Forcepoint

Email Security Cloud

Evaluation Guide

Contents

Overview

Thank you for choosing to evaluate Forcepoint Email Security Cloud.

Forcepoint Email Security Cloud provides leading protection from today's multi- channel email and web threats. The cloud protection service reduces costs and complexity while allowing businesses to retain control and eliminate uncertainty through industry-leading service level agreements.

This guide is designed to help you through your Forcepoint Email Security Cloud evaluation. It demonstrates the ease with which you can manage and analyze inbound and outbound email traffic according to the varying requirements of users and teams within your organization.

Why Forcepoint Email Security Cloud?

Today, email protection is significantly different than it was only a short time ago. Malicious threats used to be concealed primarily in attachments, but today Forcepoint Security Labs reports that 85% of unwanted email messages contain a link to a potentially malicious website. Securing email users against converged web and email threats requires email protection that is integrated with the best-in-class expertise that Forcepoint offers.

Forcepoint Email Security Cloud stops spam, virus, phishing, and other malware attacks before they reach your network, dramatically reducing email bandwidth and storage requirements. Because there is no hardware or software, business costs associated with installation, troubleshooting, and applying patches and upgrades are eliminated.

Forcepoint ThreatSeeker Intelligence continuously monitors worldwide email content for emerging threats, analyzing millions of requests a day, capturing millions of unsolicited spam, phishing, and exploit campaigns. ThreatSeeker feeds this intelligence to Forcepoint email, web, and data protection solutions, and to Forcepoint security analysts who apply the intelligence to quickly adapt Forcepoint solutions to manage the rapidly changing threat environment.

Forcepoint Email Security Cloud:

- Stops targeted attacks and the early stages of advanced persistent threats.
- Secures sensitive data against theft from external attacks and insider threats.
- Safely supports cloud technologies such as Microsoft Office 365.
- Identifies high-risk user behavior and educates users to improve threat awareness.
- Easily deploys with Forcepoint Web Security Cloud for complete, effective content security.

Forcepoint Email Security Cloud is backed by a 99% spam detection SLA and has received premium antispam certification from West Coast Labs (an independent testing facility) for stopping 99% of spam with zero false positives.

Content filtering provides granular content analysis on inbound and outbound email. It includes comprehensive and configurable lexical dictionaries and polices to help organizations comply with regulations such as HIPAA, SOX, and global privacy standards.

Encryption secures email communications among business partners and individuals to ensure that their email content is safe and private. With nothing required on-premises or at the endpoint, cloud encryption is a simple and cost-effective alternative to client- based encryption solutions, which can be difficult to deploy and maintain.

Summary and detailed reports, combined with the dashboard feature, show key email indicators and provide forensic details on the real-time email security protection provided by Forcepoint. Administrators can delegate and schedule reporting access to any department within the organization to enable appropriate managers to receive reports automatically by email.

Forcepoint has multiple global data centers, and the cloud service has been certified to ISO27001 standards to provide the highest degree of global and localized security, privacy, and confidentiality. All email is routed to 2 data centers in different geographical regions to provide redundancy and fault tolerance. The service is backed by a 99.999% uptime SLA and includes email spooling and disaster recovery provisions as standard. Built-in redundancy, failover, and business continuity ensure that email always stays up and running, even if the network is temporarily unavailable.

Methodology

This guide is designed to help you evaluate Forcepoint Email Security Cloud after you've performed the initial setup. For setup instructions, see Forcepoint Email Security Cloud Getting Started Guide.

This guide demonstrates how an IT administrator can easily configure, monitor, and analyze inbound and outbound mail delivery while taking into account the varying requirements of specific users and departments within an organization.

The guide is organized into the task areas most beneficial to the IT administrator:

- **Dashboard** – View up-to-date graphical data for email volumes, inbound email composition, and spam detection rates.
- **Directory synchronization** – Simplify user management and prevent directory harvest attacks by synchronizing Active Directory or Lotus Domino data with Forcepoint Email Security Cloud.
- **Policies and fine-tuning** – Create policies for users to enable them to use email as a productive business tool, while restricting unwanted or undesirable messages or those that pose security risks.
- **Reporting** – Examine trends and statistics for messages passing through Forcepoint Email Security Cloud.
- **Message Center** – Review quarantined messages and choose whether to deliver, forward, or discard them.
- **After Setup** – Administer the service after the initial configuration, and enable end users to manage their email.
- **Integration with Forcepoint Web Security Cloud** – The advantages of an integrated email and web protection solution.

