TREND
MICRO™

Trend Micro™

HOSTED EMAIL SECURITY™

Stop phishing, ransomware, Business Email Compromise (BEC), advanced threats, and spam before they reach your network

Email is mission-critical, but email-based threats, including ransomware and BEC, are growing exponentially and it's difficult to keep up. Even your savviest employees can mistakenly click on a malicious link and expose your enterprise to cybercrime. At the same time, other critical IT projects are demanding your attention, but that doesn't mean you can afford to neglect email security maintenance and potential targeted attacks.

Trend Micro™ Hosted Email Security™ is a no-maintenance-required solution that delivers continuously updated protection to stop phishing, ransomware, BEC, advanced threats, spam, and malware before they reach your network. It protects Microsoft® Exchange™, Microsoft® Office 365® , Gmail™, and other hosted and on-premises email solutions.
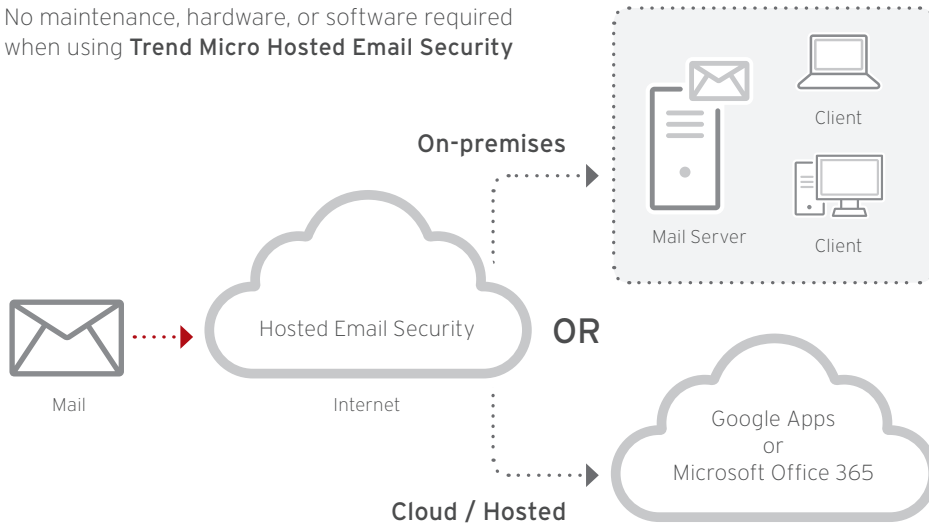
KEY FEATURES

- **Layered protection**: Provides protection for phishing, spam, and graymail with multiple techniques, including sender reputation, content and image analysis, machine learning, and more.
- **Email fraud protection**: Protects against BEC with enhanced machine learning, combined with expert rules, analyzing both the header and content of the email.
- **Document exploit protection**: Detects advanced malware and exploits in PDF, Microsoft® Office, and other documents using static and heuristic logic to detect and examine abnormalities.
- **Zero-day protection**: Combines pre-execution machine learning, anti-malware, and dynamic analysis using sandboxing to detect zero-day malware.
- **Cloud sandboxing**: Includes cloud sandboxing for automatic in-depth simulation and analysis of potentially malicious attachments in a secure virtual environment hosted by Trend Micro.
- **URL time-of-click**: Blocks emails with malicious URLs before delivery and re-checks URL safety when a user clicks on it.
- **Web reputation service**: Scans URLs embedded in emails and blocks URLs leading to malicious sites by using the enhanced web reputation services from the Trend Micro™ Smart Protection Network™.
- **Email encryption**: Policy-driven email encryption includes hosted key management service and enables recipients to read encrypted emails on any device using a web browser.
- **Data loss prevention (DLP)**: Provides DLP profiles to make it easier to track and document sensitive data, and safeguard confidential information.
- **Source verification and authentication**: Includes Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC).
- **Threat intelligence**: Uses the Smart Protection Network, one of the largest threat intelligence databases, to correlate web, email, file, domain registries, and many other threat sources to identify attacker infrastructures, before they are launched.

TREND MICRO HOSTED EMAIL SECURITY:

- Cloud sandboxing and email encryption are included in the base offer, with no extra charge.
- Cloud sandbox leverages proven Trend Micro™ Deep Discovery™ sandboxing technology, which has achieved a "Recommended" rating by NSS Labs.
- Part of the Trend Micro email security solution, a market leader in 2016 IDC MarketScape for Worldwide Email Security.

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery

100%

Breach Detection Rate
- 2017 -

RECOMMENDED 4 years in a row

No maintenance, hardware, or software required when using **Trend Micro Hosted Email Security**

On-premises

Client

Mail Server

Client

Hosted Email Security

OR

Mail

Internet

Google Apps
or
Microsoft Office 365

Cloud / Hosted

COMPLETE USER PROTECTION

Hosted Email Security is part of the **Trend Micro™ Smart Protection Complete Suite**, powered by XGen™ security. The Smart Protection Complete Suite combines the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. And it enables you to manage users across multiple threat vectors from a single management console that gives you complete user-based visibility into the security of your environment.

Hosted Email Security is also part of **Trend Micro Smart Protection for Office 365**, which provides complete threat protection against phishing, BEC, ransomware, internal email risks, and file sharing risks for Office 365. Powered by XGen™ security, it uses the optimum blend of cross-generational threat defense techniques, including machine learning, sandbox analysis, and more.

WHAT HOSTED EMAIL SECURITY CAN DO FOR YOU:

Stop phishing and spam
* Examines the authenticity and reputation of the email sender to screen out malicious senders
* Analyzes email content using a variety of techniques to filter out spam and phishing
* Uses web reputation service from the Smart Protection Network to protect against web links in emails that are malicious
* Provides time-of-click protection against malicious URLs in email messages – rewrites and analyzes URLs at the time of click and blocks them if malicious

Blocks ransomware before it ever gets to your users
* Detects and blocks ransomware with malware scanning, anti-spam, and file (including executables and macro) scanning
* Gives you advanced threat protection with cloud sandbox malware analysis, and zero-day and document exploit detection

Protects against BEC
* Includes enhanced machine learning, combined with expert rules to analyze both the header and content of the email to examine the behavior (e.g., an insecure email provider, forged domain, or a reply to a free email service) and intention (e.g., financial implication, urgency, and a call to action)
* More stringent protection can be set up for high-profile users

Gives you peace of mind
* Includes 24x7 technical support
* All emails from EMEA customers are routed to data centers in Germany and emails from the rest of the world are routed to data centers in the U.S.
* The main service is hosted on Amazon Web Services and the cloud sandbox is hosted on Trend Micro data centers certified by ISO 27001. Data centers in different regions operate independently and are not interconnected due to data privacy and sovereign considerations

SYSTEM REQUIREMENTS

Learn more

Securing Your Connected World