Trend Micro™

WORRY-FREE SERVICES SUITES

Simple and complete protection for your endpoints and beyond

As advanced threats are designed to bypass traditional cybersecurity defenses, the rise of endpoint detection and response (EDR) has proven to be an important tool in the quest to seek out these advanced threats and eliminate them before they compromise data. But while EDR is a good first step, it only focuses on endpoints.

Trend Micro™ Worry-Free™ Services is a suite of security solutions designed to match the needs of your organization, using a blend of advanced threat protection techniques to eliminate security gaps across any user activity across the endpoint and beyond.

SIMPLE, COMPLETE, TRUSTED

Powered by XGen™ security, Worry-Free Services provides a cross-generational blend of threat defense techniques and connected threat defenses that constantly learns, adapts, and automatically shares intelligence across your environment, giving you detection and response that is:

Simple

- Easy to install, simple to use, and won't slow you down.
- A single, intuitive web console for in-depth visibility and control across your entire organization.
- Manages multiple devices within a single agent.

Complete

- High-fidelity machine learning combined with other state-of-the-art detection techniques gives you the broadest protection against ransomware and advanced attacks.
- Uses a blend of advanced threat protection techniques to eliminate security gaps across any user activity, any endpoint, and any mailbox.

Trusted

- Thanks to our up-to-the-second threat intelligence network, we protect more than 250M endpoints.
- Wards off threats while you focus on your business.

Trend Micro™ Worry-Free™ Services

Cloud-based protection for endpoint and mobile devices.

Trend Micro™ Worry-Free™ Services Advanced

Cloud-based protection for your business devices and email.

Trend Micro™ Worry-Free™ XDR

Detection and response across email and endpoints.

WORRY-FREE SERVICES SOLUTIONS

FEATURES	Worry-Free Services	Worry-Free Services Advanced	Worry-Free XDR
Endpoint Security			
Windows and Mac OS support	✔	✔	✔
Anti-malware and behavior analysis	✔	✔	✔
Predictive and runtime machine learning	✔	✔	✔
Vulnerability protection/virtual patching	✔	✔	✔
Full disk encryption	✔	✔	✔
Application control	✔	✔	✔
Integrated endpoint DLP	✔	✔	✔
Device control	✔	✔	✔
Web Security			
Web reputation and URL filtering	✔	✔	✔
Mobile Security and Management			
Mobile security and management	✔	✔	✔
Email and collaboration security			
Cloud email gateway with DLP		✔	✔
API-based Microsoft 365/G Suite protection		✔	✔
Cloud sandboxing		✔	✔
BEC and credential phishing protection		✔	✔
Box & Dropbox protection		✔	✔
Cross-Layer Detection and Response (XDR)			
Correlates data automatically across email and endpoint in one console			✔
Automated detection, sweeping, hunting, and root cause analysis			✔
Advanced threat detection through cloud sandboxing			✔

* For MSPS only

TREND MICRO WORRY-FREE OPTIONS

Worry-Free Services

As most SMBs lack a dedicated security team and skillset, this leads to overworked IT teams. Trend Micro Worry-Free Services helps lessen the workload by providing an all-in-one lightweight agent with an intuitive cloud-based console that gives you in-depth visibility and control across your entire organization.

Trend Micro protects more than 250 million endpoints globally

BENEFITS

Advanced protection

- High fidelity machine learning uniquely analyzes files, not only before execution but also during runtime.
- More reliable detection of advanced malware, including fileless, cryptocurrency mining, ransomware, and more.
- Behavioral analysis against scripts, injection, ransomware, memory, and browser attacks.
- Vulnerability protection automatically shields endpoints from known vulnerabilities of Microsoft applications, significantly limits the threat vulnerabilities that can be exploited.

