proofpoint.

DATA LOSS PROTECTION | SOLUTION BRIEF

Defend Data and Manage Insider Threats

Protect information with an adaptive approach

Key Benefits

- Defend data and detect risky behavior from careless, malicious or compromised users
- Mitigate reputational damage, customer attrition and compliance risks
- Solve insider and data loss use cases across cloud, email and endpoint
- Gain actionable insights with AI/ML detections
- Reduce operational cost and scale easily with cloud-based architecture
- Ensure program success with proactive expertise

Data loss is primarily a human-centric issue. Careless users, due to indifference, negligence or a preference for convenience, can pose a risk by mishandling data. Malicious users that walk out the door with critical data as they depart the organization can devastate your business. And compromised user accounts can be used to steal cloud data.

Many data loss prevention (DLP) programs struggle to adequately assess and mitigate these risks. The challenge of predicting what data needs protection is daunting, and relying on a “know your data” measures is reactive.

Proofpoint addresses this by helping you transform your information protection program from a reactive to a proactive human-centric stance for identifying and mitigating risks to your data. This shift recognizes the importance of considering both the content and human aspects of data defense, proving effective in the ongoing mission to safeguard valuable information.

Block Your No. 1 Risk of Data Loss

According to the Ponemon Data Loss Prevention on Email report, 65% of data loss occurs through email. With Proofpoint, organizations can defend data with a layered approach using content and AI/ML based detections.

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

Prevent misdirected emails

We've all experienced that sinking feeling when we accidentally send sensitive data to the wrong person or attach the wrong file. On average, one third of employees send nearly two misdirected emails per year.

You can prevent these accidental data leaks with AI that learns employees' normal email sending behaviors, trusted relationships and how they communicate sensitive data. By using historical email behavior, the system can flag incorrect email recipients and adapt as relationships change. A pop-up alert notifies users about potential mistakes before the email is sent. This empowers users to correct mistakes, saving DLP analysts' time and reducing your risks of financial loss and damage to reputation.

Reduce risk of data loss to unauthorized and personal email accounts

Careless users sending work-related information to personal email or unauthorized accounts is risky, even if it's for well-intentioned remote work or printing. Malicious employees will steal critical business data by emailing it to a personal or burner account when they leave an organization. Many organizations forbid sending emails to freemail domains, such as @gmail, but enforcing that policy is tough. Emails to these recipients could be for legitimate business purposes, such as conducting work with clients, agencies or contractors.

Through machine learning and behavioral AI, the solution adjusts and adapts its understanding of working relationships as you hire, acquire, to prevent loss from unauthorized emails. Metrics give you data-informed insights so you can initiate dialogue to improve data-handling hygiene.

Identify sensitive content to prevent email data loss

Proofpoint prevents sensitive data from leaving your organization via email. You can identify data unique to your organization using hundreds of proven prebuilt data identifiers and dictionaries. These include financial services account numbers, local forms of ID and medical record numbers. In addition, you can easily upload or create custom dictionaries or identifiers that are unique to your organization, as well as fine tune the matching strength of dictionary terms and exceptions. This allows you to analyze the email data that matters most to your organization. With automated enforcement policies, you can block, quarantine or encrypt emails upon detection of sensitive content.

Keep business communications flowing securely

Email encryption secures external or internal-to-internal communication with a robust set of controls and no-touch key management. Enabled by a policy-based DLP engine, the solution lets you define and dynamically apply granular encryption policies at the global, group and user levels with integrations with LDAP and Active Directory. You can automate encryption by destination (i.e., business partner or supplier), sender or message attributes such as attachment types. Or you can enable users to selectively apply encryption. Email Encryption also serves as a TLS fallback to ensure fail-safe encryption. And recipients have flexible options to access encrypted messages, including a web portal, mobile browser or Outlook client.

Defend Data on Endpoints and Cloud Applications

Today's workforce works from anywhere. Employees use tools like Gen AI to make their lives easier. They access organizational data on cloud applications using personal devices. This means information security experts must enable safe adoption of these modern IT tools and practices while ensuring compliance with data privacy requirements. To achieve this, they need better visibility into cloud data and insider threats, without the burden of outdated on-premises tools.

Modernize your DLP program with a human-centric approach to data loss prevention across cloud and endpoint. DLP Transform prevents data loss from managed and unmanaged devices. Rich context on content and user behavior provides unmatched visibility into data exfiltration by careless and malicious insiders. On the endpoint, we not only collect telemetry on data movement but also on other user activities, such as renaming a file and changing its extension. This helps you understand the behavior of your riskiest users. Our unified administration and response console accelerates investigations. This saves you time and total cost of ownership. And our cloud-native platform and light weight user-mode endpoint agent deploy quickly and scale easily.

Protect Against Insider Threats

The modern workforce is highly distributed. Employees, third parties and contractors have access to more data than ever—whether that data is on their laptop, in email or in the cloud. The risk of data loss and insider threats is thus at an all-time high.

Yet not all users are the same. Risky users need more attention. This means going beyond monitoring user data interaction and gaining insights into risky behavior. By knowing the 'who, what, where, and when' before, during and after an incident, you can uncover motivations and intentions to help determine the best response. In addition, you can capture screenshots of risky user activity, helping provide irrefutable evidence and accelerate investigations.

Expertise Shortens Time to Value

Preventing data loss is not easy. It requires more than technical and product knowledge. It also requires a deep understanding of program objectives, data governance and data stewardship. We can be a trusted partner on your journey to ensure your program success. Our managed service provides you with expertise that can help you optimize your technology investment, support your continuous operations, and mature your organization's data protection strategy.

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**.

proofpoint.