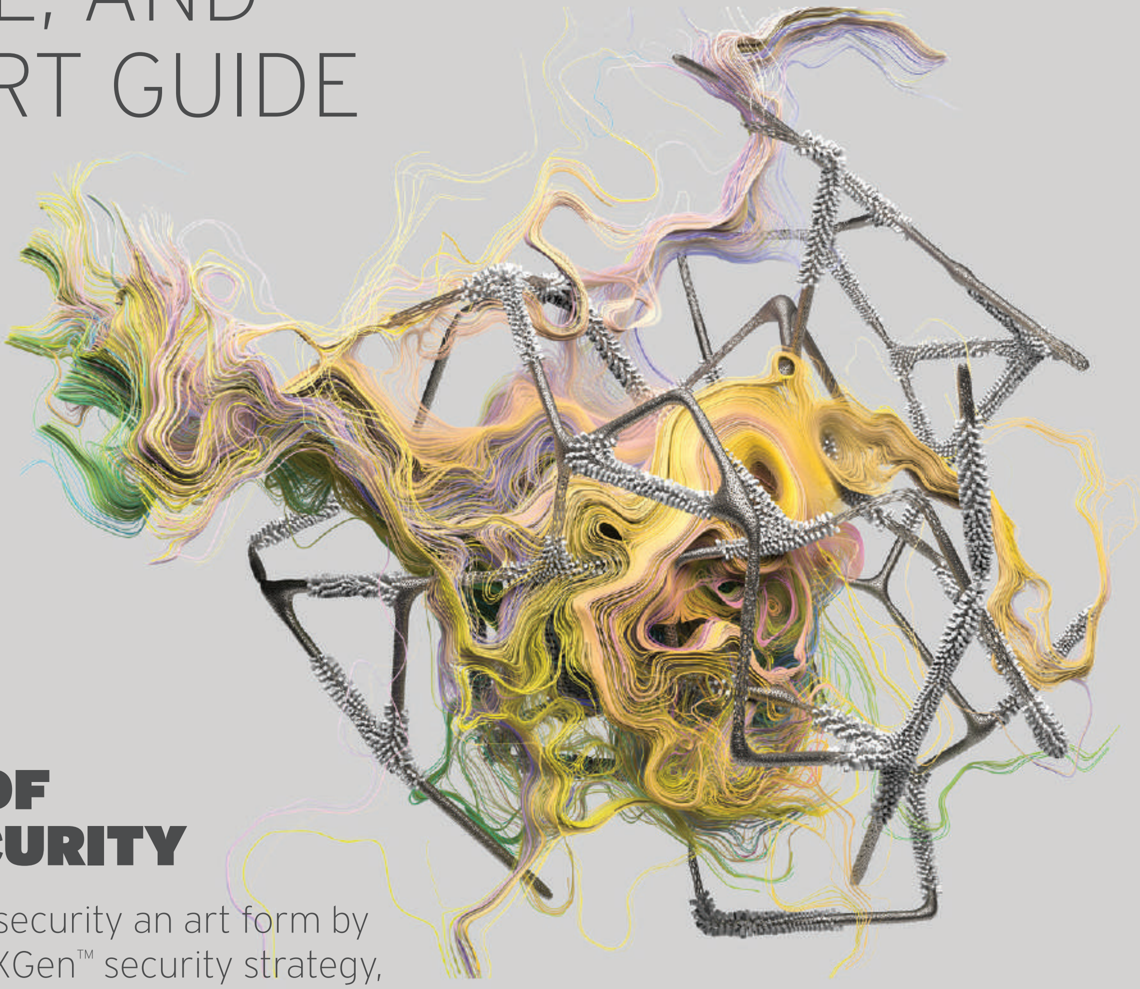
PRODUCT GUIDE

Trend Micro

SOLUTIONS, SERVICE, AND SUPPORT GUIDE



THE ART OF CYBERSECURITY

We've made cybersecurity an art form by orchestrating our XGen™ security strategy, global threat research, and passionate people to secure your connected world.

Because when you can prepare for, withstand, and rapidly recover from threats, you're free to go further and do more.

JULY 2020

THE ART OF
CYBERSECURITY

CYBERSECURITY CAN BE BEAUTIFUL

Infrastructure Shifts and Early Protection by Trend Micro
courtesy of Andy Gilmore

Contents

01 COMPANY OVERVIEW

Our vision

Making the world safe for exchanging digital information.

The cybersecurity landscape is getting more complex by the day, with increasing risk to your business, brand, and customers.

With business resilience comes freedom.

Trend Micro doesn't just protect organizations from cyber threats, we are committed to promoting resiliency. By adapting to the current and future threat landscape, organizations are given the freedom to see cybersecurity risks in a holistic and strategic way. Trend Micro helps position the cybersecurity function as a business enabler so businesses can better adapt and respond to threats as well as drive digital transformation.

Innovative security for more than 30 years

For more than 30 years, Trend Micro has been making the world secure for exchanging digital information. Built by passionate people who live and breathe cybersecurity, Trend Micro empowers you to prepare for, withstand, and rapidly recover from threats, now and in the future.

Trusted threat research

The hundreds of security experts on the Trend Micro Research Team are constantly gathering intelligence across 15 global research centers and work closely with law enforcement. This relentless focus on research and understanding the known threats of the past, the risks from vulnerabilities today, and the future of cybersecurity, inform our connected security solutions.

A better technology strategy

Just like cyber threats are continually evolving, so is our XGen™ security strategy. It's focused not only on understanding the latest in threats, but also the new environments organizations use to enable digital transformation.

People on a mission

What makes Trenders different is a genuine passion for making the world a better place for customers as well as those less fortunate. Driven by our core principles—customer value, collaboration, change, innovation, and trustworthiness—our work doesn't end with protecting and empowering customers with world-class technology.

Protecting more than 500,000 commercial organizations. Trusted by top 8 of 10 Fortune 500 companies.

Our promise

We are relentlessly focused on providing you with the insight and protection you need to deal with cyber threats in a constantly shifting technology landscape, freeing you to go further and do more in a connected world. We are passionate about doing the right thing, celebrating diversity, and giving back to make the world a safer and better place.

A global organization with a global outlook

Trend Micro was founded in California in 1988 and has sustained steady growth since day one. Now as a global company with headquarters in Japan and operating in over 65 countries across the globe, we have built up a network equipped to continuously monitor global and regional threats. This enables Trend Micro to respond quickly by providing smart, optimized, and connected solutions for our customers.

Trend Micro international locations

Americas

Ottawa
Toronto
Dallas
Austin
Chicago
Jersey City
Minneapolis
Pasadena
Reston
Roseville
San Jose
Seattle
Porto Alegre
Rio de Janeiro
São Paulo
Brasília
Mexico City

Europe

Vienna
Mechelen
Prague
Copenhagen
Espoo
Paris
Munich
Cork
Milan
Rome
Luxembourg
Amsterdam
Oslo
Warsaw
Madrid
Stockholm
Lausanne
Wallisellen
London
Moscow

Middle East & Africa

Cairo
Riyadh
Istanbul
Dubai
Tel Aviv
Johannesburg

Asia Pacific

Tokyo (Headquarters)
Osaka
Fukuoka
Nagoya
Sydney
Melbourne
Perth
Brisbane
Canberra
Auckland
Beijing
Guangzhou
Shanghai
Nanjing
Wanchai
New Delhi
Mumbai
Bangalore
Jakarta
Seoul
Kuala Lumpur
Manila
Singapore
Taipei
Hsinchu
Bangkok
Hanoi

Management

Eva Chen
CEO

Mahendra Negi
CFO

Akihiko Omikawa
Executive Vice President, Japan and Global Consumer Business

Kevin Simzer
Chief Operating Officer

Oscar Chang
Executive Vice President, Research and Development

Max Cheng
Executive Vice President, Core Technology and CIO

Leah MacMillan
Chief Marketing Officer

Steve Quane
Executive Vice President, Network Defense and Hybrid Cloud Security

Felix S. Sterling
Chief Legal Officer and Executive Vice President, Global Policy and Compliance

