Proofpoint Sigma Platform

People-centric insider-risk, data security and threat protection for the hybrid cloud

Products

- Cloud App Security Broker
- Email Data Loss Prevention
- Endpoint Data Loss Prevention
- Insider Threat Management
- Intelligent Classification and Protection
- Web Security with Proofpoint Isolation

Key Benefits

- Improve operational efficiency using a cloud-native platform with unified administration and response capabilities
- Reduce risk of people-centric data loss across email, cloud, web and endpoint
- Gain unmatched visibility into data risk using world-class threat, content and behavior detection combined with sophisticated analytics
- Streamline DLP with common data detectors, AI-powered classification and content scanning across all channels
- Ensure compliance with data privacy controls

Today's workforce works from anywhere. Employees now use their personal devices, unmanaged apps and generative artificial intelligence (AI) tools for work and in public. More critical infrastructure and data is moving to the cloud. And with careless users, insiders and cyber attackers targeting people now more than ever, the stakes to protect data have never been higher. In this kind of environment, you need to take a people-centric approach to protect data, investigate insiders and block cloud threats.

The Proofpoint Sigma information protection platform can help. It provides unmatched visibility into data risk. And its sophisticated analytics help you to stop data loss and insiders while saving on time and costs.

Proofpoint Sigma is the only information protection platform that analyzes content, behavior and threats from a single cloud-native console. And while it may be a global cloud-native platform, it can store data locally. This means you can meet region-specific data privacy and residency requirements no matter where you operate.

The platform addresses top data security challenges, such as:

- Poor visibility to cloud data, insider risks and cloud threats
- Siloed and on-premises infrastructure that is hard to manage and maintain
- Poor endpoint performance due to bloated agents
- Limited privacy controls

Protect Sensitive Data and Manage Insider Risk Across Key Channels

Proofpoint prevents data loss across email, cloud apps, web and endpoint. We offer common data detectors, classification and a tagging framework. These help you set up consistent policies across your enterprise. We combine content, behavior and threat telemetry from these channels. This way you can see if the user who triggered the DLP alert is compromised, malicious or negligent.

Insider risk and data loss at the endpoint are integrated. With our platform, you can prioritize high-risk users. You can also better detect insider risks and respond more quickly to the threats. We provide granular and real-time visibility into user activity. And we unite data loss and insider-risk alerts across data-loss channels. This helps you quickly answer the who, what, where, when and why behind each event and alert.

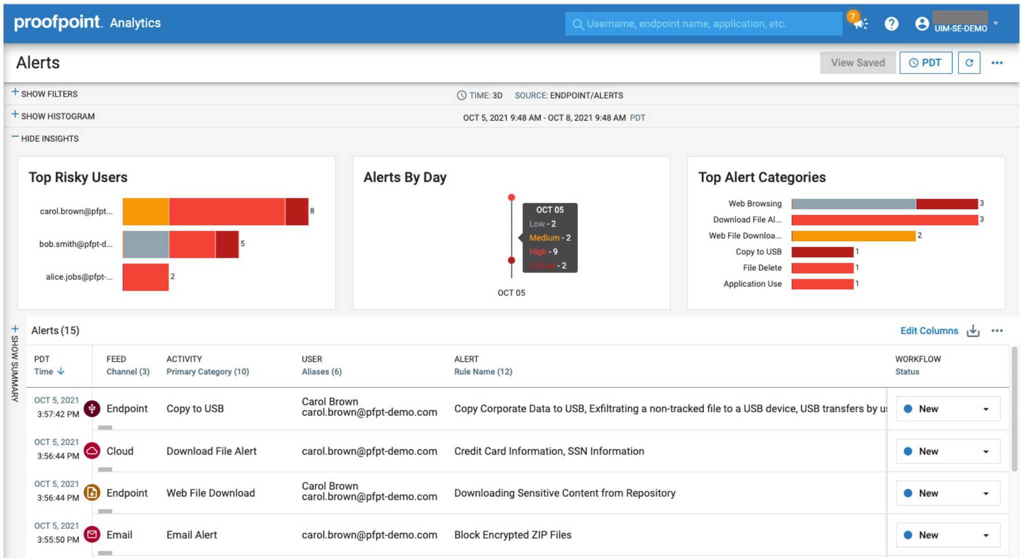
Stop Threats and Enable Risk-Adaptive Controls to Cloud and Web Apps

Proofpoint is global and cloud-native. We unify people-centric threat protection and data security with risk-adaptive people-centric controls. We secure cloud services and web apps by combining:

- **Granular controls.** These include step-up authentication and read-only access through browser isolation.
- **Rich, cross-vector threat intelligence.** This allows you to better understand threats and user risk.
- **Advanced threat protection.** This detects and remediates compromised accounts and malicious OAuth apps. It defends against ransomware, other zero-day malware and phishing sites. And it includes user and entity behavior analytics (UEBA) to detect risky changes.
- **Inline and real-time DLP.** This prevents unauthorized access to sensitive data in the cloud and ensure compliance.
- **Visibility.** This gives you insight into shadow IT, cloud app governance for software as a service (SaaS) and third-party OAuth apps as well as cloud security posture management for infrastructure as a service (IaaS) services.
- **Multimode architecture.** This provides visibility and adaptive controls. The platform lets you enforce stricter controls for high-risk users. These users can be highly targeted or vulnerable. They can also be members of privileged groups, such as admins and VIPs.

Investigate Insiders
Prevent Data Loss
Block Cloud Threats

Figure 1: One Console, One Agent, One Cloud-native platform, with common alert management and investigations, policy uniformity, privacy controls, reporting and analytics.



