

Proofpoint Protection Server



The Proofpoint Protection Server® is the industry's most powerful and complete software solution for enterprise messaging security. The Proofpoint Protection Server defends organizations against all types of inbound messaging threats and outbound content security risks at the enterprise gateway.

Secure. Effective. Easy to deploy.

Those are just a few of the ways to describe the Proofpoint Protection Server software. It's the industry's most powerful messaging security solution that offers:

- Unbeatable spam detection
- World-class virus and outbreak protection
- Comprehensive content security
- Policy-based message encryption
- Impenetrable email firewall
- Enterprise-grade performance
- Easy customization
- Flexible extensibility
- Optimal scalability architecture
- Futureproof technology

features

- Secures your network against spam, known viruses, emerging virus outbreaks, connection-level attacks, and hackers—right at the gateway.
- Proofpoint MLX™ machine learning technology provides unrivalled anti-spam effectiveness and content filtering accuracy.
- Protects your enterprise from liability created by incompliant or offensive emails.
- Protects the privacy and security of customer and employee data.
- Protects valuable intellectual property and trade secrets.
- Supports encrypted email via the optional Proofpoint Secure Messaging™ module or popular third-party secure messaging systems.
- Easily scales to filter millions of messages per day and unlimited numbers of end users.
- Proofpoint's extensible platform provides a flexible interface for developing custom messaging applications and integrating with external systems.
- Comprehensive end-user controls and group policy support meet the unique needs of every end user.
- Automatic updates and centralized administration keep total cost of ownership low.
- Integrates with enterprise identity management systems such as Active Directory, Domino Directory, and other LDAP sources.
- Intelligent perimeter security features such as MLX Dynamic Reputation™ and SMTP rate control protect against malicious connections including Denial-of-Service and Directory Harvest Attacks.
- A true “zero administration” solution with automatic updates, unified policy management, and robust reporting features.

The powerful features of the Proofpoint Protection Server are also available in a hardened and easy-to-deploy appliance—the Proofpoint Messaging Security Gateway™—with additional security features.

“For Pitney Bowes, Proofpoint is ‘set it and forget it’ technology. With the Proofpoint Protection Server, we no longer worry about spam and we had only minor configuration modifications.”

John Congiu
Manager of Enterprise Messaging
Pitney Bowes

Proofpoint Protection Server

Proofpoint MLX Technology

Advanced message security

The power behind Proofpoint's enterprise messaging security solutions—Proofpoint MLX—is an advanced, patent-pending, machine learning system developed by the scientists at the Proofpoint Attack Response Center. Based on advanced statistical techniques that include logistic regression and information gain analysis, Proofpoint MLX enables the accurate classification and identification of unstructured content, such as the contents of email messages and valuable company documents.

Unparalleled accuracy

Proofpoint MLX is the basis for the unrivalled anti-spam accuracy delivered by the Proofpoint Protection Server software. Using MLX, the Proofpoint Spam Detection module analyzes more than 200,000 structural and content attributes to accurately differentiate between spam and valid messages. Traditional anti-spam solutions evaluate only a limited number of attributes and are unable to decisively classify spam, leading to low effectiveness and a high rate of false positives. MLX is far superior to simple statistical techniques such as Bayesian filters—and it doesn't rely on signatures or fingerprinting techniques, which are easily fooled by spammers.

The highly confident spam scoring provided by Proofpoint MLX lets you take decisive action against spam messages—deleting them before they clog your internal mail servers and vastly reducing the number of “possible spam” messages that need to be quarantined.

