Trend Micro™

Email Security

Stop more phishing, ransomware, and fraud attacks by using a cross-generational blend of threat techniques

Email is mission critical, but email-based threats, including ransomware and business email compromise (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 a cyberattack.

Trend Micro™ Email Security stops more phishing, ransomware, and BEC attacks. Our solution uses an optimum blend of cross-generational threat techniques, like machine learning, sandbox analysis, data loss prevention (DLP), and other methods to stop all types of email threats. This solution minimizes management overhead and integrates with other Trend Micro security layers to share threat intelligence and provide central visibility of threats across your organization. Email Security protects Microsoft Exchange™, Microsoft 365, Gmail™, and other hosted and on-premises email solutions.

KEY FEATURES

- **Layered protection:** Provides comprehensive protection for phishing, spam, and graymail with multiple techniques, including sender, content and image analysis, machine learning, and more.
- **Email fraud protection:** Protects against BEC scams with enhanced machine learning and expert rules to analyze both the header and content of the email. Includes Trend Micro™ Writing Style DNA as an additional layer to conduct authorship analysis for BEC protection. (Trend Micro™ Cloud App Security license required for Writing Style DNA.)
- **Document exploit protection:** Detects advanced malware and exploits in PDFs, Microsoft 365, and other documents using static and heuristic logic to detect and examine abnormalities..
- **Advanced threat protection:** Discovers unknown malware using multiple patternless techniques, including pre-execution machine learning and top-rated sandbox technology from Trend Micro™ Deep Discovery™ for dynamic analysis of potentially malicious attachments or embedded URLs in a secure virtual environment.
- **File password extraction:** Heuristically extracts or opens password-protected files by leveraging a combination of user-defined passwords and message content.
- **URL time-of-click:** Blocks emails with malicious URLs before delivery and re-checks URL safety when a user clicks on it.
- **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 Trend Micro™ 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.
- **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.
- **DLP:** Includes DLP templates to make it easier to track, document, and safeguard confidential and sensitive information.
- **Email continuity:** Provides a standby email system that gives uninterrupted use of email in the event of a mail server outage.
- **Flexible reporting:** Generates reports based on scheduled and customizable content.
- **Trend Micro™ Connected Threat Defense™:** Synchronizes with Trend Micro Apex Central™ to implement a file and URL suspicious objects list.

What Email Security can do for you:

Stops 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.
- Protects against malicious URLs at delivery and at time-of-click (rewrites and analyzes URLs at the time of click and blocks them if malicious).

Detects and blocks advanced threats

- Detects and blocks ransomware and other types of zero-day malware using pre-execution machine learning, macro analysis, exploit detection, and dynamic sandbox analysis for files and URLs.
- Pre-execution machine learning filters unknown malware before sandbox analysis, enhancing efficiency and efficacy of advanced threat protection.
- Shares threat information with other security layers to guard against persistent and targeted attacks.

Protects against BEC

- Examines email behavior (an unsecure email provider, forged domain, or a reply to a free email service), intention (financial implication, urgency, or a call to action), and authorship (writing style).
- Allows you to have the flexibility to define your organization's high-profile users list for BEC protection.

Gives you peace of mind

- 24/7 technical support.
- All emails for customers in Europe, the Middle East, and Africa (EMEA) are routed to data centers in Western Europe. Emails for Australia and New Zealand are routed to data centers in Australia. Emails for Japan are routed to data centers in Japan. Emails for South and Southeast Asian countries are routed to data centers in Singapore. Emails for the rest of the world are routed to data centers in the U.S.
- The service is hosted on Amazon Web Services (AWS). Data centers in different regions operate independently and are not interconnected due to data privacy and sovereignty considerations

COMPARISON TABLE: TREND MICRO EMAIL SECURITY

CAPABILITY	STANDARD	ADVANCED
Email sender analysis and authentication by SPF, DKIM, and DMARC	Yes	Yes
Protection: Known threats (spam, malware, malicious URLs, and graymail)	Yes	Yes
Protection: Unknown malware detection	Exploit detection, predictive machine learning	Exploit detection, predictive machine learning, sandbox analysis for files
Protection: Unknown URL protection	URL time-of-click	URL time-of-click, sandbox analysis for URLs
Protection: Artificial intelligence (AI)-based fraud/BEC detection, checking email header and content	Yes	Yes
Protection: AI-based fraud/BEC detection, checking email sender authorship	–	Yes*
File-password extraction	–	Yes
Compliance: DLP and email encryption	Yes	Yes
Reporting: Customizable and scheduled reports	Yes	Yes
Syslog for exporting logs	Yes	Yes
Connected Threat Defense: Implementing of file and URL suspicious object lists from Trend Micro Apex Central	Yes	Yes
End user quarantine	Yes	Yes
Email continuity: Provides uninterrupted use of email in the event of a mail server outage	–	Yes
Mail tracking search window	30 days	60 days

*Cloud App Security license required

Service requirements

https://docs.trendmicro.com/en-us/enterprise/trend-micro-email-security-online-help/about/service-requirements.aspx