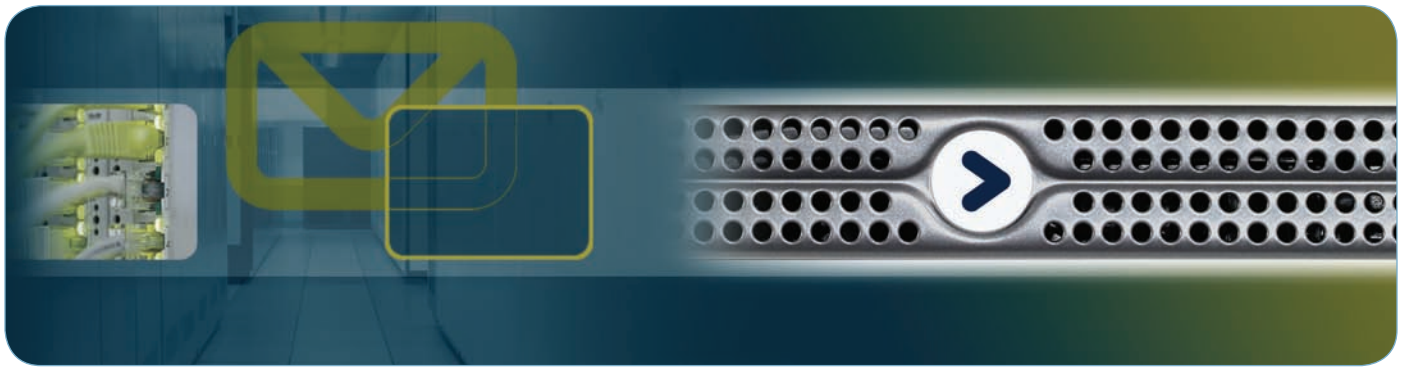
Proofpoint Messaging Security Gateway Appliances

Proofpoint on Demand Hosted Service and Proofpoint Protection Server Software



The Proofpoint Messaging Security Gateway™ appliances, Proofpoint on Demand™ service and Proofpoint Protection Server® software defend against inbound messaging threats, prevent leaks of sensitive information, encrypt messages and analyze your messaging infrastructure. Their unified architecture, modular defenses and policy management interface protect organizations against all types of messaging risks—right at the enterprise gateway.

defend, prevent, encrypt, analyze

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

All Proofpoint features—including anti-spam, anti-virus, multi-protocol content security, policy-based encryption and reporting features—are managed centrally from a single administrative GUI and deployed on a unified appliance architecture. Features can be deployed in nearly any configuration, to meet your organization's unique requirements.

Whether your deployment involves a single Proofpoint server or multiple, globally distributed appliances, all policy management and administration tasks are controlled via Proofpoint's centralized, web-based administration console.

flexible deployment options

Proofpoint's email security and data loss prevention solutions are offered in a variety of form factors for maximum deployment f exibility:

- **Hosted service:** Proofpoint on Demand delivers Proofpoint's email security and data loss prevention features in a cost-effective, highly customizable, on-demand service that doesn't require on-premises hardware or software.
- **Hardware appliance:** The Proofpoint Messaging Security Gateway is a hardened, secure, easy-to-deploy appliance that installs in minutes. A variety of appliance models are available to support enterprises of any size.
- **Virtual appliance:** The Proofpoint Messaging Security Gateway—Virtual Edition delivers the same best-in-class protection as Proofpoint's hardware appliances, combined with the many benefits of virtualization—including cost savings, rapid deployment and provisioning, simplified change management and easy backup and disaster recovery. The virtual appliance runs on any standard x86 desktop or server using VMware Server or VMware Infrastructure.
- **Software:** The Proofpoint Protection Server delivers Proofpoint's messaging security platform as software for the Red Hat Enterprise Linux operating system.

Secure. Effective. Easy to Deploy.