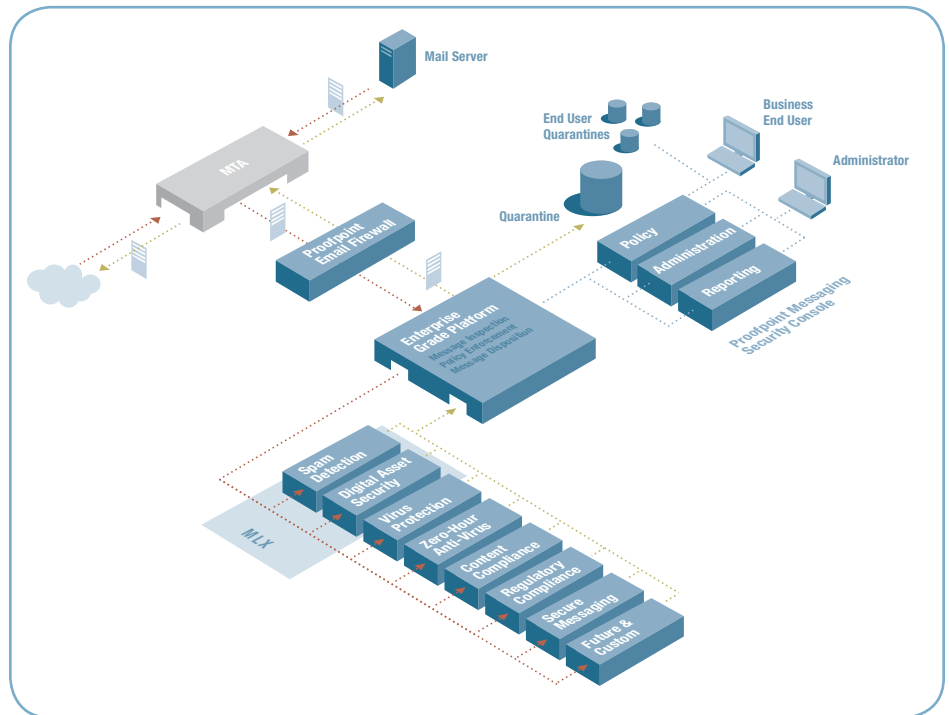
Futureproof intelligence

Proofpoint's intelligent anti-spam technology is continually being trained by Proofpoint scientists to defend against new forms of spam. This training allows MLX to predict and adapt to new forms of spam as they appear. Unlike other anti-spam solutions, Proofpoint's ability to defend against spam attacks does not degrade over time—and updates to the MLX Anti-Spam Engine™ are automatically delivered to your Proofpoint servers on a regular basis. Proofpoint MLX is constantly evolving to counter emerging threats, ensuring that your messaging infrastructure is secure against tomorrow's spammers as well as today's.

complete protection

All-in-one messaging security

Why purchase yet another point solution? Proofpoint's messaging security platform provides comprehensive defense against both inbound threats and outbound content security risks—and Proofpoint's modular architecture lets you easily deploy new defenses as your needs change.



Spam Detection

Powered by patent-pending Proofpoint MLX machine learning technology, the Proofpoint Spam Detection™ module examines more than 200,000 structural and content attributes in every email to block the most spam and phishing attacks, automatically adapting to new attacks as they appear. And the Proofpoint Dynamic Update Service™ automatically keeps your spam protection up to date, ensuring maximum effectiveness at all times. Individually controllable spam and adult content scores allow you to enforce zero-tolerance policies against pornographic spam. Anti-phishing features stop the spread of phish and other identity-theft attacks from stealing personal information from employees.

Proofpoint Spam Detection is multi-lingual and offers outstanding accuracy against spam in any language—including hard-to-analyze, multi-byte character languages such as Japanese and Chinese. And Proofpoint Spam Detection can be uniquely customized to the environment and lexicon of each organization.

Virus Protection & Zero-Hour Anti-Virus Defenses

Through strategic partnerships with leading anti-virus vendors, Proofpoint Virus Protection™ provides complete virus scanning functionality. Virus engines are deeply integrated with Proofpoint's platform, providing convenient, centralized administration of anti-virus policies from the same interface used to manage spam and content policies. Messages are efficiently scanned for viruses in parallel with spam and message content, protecting end users from viruses, worms, and other malicious code. Additionally, the Proofpoint Zero-Hour Anti-Virus™ module protects against emerging viruses in the earliest stages of their proliferation on the internet—hours before competing solutions even begin to react.

