Access and Privacy Controls for Proofpoint Information Protection

Meet compliance requirements while protecting employee rights and eliminating bias

Key Benefits

- Maintain trust with employees
- Protect critical business information
- Comply with privacy laws
- Prevent bias in investigations

Protecting the privacy of data has become increasingly important and challenging. The rapid pace of digital transformation, hybrid work and the proliferation of cloud applications have made the task of securing sensitive data more complex than ever. And as organisations continue to amass ever larger volumes of data, the perceived value of it grows. Unfortunately, this increased value also brings with it the risk of data loss and theft – including by insiders.

Despite the growing challenges, businesses cannot afford any missteps. Companies worldwide face mounting pressure to comply with strict data privacy laws that mandate strong data security and privacy measures. Non-compliance can be costly; hefty fines and market loss are common. In fact, more than one third of security professionals state that regulatory violations and fines are a consequence of data loss.[1]

Proofpoint offers a comprehensive suite of products designed to enhance data security and manage insider threats while ensuring compliance with data privacy regulations. The Proofpoint Information Protection family of solutions implements robust access and privacy controls. It restricts visibility to only those with a genuine need to know and maintains user anonymity by keeping identifying information confidential. By doing so, Proofpoint not only strengthens data security but also helps eliminate bias in your investigations. This provides you with a balanced approach to information security.

Privacy-First Approach

Proofpoint Information Protection is built from the ground up using privacy-by-design principles. This methodology takes a proactive approach to data protection. It places privacy at the forefront of system design to ensure that IT systems, infrastructure and business processes incorporate privacy as a core consideration right from the beginning. This approach integrates visibility, transparency and user-centricity into its design.

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

1 Proofpoint 2024 Data Loss Landscape Report.

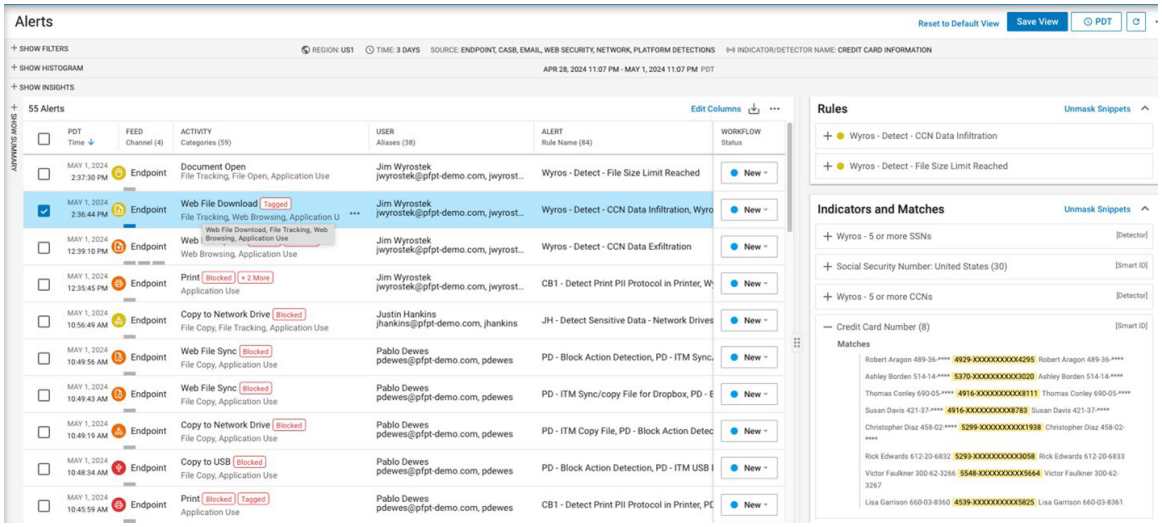

Figure 1: The masking of Credit Card numbers in Proofpoint Information Protection.

Manage Data Residency and Storage

Proofpoint strategically locates regional data centres in the United States, Canada, Europe, Australia, and Japan to address data privacy and data residency requirements. You have full control over where your data is stored across all these data centres.

To manage endpoint data storage, Proofpoint allows you to create groupings of endpoints called realms. Each realm can be mapped to a specific data centre, which lets you easily separate data geographically. For example, a US realm can manage US endpoint data, which is sent to the US data centre.

Address Privacy With Attribute-Based Access Controls

Proofpoint Information Protection's attribute-based access controls offer a flexible and efficient way to manage access to data. They help to ensure security analysts have visibility into data only on a strict need-to-know basis.

