations, movement channels, and types.

ITM also includes out-of-the-box libraries of alerts. These enable easy setup and faster time to value. They can alert you about risky data movement or interactions on endpoints. And Proofpoint can also alert you to a wider range of risky insider behavior. The insider threat library includes over 150 rules based on CERT Institute guidelines and behavior-based research. These give you a quick and easy way to detect risky behavior.

DATA ACTIVITY	BEHAVIOR ACTIVITY
Data interaction and exfiltration-related alerts, including: • 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	Behavior-related alerts, including: • Hiding information • Unauthorized access • Bypassing security controls • 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

Prevent unauthorized data exfiltration from the endpoint

Detecting risky users and data activity isn't always enough. You must also block data leakage in real time. With our solution, you can stop users from out of-policy interaction with sensitive data. This includes transferring data to and from USB devices, syncing files to cloud folders, uploading to the web, copying and pasting, printing, and copying to mobile devices, SD cards, network shares and more. You can also block users from submitting sensitive data via generative AI (GenAI) sites.

You can 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.

Simplify and accelerate investigations

Unified console

Proofpoint helps you to streamline insider investigations and responses. For multichannel visibility, you can gather telemetry from endpoints, email and cloud in one place. This unified console, known as the Data Security Workbench, provides clear visualizations to help you monitor activity, correlate alerts, manage investigations, hunt for threats and coordinate incident responses. This centralized view is a streamlined tooling solution that lowers your operating costs.

Proofpoint's powerful search and filter features help you proactively hunt for insider risk with custom data explorations. You can search for risky behaviors and activities that apply to your organization or in response to new risks. You can speed up investigations with AI-assisted search using natural language prompts. Similar to our detection capabilities, you can adapt one of the out-of-the-box threat exploration templates or build your own.

Alert triage

Investigating and resolving insider-driven security alerts is not always easy. It can be a long, costly process. And it often involves other, 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 metadata and contextualized insights with timeline-based views. Security teams can see which events they need to investigate further and which ones they can close immediately.

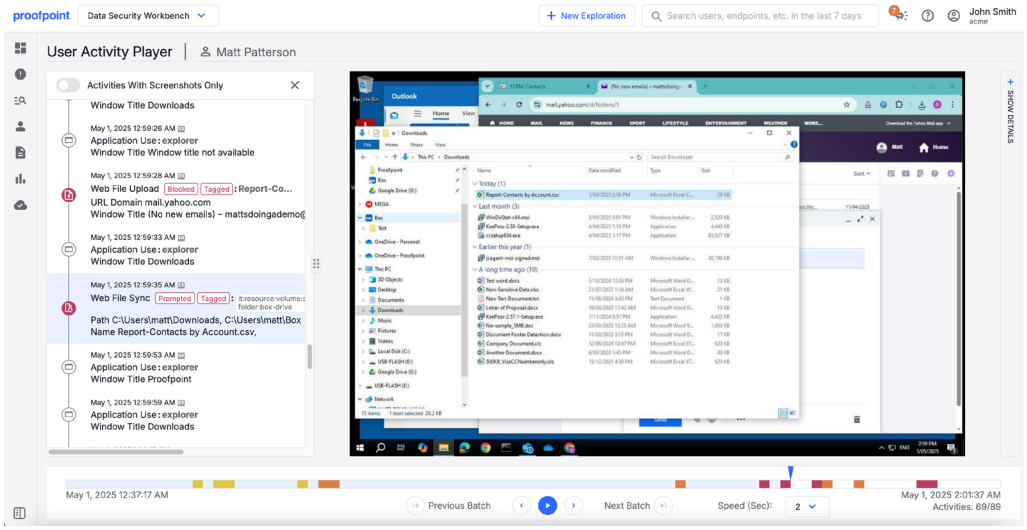


Figure 2: From the Data Security Workbench, you can view what happened before, during, and after an insider-led incident in a timeline. You can easily view screenshots for additional context and forensics evidence.

Contextualized insights from before, during and after an insider-led incident give context about a user's intentions. Understanding whether a user is careless, malicious or compromised is critical for deciding next steps.

Workflow and information-sharing features streamline cross-functional collaboration. You can export records of risky activity across multiple events in common file formats, including PDF. These exports include screenshot evidence and related context. This can help non-technical teams such as HR and legal easily interpret data for forensic investigations and make informed decisions.

Screen capture for forensics evidence

A picture can be worth a thousand words. Proofpoint can capture screenshots of user activity. Clear, irrefutable evidence of malicious or careless behavior can inform decisions by HR, legal and managers.

If you have a complex security infrastructure, you might need to maintain a single source of truth across systems. This can involve retaining screenshots, snippets or files for investigative purposes in your own storage. Proofpoint makes that easy with automatic data exports to your owned and operated storage in AWS S3, Microsoft Azure and Google Cloud Platform.