Traded
Tokyo Stock Exchange 4704

Headquarters
Toyko, Japan

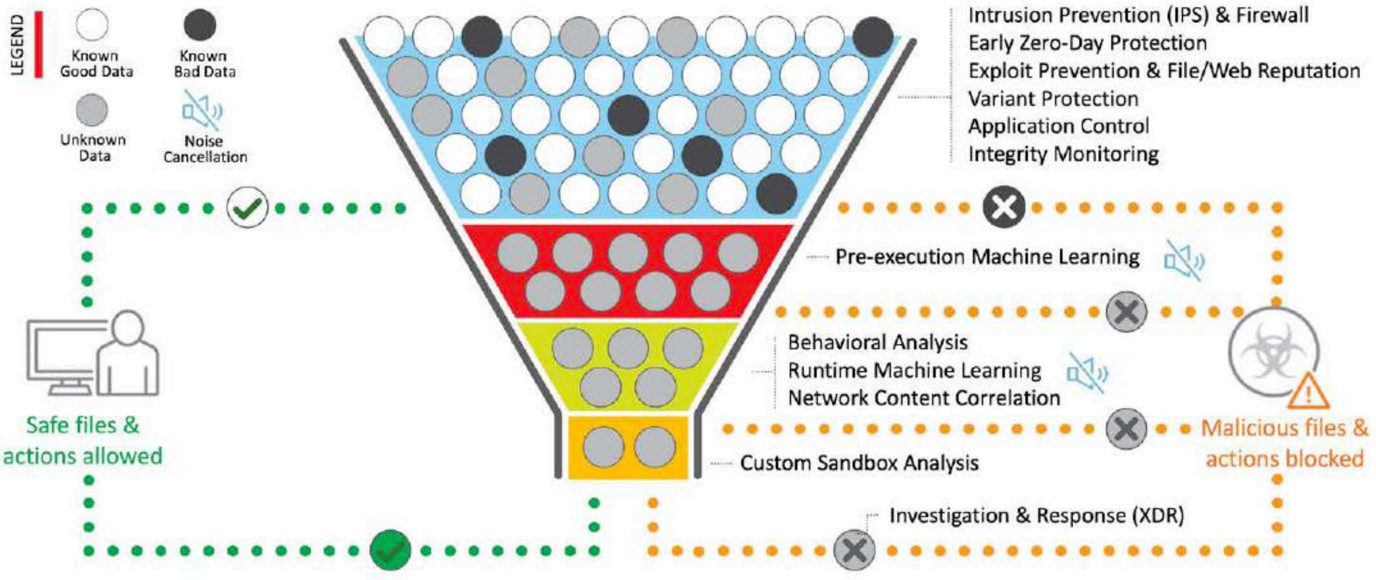
02 OUR TECHNOLOGY STRATEGY

XGen™ security

Our strategic approach to security goes beyond next-gen to address the full range of ever-changing threats—now and in the future. Instead of using separate, siloed security solutions that don't share information, XGen™ security provides a cross-generational blend of threat defense techniques along with a connected threat defense approach to protect your organization from unseen threats.

XGen™ security uses proven techniques to quickly identify known good or bad data, allowing advanced systems to detect unknown threats more quickly and accurately. Utilizing the right techniques at the right time, regardless of location and device, this identification maximizes both visibility and performance. This core set of techniques powers each of the Trend Micro solutions—hybrid cloud, network, and user environments—in a way that is optimized for each layer of security.

XGen™ security delivers the right techniques at the right time


LEGEND
Known Good Data
Known Bad Data
Unknown Data
Noise Cancellation
Intrusion Prevention (IPS) & Firewall
Early Zero-Day Protection
Exploit Prevention & File/Web Reputation
Variant Protection
Application Control
Integrity Monitoring
Pre-execution Machine Learning
Behavioral Analysis
Runtime Machine Learning
Network Content Correlation
Custom Sandbox Analysis
Investigation & Response (XDR)
Safe files & actions allowed
Malicious files & actions blocked

Trend Micro solutions, powered by XGen™ security, are:

Smart

Defends against the entire range of known and unknown threats with a cross-generational combination of defense technologies. Powered by global threat intelligence, Trend Micro solutions employ the right method when needed.

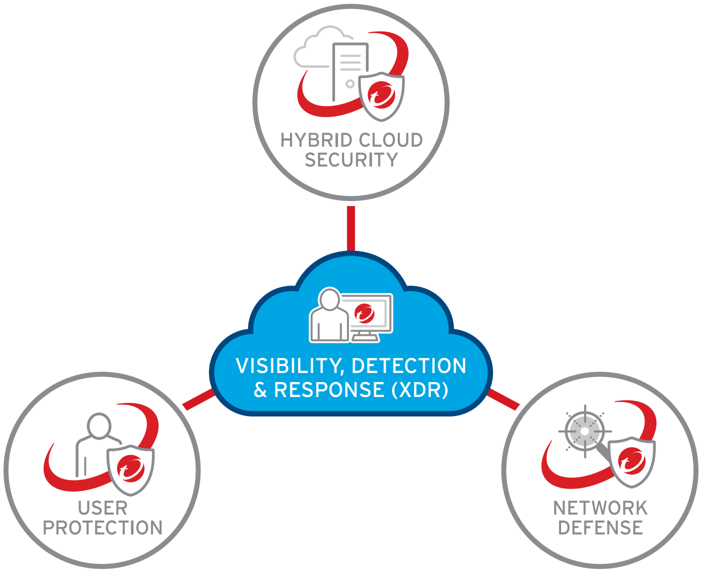
Optimized

Delivers security solutions to protect users, networks, and hybrid cloud environments.

Trend Micro solutions are specifically designed for and tightly integrated with leading platforms and applications.

aws Azure Google Cloud

Microsoft 365 vmware®



Connected

Speeds time to response with centralized visibility and investigation, with automatic sharing of threat intelligence across security layers.

Threat Intelligence

The Trend Micro™ Smart Protection Network™

The Trend Micro Smart Protection Network continually monitors and collects threat data from around the world. The Smart Protection Network employs advanced detection analytics to enable our products to instantly stop attacks before they can do you harm. Plus, the same accelerated cloud security powers all of our products and services, protecting millions of businesses and users across the globe.

By the numbers

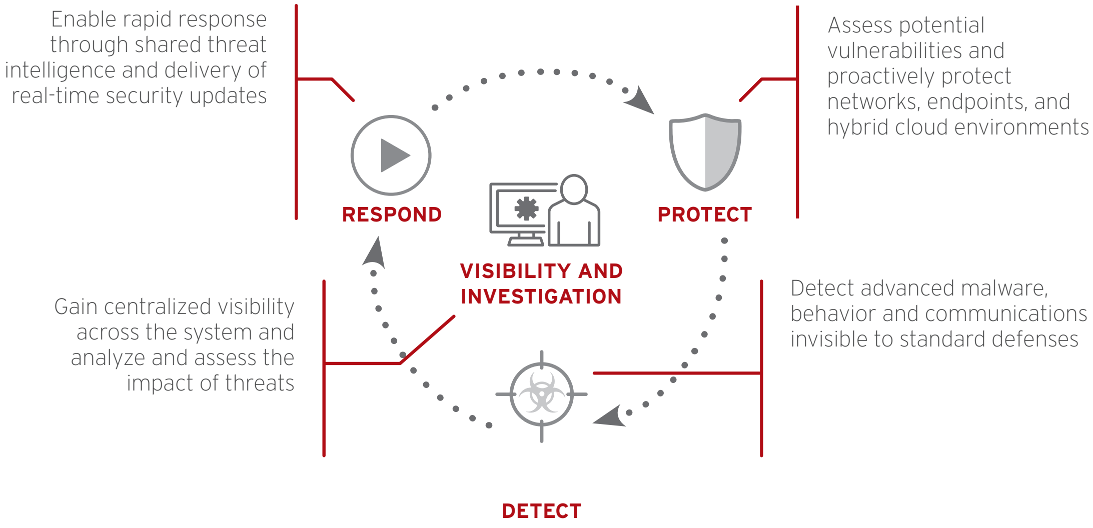
The Trend Micro Smart Protection Network:

- Leverages data from over 250 million global sensors.
- Receives trillions of threat queries per year.
- Identifies billions of new, unique threats yearly.
- Enables our solutions to block hundreds of millions of threats targeting our customers daily.
- Analyses hundreds of terabytes of threat data per day.