For detailed information on any aspect of Forcepoint Email Security Cloud, refer to Forcepoint Cloud Security Gateway Portal Help. You can click the **Help** menu in the cloud portal to access this guide at any time.

Dashboard

The dashboard provides a snapshot view of how Forcepoint Email Security Cloud is performing. To view your dashboard, click **Dashboard** on the portal's main menu bar.

Note the following significant features:

- The **Email activity overview** displays the number of inbound and outbound email requests processed for your account in the last 7 days.
- **Inbound Composition Categories** and **Outbound Composition Categories** - reports how Forcepoint Email Security Cloud categorized your inbound and outbound email. Composition categories include:

Spam	Messages marked as spam by the Antispam rules.
Valid	Messages that pass analysis or that are allowed.
Content	Messages that triggered a Content Filter rule.
Viruses	Messages detected by Antivirus or ThreatSeeker as containing a virus.
Phishing	Messages maliciously designed to acquire information, such as user names, passwords, or credit card information by masquerading as a trusted or well-known entity.
Commercial Bulk	Solicited bulk email, such as newsletters
Backscatter	Maliciously generated bounce messages (e.g., non-delivery report/ receipt (NDR); delivery status notification (DSN); and non- delivery notification (NDN) messages) sent by spammers to spoofed return addresses
Access	Messages to which Notifications and Annotations rules were applied.
Other	Messages flagged for other reasons, such as having a message loop, encryption, or generating a system or operational error.

- **Top 5 viruses** indicates the top 5 viruses seen in your account along with the number of emails carrying each of these viruses.
- **URL categories in email** reveals how Forcepoint Email Security Cloud classified all of the URLs found in your organization's email.
- **Cloud email spam detection rate** indicates, from an email flow of known spam messages (separate from all subscriber email flow), the percentage of messages classified as spam by Forcepoint Email Security Cloud analysis.

You have the option of viewing this data in either a bar graph or pie chart.

Directory Synchronization

Organizations that use Microsoft Active Directory, Lotus Domino, and other LDAP services can synchronize primary and secondary email addresses and groups into the portal. This has the following advantages:

- Administrators can manage email address and group details from the Active Directory instead of from the cloud service portal, greatly reducing the time spent maintaining service configuration.
- Scheduled synchronization means new employees in a company can be added to the cloud service automatically; likewise, those leaving can be removed from the service automatically.
- Improves spam detection by quarantining email sent to unknown users.
- Helps to prevent directory harvest attacks, by checking the validity of email addresses and domains when a server is trying to send large numbers of messages for the purposes of directory harvesting.

For full instructions on setting up and using directory synchronization, see **Forcepoint Cloud Security Gateway Portal Help** and the **Directory Synchronization Client Administrator's Guide**, both available at the Forcepoint Support site.

Policy Setup

The default policy provided with Forcepoint Email Security Cloud allows most organizations to get up and running quickly and easily with minimal configuration.

The administrator can modify or create new policies as necessary to manage email traffic to comply with business needs, goals and objectives of the organization.

Policies encompass several elements, including:

- Rules for spam and virus protection
- Phrases and lexical rules for content filtering
- Notifications of quarantined email

Policy decisions and levels of control may be different for different user groups, but in all cases should be constructed to allow users to effectively use email as a business tool while protecting the company from spam, objectionable or illegal content, and viruses.

A default policy is provided with Forcepoint Email Security Cloud, and administrators can also create custom policies to support mail aliases or domains that require differing configurations.

To access the current policies in your account and to create new policies, click **Email** in the portal's main menu bar, then click **Policies**.

Click a policy name to view and edit the policy settings. Note that each policy has multiple tabs to configure.

Setting up antispam rules

It is estimated that 90–95% of all email is spam. Forcepoint Email Security Cloud provides market leading antispam protection through a combination of techniques powered by ThreatSeeker Intelligence. The Forcepoint approach is unique in that we integrate our web intelligence into our email protection engine, which enables the service to detect blended threat attacks in real-time. ThreatSeeker Intelligence technologies include a Forcepoint reputation service, integrated Forcepoint URL database, heuristics, fingerprinting, auto-learning technologies, and more.