These are just a few of the ways to describe Proofpoint's unified email security and data loss prevention platform. It's the industry's most powerful solution—packaged as an enterprise-ready appliance, virtual appliance or software that offers:

- Unbeatable spam detection and connection management
- World-class virus and outbreak protection
- Comprehensive, multi-protocol data loss prevention and content security
- Policy-based email encryption
- Advanced reporting and analysis
- Unified policy management
- Enterprise-grade performance
- Rapid deployment and provisioning
- Optimal scalability architecture

"Pacific Sunwear evaluated quite a number of anti-spam, anti-virus and content scanning products, and Proofpoint was the first company to deliver a platform that resolves all our email and messaging challenges in a single, easy to deploy and easy to manage solution. The Messaging Security Gateway appliance has restored our email channel to its rightful place as a strategic conduit for business communications, rather than a revolving door for message-borne threats."

Ron Ehlers
VP of Information Systems
Pacific Sunwear

Proofpoint Messaging Security Gateway and Proofpoint Protection Server

Proofpoint MLX Technology

Advanced machine learning

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 including logistic regression and information gain analysis, Proofpoint MLX enables the accurate classification and identification of unstructured content, as found in email and other documents.

Unparalleled accuracy

Proofpoint MLX is the basis for the unrivalled anti-spam accuracy delivered by the Proofpoint Spam Detection module. Using MLX, Proofpoint analyzes hundreds of thousands of structural, image, content and reputation 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.

Futureproof intelligence

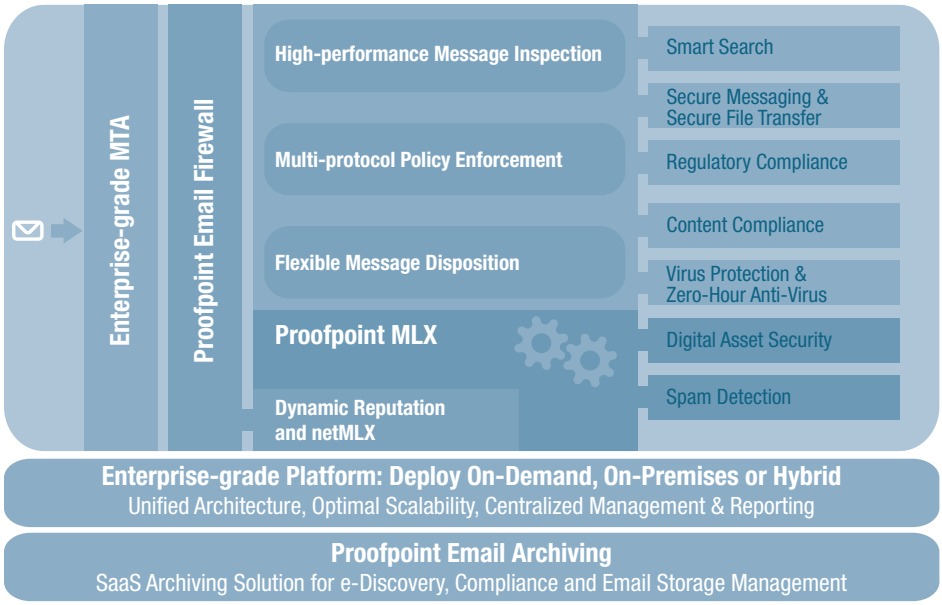
Proofpoint's anti-spam technology continually updates itself to defend against new forms of spam. Ongoing self-training and new techniques developed by Proofpoint scientists allow MLX to predict and adapt to new forms of spam as they appear. MLX updates are automatically delivered to all customers several times per day.

As a result, Proofpoint MLX offers 99.8% or higher effectiveness, even against difficult forms of spam including image, PDF, attachment, "backscatter" and foreign language spam.

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 enterprise 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.

Proofpoint MLX 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 Dynamic Reputation service. Proofpoint is the only vendor to apply these powerful machine learning techniques to email security and data loss prevention.

complete protection



defend against inbound threats

Advanced Spam Detection, Powered by Proofpoint MLX™

Powered by patent-pending Proofpoint MLX machine learning technology, the **Proofpoint Spam Detection**™ module examines hundreds of thousands of attributes in every email—including message envelope headers and structure, images, sender reputation as well as unstructured content in the message body—to block spam, image-based spam and phishing attacks, while automatically adapting to new attacks as they appear. 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 prevent the theft of personal information from employees. Bounce management features including Bounce Address Tag Validation (BATV) specification support block 100% of "backscatter" spam (Non-Delivery Report messages).