Connected Threat Defense

Protection from advanced threats

Trend Micro™ Connected Threat Defense™ is a layered security approach that gives you a better way to quickly protect, detect, and respond to new and targeted threats while simultaneously improving visibility and investigation throughout the corporate network.



Enable rapid response through shared threat intelligence and delivery of real-time security updates

Assess potential vulnerabilities and proactively protect networks, endpoints, and hybrid cloud environments

Gain centralized visibility across the system and analyze and assess the impact of threats

Detect advanced malware, behavior and communications invisible to standard defenses

Connected Threat Defense in Action

Here is how a Connected Threat Defense approach can help:

- The attack begins with the arrival of an email in a user's inbox, complete with an attachment containing a zero-day information-stealing threat. It could be stopped at the "Protection" stage by any of the numerous advanced security techniques.
- However, this zero-day threat has been designed to bypass traditional techniques, which makes the "Detection" stage vital. The messaging layer submits the attachment to the sandbox which identifies the file as malicious, but also identifies command and control (C&C) communication data.
- After analysis of a sophisticated threat must come the response via prioritized analysis of all environments for additional potential related threats. In addition, response should include real-time data sharing across all endpoint, server, and network security components. Failure to do this means the threat won't be blocked automatically the next time it's encountered—multiplying risk.
- "Response" also includes remediation steps like automatically cleaning computers of any malware, and in doing so, maximizing user productivity.
- With Central Visibility, organizations can quickly see who else got that email or threat and respond before it spreads laterally through the network.

Protection for the entire threat life cycle

In today's complex threat landscape, organizations often employ a wide variety of security products to defend against increasingly sophisticated attacks, though managing several security solutions can turn into an expensive, time-consuming, and complex task. Trend Micro Connected Threat Defense provides a comprehensive view of your company's networks, endpoints, email, and hybrid cloud environments. This layered approach provides a better way of protecting and detecting threats and responding to them.

RESPONSE

The response is the next critical step after a threat has been detected. Through Trend Micro™ XDR, this quadrant delivers prioritized alerts based on one expert alert schema to interpret data in a standard and meaningful way, a consolidated view to uncover events and the attack path across security layers, and guided investigations to understand the impact and identify the path to resolution.

PROTECTION

The protection quadrant focuses on proactively defending your networks, endpoints, email, and hybrid cloud environments. Trend Micro solutions incorporates a cross-generational blend of protection techniques. This includes highly-effective traditional approaches like anti-malware, intrusion prevention, whitelisting, encryption, and data loss prevention. They also include state-of-the-art techniques like high fidelity machine learning and behavior analysis.

VISIBILITY AND INVESTIGATION

These connected elements give you comprehensive visibility of your email, endpoints, networks, servers, hybrid cloud environments, and network. Integration between these quadrants makes it possible to have visibility and share threat intelligence across all security layers. This results in simplified threat investigation and security management through centralized visibility and reporting.

DETECTION

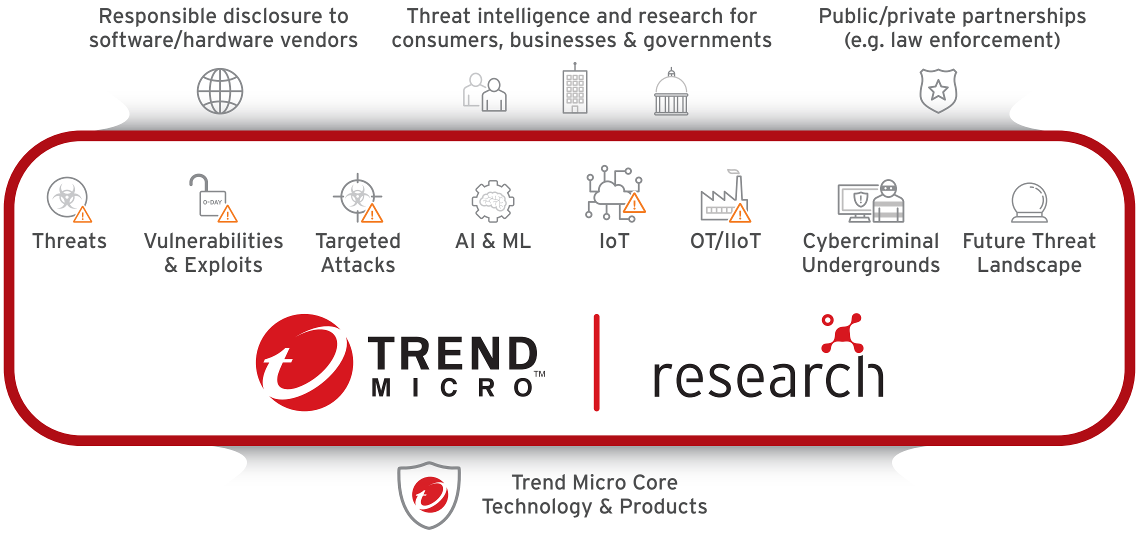
Despite the strength of its techniques, the "Protection" quadrant will not block 100% of malware or attacks. That's why you need the "Detection" quadrant to employ techniques that will help you to detect advanced malware, malicious behavior, and communications invisible to standard defenses. Trend Micro XDR applies the most effective AI and expert analytics to the activity data, producing fewer, higher-fidelity alerts. Global threat intelligence from the Smart Protection Network, combined with expert detection rules continually updated from our threat experts, maximize the power of AI and analytical mode to limit malicious applications and their impact on your system.

03 TREND MICRO RESEARCH

Trend Micro Research

Keeping up with today's threat landscape is non-negotiable. Enterprises, service providers, and the internet-at-large benefit from knowing the latest in technology and threats so they can actively secure their data and systems against compromise. Skimming security news provides a high-level idea of what's going on in the real world, but to build effective security strategies, organizations and individuals need to get a better look of what goes on beyond the surface.

For over three decades, Trend Micro Research, our global threat research organization has helped us successfully bet on upcoming technology trends–proactively securing new environments like virtualization, cloud, and containers so you can take full advantage of them. Our research doesn't just provide our solutions with industry knowledge so your organization can react faster, but responsibly discloses new threat information to software and hardware vendors as well as public organizations like the FBI.


Responsible disclosure to software/hardware vendors
Threat intelligence and research for consumers, businesses & governments
Public/private partnerships (e.g. law enforcement)
Threats
Vulnerabilities & Exploits
Targeted Attacks
AI & ML
IoT
OT/IIoT
Cybercriminal Undergrounds
Future Threat Landscape
TREND MICRO
research
Trend Micro Core Technology & Products

Trend Micro Research has:

- Hundreds of internal threat researchers and data scientists.
- Over 10,000 external white hat researchers supporting our bug bounty program, The Zero Day Initiative™.
- Invested in AI and machine learning since 2005.
- Remained the top reporter of Microsoft and Adobe vulnerabilities worldwide.
- Detected 1.8B+ suspicious events and attacks in home networks alone in 2019.
- Remains the top vulnerability supplier for ICS-CERT.

