proofpoint.

SOLUTION BRIEF

Buyer's Guide to Data Loss Prevention Solutions

This buyer's guide highlights the most important capabilities for a modern information protection solution. It sums up what Proofpoint has learned building successful data loss prevention (DLP) programmes for organisations of all sizes around the globe and across all verticals. It's meant to be a handy reference guide for readers who are just starting out on their DLP journey or who are updating their existing DLP systems.

Begin with human-centric security

To defend data against unique and common threats, you need a platform that supports a human-centric security model. What is a human-centric security model? Essentially, it provides complete visibility into how users interact with sensitive data and tracks any risky behaviour. This ensures you get important context about their intent when data is lost or stolen, or when something they do looks suspicious.

With a solution that takes a human-centric approach, you can quickly see your data loss risk across email, endpoints and cloud apps like Microsoft 365, Google Workspace, Salesforce and others. These insights ensure you can move fast and take the right steps to prevent any data loss incidents.

Key elements of a modern DLP solution

If you want to manage data loss and stop insider threats, you need to be able to detect, analyse, prevent and respond to incidents. It's only when you do all this in a coordinated way that you decrease your risks.

Monitor

To protect data, you can't focus on content alone. You need visibility into what users are doing with it. When you monitor the data activity of all users across endpoints, email, cloud and web, you get a holistic view and contextualised insights.

85%

of organisations reported one or more data loss incidents in 2023

50%

of working adults who changed jobs within the last two years admitted to taking data when they left

Detect

You need a solution that can detect, in as close to real time as possible, when a user takes a risky action or when data is potentially exposed – even if it doesn't reach the level of a full-blown incident. Detection capabilities must strike the right balance when it comes to alerts, which should be both timely and actionable. There shouldn't be so many alerts that they cause fatigue.

Analyse

With good analytics, you can analyse trends in user behaviour and hunt for threats. But you can only do this when a DLP solution combines user activities from multiple channels. Doing so ensures you can catch any risky user behaviour. While this can be done automatically, analysts should also be able to dig deep into the data itself, which is critical for success.

Respond

It's important to investigate and respond to incidents quickly and efficiently. The longer an insider threat persists, the more damage it can do to your reputation and bottom line. A modern DLP solution can automatically enforce policies and remediate threats. Automation will help keep your most valuable data safe and increase your security team's efficiency.

Prevent

Prevention is the ability to stop a user from accidentally or intentionally violating your security policies. This is done with user education, real-time reminders and blocking user activity when necessary.

3 Primary use cases

There are three primary ways that organisations lose data. All of them are caused by people. A human-centric information protection platform must address:

- Careless users, who are not careful with sensitive data
- Careless users, who expose sensitive data when using generative AI (GenAI) apps
- Malicious insiders, who intend to cause harm

$3.5B total projected DLP spending by 2025.[1]

77 DAYS to resolve insider threats.[2]

85% of organisations are targeted by cloud attacks.[3]

56% of inicdents relate to user carelessness.[4]

1: Careless users and common mistakes

Careless users are the leading cause of data loss, according to the Proofpoint 2024 Data Loss Landscape report. These users don't mean to lose data. Rather, they just want to get their work done as efficiently as possible. However, their mistakes can have severe consequences, such as business disruption, brand damage, a weakened competitive position, regulatory violations and fines, and lawsuits.

Here are some of the ways these users create risk:

- Sending emails to the wrong person, either with or without attachments
- Visiting phishing sites
- Installing unauthorised software
- Sharing sensitive files and data publicly
- Emailing personally identifiable information (PII) to a personal email account
- Saving sensitive corporate data to personal devices

Protecting against careless behaviour

An effective human-centric information protection system will block risky activities. It will also provide careless users with coaching to help them understand what's wrong with their behaviour so that they can change it.

What to look for:

- **Classification.** Make sure that email, data and content are consistently monitored both manually and with artificial intelligence (AI) to identify and classify risky users. Once a user is classified as high risk, the system will assign a risk score to protect data accordingly.
- **Detection.** The system should monitor email, documents and data, constantly assessing compliance risks. As content is in motion across channels – whether endpoint, email, cloud or web – it should be scanned to make sure that this movement or sharing doesn't violate your organisation's policies. If a violation is detected via email, the system should allow security teams to either block the email or track it for further investigation.
- **Prevention.** Users should be blocked from exfiltrating sensitive data across channels and devices. That includes misdirected emails with and without attachments, USB, web upload, cloud sync and print. If they make a mistake, they should receive a contextual warning message in the moment, allowing them to remediate and prevent the data loss incident in real time with no administrator input. When warranted, users can explain why they need access to it. This, in turn, will notify the security team, which can allow or deny that request.