Alerts (15)

PDT Time ↓	FEED Channel (3)	ACTIVITY Primary Category (10)	USER Aliases (6)	ALERT Rule Name (12)	WORKFLOW Status
OCT 5, 2021 3:57:42 PM	Endpoint	Copy to USB	Carol Brown carol.brown@pfpt-demo.com	Copy Corporate Data to USB, Exfiltrating a non-tracked file to a USB device, USB transfers by u:	● New
OCT 5, 2021 3:56:44 PM	Cloud	Download File Alert	carol.brown@pfpt-demo.com	Credit Card Information, SSN Information	● New
OCT 5, 2021 3:56:44 PM	Endpoint	Web File Download	Carol Brown carol.brown@pfpt-demo.com	Downloading Sensitive Content from Repository	● New
OCT 5, 2021 3:55:50 PM	Email	Email Alert	carol.brown@pfpt-demo.com	Block Encrypted ZIP Files	● New

Figure 2: A unified administration and response console.

Unified Console With Sophisticated Analytics Tools

Our unified admin and response console speeds up investigations. It features the following tools:

- Policy management
- Incident and investigative workflow
- Threat hunting and explorations
- Reporting and analytics
- Administration and data privacy controls

Policy management

The platform lets you:

- Manage all cloud and data access policies in a single console
- Create sophisticated rules across multiple channels using:
  - **Common data classifiers.** These can include things like smart IDs and dictionaries.
  - **Detectors.** These are for proximity matching.
  - **Detector sets.** These are for user groups, regions, use cases, channels and more.
  - **Sensitivity labels**
  - **Advanced threat intelligence and detection**

Incident and investigative workflow

The platform lets you:

- Collect threat, DLP and user-behavior alerts into a unified alert manager to give you a holistic risk profile for the user
- Always know the who, what, where, when and why behind each security event
- Investigate user behavior to determine intent and severity of risk
- Manage alert status cross-functionally from discovery to resolution

Threat hunting and explorations

The platform lets you:

- Hunt proactively for new threats
  These threats can include cloud account compromise, data exfiltration, data leakage, insider risks, unsanctioned use of apps and more.
- Build watch lists that organize and prioritize users by risk profile and others on HR watch lists
  Risk profiles can include executives, Very Attacked People™ (VAPs), departing users, privileged users, human resources staff, contractors and more.
- Search with powerful filters to customize out-of-the-box explorations

Reporting and analytics

The platform lets you:

- View user and data activity across multiple channels with intuitive timeline-based views
- Share with business partners reports of risky activities based on user intent
- Correlate multichannel activities and alerts with data from other security tools
  This is done through seamless integration with security information and event management (SIEM); security, orchestration, automation and response (SOAR); and ticketing systems.

Administration and data privacy controls

The platform lets you:

- Manage alerts and investigations cross-functionally with role-based access controls
- Address data privacy concerns with granular, attribute-based access controls, masking of sensitive data and anonymization of identifiable user data in the console
- Authenticate platform users with your single sign-on (SSO) provider (such as Microsoft, Okta Identity Cloud, Google Cloud IAM and others) through OAuth

Products

Proofpoint Sigma lets you bring together Proofpoint CASB; Email DLP; ITM and Endpoint DLP; Web Security with Isolation; and Intelligent Classification and Protection. This section describes these solutions in more detail.

Proofpoint CASB

Proofpoint CASB delivers people-centric threat protection, data security (including inline DLP) and cloud app governance. It protects users from cloud account takeovers and malicious cloud files. It safeguards sensitive data and governs cloud and OAuth apps. And it helps you stay privacy and data security compliant. This multimode CASB supports both API and proxy-based deployment models.

Proofpoint Email DLP

Proofpoint Email DLP helps prevent the loss of sensitive data through email. It also helps you comply with regulatory requirements, such as those for PCI, PII, GDPR, SOX and HIPAA, with out-of-the-box policies that align with these standards. You can also create custom dictionaries, including AI-powered classification, to identify and protect data that is unique to your organization. Proofpoint Email DLP is easy to deploy. You can set it up as part of an existing email security system or you can integrate it into an enterprise-wide DLP approach.

Proofpoint ITM and Proofpoint Endpoint DLP

Proofpoint ITM and Proofpoint Endpoint DLP protect against data loss and brand damage from insiders who act maliciously, carelessly or unknowingly. Proofpoint correlates user activity and data movement. This allows you to identify user risk, detect insider-led data breaches and accelerate incident response. It also helps you prevent data exfiltration through USB, cloud sync folders, print and more. And with a single, lightweight endpoint agent, you have the flexibility to monitor every day and risky users.

Proofpoint Web Security and Proofpoint Isolation

Proofpoint Web Security protects against data loss and threats when users browse the web. It inspects all internet traffic, including encrypted traffic, to deliver access control to users. It enforces your acceptable use policy and it controls access to cloud apps. This helps with the issue of shadow IT. It also allows but isolates access to unknown or suspicious sites. And it preserves privacy of your people during personal browsing. Web Security integrates with our industry-leading threat intelligence. This makes it easier for you to block the most sophisticated, web-borne threats. And it enforces inline and real-time DLP to prevent data loss from the web channel.

Proofpoint Intelligent Classification and Protection

Proofpoint Intelligent Classification and Protection simplifies the process of identifying business-critical data. And it augments your enterprise DLP program with AI-powered classification. It analyzes a smart sample of data to generate dictionaries and detectors automatically. It also provides recommendations that help improve detection by Proofpoint DLP solutions. It reduces risk, lowers false positives and saves time.

Managed Services

With Proofpoint Managed Services, our experts will help comanage your data security program. We reduce operational burdens from system management to policy governance to incident triage. We also provide executive summaries and reporting. These allow you to show your stakeholders how your security posture is improving over time and how your investment is producing healthy returns.

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 75 percent 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.