

Proofpoint Cloud DLP

Gain visibility and control over sensitive data across cloud apps

Key Benefits

- Gain visibility into cloud threats, risky data movement, cloud data exposure and risky cloud app usage
- Protect sensitive data with data loss prevention (DLP) combining content, behaviour and threat telemetry
- Simplify DLP operations across cloud, email, web and endpoints with a unified alert manager
- Protect against account takeovers, OAuth app abuse, persistent access and malicious file-based attacks
- Detect cloud insider risk with machine learning models built to spot unusual downloads, sharing and data exfiltration
- Accelerate remediation with automated actions that remove shares, reduce permissions, lock accounts, revoke OAuth access and contain risk

Proofpoint Cloud DLP employs a human-centric approach to protect your sensitive data and users from cloud threats. It helps organisations track data exposure, govern SaaS usage and control third-party OAuth app access.

Cloud security starts with protecting IT-approved apps containing your most valuable data, such as Microsoft 365, Google Workspace, Salesforce and Box. Proofpoint Cloud DLP gives you human-centric visibility into cloud threats, data exposure, user behaviour and data movement. This helps organisations build and maintain a strong cloud security posture.

Part of the Proofpoint Data Security Platform, Cloud DLP correlates threats and user behaviour, and applies consistent DLP policies across cloud apps, email, web and endpoints.

Proofpoint Cloud DLP helps you stop sensitive data oversharing and loss, reduce insider risk and lower risky user behaviour. With Cloud DLP, you can defend against account takeover attacks, malicious files and OAuth abuse.

Extend Human-Centric Visibility to Cloud Apps

Proofpoint Cloud DLP gives you human-centric visibility into cloud and email threats. We help you identify your Very Attacked People™ (VAPs) and protect their cloud accounts and data. Not only can you see the files that violate DLP rules, but you can also see who owns them as well as who downloads, shares and edits them. And our analytics and adaptive controls help you grant the right levels of access to users and third-party OAuth apps based on the risk factors that matter to you.

Protect Users, Apps and Data from Cloud Threats

Proofpoint Cloud DLP combines user context with cross-channel threat intelligence from Proofpoint Behavior Graph. Machine learning and threat correlation help you detect when a cloud account has been compromised and is being used for suspicious activity. This may include sending or forwarding email or exfiltrating data.

The intuitive Proofpoint Cloud DLP dashboard lets you investigate alerts for suspicious logins, file activity and administrative activity. You can export forensics data to a security information and event management (SIEM) solution for further analysis. You can do this manually or with REST APIs.

With Proofpoint Cloud DLP's robust policies and real-time alerts and automated responses, you can achieve the following:

- Protect against cloud account takeover and suspend compromised accounts
- Apply risk-based authentication and adaptive access controls
- Prevent data theft and OAuth application abuse by identifying and revoking risky third-party access

- Detect and quarantine malicious files
- Remove inappropriate file shares and permissions
- Restrict access to sensitive content
- Lock user accounts and automate remediation workflows
- Investigate and respond to suspicious cloud administrative activity

Proofpoint Cloud DLP also helps identify cloud insider risk. Purpose-built machine learning models detect behaviour often linked to insider threats and departing employees. This includes anomalous downloading, excessive sharing, unusual data access patterns and potential data exfiltration relative to user and organisational baselines.

The optional SaaS Isolation add-on also lets you protect users, apply DLP on unmanaged devices and integrate your identity management solution through Security Assertion Markup Language (SAML) authentication.

Unify DLP Across Channels

Proofpoint Cloud DLP shares DLP classifiers with other Proofpoint data security solutions. These classifiers include built-in smart identifiers, dictionaries, rules, templates and Autonomous Custom Classifiers (ACC) that use large language models (LLMs) to automatically discover and classify organisation-specific sensitive content.

This sharing helps you identify and protect sensitive data faster. As part of the Proofpoint Data Security Platform, you can deploy consistent DLP policies across SaaS applications, email, web and endpoints.

We combine content, behaviour and threat telemetry from these channels. This helps you see whether the

user who triggered the DLP alert is compromised, malicious or negligent. You can also unify DLP alert management for multiple channels.

More than 240 built-in classifiers cover data that is subject to PCI, PII, PHI and GDPR regulations. Advanced detection technologies help you create tailored controls. These include exact data matching and contextual policies. And you can restrict data access from unmanaged devices, prevent sensitive file uploads to unapproved cloud apps and reduce excessive sharing permissions. You can also identify broadly exposed sensitive files and correlate suspicious login activity with DLP incidents.

Govern Cloud and Third-Party Apps

Proofpoint Cloud DLP shows you shadow IT and discovers cloud apps in your organisation. Our catalogue has 46,000 apps. Each app has more than 50 attributes. And you can categorise cloud apps by type and risk score. This helps you assess security risks, data loss vulnerabilities and compliance gaps. You can block risky apps or grant users read-only access to them.

We detect and assess OAuth permissions for third-party apps that access your IT-approved core cloud services. Our analysis helps identify risky apps and reduce your attack surface. You can define or automate actions based on risk score and context.

Deploy Quickly

Our multimode architecture helps you get value faster. In under four weeks, you can integrate with cloud-service APIs, hybrid identity management tools and security orchestration products (including Proofpoint Threat Response).

This lets you automatically detect threats, contain them and secure data. Risk-based SAML authentication and SaaS isolation help block unauthorised access to corporate apps and support BYOD strategies.

Gain More with Proofpoint Cloud DLP

Proofpoint Cloud DLP combines data protection, cloud threat defence, insider-risk detection, cloud data exposure visibility and adaptive human-centric controls in a single solution. By integrating cloud activity, user behaviour, threat intelligence and DLP telemetry, organisations can better protect sensitive information while reducing operational complexity.

Learn More

For more information, visit proofpoint.com/uk

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises and millions of smaller organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organisations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or trade name of Proofpoint, Inc. in the United States and/or other countries. All other trademarks contained herein are the property of their respective owners.

proofpoint[®]

