DARKTRACE

Darktrace / EMAIL - DLP

Secure outbound communications effortlessly with the industry's first label-free behavioral DLP with a proprietary DSLM.

Data breaches are costly

As a business, your data is one of your most precious assets. And the repercussions of a data breach are significant – and expensive.

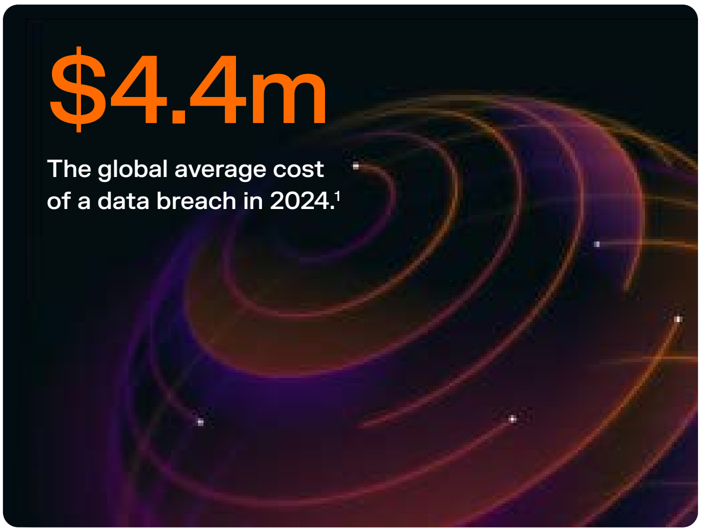
From misdirected emails and poor data labeling to purposeful insider threat, a comprehensive data loss prevention (DLP) solution is essential to reduce your risk of a data breach, protect your brand, and secure sensitive communications.

Existing DLP solutions don't cut it

Traditional DLP solutions often depend on rigid policies and labeling, missing behavioral indicators of insider threats or accidental data loss – such as misdelivery, forwarding to personal accounts, or reply-with-attachment.

These incidents often include PII, which is involved in 53% of breach incidents[1] and can cause significant reputational damage.

Label-centric DLP relies on data classification, which is a lengthy ongoing process for the SOC. It not only creates gaps for mislabeled or unlabeled content, but also lacks sender-recipient history and relationship context. In today's world of constantly changing data, regular expression, payload analysis and fingerprinting are no longer enough.



$4.4m

The global average cost of a data breach in 2024.[1]

Stop data loss before it happens, without rigid rules or manual labels

Darktrace / EMAIL – DLP protects sensitive data by understanding behavior and context, not just content. Our AI-driven approach combines behavioral and content analysis to detect and stop data loss in real time without manual classification.

It blocks labeled and unlabeled data leaks from human error or insider threat, using a domain-specific language model that understands entities, PII patterns, and message context. For full protection, extend data loss analysis to Microsoft Teams with the Darktrace / EMAIL – Teams module.

Secures all your data

Labeled data
Extends Microsoft Purview policies and sensitivity labels to avoid duplicate security workflows, combining both approaches to maintain data control and visibility.

Unlabeled data
Today's data is too diverse and fast-moving to be reliably labeled, even with automation. Darktrace analyzes the content and context of outbound mail to judge its status and take appropriate action.

Sensitive data (PII)
Our behaviorally enhanced PII detection identifies 35+ new categories of personal, financial, and health data to protect the most commonly compromised asset: customer PII.

Human error
By understanding each user's normal behavior, Darktrace detects misdirected emails. Even when data is correctly labeled or not sensitive, it spots risky sending contexts that could indicate data loss and warns the user.

Insider threat
Correlates data from account activity, inbound, outbound, and even network data to spot when an account has been compromised – before data exfiltration occurs.

[1] 2025 IBM Cost of a Data Breach Report

Integrated into your SOC workflows

Microsoft 365 sends outbound emails to Darktrace / EMAIL for assessment before they are sent to the recipient, holding emails that constitute potential data loss for further investigation and optionally alerting the SOC.

Within the Darktrace / EMAIL console, you can view types of data loss alongside the users responsible.

Using the logs, you can view the anomaly score of an email and Cyber AI Analyst narratives that explain detection logic, making it easier to investigate and escalate incidents. DLP is also a helpful indicator of account compromise, which feeds into Darktrace / EMAIL's wider understanding of a user's profile.

Use Case		Darktrace / EMAIL +	Darktrace / EMAIL – DLP add-on module
Insider Threats	Detect and prevent employees from emailing sensitive data to unauthorized recipients	Detect-only	Autonomous prevention
Misdirected Recipients	Stop emails containing sensitive information from being sent to the wrong people	Detection and autonomous prevention (via add-in)	Autonomous prevention via your DLP deployment, with actions taken directly via mailflow interference
Account Compromise	Identify and block unauthorized email access attempts	Detect-only	Autonomous prevention
Regulatory Compliance	Ensure emails comply with data protection laws and standards	Detect-only	Autonomous prevention
Sensitive File Transfer	Monitor and control the emailing of sensitive files	Detect-only	Autonomous prevention
Human Error	Mitigate risks from accidental data leaks via email	Detect-only	Autonomous prevention
Personal Account File Transfer	Block sensitive data from being emailed to personal accounts	Detect-only	Autonomous prevention
Anomalous File Transfer	Detect and block unusual file transfer activities via email	Detect-only	Autonomous prevention
Personally Identifiable Information (PII)	Stop 35+ PII categories from exposure via email		Detection and autonomous prevention

■ About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com