Safeguards your sensitive data

- Integrated DLP, encryption management, and device control capabilities cover the broadest range of devices, applications, and file types to ensure:
  - Maximum visibility and control
  - Confidentiality and compliance with GDPR, HIPPA, and other rapidly evolving regulations
  - Granular policies for device control and data management
  - Management and visibility for Microsoft® BitLocker®

Stops malicious software with application control

- Utilizes application monitoring, whitelisting, and lockdown.
- Blocks unauthorized or unknown applications from executing attacks, like ransomware.
- Enforces easy-to-manage, simple rules.
- Enables you to run only applications you have authorized.

Worry-Free Services Advanced

Email has quickly become the number one entry point for malware. According to Verizon's 2019 Data Breach Investigation Report, 94% of malware detected by an organization was delivered via email[1]. Worry-Free Services Advanced provides cloud-based protection for your business devices and email to stop email threats in the cloud before they reach your network and protect your devices from spear phishing and advanced targeted attacks.

Trend Micro Cloud App Security blocked 12.7 million high-risk email threats in 2019–in addition to those detected by Microsoft 365 and Gmail built-in security

1 Trend Micro Cloud App Security Report 2019

BENEFITS

- Provides the same advanced protection, data defense, and application control capabilities as Worry-Free Services, plus:
  - Complete email and collaboration protection
  - Trend Micro Email Security™, a cloud-based email gateway, to protect your on-premises email
  - Trend Micro™ Cloud App Security, an API-based protection to protect your Microsoft 365® email and Google G Suite™ Gmail™
  - Advanced threat and data protection for Microsoft 365, G Suite, and collaboration tools such as Dropbox™, and Box™.
- Proven email and Microsoft 365 protection uncovers ransomware, business email compromise (BEC), credential phishing, and advanced targeted attacks

1 Trend Micro Cloud App Security Report 2019

Worry-Free XDR

Even organizations with the most advanced protection layers aren't immune to cyber threats, as there's no such thing as 100% prevention. As there is very serious risks and costs associated with undetected, or slow to detect, threats in the organization, the goal is to detect and respond threats as soon as possible, before significant damage is done.

Trend Micro Worry-Free XDR bundle provides detection and response capabilities across email and endpoints to help you discover and respond to targeted attacks more effectively. By correlating threat data from endpoints and email, a clearer picture is available to determine the source and spread of advanced attacks.

BENEFITS

- Combines Worry-Free Services Advanced and Trend Micro™ Endpoint Sensor to provide automatic detection and response across email and endpoint, giving you:
  - Automatic data correlation from sensors that collect detection and activity data across endpoint and email—the #1 threat vector
  - Automated sweeping and root cause analysis, including step-by-step recommended actions, allowing IT admin to mitigate issues quickly
  - One console (Worry-Free Services) with native integration to endpoint and email
  - Advanced threat detection through cloud sandboxing
- Most advanced threats start with a phishing email, so combining advanced email protection with the ability to trace a threat to its entry point is an effective defense against the latest in email attacks

SYSTEM REQUIREMENTS

For full system requirements, visit **https://docs.trendmicro.com/en-us/smb/worry-free-business-security-services-67-server-help/security-agent-insta/preparation/wfbs-svc-system-requ.aspx**

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers by providing connected security across the IT infrastructure. **www.trendmicro.com**

vodafone business

Please contact your Vodafone sales representative for more information

WHY CHOOSE TREND MICRO FOR YOUR SECURITY PARTNER?

- 30+ years of security expertise for business and consumers
- Worry-Free Business Security solutions that protect over 600,000 businesses worldwide
- Solutions that are powered by Trend Micro™ Smart Protection Network™, a cloud-based global threat intelligence infrastructure supported by over 1,200 threat experts worldwide

To learn more, contact your trusted IT partner or your local Trend Micro sales office.

See how we stack up

The Forrester Wave™: Enterprise Detection and Response, Q1 2020.

Trend Micro is a leader in the Forrester Wave™ for Enterprise Email Security, Q2 2019.

Trend Micro is named a leader in The Forrester Wave™: Endpoint Security Suites, Q3 2019.

