

Trend Micro™

# CLOUD EMAIL GATEWAY SERVICES

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 cybercrime.

Trend Micro™ Cloud Email Gateway Services are smart, optimized, and connected to stop more phishing, ransomware, and BEC attacks. Powered by XGen™ security, the services use an optimum blend of cross-generational threat techniques, including machine learning, sandbox analysis, data loss prevention (DLP), and other methods to stop all types of email threats. The solutions minimize management overhead and connect with other Trend Micro security layers to share threat intelligence and provide central visibility of threats across your organization. The solution protects Microsoft® Exchange™, Microsoft® Office 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 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:** Discovers unknown malware using multiple pattern-less techniques, including pre-execution machine learning and sandbox analysis.
- **Advanced threat protection:** Includes top-rated Trend Micro™ Deep Discovery™ sandbox technology for dynamic analysis of potentially malicious attachments in a secure virtual environment.
- **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.
- **Connected Threat Defense:** Synchronizes with Trend Micro Control Manager™ to share and implement a file and URL suspicious objects list.



A leader in IDC MarketScape report for Email Security



## WHAT CLOUD EMAIL SECURITY SERVICES 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
- 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

- Includes enhanced machine learning, combined with expert rules to analyze both the header and content of the email to examine the behavior (an unsecure email provider, forged domain, or a reply to a free email service) and intention (financial implication, urgency, or a call to action)
- Allows you to have the flexibility to define your organization's high-profile users list for BEC protection

### Gives you peace of mind

- Includes 24x7 technical support
- All emails from Europe, the Middle East and Africa (EMEA) customers are routed to data centers in Western Europe, and emails from the rest of the world are routed to data centers in the United States\*
- The main service is hosted on AWS 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

## COMPARISON TABLE: CLOUD EMAIL GATEWAY SERVICES

CAPABILITY	STANDARD (Trend Micro™ Hosted Email Security™)	ADVANCED (Trend Micro™ Email Security™ 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, machine learning, sandbox analysis	Exploit detection, machine learning, sandbox analysis
Protection: Unknown URL protection	URL time-of-click	URL time-of-click
Protection: Artificial intelligence (AI)-based fraud/BEC detection	Yes	Yes
Compliance: DLP and email encryption	Yes	Yes
Email continuity	-	Yes
Mail tracking: High performance log search	-	Yes
End user quarantine: Automatically combine multiple aliases into one quarantine account	-	Yes
Reporting: Customizable and scheduled reports	-	Yes
External log sharing to security information and event management (SIEM)	via Trend Micro Control Manager	via Trend Micro Control Manager or Syslog directly to SIEM
Connected Threat Defense: Sharing/implementing of file and URL suspicious objects	-	Yes

## SYSTEM REQUIREMENTS

### [Hosted Email Security](#) | [Trend Micro Email Security](#)

\*For Trend Micro Email Security Advanced customers in Australia and New Zealand, emails are routed to data centers in Australia.



©2019 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, Apex One(TM), and Trend Micro Control Manager 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. [DS01\_Email\_Cloud\_Gateway\_190624US]