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. Anti-spam policies can be customized at the global, group and end-user levels with full integration to LDAP or Active Directory to streamline ongoing administration.

Integrated Email Firewall Protection

The **Proofpoint Email Firewall™** provides a stateful, first line of defense against spam and malicious connections by testing numerous connection-level data points including DNS, MX record verification, SPF, recipient verification, Proofpoint Dynamic Reputation information and optional netMLX data.

Innovative Connection Management

Proofpoint Dynamic Reputation™—powered by **Proofpoint netMLX™**—adds the industry's most powerful connection management features to your Proofpoint deployment. It's the only email reputation service that uses a combination of local, predictive behavioral data and globally-observed reputation—analyzed by powerful machine learning algorithms—to block incoming connections from malicious IP addresses.

defend against inbound threats (continued)

All Proofpoint appliances and software deployments provide built-in, predictve, behavioral analysis of local IP traffic that responds in real-time to eliminate email traffic spikes caused by target attacks and to block or throttle malicious connections from botnets.

Customers with high email volumes can add the enhanced protection of Proofpoint netMLX to their deployments to reduce inbound connection volumes by a total of 80% or more. Proofpoint netMLX creates the industry's most accurate and up-to-date database of reputation for IP addresses sending email across the Internet. Each minute, hundreds of data points for all IP addresses are parsed with advanced machine learning algorithms to generate a score that represents the sender's reputation. Proofpoint Dynamic Reputation then uses these scores, combined with local behavioral data, to make intelligent decisions about accepting, throttling or rejecting incoming email connections.

Virus Protection and 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—stopping them hours before competing solutions even begin to react.

prevent leaks of information across multiple protocols

Proofpoint's advanced data loss prevention features can protect outbound email as well as additional message streams including web-based email, blog postings, message board postings and other HTTP- or FTP-based activity.

Content Compliance: Easily Enforce Acceptable Use Policies

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 rules related to file types, message size, and message content. These 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.

Regulatory Compliance: Keep Private Data Secure

More than ever, enterprises need to safeguard the privacy and security of customer and employee data. The **Proofpoint Regulatory Compliance**™ module enforces best practices for securing private data and protects your organization from liabilities associated with privacy and data security regulations (such as HIPAA, GLBA, PCI, SEC rules and others). Customizable rules, managed dictionaries and "smart identifiers" are used to automatically scan for non-public information—such as protected health information and personal financial information—and reject or encrypt messages as appropriate.

Proofpoint's smart identifiers are more sophisticated than simple regular expressions. They look for the correct number of digits or characters, but also perform complex algorithmic processing to ensure high detection accuracy while minimizing false positives.

Digital Asset Security: Protect Confidential Documents

As email, webmail and other messaging systems have become the most important communication channels, they've also become a conduit for the exposure of sensitive or confidential information. The **Proofpoint Digital Asset Security**™ module keeps valuable corporate assets and confidential data from leaking outside your organization via email and other messaging protocols. Powerful MLX machine learning technology analyzes and classifies your confidential documents and then monitors for that information (or parts of that information) in the outbound message stream—stopping content security breaches before they happen.

Centralized Management

Web-based policy management, administration and end-user controls

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 messaging infrastructure and define messaging policies. You can even define and enforce different policies for different groups of end-users. As additional Proofpoint modules are added to your deployment, the same convenient interface is used for policy management.

The Ajax-based interface gives you "drag and drop" customization of the reports, status information, RSS feeds and other components displayed. Even create "mashups" of information from external sources.

Proofpoint's outstanding ease-of-use extends to end-users as well. Easy-to-understand reports and controls, such as Proofpoint's end-user digest, web-based quarantine and personalized safe- and block-lists, give users complete control over their own spam preferences.

Robust reporting

The Console also provides access to more than 60 real-time, graphical reports and alerts that give total 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 (e.g., simply click a link to block an abusive sender).

Zero Administration

Always up-to-date protection, maximum ease-of-administration

Automatic installation and notification of updated components makes ongoing administration simple. 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 your Proofpoint software or appliance deployment, including the hardened operating system and MTA, spam and virus engines, lexicons (such as the dictionaries used by the Proofpoint Regulatory Compliance module), application components and customized hot fixes.

