Proofpoint Email Protection helps you secure and control inbound and outbound email through an easy-to-use cloud-based solution. With Email Protection, you can protect your people, data, and brand from today’s threats and common nuisances such as:

- Impostor email
- Phishing
- Malware
- Spam
- Bulk mail

**Threat Prevention**

Effective threat protection starts with accurate detection. Email Protection uses multiple layers of technology to accurately detect threats, including malicious content and malware.

**Multilayered Content Analysis**

Email Protection uses several techniques to protect against both known and emerging threats. Signature-based detection prevents known threats while dynamic reputation analysis continually assesses local and global IP addresses to determine whether to accept, reject or throttle email connections. Together, these features help protect you at the first signs of malicious activity.

**Protection from malware-free threats**

Email Protection detects threats that don’t involve malware, such as credential phishing and impostor email. It assesses the reputation of the sender by analyzing hundreds of thousands of email attributes, including the sender/recipient relationship, headers, and content. Impostor email—also known as business email compromise or CEO fraud—is a fast-growing threat that can cause huge losses.

**Control**

**Accurate Email Classification and Quarantine**

Protect against email threats and other unwanted messages in just about any language with multilingual analysis. Email classifiers divide incoming email into separate quarantines by type. This feature gives you granular control over a wide range of email, including:

- Spam
- Phishing
- Impostor email
- Malware
- Bulk email
- Adult content

**Graymail Management**

Reduce the amount of inbox clutter and give users personal control over bulk email. Big data analysis techniques accurately identify graymail and deliver it to a separate low-priority inbox. Users can then “promote” wanted email to their regular inbox or “demote” unwanted email to their quarantine.
Policy Creation
Email Protection supports the demands of the largest enterprises in the world. Our policy engine gives you complete flexibility with custom rules at the global, group and user level. With our deep content inspection, you can easily enforce your unique acceptable-use policies.

Email Continuity
If you’re moving to cloud-based inbox platforms such as Microsoft Office 365, service outages can be a concern. Email continuity lets you continue to send and receive email when mail servers are unavailable; this always-on capability that means important messages get through—and your business keeps running. When email service is restored, all sent and received emails can be synced back to the server.

VISIBILITY
Message Tracing
Email Protection gives you a wealth of data and search tools. Our advanced message tracing features a high-performance search engine to help you quickly pinpoint hard-to-find log data based on dozens of search criteria.

Reporting
Get more than 60 real-time reports for detailed visibility into mail flow and trends. This data can help you proactively address issues and trends as they emerge.

End User Controls
Give your people self-service control over their email preferences such as:
• Quarantines
• Safe and block lists
• Bulk mail delivery
You can even allow users to opt in or out of various spam policies. All end-user services are easy to brand allowing providing familiarity for end-users who access these tools. And with support for numerous languages, you can deploy them globally.