[1] The Radicati Group. "Data loss prevention (DLP) market value revenue forecast worldwide from 2019 to 2025." May 2022.

[2] Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

[3] Assaf Friedman and Itir Clarke (Proofpoint) "How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps." May 2021.

[4] Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

2: Careless users and GenAI apps

Users can make great leaps in productivity when they use ChatGPT and other GenAI tools. However, sensitive data is often leaked this way. To avoid data loss without stifling productivity, you need robust data protection measures. The problem is that you can't enforce acceptable use policies for GenAI if you don't understand your content and how employees are interacting with it.

Protecting against careless GenAI behaviour

Robust data protection measures are important to protect sensitive data from being leaked through GenAI tools. You can't just block access to GenAI tools entirely. It's important to find ways to give users access because these tools increase productivity and drive innovation.

If you want employees to use GenAI tools without putting data security at risk, you need to take a human-centric approach to data loss. A solution that uses this approach will surgically allow and block employees from using GenAI tools based on their behaviour and content inputs, even if the data has been manipulated or has gone through multiple channels.

What to look for:

- **Sensitive content identification.** When a system can identify which content is important to protect, it can stop data loss much more effectively. Look for advanced methods of identifying and classifying content, such as Optical Character Recognition, Exact Data Matching, and Indexed Document Matching.
- **User monitoring.** There should be visibility into who's using GenAI tools across your environment and how. The system should be able to detect, block and alert on many types of user actions. This includes the uploading of source code files and the pasting of corporate intellectual property.
- **Proactive risk management.** By building and saving custom explorations your teams can regularly search for data exfiltration and other risky activities associated with GenAI tools.

3: Malicious users

Malicious users are dangerous because they're in the ideal position to take sensitive data. And departing employees are one of the riskiest types of insiders. Over a nine-month period in 2023, departing employees caused 87% of anomalous file exfiltration among cloud tenants using the Proofpoint Information Protection platform. These users often feel entitled to take information when they leave because of how much time they've spent on their projects.

What makes malicious insiders such a threat is that they can bide their time and use their privileged access to find valuable data and security weak spots. Plus, companies often make it worse for themselves by allowing employees to access and store data on their personal devices. This jst makes it easier for employees to steal sensitive data.

A human-centric system will monitor some users more closely than others. And it will apply tighter security controls to the riskiest users.

Protecting against malicious users

A human-centric system will monitor some users more closely than others. And it will apply tighter security controls to the riskiest users. Also, it will proactively block malicious actions based on risk factors, like when an employee resigns or is terminated.

What to look for:

- **Visibility.** Visibility across endpoint, email, cloud and web provides a holistic view and gives you contextualised insights into what a user is doing. Telemetry of user interactions with data and systems should be collected – like when they rename a sensitive file or upload it to an unauthorised website or cloud sync folder. If a user installs or runs unauthorised applications, these activities should also be monitored. And the security team should be able to monitor anyone who triggers an alert in real time.
- **Investigations.** You want a comprehensive threat library of alerts for the most common use cases (time fraud, data exfiltration, bypassing security controls). This will ensure you can get up and running quickly. Security team alerts should include detailed metadata and screen shots of user activities. And contextualised timeline of events will help investigators understand the "who, what, when, where" of user activity.
- **Modern architecture.** The benefit of a cloud-native platform is that it can scale for hundreds of thousands of users. When it includes features like attribute-based access controls, data masking and anonymisation, and multi-regional data centre support, you can meet data privacy and residency requirements. Also, a modern system will extend your security system. That's because it will be easy to integrate with a variety of tools, including:
  - Security orchestration, automation and response (SOAR)
  - Security information and event management (SIEM)
  - Incident response
  - Ticket management systems

Required capabilities

Now that you know how modern, human-centric DLP systems help protect you, let's take a closer look at the exact capabilities you'll need. They fall under three categories:

- Detect and prevent data loss risk
- Analytics and response
- Deployment and implementation

Detect and prevent data loss risk

When security teams have insights into user behaviour and sensitive content, they can respond to data risk in an appropriate way and with greater accuracy.