Proofpoint Messaging Security Gateway and Proofpoint Protection Server

encrypt sensitive information

Proofpoint Secure Messaging™ adds powerful, content-aware encryption capabilities to your Proofpoint deployment, automatically encrypting messages based on your organization's policies. It automatically and consistently applies your encryption policies, without requiring end-users to take any special actions. Voltage IBE (identity based encryption) technology provides powerful, easy-to-use encryption without the key and certificate management hassles of other solutions. Proofpoint's hardware and virtual appliances also support digital certificates and enable gateway-to-gateway secure transfer and receipt of email using Transport Layer Security (TLS).

optimize your messaging infrastructure

Extend your Proofpoint deployment with a variety of enhancements that improve the usability and manageability of your email infrastructure. **Proofpoint Smart Search™** enhances Proofpoint's built-in logging and reporting features with advanced message tracing, forensics and log analysis capabilities—offering easy, real-time visibility into message f ows across your entire messaging infrastructure. Search, analyze and export message logs from one convenient, easy-to-use GUI—even across globally distributed Proofpoint deployments. **Proofpoint Secure File Transfer™** adds secure, large file transfer capabilities to your Proofpoint deployment. It lets end users send large files (or files that require enhanced security) quickly and easily—while minimizing the impact of large attachments on your email infrastructure. The on-demand **Proofpoint Email Archiving™** solution addresses email storage management, legal discovery and regulatory compliance challenges without the overhead of managing an in-house email archive.

high-performance, easy deployment, optimal scalability

Proofpoint was designed to meet the unique needs of large enterprises, ISPs, universities and government organizations. It offers all of the performance, f exibility, scalability, customization and end-user control features needed in large-scale deployments.

Each and every component of the Proofpoint system is engineered to meet the rigorous demands of enterprise performance. From the hardened, messaging-optimized OS used in Proofpoint appliances, to Proofpoint's unique, queue-less architecture that allows all message scanning functions to be performed in memory, Proofpoint provides the high performance required in even the most sophisticated deployments.

Proofpoint appliances scale indefinitely to support many millions of messages per day. They can easily be deployed in master/agent 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 even supports hybrid deployments with hardware and virtual appliances working together.

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.

Proofpoint further reduces 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 is also compatible with—and minimizes the burden on—overtaxed email server solutions such as Microsoft Exchange® and Lotus Notes®.

free trial version—try it today!

Experience the power of Proofpoint. Visit **www.proofpoint.com/trial** and register to download a fully-functional, 45-day trial version of the Proofpoint Messaging Security Gateway—Virtual Edition that can be deployed in minutes. Or visit **www.proofpoint.com/trypod** to register for a free trial of the Proofpoint on Demand SaaS email security solution.

Proofpoint Speaks Your Language

In addition to delivering outstanding anti-spam performance against spam in any language, Proofpoint's policy and content scanning engines detect and "understand" text in any language, including multi-byte languages. Data loss prevention policies can match non-English keywords and dictionary terms written in international character sets including Japanese, Chinese and Cyrillic. Administrators can create policies that are triggered based on the language detected in the content of an email. For example, attach language-specific disclaimers to an outbound message depending upon the language in which it was written.

End-user interfaces for message digests, and web-based quarantine are available in Chinese, Dutch, English, German, Finnish, French, Italian, Japanese, Portuguese, Russian, Spanish and Swedish.

Proofpoint's administrative GUI, product documentation and online help are currently available in both English and Japanese versions. As with Proofpoint's end-user interfaces, administrators can set their language preferences on an individual basis.

Appliance Versions

The Proofpoint Messaging Security Gateway appliance is available in a variety of hardware configurations to support deployments of any size. For up-to-date information on Proofpoint appliance models, please visit:

www.proofpoint.com/products/msg.php

Supported Browsers

All configuration and administration tasks—for the hardware appliance, virtual appliance or software versions—are handled through Proofpoint's 100% browser-based interface. Supported browsers include:

Microsoft® Internet Explorer 6.0 or higher

Mozilla Firefox 2.0 or higher

Proofpoint, Inc. 892 Ross Drive Sunnyvale, CA 94089 USA

www.proofpoint.com ☎ 1 408 517 4710