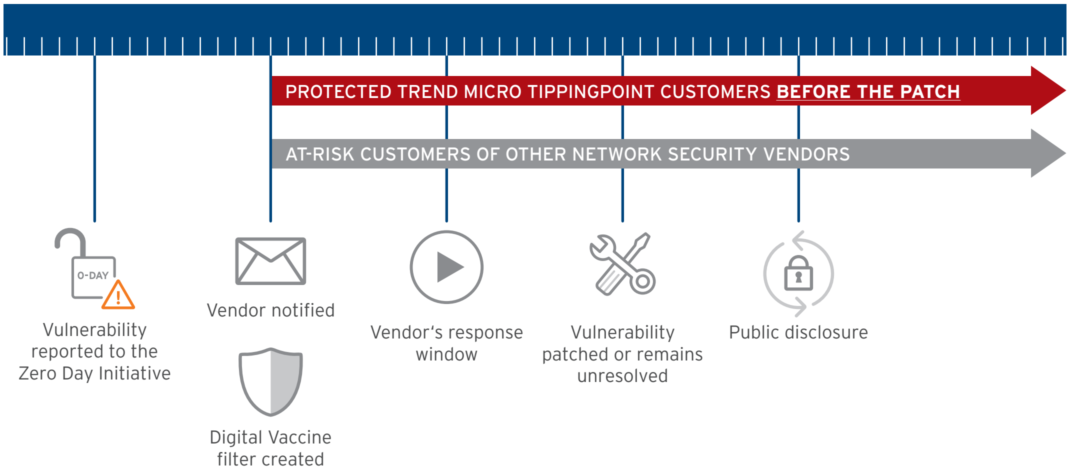
How do Trend Micro customers benefit from Trend Micro Research?

Trend Micro Research ultimately leads to more secure products and better protection for customers. This includes research on current, potential, and future threats. For example, without the help of our vulnerability research and bug bounty program, the Zero Day Initiative™, many vulnerabilities would remain undisclosed or would be sold on the black market and used for malicious purposes. Before the vendor delivers a patch, customers already benefit from pre-emptive protection because they have exclusive access to vulnerability intelligence reported to the Zero Day Initiative. They also get protection for older software, even if it is no longer supported.

Thanks to our established relationships with leading software vendors and the research community, we will continue to improve security in the product development cycle.

Zero Day Initiative

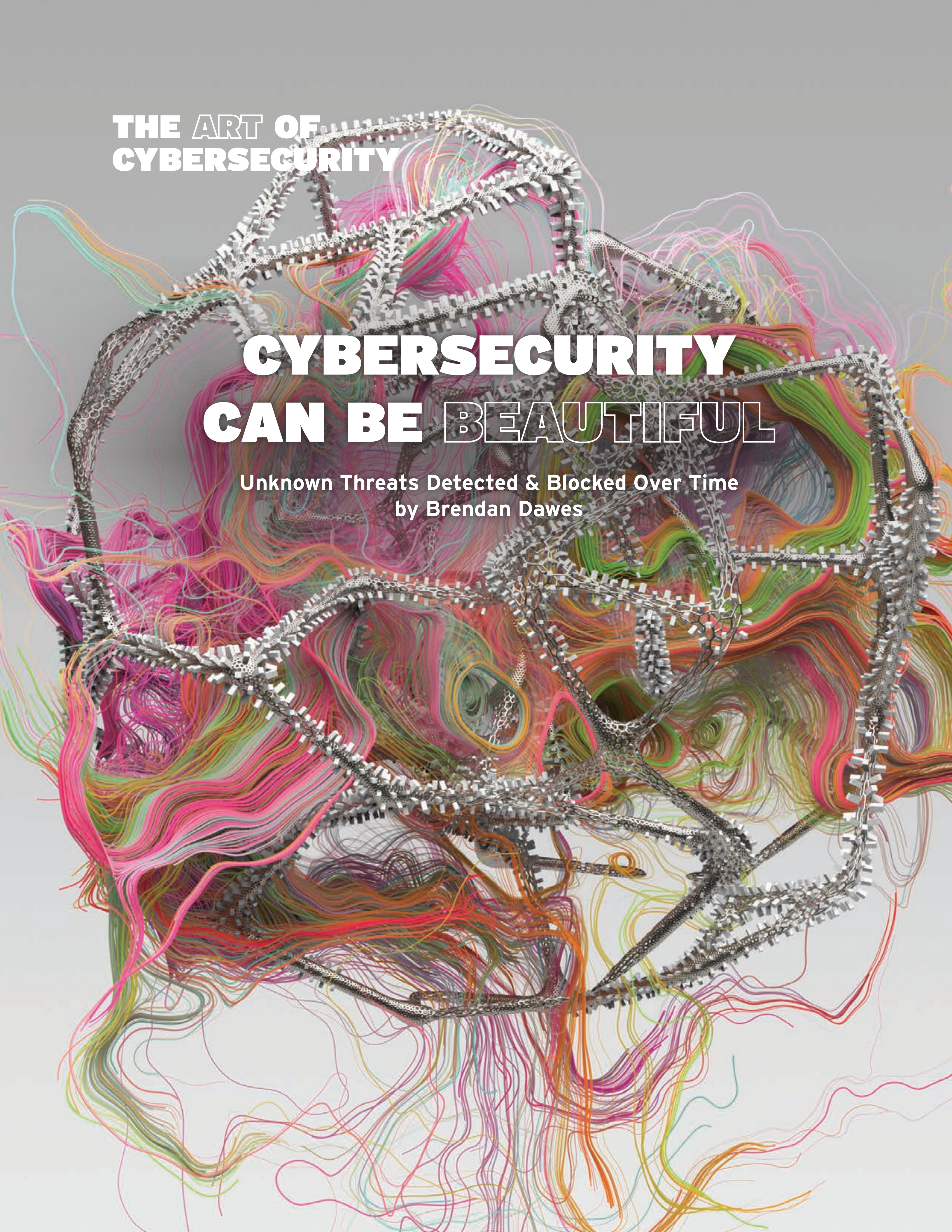
The Zero Day Initiative™, as a part of Trend Micro Research, conducts its own investigations internally, while the external community of over 10,000 researchers continues to provide a valuable contribution to the program.


PROTECTED TREND MICRO TIPPINGPOINT CUSTOMERS BEFORE THE PATCH
AT-RISK CUSTOMERS OF OTHER NETWORK SECURITY VENDORS
0-DAY
Vulnerability reported to the Zero Day Initiative
Vendor notified
Digital Vaccine filter created
Vendor's response window
Vulnerability patched or remains unresolved
Public disclosure

Hunting for vulnerabilities in software is unfortunately still considered a shady practice, giving rise to the perception that it is done only by hackers for nefarious purposes. While skilled, malicious attackers do exist, they remain a small minority of the total number of people who actually discover new flaws in software. A much larger group are dedicated researchers with the requisite expertise who discover vulnerabilities as part of their daily security work.

Find out more about the program at **https://www.zerodayinitiative.com**.