TREND MICRO™

Securing Your Connected World

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy

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 cybercrime.

Trend Micro™ Email Security stops more phishing, ransomware, and BEC attacks. Powered by XGen™ security, 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 Office 365, Gmail™, and other hosted and on-premises email solutions.

FORRESTER®
WAVE LEADER 2021
Enterprise Email Security

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 Office, 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.
- **Connected Threat Defense**: Synchronizes with Trend Micro Apex Central™ to implement a file and URL suspicious objects list.

WHAT TREND MICRO 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 from customers in Europe, the Middle East, and Africa (EMEA) are routed to data centers in. Western Europe. Emails from Australia and New Zealand are routed to data centers in Australia. 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 (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: 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 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

Email Security

TREND MICRO™

Securing Your Connected World

[DS02_Trend_Micro_Email_Security_210719US]

Trend Micro™

CLOUD APP SECURITY

Advanced threat and data protection for Microsoft® Office 365®, Gmail, and cloud file-sharing services

As you adopt cloud-based enterprise applications, such as Microsoft® Office 365®, G Suite™, Box™, and Dropbox™, you need to be more vigilant about security than ever. While these applications are delivered in a safe manner, you share the responsibility to secure the content that passes through them.

What are the risks?

- Ninety-four percent of ransomware attacks[1] and over 90% of targeted attacks start with email.
- According to the FBI, BEC scams amounted to **£1.36 Billion in losses** in 2019—half of the year's total losses due to cybercrime—with an average of £60,000 per incident[2].
- Remote workers, partners, and customers may unknowingly share malicious files using cloud file-sharing services.
- The security included with Office 365 (E3 and below) is designed to detect *known* malware but over 95% of malware is *unknown*.

The potential costs are too high to accept baseline security that only protects against a small portion of threats.

Trend Micro™ Cloud App Security enables you to embrace the efficiency of cloud services while maintaining security. It protects incoming and internal emails from Office 365 and Gmail against advanced malware and other threats, and enforces compliance on other cloud file-sharing and collaboration services, including Box, Dropbox, Google Drive™, Microsoft® SharePoint® online, Microsoft® OneDrive® for business, and Microsoft® Teams.

Cloud App Security integrates directly with Office 365, Google G Suite™, and other services using application programming interfaces (APIs), maintaining all user functionality without rerouting email traffic or setting up a web proxy. This second layer of defence catches threats beyond those detected by the cloud email services' built-in security.

KEY ADVANTAGES

Protects Office 365 and Gmail email from phishing and advanced malware

- Discovers unknown malware using multiple patternless techniques, including pre-execution machine learning and sandbox analysis.
- Uses multiple operating systems and extensive anti-evasion technology on our award-winning[3] sandboxing technology.
- Identifies BEC attacks by using artificial intelligence (AI), including expert system and machine learning, to examine email header, content, and authorship, while applying more stringent protection for high-profile users.
- Prevents executive spoofing scams using Writing Style DNA. This unique technology detects impersonations of high-profile users (such as the CEO, VP, GM) by analyzing the writing style of a suspicious email and comparing it to an AI model of that user's writing.
- Finds malware hidden in common Office file formats and PDF documents with the unique document exploit detection engine.
- Protects internal email and allows manual scan to uncover attacks already in progress.
- Prevents credential phishing by blocking URLs which disguise as a legitimate logon website.

Enforces compliance for cloud file-sharing and collaboration services

- Provides Trend Micro™ Integrated Data Loss Prevention (DLP) and advanced malware protection for Box, Dropbox, Google Drive, SharePoint, OneDrive, and Teams.
- Enables consistent DLP policies across multiple cloud-based applications.
- Discovers compliance data in existing stored files and email by scanning databases.
- Simplifies setup with more than 240 pre-built compliance templates, user/group policies, and support for Microsoft® Rights Management services.

