Proofpoint DLP Transform

Transform your data loss prevention program and architecture

Key Benefits

- Quickly detect impactful data loss risk across cloud and endpoints and take appropriate action
- Accelerate incident resolution, including DLP alert triage, investigations and response
- Deploy quickly, scale automatically and maintain with ease, saving time
- Ensure the success of your DLP program

Today's workforce works from anywhere. Employees use unapproved tools like generative AI to make their lives easier. And they access organizational data on cloud applications using their personal devices. Information security experts must enable safe adoption of these modern IT tools and practices while still ensuring compliance with data privacy requirements. To achieve this, they need better visibility to cloud data and user behavior. Legacy data loss prevention (DLP) tools do not adequately address these needs. Worse, they are often siloed, costly, hard to maintain and difficult to scale.

You can modernize your DLP program and architecture with Proofpoint DLP Transform. This solution employs a human-centric approach to data loss prevention. It accurately identifies sensitive content and provides deep visibility into user behavior. Analysts can quickly assess data risk across cloud and endpoints, reach high-fidelity verdicts and take appropriate action. The unified console and powerful analytics accelerate incident resolution. The solution is built on a cloud-native architecture with modern privacy controls and a highly stable agent. It deploys quickly, scales automatically and is easily maintained.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Detect Impactful Data Loss Risk Across Cloud and Endpoint

Deep visibility into user behavior

With a human-centric approach, you can quickly detect impactful data loss risk across endpoints and cloud applications such as Microsoft 365, Google Workspace, Salesforce and more. Insights into user intent enable you to respond to data risk in an appropriate manner. To achieve this, DLP Transform monitors for user interactions with data across managed and unmanaged endpoints and cloud. It detects and prevents sensitive data exfiltration, such as copying files to an unauthorized USB or uploading them to a personal cloud folder. In cloud applications, it detects broad sharing of sensitive files and can reduce file sharing permissions automatically. It also collects telemetry on:

- File manipulation, such as renaming files with sensitive data or changing their file extensions (see Figure 1)
- Website and application usage like downloading data backup or hacking tools from the web and installing them
- Riskiest users' dangerous behaviors, such as manipulating the Windows registry to remove controls..

Accurate content identification

DLP Transform protects data using advanced methods of content identification. For example, in the cloud, you can use exact data matching and optical character recognition to detect medical record numbers in images. This helps a healthcare provider greatly reduce false positives and negatives.

