proofpoint.

SOLUTION BRIEF

Proofpoint Information and Cloud Security Platform

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

Products

- Proofpoint Cloud App Security Broker
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access
- Proofpoint Insider Threat Management and Endpoint Data Loss Prevention
- Proofpoint Email Data Loss Prevention

Key Benefits

- Cloud-native platform with unified administration and response capabilities
- People-centric visibility and controls across email, cloud, web and endpoint
- World-class threat, content and behavior detection combined with sophisticated analytics
- Common data classifiers and content scanning across email, cloud apps, web, and endpoint
- SASE-ready security architecture with flexible deployment models

The network perimeter is dissolving. And a people perimeter is taking its place. Today's workforce has gone remote. Employees now use their personal devices and unmanaged apps for work. Critical infrastructure and data increasingly reside in the public cloud. And cyber attackers target people now more than ever. In this changing environment, you must take a people-centric approach to cloud security and protecting your data.

Your users need secure access to the web, cloud services and private apps. This requires not just one, but a combination of solutions. This combination should include access controls, threat protection, data security, app governance and zero-trust policy controls. To secure user and data activity across endpoints these controls must be enforced by sensors across all channels. And they must be backed by a common analytics, investigation and policy-management platform.

The Proofpoint Information and Cloud Security platform fills this bill. The platform combines many of our products to address secure access, data loss prevention (DLP) and insider-risk use cases. It offers world-class threat, content and behaviour detection. The platform also delivers people-centric visibility and access controls for web, cloud and private apps. It features a unified administration and response console. And it offers sophisticated analytics to simplify operations and shorten response times.

The Proofpoint Information and Cloud Security platform is powerful and cloud-native. And it aligns to the industry vision of a secure service edge (SSE) architecture. (SSE applies secure access and threat protection as people access apps and data, no matter where they are or what device they are using.) Our platform is also global but it can store data locally. This means you can meet region-specific data-compliance requirements no matter where you operate.

The platform includes the following products:

- Proofpoint Enterprise DLP
- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Email DLP and Encryption
- Proofpoint Insider Threat Management (ITM) with Endpoint DLP
- Proofpoint Web Security with Browser Isolation
- Proofpoint Zero Trust Network Access (ZTNA)

Stop Threats and Secure Access to Cloud, Web and Private Apps

Proofpoint Cloud Security is global and cloud-native. It unifies people-centric access controls, threat protection and a zero-trust network. It secures cloud services, web and private apps by combining:

- **Granular controls.** These include step-up authentication, read-only access via browser isolation and microsegmented app access.
- **Rich, cross-vector threat intelligence** on user risk.
- **Advanced threat protection.** It detects and remediates compromised accounts and malicious OAuth apps. The protection also defends against malware. And it includes user and entity behaviour analytics (UEBA) to detect risky changes.
- **Inline and real-time DLP.** These prevent unauthorised access to sensitive data in the cloud and ensure compliance.
- **Visibility** into shadow IT, cloud app governance for SaaS and third-party OAuth apps and cloud security posture management for infrastructure as a service (IaaS) services.
- **Multimode architecture** for visibility and adaptive controls.

Our 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.

Protect Sensitive Data and Manage Insider Risk Across Key Channels

Proofpoint Information Protection discovers sensitive data in the cloud and prevents data loss. It works across email, cloud apps, web and endpoint. With our common data classifiers, detectors and tagging framework, you can set up consistent policies across the enterprise. We combine

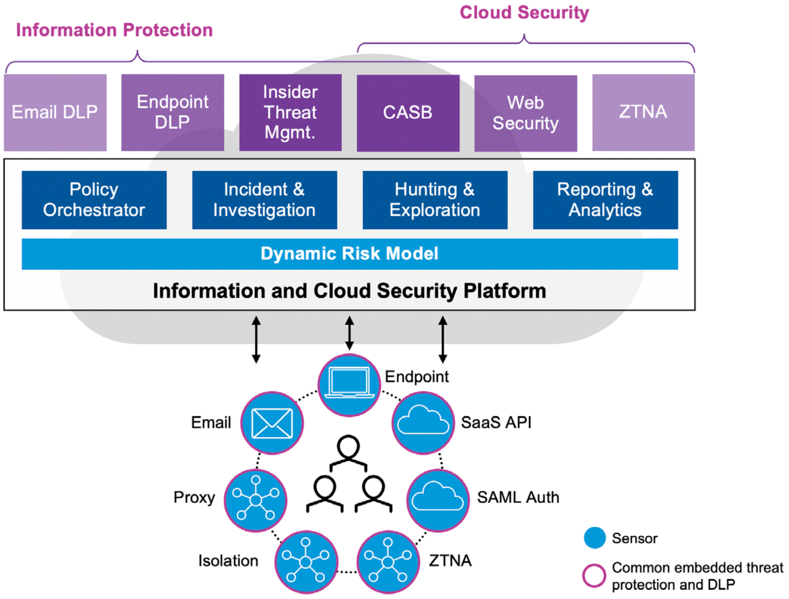
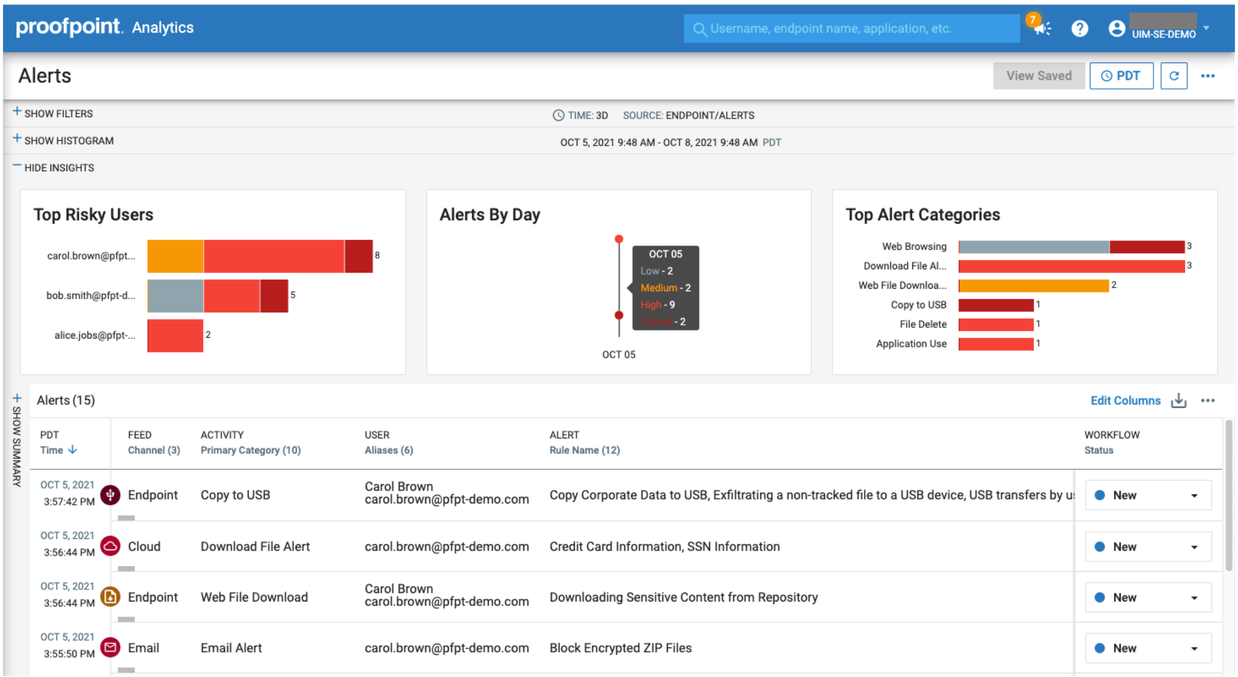