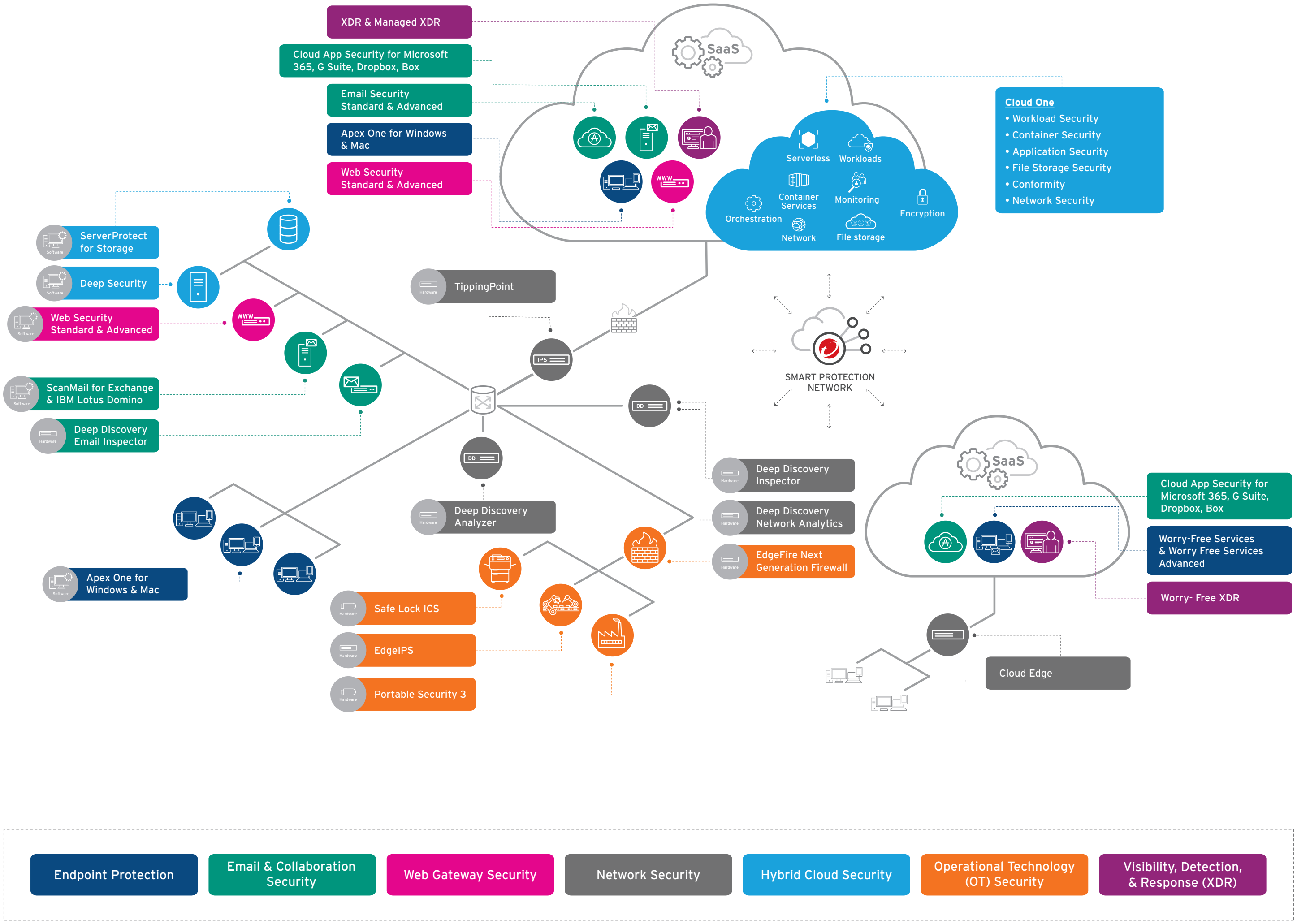
CYBERSECURITY CAN BE BEAUTIFUL



Unknown Threats Detected & Blocked Over Time
by Brendan Dawes

04 OVERVIEW OF SOLUTIONS

For over 30 years, Trend Micro has been singularly focused on developing security solutions to protect our customers. Our comprehensive portfolio includes solutions across multiple IT layers, from endpoints and email, to data centers, the cloud, as well as the network. As the leading[1] cloud and virtualization security provider, Trend Micro is able to provide optimal support for its customers in implementing cloud and virtualization projects. We also offer solutions for our customers to meet the challenges posed by targeted attacks, compliance requirements such as the General Data Protection Regulation (GDPR), and best practices for BYOD. Companies also benefit from reduced operating and management expenses for IT security.


XDR & Managed XDR
Cloud App Security for Microsoft 365, G Suite, Dropbox, Box
Email Security Standard & Advanced
Apex One for Windows & Mac
Web Security Standard & Advanced
SaaS
Serverless
Workloads
Container Services
Monitoring
Orchestration
Encryption
Network
File storage
Cloud One
• Workload Security
• Container Security
• Application Security
• File Storage Security
• Conformity
• Network Security
ServerProtect for Storage
Deep Security
Web Security Standard & Advanced
ScanMail for Exchange & IBM Lotus Domino
Deep Discovery Email Inspector
Apex One for Windows & Mac
TippingPoint
IPS
DD
SMART PROTECTION NETWORK
Deep Discovery Analyzer
Deep Discovery Inspector
Deep Discovery Network Analytics
EdgeFire Next Generation Firewall
Safe Lock ICS
EdgeIPS
Portable Security 3
SaaS
Cloud App Security for Microsoft 365, G Suite, Dropbox, Box
Worry-Free Services & Worry Free Services Advanced
Worry- Free XDR
Cloud Edge
Endpoint Protection
Email & Collaboration Security
Web Gateway Security
Network Security
Hybrid Cloud Security
Operational Technology (OT) Security
Visibility, Detection, & Response (XDR)

[1] Source: IDC, 2019

Key	
Included	✓
Additional product required	▲
Limited features	◆
Not included	–

User Protection Solution

Suites	Malware Protection	Web Reputation	Firewall	Machine Learning	IDS/IPS	Application Control	DLP	Sandbox Analysis	Device Control	Endpoint Encryption	Mobile Security	Optimized for VDI Environments	Mail Gateway	Cloud Email/App Protection	Web Gateway	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Smart Protection Complete	✓	✓	✓	✓	✓	✓	✓	▲	✓	✓	✓	✓	✓	✓	✓	▲	▲
Smart Protection for Endpoint	✓	✓	✓	✓	✓	✓	✓	▲	✓	✓	✓	✓	–	–	–	▲	▲
XDR for Users	✓	✓	✓	✓	✓	✓	✓	▲	✓	–	–	✓	–	✓	–	✓	▲

Endpoint	Malware Protection	Web Reputation	Firewall	Machine Learning	IDS/IPS	Application Control	DLP	Sandbox Analysis	Device Control	Obtain Suspicious Objects	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Apex One and Apex One as a Service (Windows endpoint)	✓	✓	✓	✓	✓	✓	✓	▲	✓	▲	▲	▲
Apex One and Apex One as a Service (Mac endpoint)	✓	✓	–	✓	–	–	–	–	✓	–	▲	▲

Email and Collaboration	Malware Protection	Web Reputation	Spam Protection	Phishing Protection	Internal Email Protection	DLP	Email Encryption	Sandbox Analysis	Obtain Suspicous Objects	BEC	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Cloud App Security	✓	✓	◆	✓	✓	✓	–	✓	✓	✓	▲	▲
Email Security Standard	✓	✓	✓	✓	–	✓	✓	–	✓	✓	▲	▲
Email Security Advanced	✓	✓	✓	✓	–	✓	✓	✓	✓	✓	–	–
ScanMail for Microsoft Exchange	✓	✓	✓	✓	✓	✓	–	▲	▲	✓	–	–
ScanMail for IBM Domino	✓	✓	✓	✓	✓	✓	–	▲	▲	–	–	–
Deep Discovery Email Inspector	✓	✓	✓	✓	–	✓	✓	✓	✓	✓	–	–

Web Gateway	Malware Protection	Web Reputation	URL Filter	Machine Learning	Cloud App Access Control	DLP	Application Control	HTTPS/ SSL	Sandbox Analysis	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Web Security Standard	✓	✓	✓	–	–	–	✓	✓	–	–	–
Web Security Advanced	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Small Business

	Malware Protection	Web Reputation	Firewall	Machine Learning	URL Filter	Spam Protection	DLP	Sandbox Analysis	Device Control	Phishing Protection	Protection for Mac	Mobile Security	Email Protection	Detection & Response (XDR)
Worry-Free Services	✓	✓	✓	✓	✓	–	✓	–	◆	–	✓	◆	–	–
Worry-Free Services Advanced	✓	✓	✓	✓	✓	✓	✓	–	◆	✓	✓	◆	✓	–
Worry-Free XDR	✓	✓	✓	✓	✓	✓	✓	✓	◆	✓	✓	◆	✓	✓
Cloud App Security	✓	✓	–	✓	–	–	✓	✓	–	✓	–	–	✓	▲
Cloud Edge*	✓	✓	✓	✓	✓	✓	–	✓	–	✓	–	–	✓	–