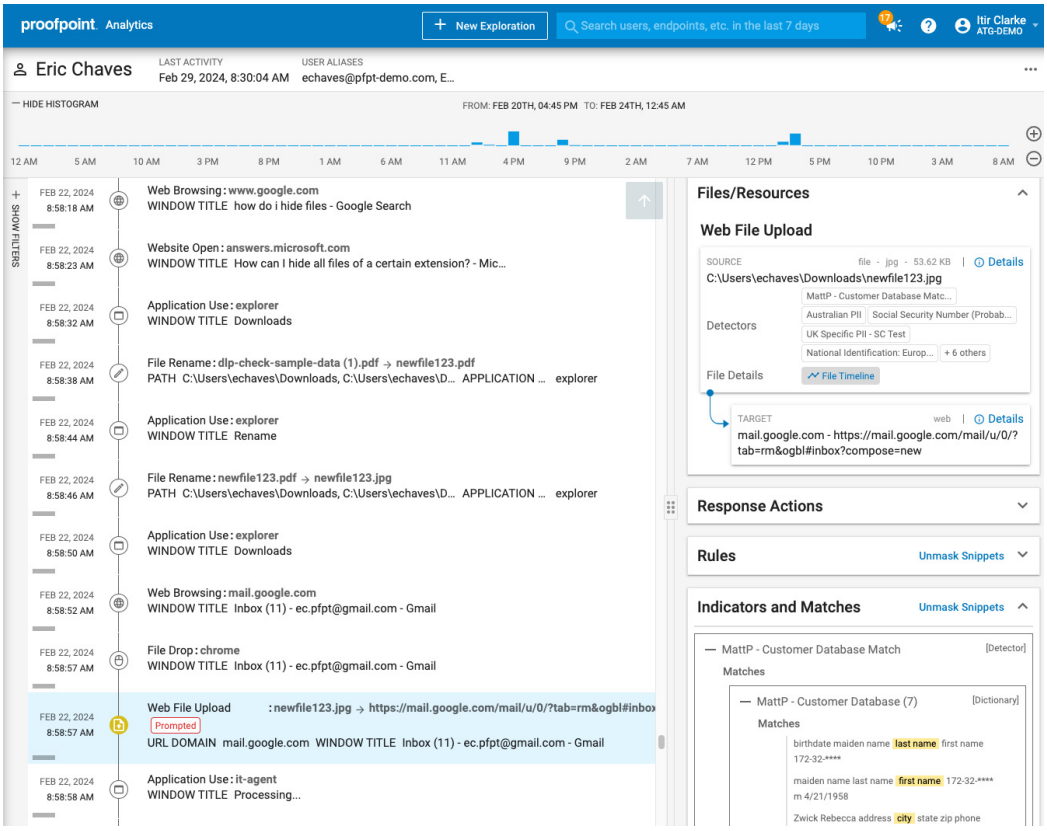

Figure 1: A user renames the "dlp-check-sample-date.pdf" file to "newfile123.pdf," changes the file's extension to jpg and uploads the sensitive data to his personal webmail. This timeline of user behavior and identification of sensitive content suggests to the analyst that this user is trying to circumvent company policy, and further investigation is required.

Accelerate Incident Resolution Through a Unified Console

Efficient cross-channel DLP operations

Security teams using legacy or siloed DLP tools are often burdened with extended investigations and missed violations. DLP Transform gathers telemetry from not only cloud and endpoints but also email to provide in one place cross-channel visibility into data risk. This streamlines alert triage across channels, including Proofpoint Email DLP, investigations and response. The console provides powerful analytics, including intuitive visualizations, and workflows to help you:

- Triage and correlate alerts (see Figure 2)
- Investigate user interactions with data in a timeline view to determine intent and severity of risk (see Figure 1)
- Trace a file's lineage as it is being created, modified and shared
- Coordinate incident response
- Use out-of-box executive reports to demonstrate efficacy and coverage and generate flexible reports for audit purposes
- Manage DLP policies and admin controls for data access and privacy

Proactive data security

The console's sophisticated search-and-filter feature helps you build custom explorations to proactively manage data risks. You can search for data exfiltration as well as risky activities that apply to your organization or in response to the adoption of new tools such as generative AI. And the timeline view of user activities helps you to understand the who, what, where, when and why behind each security incident.