Content Compliance

Proofpoint Content Compliance™ makes it easy to define and enforce corporate acceptable-use policies for message content and attachments. A convenient point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content. Proofpoint's content compliance features can be used to identify and prevent a wide variety of inbound and outbound policy violations—including offensive language, harassment, file sharing, and violations of external regulations. Noncompliant messages can be acted on with a wide variety of options, including quarantine, reroute, reject, annotate, and other actions.

Digital Asset Security

As email has become the most important communications channel in today's enterprise, email systems have become the main repository for sensitive, confidential, and mission-critical information. The Proofpoint Digital Asset Security™ module keeps valuable corporate assets and confidential information from leaking outside your organization via email. Powerful MLX machine learning technology analyzes and classifies your confidential documents and then continuously monitors for that information in the outbound message stream—stopping content security breaches before they happen.

Regulatory Compliance: Keeping private data private

More than ever, enterprises need to protect the privacy and security of customer and employee data. The Proofpoint Regulatory Compliance™ module helps enforce best practices for securing private data and protects your organization from liabilities associated with privacy and data security regulations (such as HIPAA, GLBA and others). Predefined rules and “smart identifiers” automatically scan for non-public information, such as protected health information and personal financial information, and act on noncompliant communications, rejecting or encrypting messages as appropriate. Proofpoint's Dynamic Update Service ensures that your compliance dictionaries and rules are always up to date.

Secure Messaging

The Proofpoint Secure Messaging™ module adds powerful, content-aware encryption capabilities to your Proofpoint deployment, automatically encrypting messages based on your organization's policies. Proofpoint Protection Server is also compatible with a wide variety of leading third-party secure messaging solutions.

unparalleled security

Proofpoint Email Firewall for complete perimeter security

The integrated Proofpoint Email Firewall™ provides the SMTP-level, perimeter security features demanded by today's enterprise, creating an impenetrable shield around your messaging systems. Proofpoint's MLX Dynamic Reputation technology and SMTP rate control features work together to protect your network from all types of malicious connections.

MLX Dynamic Reputation and SMTP rate control

Proofpoint MLX Dynamic Reputation technology constantly monitors SMTP connections at the IP address level, looking for suspect or malicious activity. Proofpoint monitors the number of connections, type of activity, recipient validity and content of messages coming from each IP address. Proofpoint MLX machine learning techniques are used to analyze network activity in real time and assess the risk associated with each connection.

Based on this analysis, the Proofpoint Protection Server takes automatic, corrective action using SMTP rate control. Malicious connections are automatically blocked or throttled based on fully customizable mail traffic policies.

The Proofpoint Email Firewall provides impenetrable defense against a wide variety of network-level attacks, including Denial-of-service, Dictionary, and Directory Harvest Attacks, keeping your network and email users safe while preserving network bandwidth. Only Proofpoint offers this dynamic, real-time, and self-tuning perimeter security solution.

MLX and content security

Proofpoint MLX technology also powers the advanced content security features of the Proofpoint Digital Asset Security module and the intelligent perimeter security features of the Proofpoint Email Firewall and MLX Dynamic Reputation service.

Ongoing advances

Proofpoint is the only vendor to apply these powerful machine learning techniques to messaging security. Scientists at the Proofpoint Attack Response Center continue to conduct primary research into new, advanced statistical techniques and to develop new defenses based on MLX. This ongoing research and development ensures that Proofpoint's solutions are always one step ahead of threats to the security of your messaging infrastructure.

Protection Beyond SMTP Email

Proofpoint Network Content Sentry™

Proofpoint's advanced content security features can optionally be extended to protect additional message streams including web-based email, blog postings, message board postings and other HTTP- or FTP-based activity.

