Forcepoint

Solution Brief

Forcepoint Data Loss Prevention for Cloud Email

Secure and control your email, leveraging the industry's most trusted DLP technology

Challenge

- Sensitive data is leaving organizations in increasing amounts via multiple channels.
- Email is cited as the most popular threat vector for attack .
- Securing data without stifling business productivity has never been more important or complex.

Solution

- Forcepoint extends the industry's most trusted Data Loss Prevention (DLP) solution to the email channel.
- Precisely monitor and prevent sensitive data loss through email.
- Leverage a fully managed cloud solution to scale outbound email protection to meet the demands of your business.

Outcome

- Gain efficiency by dramatically reducing the number of false-positive incidents through email
- Increase compliance with 3x more pre-defined policies than any other DLP provider.
- Migrate your DLP to Forcepoint in as little as 6 weeks leveraging Forcepoint expertise, out-of-the box policies and top of the line knowledge transfer.

Data security continues to grow as a major focus for organizations globally. Whether employees are working within the traditional confines of an office or within the new norm of hybrid or remote work, keeping data secure across multiple channels has increased in complexity. Email is a critical channel for organizations to gain visibility and control over to stop unwanted data exfiltration of valuable files, IP, and data. Common examples of data loss through email include:

→ **Sending an organization's files or data** to private email accounts via company email.

→ **Sensitive data** leaving the organization by way of user negligence or compromised accounts.

→ **A malicious insider actor sending sensitive data and files** to external competitors, news sources, and websites. Often the intent is to commit fraud, sabotage the organization, or steal proprietary data.

→ **As a result of phishing and malware attacks or adware and spam,** well-intentioned internal users unwittingly cooperate with bad actors to exfiltrate critical data and IP.

"Email is the most popular threat vector for attackers to use for delivering malware to an organization. Email is also a direct line of contact between users and cybercriminals, leading to billions of dollars of fraud and business email compromise every year."

IDC, WORLDWIDE MESSAGING SECURITY MARKET SHARES, 2021: HYBRID WORK DRIVES NEED FOR THREAT INVESTIGATION INTEGRATION, DOC # US49144522, JUNE 2022

It's imperative that organizations have strong visibility and control into their outbound email to protect intellectual property from targeted attacks as well as accidental exposure. The technology that accomplishes this is DLP. According to IDC "The past 24 months have seen a renaissance in the data loss technologies market. Manual and arcane classification techniques are being replaced by machine learning and automation. Context has become the great enabler. The effectiveness and efficiency of the solutions have gotten better." [1] Email security combined with all the new advances in DLP that discovers, protects, and controls sensitive information is essential in controlling the important email vector. Without strong DLP capabilities in place, email security breaches may gravely harm your organization's business and reputation.

Forcepoint DLP for Cloud Email advantage

As a leader in data security solutions, Forcepoint DLP for Cloud Email brings unprecedented visibility and control for outbound email. In combination with DLP for Endpoints, Cloud, Web and Network, DLP for Cloud Email delivers a powerful multi-pronged solution for safeguarding an organization's data. Forcepoint's DLP is designed to prevent data loss everywhere your people work and wherever your data resides.

Extreme data identification

Forcepoint's DLP provides over 1,600 classifiers and pre-defined templates that allow for rapid deployment and sensitive data identification. It also leverages advanced technologies, utilizing natural language analysis, machine learning, and one of the strongest fingerprinting technologies in the industry to precisely identify data at rest, in motion, and in use. For data security, visibility is key and Forcepoint's DLP Discover allows for strong visibility followed by formal identification of data so that all forms of data can receive adequate control. This is important for multiple purposes:

- → **Compliance.** Forcepoint DLP covers critical regulations such as GDPR, HIPA, and many more across 83 countries to make sure that organizations are constantly meeting compliance standards.
- → **Simplicity.** Creating and implementing classifiers that meet the needs of an organizations needs and business requirements consumes huge amount of time and resources for a DLP deployment. With Forcepoint's pre-defined templates and classifiers, organizations can rapidly deploy classifiers specific to a range of industries and data types, dramatically simplifying DLP.
- → **Efficiency.** With Forcepoint's comprehensive data identification technology, Forcepoint DLP dramatically reduces the number of false positives, while ranking and prioritizing critical incidents for investigation.

Unified policy control

A strong DLP strategy must extend across all core channels, such as endpoint, cloud, web, and email. Often organizations will treat each of these channels in silos with disparate DLP products that focus on one channel alone such as cloud or email. With Forcepoint you can secure all these channels with one solution and manage them from a single policy. Write once and deploy multiple times brings unequaled control over the data in your organization, giving you a single pane of glass across all the critical channels where data loss happens. Using policies through DLP for Cloud Email can also allow for visibility into additional devices such as tablets and phones, which are not typically covered with common endpoint solutions.

