



Trend Micro™

Email Security Platform for Service Providers

Email is the most prevalent form of communication. Because of its mission-critical status, it has become vulnerable to a wide range of threats, including spam, phishing, malware, inappropriate content, and data leakage. These threats can weaken productivity, consume infrastructure resources, and expose organizations to compliance and legal issues. However, email's use and complexity continues to grow, and so must the ability of users to adapt to evolving security risks.

Email Security Platform for Service Providers allows Service Providers to offer complete end-to-end hosted email security services to their customers. It provides email filtering, anti-spam, antivirus, and policy compliance within a centrally managed, highly scalable architecture—complete with a customizable user interface and tiered administration levels.

Service Providers can choose to offer the white-label version hosted by Trend Micro with no capital expenditure or to deploy the platform in their own datacenter for tighter integration with existing monitoring and billing tools. Designed to adapt to the desired service model or to specific customer requirements, this software solution is capable of supporting hundreds of thousands of email accounts.

KEY FEATURES

Maximum Security

- Industry-leading anti-malware and anti-spam engines stop more than 99% of incoming spam and eliminate malware found in attachments.
- Spam filtering for outbound messages includes a global policy for minimal false positives.
- Content filtering for inbound messages supports basic attachment blocking based on extension and characteristics.

Unique Point of Deployment (PoD) Architecture

- *Low Total Cost of Ownership (TCO)*. The reference architecture is designed around a list of commodity hardware, enabling easy datacenter build-out and trouble-free cold swapping in case of server failure.
- *Capacity*. A basic PoD supports approximately 500,000 seats and 50 million messages per day.
- *Redundancy*. PoDs are fully internally redundant, eliminating any single point of failure.
- *Availability*. PoD architecture ensures “always-on” availability while allowing maintenance and support. Mail can be seamlessly rerouted via other PoDs if one becomes unavailable.
- *Scalability*. As replicable units, PoDs can be quickly built to expand capacity when needed. Also, additional hardware can be easily inserted into a PoD, such as extra MTAs (mail transfer agent) and quarantine storage for increased throughput and retention.

Flexible Role-based Administration

- Role-based access control (RBAC) enables multiple levels of administration access.
- Policy management and creation is designed to support multiple accounts and domains.
- The Service Provider is allowed to assign appropriate roles—permissions to perform particular system functions—to administrators and end-users.
- At any point, the Service Provider can assume the role of any child account to view settings or make configuration changes.

Intuitive User Interface (UI)

- The simplified layout allows easier management of multiple customers and domains.
- Functionalities such as search boxes and graphs are enabled for easy location and presentation of information.

Comprehensive White-Labeling Support

- For white-label SaaS (Software-as-a-Service) solution: The Service Provider is provided a standard template UI with comprehensive rebranding options.
- For partner-hosted platform: The Service Provider is provided the option to rewrite the UI to suit their specific needs. Any aspect of the UI can be changed, such as location of information, data displayed, policy layout, language, etc.

BENEFITS TO SERVICE PROVIDERS

- Easy management of multiple customer domains, user accounts, policies, and messages
- Guided analysis of security events and mail flow through graphical reports and a summary dashboard
- Integrates seamlessly with any system infrastructure
- Significant recurring revenue opportunity through subscription business model
- Increased average revenue per customer through flexible pricing plans
- Flexible pay-as-you-go billing minimizes financial risk
- For white-label SaaS solution: Low total cost of operation
- For partner-hosted platform: No prohibitively expensive single-purpose appliances

BENEFITS TO CUSTOMERS

- Industry-leading, cloud-based anti-malware and anti-spam technology ensures data protection and faster threat response
- Drastic reduction of spam frees bandwidth and increases productivity
- End-user quarantine provides personalized reports of blocked messages and allows users to release these on their own authority

Easy Integration through Web Services Application Programming Interfaces (APIs)

- Web Services APIs provide a scriptable configuration layer for easy integration with third-party systems in customer environments.
- Web Services create a platform for rapid development of new features and enable specific functionalities that Email Security Platform for Service Providers does not support.

End-to-end Mail Tracking

- End-to-end mail tracking enables message forensics, mail flow analysis, reporting, and troubleshooting.
- Detailed mail tracking information generated is viewable by the Service Provider or the end-user.

End-user Quarantine

- End-users are allowed to manage their own spam quarantines, including individual white lists, removing administration overhead from the Service Provider.
- This feature is scalable to accommodate thousands of accounts, with retention policies dictated by the Service Provider.

Industry-leading Service Level Agreement (for White-label SaaS Solution)

- 100% service uptime with up to three times stronger remediation penalties than other vendors
- 99%+ spam-blocking effectiveness
- Zero email-based virus infections
- No more than three in one million emails incorrectly classified as spam
- No more than one minute of email delivery latency, regardless of the customer's location
- 24x7 support responsiveness

TREND MICRO SMART PROTECTION NETWORK

Trend Micro Email Security Platform for Service Providers is powered by the Smart Protection Network, a next-generation cloud-client content security infrastructure designed to protect customers from Web threats.

The Smart Protection Network powers both on-premise and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight clients to access its in-the-cloud correlation of email, Web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats.



©2010 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

www.trendmicro.com