Figure 1: Proofpoint Information and Cloud Security Platform.



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.

content, behaviour and threat telemetry from these channels. This helps you see if the user who triggered the DLP alert is compromised, malicious or negligent. We also unite DLP alert management across these channels. This lets you better prioritise warnings and respond faster to them.

Insider risk and data loss at the endpoint are intertwined. With our platform, your security teams can prioritise high-risk users, detect insider risks and respond quicker 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.

Unified Console with Sophisticated Analytics Tools

Our unified admin and response console accelerates investigations with the following advanced 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 single console
- Create sophisticated rules across multiple channels using:
  - Common data classifiers (smart IDs, dictionaries)
  - Detectors (proximity matching)
  - Detector sets (for user groups, regions, use cases, channels)
  - Sensitivity labels
  - Advanced threat intelligence and detection

Incident and investigative workflow

The platform lets you:

- Collect threat, DLP and user-behaviour alerts into a unified alert manager. This gives you a holistic risk profile for the user.
- Always know the who, what, where, when and why behind each security event.
- Investigate user behaviour 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 organise and prioritise users by

risk profile (such as executives, Very Attacked People™ (VAPs), departing users, privileged users, human resources staff, contractors) and others on HR watch lists.
- Get search functionality with powerful filters to customise 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
- Authenticate platform users with your organisation's single sign-on (SSO) provider (such as Microsoft, Okta Identity Cloud, Google Cloud IAM and others) through OAuth

Products

The Proofpoint Information and Cloud Security Platform brings together Proofpoint CASB; Email DLP; ITM and Endpoint DLP; Web Security with Browser Isolation; and ZTNA. This section describes each product.

Proofpoint CASB

Proofpoint CASB combines compromised cloud account detection, DLP, cloud and third-party apps governance with people-centric controls. It helps you secure Microsoft 365, Google Workspace, Box, Salesforce, AWS, Azure, Slack and more. Our multimode CASB supports both API and proxy-based deployment models.

Proofpoint Email DLP

Proofpoint Email DLP mitigates the risk of data breach via email. It satisfies compliance with more than 240 built-in classifiers for PCI, PII, PHI and GDPR. And it gives you out-of-the-box visibility and enforcement, which is much less complex and much less expensive compared with disparate solutions.

Proofpoint ITM and Proofpoint Endpoint DLP

Proofpoint ITM and Endpoint DLP protect you against data loss and brand damage caused by insiders. They prevent data exfiltration via USB, cloud synch folders, print and more. The products defend against authorised users who might act with malice or negligence. They give you complete visibility into endpoint-based data interactions. And they correlate activity and data movement to protect you from insider-led data breaches and accelerate your incident responses.

Proofpoint Web Security and Browser Isolation

Proofpoint Web Security protects your workers against advanced threats when they browse the web. It defends them from sophisticated cyber threats and data loss. And it keeps them safe with people-centric policies that reduce risk. Proofpoint Web Security delivers dynamic access controls, advanced threat protection and DLP policies. It uses Proofpoint's best-in-class threat intelligence, powered by Nexus Threat Graph. Web Security is also cloud-native. And it can apply granular controls to isolate unknown, suspicious or personal use sites, such as web mail.

Proofpoint ZTNA

Proofpoint ZTNA is the zero-trust alternative to VPN. It secures remote access to any enterprise app, no matter its location. With our people-centric solution, you can provide users with microsegmented secure access to hundreds of cloud instances. You can also automate cloud-to-cloud connectivity. And you can enable hybrid cloud networking between on-premises servers and public clouds.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations 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.