Unprecedented scalability

Forcepoint DLP for Cloud Email has the advantage of being a fully managed service in the cloud, delivering the elasticity of resources common in cloud deployments. If, for example, there is a burst of outbound email at any point of time, DLP for Cloud Email allows for a rapid expansion and then reduction of resources to effectively meet the demands of the burst. It also enables continuous DLP service to meet the growing demands of your organization without having to deploy and configure additional hardware to meet those demands.

Risk-adaptive protection

Forcepoint is the industry's first provider to deliver risk-adaptive DLP. Through continuously monitoring user activity, the solution allows your people to be free to do more and only steps in when it identifies high-risk activity or patterns of risky behavior. Automation allows for near real-time enforcement; in other words, it can anticipate and stop a breach before it happens.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: DLP IS Dead, Long Live DLP, Doc # US48261521, October 2021

Forcepoint DLP for Cloud Email

DLP for Cloud Email - securing outbound data

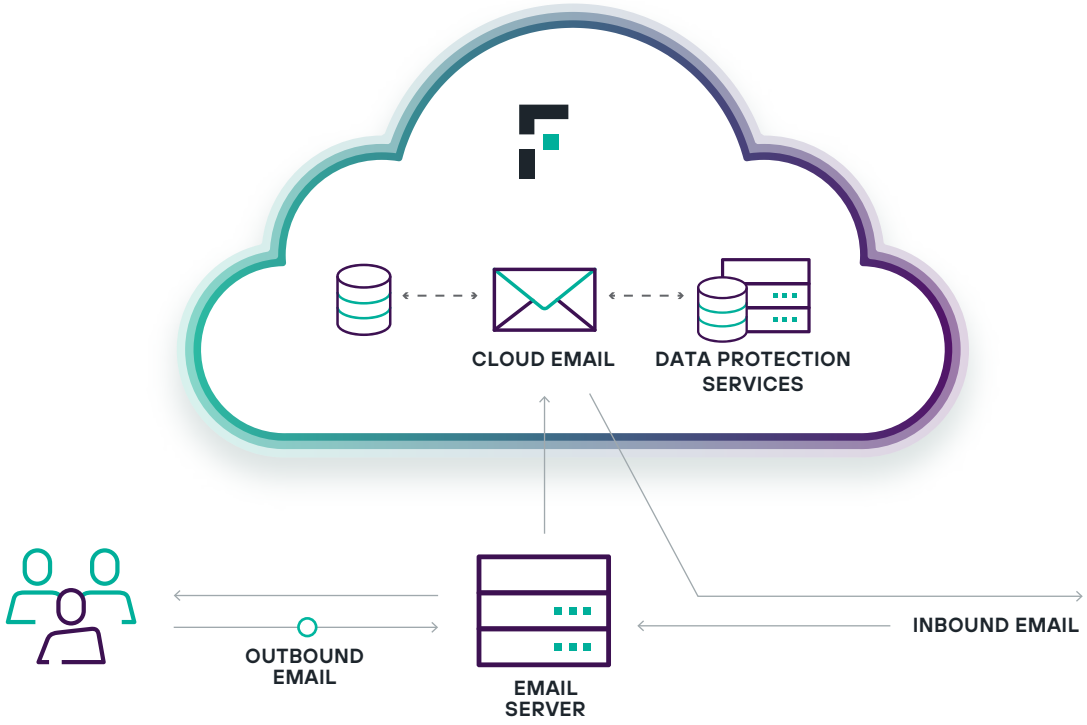
Forcepoint simplifies deployment of DLP for Cloud Email by working inline with your existing email security vendor to scan outbound emails. Utilizing DLP for Cloud Email Universal connectors, Forcepoint integrates popular third-party vendor products such as Google and Microsoft to forward all or selected outbound emails to the Forcepoint Cloud. There, Forcepoint DLP scans according to the DLP policies and actions according to your pre-defined DLP plan. Emails can be permitted, quarantined, or encrypted (with the separate encryption module) before sending. Notifications are sent on quarantined email, which can be configured to be retained for up to 30 days unless released by an authorized administrator. In order to maintain the reputation of an organization, all outbound emails are also scanned for spam, viruses, and malware.

Standard features:

- → **Simple policy interface** providing protection across virus, malware, and spam
- → **Dashboards, logs, and presentation reports**
- → **Personal email subscription**

Add-ons:

- → **Forcepoint Cloud Email Extended Reporting History** (options for 6, 12, and 18 months)
- → **Forcepoint Email Security Encryption Module**
- → **Forcepoint Email Security Image Analysis Module**



forcepoint.com/contact