The email protection engine uses a combination of techniques to analyze each email message and assign the message a "spam score." This spam score is used to determine the likelihood of the message being spam. The result of the various spam tests may be a positive score (to indicate spam) or a negative score (to indicate valid email). Message scoring above the "spam threshold" defined by the customer are classified as spam. The results of all tests are taken into account, and this helps to improve accuracy.

To view and edit the current antispam rules for a policy, click the **Antispam** tab.

You can define what happens to spam depending on the score it receives. For example, you might want to create a rule that forces all email with a spam score greater than 6.0 to be forwarded to an administrator, all email with a score greater than 7.0 to be quarantined, and all email with a score over 10.0 to be discarded.

Lower values detect more spam at the risk of false positives - email wrongly detected as spam. Higher values reduce the risk of false positives but could miss some spam. Forcepoint Email Security Cloud aims to ensure that no false positives occur with spam scores over 6.0. This is the recommended default setting for quarantining email.

Content Analysis

Forcepoint Email Security Cloud can perform the following granular content analysis on both inbound and outbound email messages:

- **Executables** – Messages containing scripts and executables can be quarantined. This feature can be set up on a per-user basis within a policy.

- **Attachments** – Attachments can be quarantined by file. This feature can be controlled by including or excluding specific file types. You can also mask attachments; this changes the file to prevent automatic execution.

- **Parking** – Attachments can be parked in the cloud service infrastructure and the original email sent on to the recipient with a URL that locates the attachment for subsequent download if needed. This enables you to minimize the use of Internet bandwidth.

- **Lexical Analysis** – The lexical rules feature scans for words and phrases against both pre-defined and custom dictionaries using Boolean operators and custom weighting and thresholds. This enables you to scan email for profanity and other undesirable content entering your organization. You can also check outbound messages for phrases that might include company confidential information, or could cause embarrassment, loss of reputation, or business.

Editing Content Filtering rules

To view and edit the current content filtering rules for a policy, click the **Content Filter** tab.
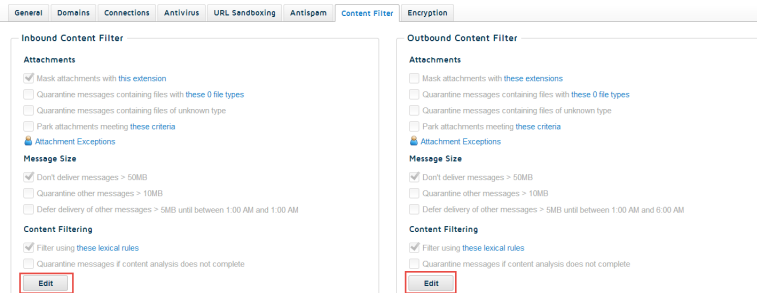
For example, if an administrator wants to set up an inbound content filter that masks attachments with an XLS file extension:

Steps

1) Under Inbound Content Filter, mark the box labeled **Mask attachments with these extensions**.

2) Click the '**these extensions**' link.

3) Click **Add**.

4) In the **File Extension** field, type XLS.

5) In the **Description** field, optionally type a suitable description of the file extension.

Add to Inbound Attachment Masking

File Extension	XLS	*Omit leading punctuation (DOC, JPG, PPT)*
Description	Microsoft Excel spreadsheets	

6) Click **Submit**.

Encryption

The Forcepoint Email Security - Encryption Module secures delivery of email by ensuring that it is not forwarded as plain text 'in the clear.' The Encryption Module encrypts the transport layer protocols being used to deliver the email at the edge of the network - the point where it leaves the secure environment of the local area network. This enables administrators to configure secure email communications among business partners and individuals, using either a transport layer encrypted 'tunnel' between specified email servers or mail transfer agents, ad hoc encryption for mail transfer agents that do not support TLS, or advanced identity-based encryption available with the Encryption Module.

To view and configure encryption settings for a policy, select the **Encryption** tab. See Forcepoint Email Security Cloud Help for details.

Reporting

Forcepoint Email Security Cloud provides exceptional reporting functionality that provides a 360 degree view of email traffic and usage. Administrators can view summary reports and drill down for detailed forensics. Reports can be scheduled to run automatically and be emailed to a designated manager.

The email Report Center includes Report Catalog with a number of predefined reports covering common scenarios, and a Report Builder tool that can be used to create flexible, multi-level reports that allow you to analyze information from different perspectives and gain insight into your organization's email message trends. If a high-level summary shows areas of potential concern, you can drill down to find more detail.