KEY BENEFITS

- Protects Office 365 email and Gmail, along with other cloud file-sharing and collaboration services
- Detects ransomware and other malware hidden in Office file formats or PDF documents
- Identifies BEC attacks using artificial intelligence
- Protects internal email and allows on-demand scanning for mail store
- Gives visibility into sensitive data use with cloud file-sharing services
- Preserves all user functionality, on any device, with simple API integration

> "In 2019, Trend Micro Cloud App Security blocked 12.7 million high-risk threats that passed through Office 365 and G Suite built-in security."

Trend Micro Cloud App Security Report 2019

FORRESTER®
WAVE LEADER 2019
Enterprise Email Security

Optimised for minimum impact to administrators and users

- Preserves all user and administrator functionality.
- Provides direct cloud-to-cloud integration for high performance and scalability.
- Minimises latency impact by assessing the risk of files and URLs before sandbox analysis.
- Supports hybrid Office 365 and on-premises Microsoft® Exchange™ architectures in conjunction with Trend Micro™ ScanMail™.
- Integrates with Trend Micro Apex Central™ for central visibility of DLP and threat events across your organisation's endpoints, servers, and web traffic.
- Provides programmatic access through Cloud App Security automation and integration to Representational State Transfer (REST) APIs, allowing the security team of your organisation to investigate, detect, and respond to security issues.

Deploys automatically with no software or device changes

Cloud App Security's cloud-to-cloud API integration doesn't rely on redirecting email or web proxies. As a result, it:

- Adds security without burdening IT with changing devices or user settings, installing software, setting up a web proxy, or changing the MX record to reroute email.
- Integrates quickly and automatically with Office 365, Google G Suite, and other cloud services.
- Extends the capabilities of your Cloud App Security with advanced Trend Micro™ XDR functionality, providing investigation, detection, and response across your endpoints, email, and servers.

Detection and response for email and beyond

One hundred percent detection is the goal, but in reality, no security can prevent 100% of attacks 100% of the time. When malware is found on an endpoint, chances are it came from an email. You want to know who else received the email and if this malicious attachment is in any other mailboxes. You then need to take action by quarantining the emails and possibly resetting passwords on the affected email accounts. Trend Micro XDR combines detection and response for email and endpoint.

Trend Micro™ Managed XDR

Trend Micro can provide 24/7 alert monitoring, alert prioritisation, investigation, and threat hunting as a managed service. With Managed XDR, you can benefit from detailed threat investigations and hunting without the extensive in-house resources.

SYSTEM REQUIREMENTS

For more details and the latest supported version visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

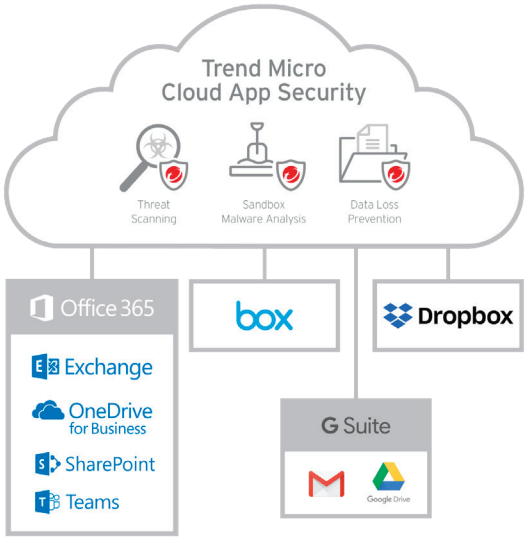
> "Cloud App Security reliably catches even unknown threats that are difficult to detect with Office 365. It reminds us of the power of multilayered defence."
>
> **Hironori Araya,**
> Head of PR and Information Group,
> Tohoku Electrical Safety
> Inspection Association

TREND MICRO™

Securing Your Connected World

vodafone business

Please contact your Vodafone sales representative for more information



[1] TrendLabs 2017 Security Roundup, March 2018
[2] FBI, 2020
[3] 2017 NSS Labs Breach Detection Systems Report