**Cloud Edge is available only to MSP partners*

Hybrid Cloud Security Solution

	Malware Detection / Protection	Analysis & Machine Learning	Web Reputation	Host Firewall	IDS/IPS (Virtual Patching) / Vulnerability Scanning	File Integrity Monitoring	Application Control	Log inspection	Secrets (Passwords / Keys) / IoC Scanning	Compliance Scanning	Web App Threat Detection / Protection	SAP Security	Sandbox Analysis/ Suspicious Objects	Agentless VM / VDI Protection*	Cloud File Storage Security (e.g. S3)	Container Image Scanning	Cloud Infrastructure Posture & Visability	Serverless & Web Application Security	DevOps / API Ready	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Software																					
Deep Security Software	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	▲	✓	✓	–	–	–	–	✓	–	▲
Deep Security Smart Check - Container Image Security	✓	✓	–	–	✓	–	–	–	✓	✓	–	–	–	–	–	✓	–	–	✓	–	–
Deep Security Smart Check - File Storage Security	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	✓	–	–
ServerProtect for Storage	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

	Malware Detection / Protection	Analysis & Machine Learning	Web Reputation	Host Firewall	IDS/IPS (Virtual Patching) / Vulnerability Scanning	File Integrity Monitoring	Application Control	Log inspection	Secrets (Passwords / Keys) / IoC Scanning	Compliance Scanning	Web App Threat Detection / Protection	SAP Security	Sandbox Analysis/ Suspicious Objects	Agentless VM / VDI Protection*	Cloud File Storage Security (e.g. S3)	Container Image Scanning	Cloud Infrastructure Posture & Visability	Serverless & Web Application Security	DevOps / API Ready	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
SaaS																					
Cloud One - Workload Security	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	✓	▲	▲
Cloud One - Container Security	✓	✓	–	–	✓	–	–	–	✓	✓	–	–	–	–	–	✓	–	–	✓	–	–
Cloud One - Application Security	✓	✓**	–	–	✓	–	–	–	–	–	✓	–	–	–	–	–	–	✓	✓	–	–
Cloud One - Network Security	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–
Cloud One - File Storage Security	✓	–	–	–	–	–	–	–	✓	✓	–	–	–	–	✓	–	–	–	✓	–	–
Cloud One - Conformity	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	✓	–	–

*VMware with NSX
**Behavioural analysis for Application Security – studies the behaviour of the application

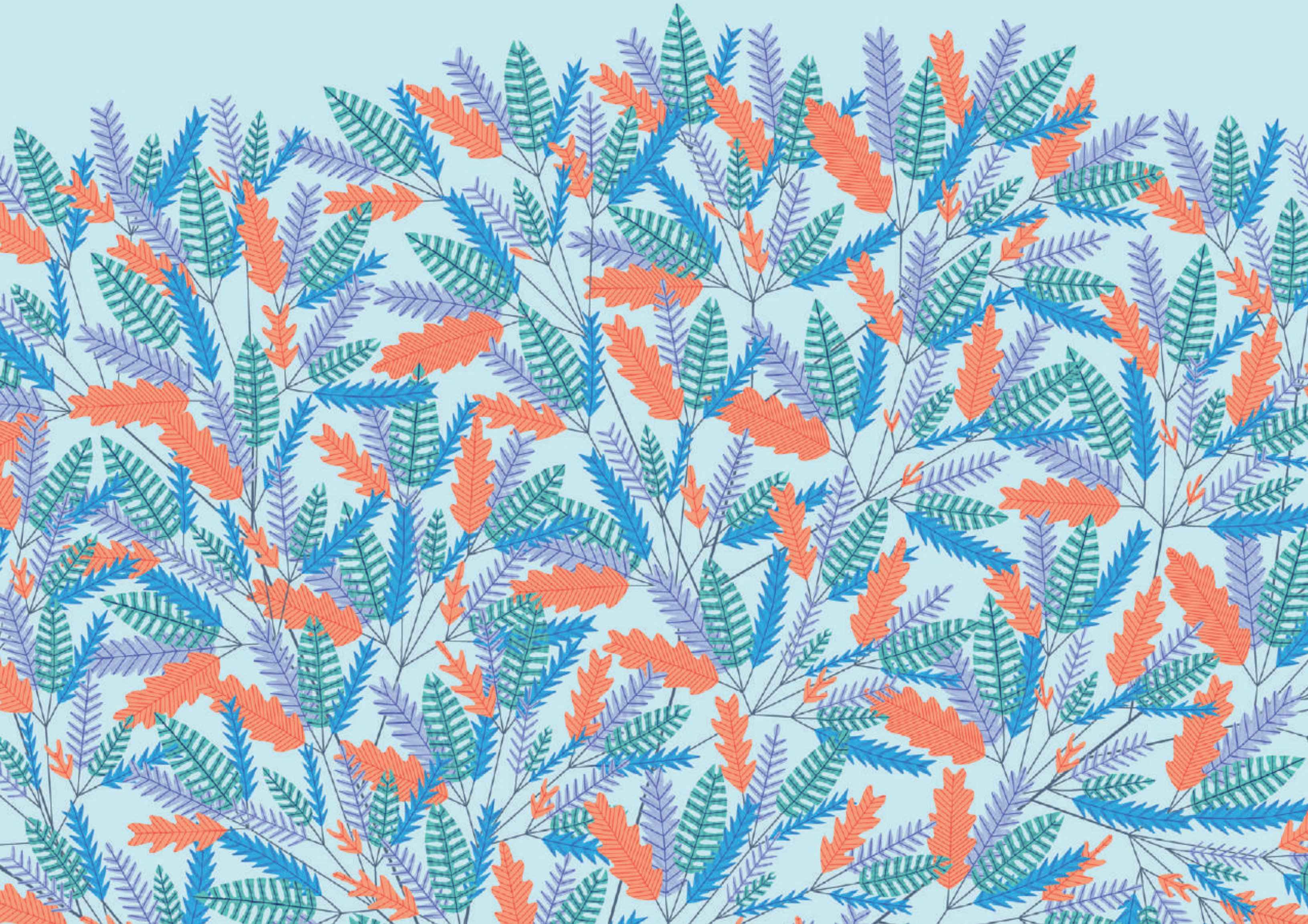
Network Defense Solution

Network Security	Detection of Entry Points	Detection of C&C Communications	Detection of Internal Spread	Analysis of Known Threats	Analysis of Unknown Threats	Blocking	Submission of Suspicious Threats	Sandbox Analysis	Submission of "Indicators of Compromise"	Correlation of Threat Events	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Deep Discovery Inspector	✓	✓	✓	✓	✓	–	✓	✓	✓	–	▲	▲
Deep Discover Analyzer	▲	✓		✓	✓	–	✓	✓	✓	–	▲	–
Deep Discovery Network Analytics	▲	▲	▲	▲	▲	–	–	–	–	✓	✓	–
TippingPoint TX Series	✓	✓	✓	✓	✓	✓	–	▲	–	–	–	–

Operational Technology Security	Network Routing / Segmentation	Asset Detection	Intrusion Prevention	Lateral Movement Visibility and Protection	ICS Protocol Filtering	IP and Protocol Filtering	Malware Protection	Application Control	System Lockdown	Detection & Response (XDR)	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
TXOne EdgeFire	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
TXOne EdgeIPS	–	✓	✓	✓	✓	✓	–	–	–	–	–	–
Safe Lock ICS	–	–	–	–	–	–	–	✓	✓	–	–	–
Portable Security 3	–	–	–	–	–	–	✓	–	–	–	–	–

CYBERSECURITY CAN BE BEAUTIFUL

Endpoint Threats Detected & Blocked Over Time
by Stefanie Posavec



05 USER PROTECTION

Trend Micro user protection strategy brings you security that can adapt, predict, and stay ahead of today's ever-changing threats; like fileless malware, targeted attacks, ransomware, and cryptocurrency mining.