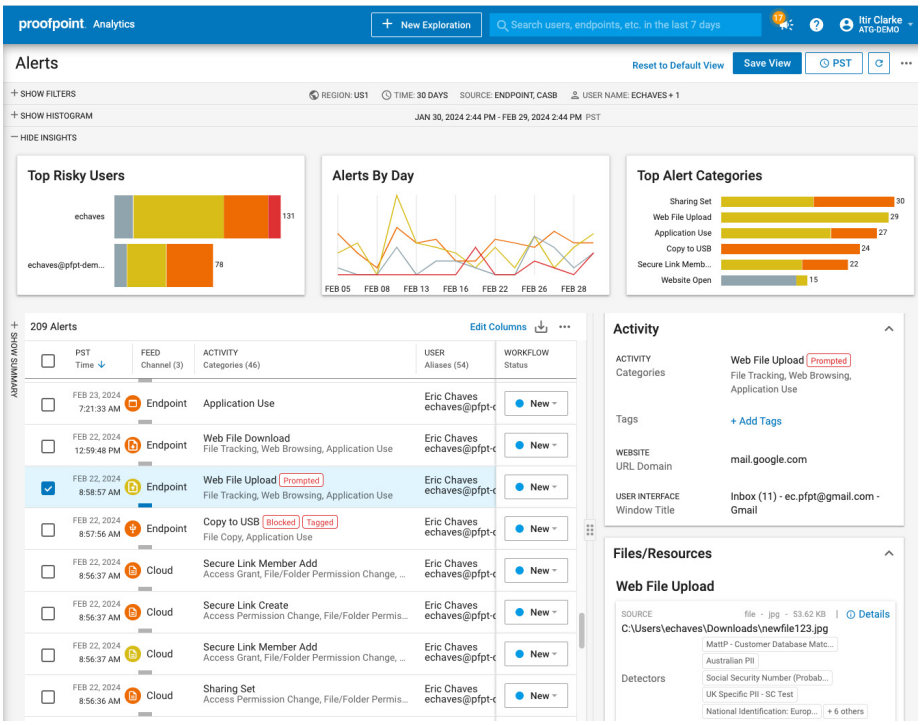

Figure 2: Unified console streamlines alert management across cloud and endpoint without having to switch among multiple consoles. In this example, the analyst has filtered alerts for a specific user. The user has generated alerts uploading sensitive data to his personal Gmail account (highlighted in blue), copying file to USB and sharing a corporate cloud file.

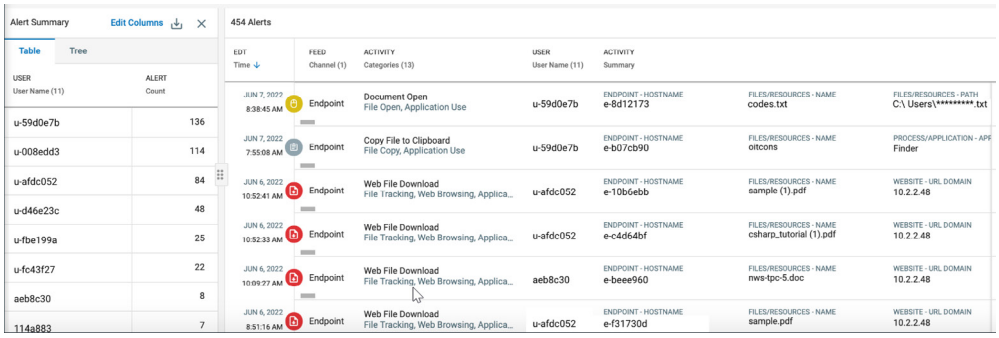

Figure 3: Anonymization of user identifying information in the console ensures privacy of the user being investigated and eliminates analyst bias.

Deploy Quickly and Scale Automatically With a Modern Architecture

Available as software as a service (SaaS), DLP Transform saves valuable time. It deploys quickly, scales automatically and is easily maintained. The solution is modular with shared services built on the cloud. Our multitenant cloud-native platform is highly scalable and API-driven. It can be extended to hundreds of thousands of users per tenant. The platform supports API integrations with Proofpoint Email DLP and ecosystem partners like Microsoft, Okta, Splunk, ServiceNow and more.

Granular-data privacy controls

While DLP Transform offers a global cloud-native console, it can store data in multiple regions. You can manage alerts and investigations cross-functionally and according to regional roles with attribute-based access controls. And you can mask sensitive data and anonymize user-identifying data in the console. This means you can meet region-specific data privacy and residency requirements no matter where you operate.

Highly stable endpoint agent

Our user-mode, lightweight agent is stable and quick to deploy. It is also unique in its ability to detect data loss, but also elevate visibility to potential insider threats. By simply changing the policies in the platform, a security admin can change the behavior of the agent instantly. And unlike kernel-mode agents, it assures a reliable user experience, eliminating help desk tickets and saving time.

Ensure Success of Your DLP Program with Proactive Expertise

If you need help to start or transform your DLP program, you can opt for Proofpoint Managed Information Protection Services. We provide you with highly skilled experts to design, implement and comanage your DLP program. You can guarantee staff continuity and have access to executive-level metrics and more, ensuring the success of your DLP program.

LEARN MORE

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