For instance, you can write granular policies and assign access so that a US-based security analyst can see only US data, not data out of Europe or the Asia-Pacific region. This level of specific access control significantly reduces the risk of unnecessary data exposure. And when an analyst needs to access a specific user's data for an investigation, the systems administrator can also "time bound" that access, which means they can specify how long the analyst can see that data.

Keep Data Private With Snippet Masking

Proofpoint Information Protection features data masking to keep data private. Data masking obscures sensitive forensics data, such as protected health information (PHI) and personally identifiable information (PII) in the console, rendering that information unidentifiable. This approach ensures that only the people who need access to the data can see it in its full, unmasked form.

System administrators can configure the data identifiers they want to mask. They can, for example, decide to show only the last four digits of a credit card number and mask everything else. They can also decide what and how much data users can see based on their role. For instance, they might specify that only authorised analysts can see snippets of sensitive data.

Protect User Data With Anonymisation

Proofpoint Information Protection also protects user data with anonymisation, which allows you to hide a user's identity. You can anonymise the username, host name, IP address, location info and filenames.

Anonymisation ensures that only authorised security analysts can see the identifying data of monitored users. The process helps eliminate bias in investigations as well. Consider the scenario where a user who just violated corporate policy is a C-level executive. If their identity is known, the incident may be handled differently, or a security analyst may look the other way.

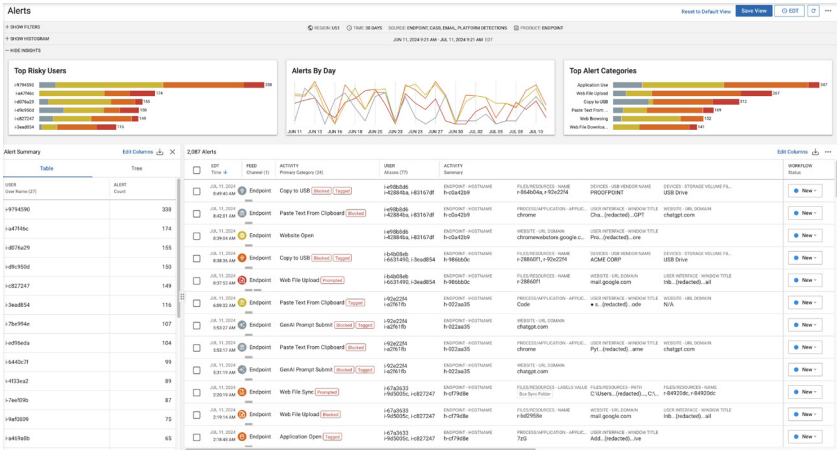

Figure 2: A view of anonymised user data in Proofpoint Information Protection.

When a user's identity must be known further downstream in an investigation, the security analyst can request de-anonymisation, which an administrator can grant.

Balance Data Privacy and Security

Balancing data security and privacy is important for every organisation. To do so successfully, keep these principles in mind:

- **Monitor key data loss channels.** Focus your data security efforts on the way people work. Most data leakage and exposure happen via email, cloud applications and USB drives.
- **Be clear and transparent.** Make sure your employees know your corporate policies around data security and privacy. And let them know exactly what you're monitoring. Doing so builds trust.
- **Educate users with automated notifications.** When a user violates corporate policy, a notification can be automatically generated to let the user know. Using an automated notification helps educate the user about their risky behaviour while eliminating the shame and emotion involved in talking to HR or their manager.
- **Be selective.** You don't need to collect data about everything and everyone. Decide which data is important and how much you really need to know about employees' activities.
- **Control access to data.** While security admins, analysts, legal and HR might have full access to data about employees, that's not always good for privacy. So make sure to use access controls that come with DLP and ITM tools.

Ensure Data Privacy With Proofpoint

You can use Proofpoint Information protection solutions such as Data Loss Prevention and Insider Threat Management to maintain the strongest data protection while ensuring compliance with data privacy regulations. It can help to eliminate bias in your investigations, too. Proofpoint Information Protection is content and behaviour aware so that you can identify sensitive or regulated data as well as flag risky user activity and malicious intent – all from a centralised console that provides visibility across channels, including endpoint, email, cloud and web.

Proofpoint Managed Information Protection brings together the right people, process and technology. This helps you help you design, implement and evolve your programme to optimise data protection and ensure data privacy.

LEARN MORE

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