CUSTOMER NEED	REQUIRED CAPABILITIES
Detecting sensitive content	Detect and analyse sensitive data in email, endpoint, cloud and the web
	Built-in ability to classify sensitive data based on business context
	AI-augmented data classification with large language models (LLM)
	Advanced methods of identification, including: • Optical Character Recognition (OCR) • Exact Data Matching (EDM) • Indexed Document Matching (IDM)
	Pre-built policies to detect sensitive data, such as: • PII • PCI, SOX, GLBA, SEC insider trading terms • PHI, HIPAA, ICD-9, ICD-11 National Drug Code • GDPR, UK-DPA, EU-DEPD, PIPEDA
	Ability to set policies to read and apply Microsoft Information Protection (MIP) sensitivity labels to identify business critical data

CUSTOMER NEED	REQUIRED CAPABILITIES
Monitoring user behaviour	A human-centric approach enabling analysts to respond quickly by providing insights into: • User intent • Data access patterns • Applications access patterns
	Ability to monitor user interactions with data across managed and unmanaged endpoints and cloud, such as: • File renaming • Changing file extensions • Web upload and download • Copy to USB • Cloud share sync • Document open • Anomalous file activit
	Monitors website and application use, such as: • Uploading, pasting or typing content to GenAI sites • Downloading and installing data back-up or hacking tools
	Monitors behaviour of your riskiest insiders to understand intent and mitigate risk, such as manipulating Windows registry to remove controls
	Proactively monitor risky users by only capturing screenshots when an alert is triggered to ensure privacy
	Ability to coach users and ask for justification to access sensitive data, rather than block and impact productivity (email, endpoint, cloud, web)
Preventing data loss	Security awareness training that helps change user behaviour by learning how to avoid cybersecurity risks and protect sensitive data
	Prevent sensitive data exfiltration from managed endpoints, such as: • Copying files to an unauthorised USB • Uploading files to a personal cloud folder • Printing sensitive documents • Pasting sensitive content from clipboard • Network shares
	Remediate broad sharing of files in cloud applications and reduce file sharing permissions automatically
	Enable secure access to sensitive files in IT-approved cloud applications from unmanaged devices
	Automatically detect and prevent emails sent to the wrong person, either with or without an attachment
	Automatically detect and prevent emails sent to the correct person, but with the wrong file attached
	Prevent sharing of sensitive data that hasn't yet been pre-defined to personal email accounts and other unauthorised accounts

Analytics and response

It's important for security teams to resolve incidents quickly across channels. You also want to limit data exposure, which protects privacy.

CUSTOMER NEED	REQUIRED CAPABILITIES
Cross-channel incident resolution	A unified, cross-channel, console for email, endpoint, and cloud used for: • Alert triage • Investigations • Custom explorations • Response
	Cross-channel analytics that show: • User activities over time • File activities over time, as they are being created, modified, shared
	Proactive exploration capabilities that provide real-time visibility to risky user behaviour
	Integration with your organisation's SIEM that allow triage workflows with your existing tools
	Ability to detect and automatically respond to data loss risks from compromised users by: • Terminating sessions • Resetting passwords • Remediating risk • Identifying impact
Privacy	Flexible access controls that ensure analysts only see data on a need-to-know basis
	Anonymised user identifying information and masking of sensitive content to protect data and eliminate analyst bias

Deployment and implementation

After you select the best DLP solution for your organisation you will need to deploy it. The key to a smooth implementation process is to choose the right partners to help you on your DLP journey.

CUSTOMER NEED	REQUIRED CAPABILITIES
Deployment	A cloud-native solution that may be deployed quickly
	A highly scalable solution that can easily be extended to hundreds of thousands of users per tenant
	An easily maintained solution that requires minimal care and feeding of the solute, where updates are clearly communicated and vendor assistance available as needed
	Centralised policy and administration that meets multi-region data residency requirements
	A flexible platform that integrates with your security ecosystem, including solutions such as: • Microsoft • Okta and Sailpoint • CrowdStrike • Splunk and Service Now • Zscaler and Citrix ShareFile
	A lightweight, user mode endpoint agent that: • Elevates visibility to potential insider threats • Enhances user productivity • Eliminates stability problems • Does not conflict with other solutions
Implementation	Professional services that can help you deploy quickly with a team of experienced experts and tune your system to your needs. Implementing a DLP solution requires many steps, namely: • Requirements gathering • Design • Customising the solution • Testing and tuning • Training administrators and users • Documentation
Managed DLP	For organisations of any size, utilising a managed DLP offering should be considered. A managed services offering provides you with experienced experts who will design, deploy and co-manage your programme, guaranteeing staff continuity

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 85 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.