Our solutions apply multiple layers of protection across endpoint, email, web, and software as a service (SaaS) applications to protect your users regardless of device, application, network, or location.

User Protection Suites

Maximum protection with minimal resource footprint

Trend Micro™ Smart Protection™ Suites, powered by XGen™ security, employs a combination of threat protection technologies to eliminate security gaps in all user activities and at every endpoint. A single, streamlined agent for comprehensive security, including detection, investigation, response, and data protection provides you with:

- Connected, layered security
- Maximum flexibility—on-premises or SaaS

	Smart Protection Complete (SaaS and on-prem)	Smart Protection for Endpoint (SaaS and on-prem)	XDR for Users (SaaS only)
Central Management	✓	✓	✓
Endpoint Security Advanced detection and response Application control Vulnerability protection Data loss prevention	✓	✓	✓
Endpoint Encryption	✓	✓	
Mobile Security	✓	✓	
Web Security	✓		
Email and Collaboration Security Email gateway security Microsoft 365 and Gmail protection Collaboration security for cloud sharing	✓		(Microsoft 365 and Gmail protection)
Endpoint Detection and Response Expanded value with XDR—available for endpoints and email	Optional	Optional	✓
Managed Detection and Response Expanded value with XDR—Available for email, endpoint, servers, cloud workloads, and network	Optional	Optional	Optional
Sandbox as a Service	Optional	Optional	Optional

Smart Protect Suites are available in two options:

	Smart Protection for Endpoints	Smart Protection Complete
TOOLS TO SIMPLIFY ONGOING MANAGEMENT AND SUPPORT OF THE SOLUTION		
Central Management	✓	✓
On-premises, Cloud, or Hybrid Deployment	✓	✓
24/7 Support	✓	✓
Integrated Data Loss Prevention	✓	✓
ENDPOINT		
XGen™ Anti-Malware	✓	✓
Vulnerability Protection	✓	✓
Virtual Desktop Integration	✓	✓
Mac and Windows Security	✓	✓
Server Security	✓	✓
Endpoint Application Control	✓	✓
Endpoint Encryption	✓	✓
Mobile Security and Management	✓	✓
Advanced Detection and Response	✓	✓
EMAIL AND COLLABORATION		
Messaging Gateway		✓
Mail Server Security for Microsoft Exchange		✓
Mail Server Security for IBM Domino		✓
Instant Messaging Security for Microsoft Lync		✓
Microsoft SharePoint Security		✓
Security for Microsoft 365, Box, Dropbox, Google G Suite		✓
WEB		
Secure Web Gateway		✓

Trend Micro™ Smart Protection™ Complete

Trend Micro™ Smart Protection™ for Microsoft 365

Smart Protection for Microsoft 365 offers two valuable Trend Micro products in one bundle; Trend Micro™ Email Security Advanced and Trend Micro™ Cloud App Security. The dual layer email protection combines the benefits of both email gateway and API-based service integration.

Email Security Advanced is a secure email gateway service that uses an optimum blend of cross-generational threat techniques to stop phishing, ransomware, business email compromise (BEC), spam, and other advanced email threats before they reach your network.

Cloud App Security provides a second layer of protection at the email service layer. It protects incoming and internal email from advanced malware and other threats. It also enforces compliance on cloud file sharing and collaboration services, including Box™, Dropbox™, Google Drive™, Microsoft® SharePoint®, and Microsoft® OneDrive®.

Expand your smart protection with the following features:

Endpoint detection and response (EDR) investigate targeted attacks with integrated tools such as 24/7 alert monitoring and threat hunting services, along with sandboxing as a service to analyze suspicious objects. This service is also available as managed endpoint detection and response.

Trend Micro™ Smart Protection for Endpoints

Trend Micro Smart Protection for Endpoints are smart, optimized, and connected to provide optimal protection for users.

Smart

Innovative solutions are powered by a unique blend of XGen™ cross-generational threat defense techniques and market-leading global threat intelligence that protect more effectively across the broad range of threats. This includes ransomware, malware, exploits, business email compromise (BEC), vulnerabilities, fileless malware, and more.

Optimized

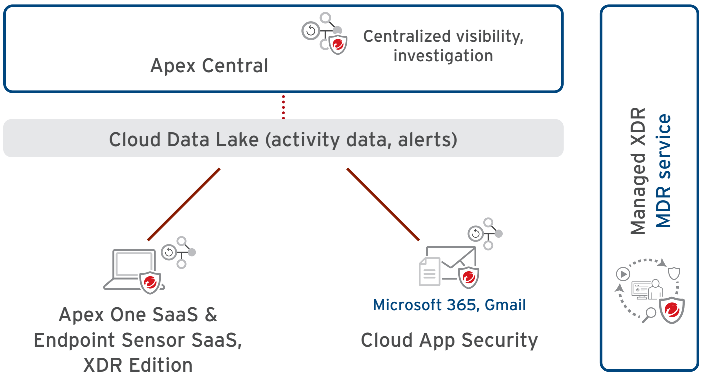
Smart Protection for Endpoints minimizes IT and administrator impact with efficient solutions that are specifically designed for and integrated with leading customer platforms (endpoint and mobile), enterprise business applications, and cloud applications.

Connected

Smart Protection for Endpoints speeds time to response with centralized visibility and control and automatic sharing of threat intelligence across security solutions (or layers).

Trend Micro™ XDR for Users

Trend Micro XDR for Users is a complete software-as-a-service (SaaS) offering that includes protection, detection, and response across endpoints and email through Trend Micro Apex One™ and Trend Micro™ Cloud App Security solutions. It also includes Trend Micro Apex Central™, a centralized management console where users can view all available detection and threat information, and perform investigation tasks like indicators of compromise (IoC) sweeping, root cause analysis, and threat hunting. With XDR for Users, customers can respond more effectively to threats, minimizing the severity and scope of a breach.


Apex Central
Centralized visibility, investigation
Cloud Data Lake (activity data, alerts)
Apex One SaaS & Endpoint Sensor SaaS, XDR Edition
Microsoft 365, Gmail
Cloud App Security
Managed XDR
MDR service

Key protection capabilities

- High-fidelity machine learning (pre-execution and runtime).
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks).
- Web reputation.
- Exploit prevention (host firewall, exploit protection).
- Command and control (C&C) blocking.
- Vulnerability protection.
- Application control.
- Data loss prevention (DLP).
- Device control.
- Sandbox and breach detection integration.
- Inbound and internal phishing protection.
- Credential phishing detection with computer vision.
- Business email compromise detection with writing style analysis.

Key detection and response features

- IoC sweeping.
- IoA hunting.
- Root cause analysis.
- Impact analysis.
- Automated response.
- Open APIs and custom intelligence.

Endpoint Protection

The threat landscape used to be black and white—you kept the bad stuff away from your network and kept valuable data from being lost. Now it is harder to tell the good from the bad. Traditional, signature-based approaches to antivirus security alone are only a weak line of defense against ransomware and unknown threats that often slip through. Installing multiple anti-malware tools on a single endpoint quickly results in confusion and too many products that do not work together. Further complicating matters is the increasing number of employees who access company resources or even cloud services from a variety of locations and devices. Companies need smart, optimized, and connected endpoint security from a trusted provider you can truly rely on.

Trend Micro Apex One™—endpoint security redefined

Automated

Effective detection & response

- Blocks the latest threats, including fileless attacks and ransomware
- The industry's most up-to-date vulnerability protection—immediate protection against distribution, usually before an official patch is even deployed

Actionable

Central visibility & control of all features

- Advanced EDR toolset, strong SIEM integration and open APIs
- MDR service option to assist security teams

All-in-one

Detection, Investigation & response

- All-in-one lightweight agent
- Flexible delivery options as software-as-a-service (SaaS) and on-premises

Apex One is an all-in-one package for modern endpoint security. With a single, lightweight agent on the endpoint, Apex One provides the functionality of Trend Micro™ OfficeScan™, Trend Micro™ Vulnerability Protection™, Trend Micro™ Application Control, and Trend Micro™ Endpoint Sensor. This greatly simplifies implementation and eliminates the need to deploy multiple products from different vendors

Apex One protects all PCs, Macs, and virtual desktops inside and outside the corporate network. The solution can be rolled out with almost the same features as software as a service (SaaS) and on-premises.