The Proofpoint Network Content Sentry is a separate appliance that inspects all outbound network traffic in real-time, monitoring for confidential information, private customer or employee data (including private healthcare, financial or identity information) and other sensitive content that may leak outside the enterprise. When such breaches are detected, the Proofpoint Network Content Sentry actively alerts managers (such as compliance officers) so appropriate actions can be taken.

Proofpoint Protection Server

engineered for enterprises

The Proofpoint Protection Server was designed to meet the unique needs of large enterprises, universities, and government organizations. It offers all of the flexibility, scalability, customization, and end-user control features needed in large-scale deployments.

The Proofpoint Protection Server stops threats at the front door of your enterprise and delivers the lowest total cost of ownership by easily integrating with any IT infrastructure, no matter how distributed. A GUI-based LDAP command console and Microsoft Active Directory® support make directory server integration easy. Proofpoint Protection Server is also compatible with and minimizes the burden on overtaxed email server solutions such as Microsoft Exchange® and Lotus Notes®. Moreover, no desktop software or agents are required, minimizing the time and resources required for installation and ongoing support.

Flexible deployment, optimal scalability

Proofpoint Protection Server scales indefinitely to support many millions of messages per day. Proofpoint servers can be easily deployed in industry-standard cluster configurations to support complex or geographically distributed data centers—offering the security of 100% redundancy combined with the convenience of a single administrative interface. Proofpoint's optimal scalability architecture lets you manage all agent servers from a single master console. Automatic configuration propagation, a centralized message quarantine, and centralized reporting simplify maintenance and reduce total cost of ownership.

Centralized administration, complete end-user control

The Proofpoint Messaging Security Console™ provides a centralized, 100% web-based administration interface to Proofpoint's unified policy management framework, ensuring consistent application of corporate messaging policies. The Console makes it easy to monitor and control your global messaging infrastructure and define messaging policies. As optional Proofpoint modules (such as Digital Asset Security) are added to your deployment, the same convenient interface is used for policy management.

The Console also provides access to more than 45 real-time, graphical reports and alerts that give complete visibility into the state of your enterprise messaging system. Reports can be easily emailed or posted as HTML/XML. Proofpoint's "active" reports deliver key information but also allow administrators to take immediate action (for example, simply click a link to block an abusive sender).

Easy-to-understand end-user reports and controls—such as Proofpoint's end-user digest, personalized quarantine, and personalized safe- and block-lists—give each user complete control over their own spam preferences. Delegation mode allows one user (such as an executive admin) to manage another user's quarantine. The look and feel of these controls is completely customizable for your organization.

Proofpoint Protection Server also makes it easy to define and enforce different policies for different groups of end users. This feature is useful for deployments where different groups of users require different strengths of spam blocking, such as groups that need spam tagged and forwarded rather than quarantined. Administrators can optionally allow end users to choose from a set of group preferences. Full integration with LDAP and Active Directory greatly simplifies and streamlines ongoing group maintenance.

Always up-to-date protection with zero administration

With automatic installation and notification of updated components, Proofpoint provides a true "zero administration" solution. The Proofpoint Dynamic Update Service ensures that your network always has the highest level of protection from message-borne threats. It provides continuous updates for every component of the Proofpoint Protection Server, including spam and virus engines, lexicons (such as the dictionaries used by the Proofpoint Regulatory Compliance module), application components, and customized hot fixes.

System requirements

The Proofpoint Protection Server is compatible with any email server. The software is available for both Sun and Linux hardware platforms and administration, configuration, and reporting is handled through a 100% browser-based interface.

Sun platforms

Solaris™ 8

Solaris™ 9

Linux platforms

Red Hat Enterprise Linux ES 3.0 or 4.0

Red Hat Enterprise Linux AS 4.0

Browsers

Microsoft® Internet Explorer 6.0 or higher

Mozilla Firefox 1.2 or higher

Netscape® 7.0 or higher

© 2006 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint MLX, MLX Dynamic Reputation, MLX Anti-Spam Engine, Proofpoint Dynamic Update Service, and Proofpoint Messaging Security Console are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 3/06