Balance privacy and security controls

A successful insider risk management program balances user privacy and data security in adherence with data privacy regulations. Proofpoint takes a privacy-by-design approach that embeds privacy into the product design. This helps you protect employee rights, comply with privacy laws and prevent bias during investigations.

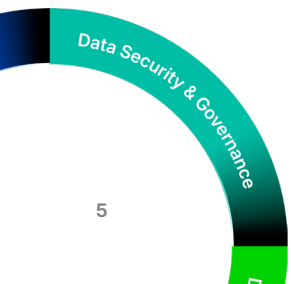
Data residency and storage

Proofpoint provides multi-region data center support. This can help you meet data privacy and data residency requirements. We currently have data centers in the United States, Canada, Europe, United Arab Emirates, Australia and Japan.

You can control endpoint data storage using endpoint groupings. Each grouping, or realm, can map to a data center for storage. This enables customers to easily separate data geographically.

Attribute-based access controls

To address privacy requirements, you need flexibility and control over data access. With Proofpoint, you can ensure that security analysts see only the data that they need. For example, you can give an analyst access only to a specific user's data or limit how long they have access.



Anonymization and data masking

Anonymization of personal information ensures user privacy and removes bias during investigations. Proofpoint anonymizes the user data it collects; it doesn't store full names or employee IDs of users who trigger alerts. Instead, analysts investigate alerts based on unique, anonymized identifiers. When a user identity must be known, the security analyst can request de-anonymization, which an administrator can grant.

Data masking also keeps data private. You can mask sensitive data such as protected health information (PHI) and personally identifiable information (PII). This makes the data unidentifiable in the user interface. Only people who need access to the data can see it in full.

Enable business agility with a modern approach

Scale quickly and easily

Proofpoint is a cloud-native solution that easily scales and adapts to your changing business needs. It can support hundreds of thousands of users per tenant. What's more, it deploys rapidly and is easy to maintain. This ensures quick time to value. Proofpoint also integrates easily into your existing ecosystem with an API-first approach. Webhooks make it easy for your security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools to ingest alerts. This helps you identify and triage incidents quickly.

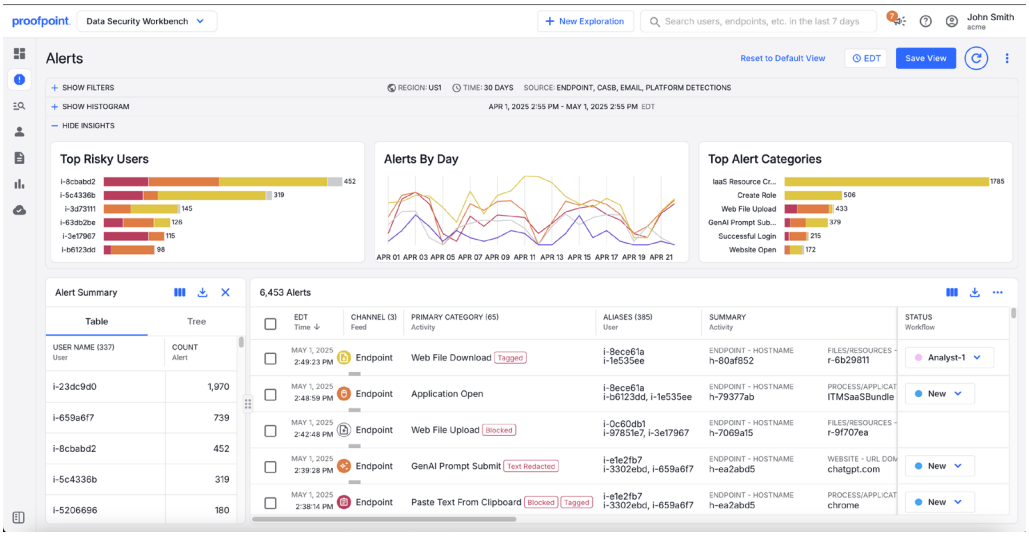


Figure 3: Anonymization protects user identity, helping ensure privacy while eliminating bias during investigations.

Support enterprise-wide changes

Organizational changes can bring doubt and uncertainty. This creates an ideal environment for insider threats. Mergers and acquisitions, impending layoffs or new technologies such as generative AI can be triggers for an insider risk to become an insider threat. Insider risk teams need visibility and controls to support changes when they do occur. Proofpoint enables this with an adaptive, risk-based approach that provides proactive detection and prevention.

Build and mature your program

An effective insider risk program is a combination of people, process and technology. Proofpoint can be your trusted partner on the journey to a successful insider risk program. Our premium services provide the expertise you need to optimize your program, leverage your investments in technology and ensure stakeholder buy-in and engagement. Advisory services provide strategic advice and ongoing services as you build and enhance your program. Applied services help you optimize your technology investment, support your continuous operations and mature your insider risk program.

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 85% of the Fortune 100, 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.

Connect with Proofpoint: X | LinkedIn | Facebook | YouTube

DISCOVER THE PROOFPOINT PLATFORM →