A set of legacy email reports is also available, providing common email metrics. To access the reporting features, click **Reporting** in the portal main navigation panel, and select an item from the Report Center or Legacy Email Reports menus.
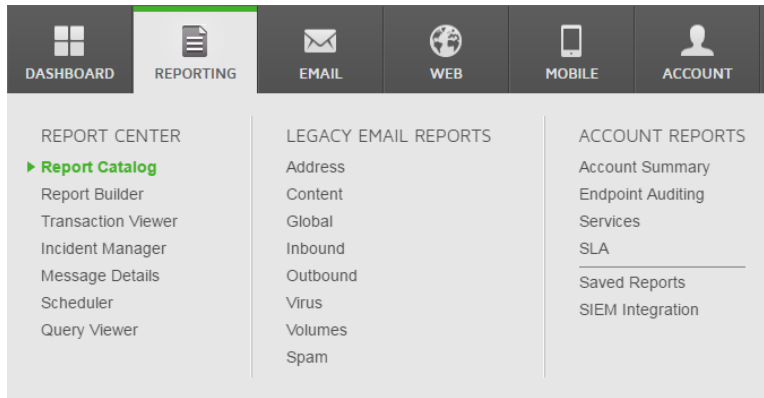
After opening a standard report in the Report Catalog, you can customize it using Report Builder, dragging additional attributes and metrics into the report in order to find the information you need. The Message Details option is used to view the details of individual email transactions

Message Center

The Forcepoint Email Security Cloud Message Center is a powerful message tracking and management tool that provides access to all quarantined messages and message logs for your account.

To access the Message Center, click **Email** on the portal's main menu bar, then select **Messages** > **Message Center**. You are presented with a search form.

Numerous options are available to help you narrow your results and reduce search time. This is especially important for large accounts. It is easy to quickly determine whether a message was blocked or delivered by simultaneously searching the quarantine and accepted message logs.

Administrators can perform actions on the messages found by the search, for example releasing, forwarding, or deleting one or more messages.

Following Setup

Once the administrator has set up users and customized polices to meet the needs of an organization, there is little ongoing maintenance or configuration required with Forcepoint Email Security Cloud. However, it is good practice to periodically use the dashboard and run reports to review and report on the ongoing email security protection provided by the service.

Administrators can schedule non-graphical versions of account summary reports to be sent to an email address on a daily, weekly, biweekly, or monthly basis.

End user quarantined message management

The Forcepoint Email Security Cloud service allows end users to manage their own quarantined spam by providing a personal message report. End users can request these reports independently or administrators can initiate them on the Personal Email Subscriptions page. Administrators can also enable end users to populate individual white lists and black lists. This functionality is very easy to roll out to employees with little administrative overhead. It is documented in **Forcepoint Email Security Cloud Getting Started Guide** and **Forcepoint Email Security Cloud End User Guide**, both available in the [Forcepoint Support site](#).

Integration with Forcepoint Web Security Cloud

The close integration of Forcepoint Email Security Cloud and Forcepoint Web Security Cloud enables organizations to secure and optimize their email traffic, while doing the same for web traffic. Customers gain complete web and email protection with the benefits of integrated management, reporting, and the value of a consolidated security strategy with the following benefits:

- Blocks web and email threats before they reach your network, improving network efficiency and saving business costs.
- Approximately 85% of email contains a link to a website. Real-time ThreatSeeker Intelligence used by Forcepoint Web Security Cloud protects end users from the risks of accessing inappropriate and malicious content, including spyware, phishing, botnets, and other threats, via both Internet browsing and email.
- Email and web protection can be configured through a single portal, requiring the administrator to manage only one set of users and groups and monitor usage through a single dashboard.

Summary

This guide has highlighted the most important aspects of administering Forcepoint Email Security Cloud, and demonstrated the following benefits:

- Threats are blocked before they reach your network, as shown by the statistics on the dashboard. This means reduced bandwidth, storage, and maintenance costs for your organization.
- Default policies enable immediate and effective email protection with little administrative time required. Policies can be customized to meet the precise needs of your users while ensuring complete and effective email protection.
- The Message Center and reporting functions enable you to track every aspect of email usage, protection, and management.
- Integration with Forcepoint Web Security Cloud provides a complete protection solution with centralized policies and reporting.

Thank you for evaluating Forcepoint Email Security Cloud.