Depending on existing permissions, additional licenses may be required for specific features, such as EDR Investigation.

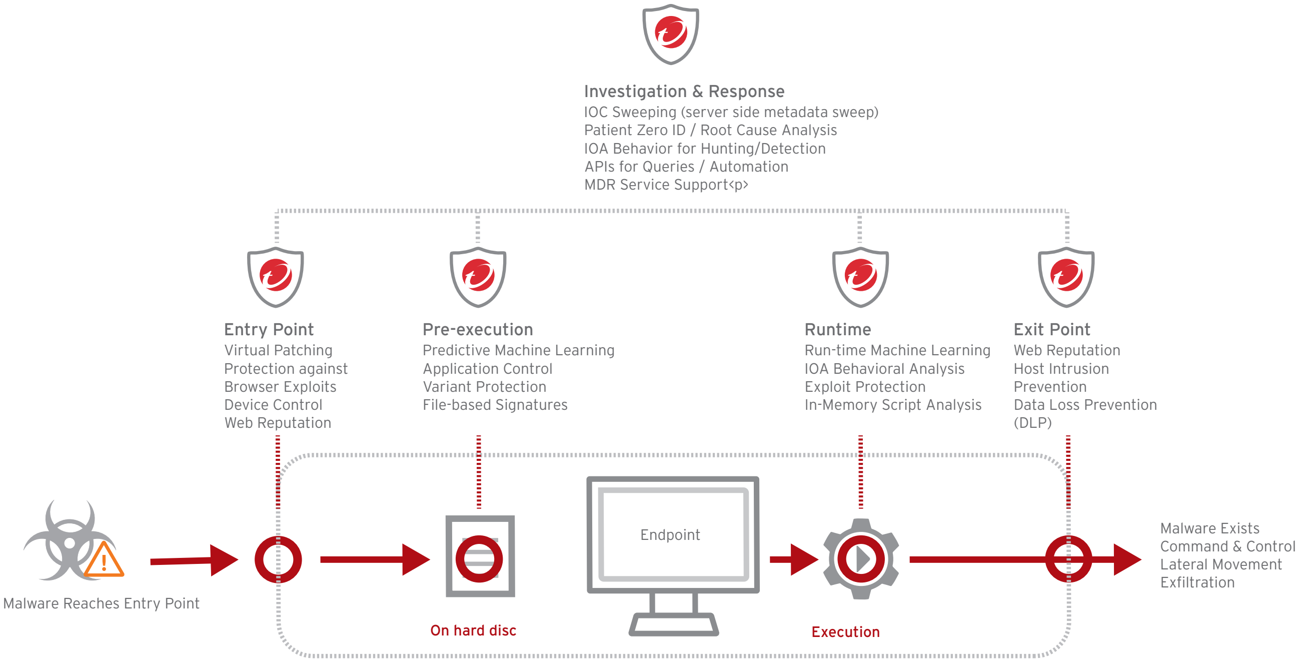
Apex One constantly learns, adapts, and automatically shares threat intelligence across the entire environment. This blend of protection is delivered via an architecture that uses resources more efficiently.

Benefits

- Protects against known and unknown threats with a single agent on the endpoint.
- Always utilizes the best technology for the situation, including machine learning, behavioral analysis, application controls, web and file reputation.
- Ensures the industry's fastest vulnerability screening based on leading vulnerability research.
- Integrates highly advanced EDR features and the optional managed detection and response (MDR) service in which Trend Micro handles the threat hunting.
- Communicates with other local security products and uses up-to-date information from the Trend Micro Smart Protection Network.
- Provides centralized visibility and control over the entire functionality via a single console when deployed through Trend Micro Apex Central.
- Integrates mobile security through Apex Central, including protection for mobile devices and mobile app/mobile device management.
- Enables adaptation to individual requirements using optional modules.
- Simplifies provisioning thanks to software-as-a-service and on-premises options.

Trend Micro Apex One™ Security for Mac

- Advanced detection capabilities such as machine learning and an option for EDR.
- Reduces exposure to web-based threats, including Mac-targeting malware.
- Adheres to Mac OS X look and feel for positive user experience.
- Saves time and effort with centralized management across endpoints, including Macs.



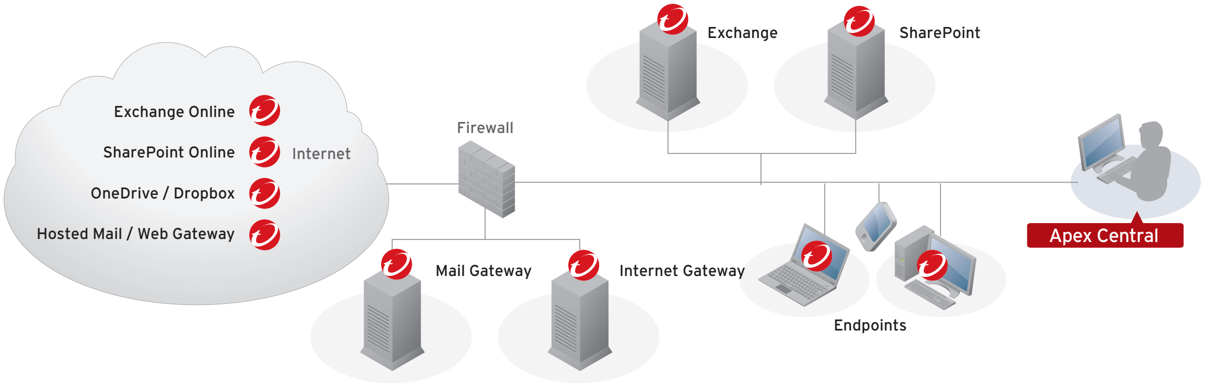
Features

- **Web reputation:** Blocks connections at the kernel level (not only in web browsers).
- **Predictive machine learning:** Evaluates files against cloud-based or local/offline models to detect previously unknown threats.
- **Runtime machine learning:** Evaluates real-time behavior against a cloud model to detect previously unknown threats.
- **IoA behavioral analysis:** Detects behavior matching known indicators of attack (IoA), including encryption by ransomware and script launches.
- **Virtual patching:** Blocks new exploits with the industry's latest vulnerability research
- **Application control:** Blocks execution of everything not on the easy-to-manage whitelist.
- **Host intrusion prevention:** Detects and blocks lateral movement
- **Virtual desktop integration VDI plug-in (only in on-premises deployments):** Cleans, scans RAM, and monitors behavior.
  - Automatically detects whether an agent is located on a physical or virtual endpoint.
  - Reduces search time on virtual desktops.
- **Central visibility and control:** Integration with Apex Central provides convenient security management via a central console. Policies, events, and reporting are consolidated across multiple solutions.
- **Root cause analysis:** Monitor with the aid of EDR technology sand- box analysis.
- **Integrated DLP:** Trend Micro™ Data Loss Prevention™ (DLP) detects and blocks breaches of sensitive data on the endpoint.
- **Device control:** Blocks unknown removable media.
- **Protection against browser exploits:** Detects exploits based on script inspection and site behavior.
- **Detection of packed files:** Identifies packed malware in memory during unpacking and prior to execution.
- **Variant protection:** Detects malware mutations based on known code fragments.
- **File-based signatures:** Detects known malicious files (3 billion detections globally in H1 2018).
- **Runtime analysis in RAM:** Detection of malicious scripts, malicious code injection, and unpacking at runtime.

Features depend on licence purchased

Trend Micro Apex Central

Streamline administration of Trend Micro security solutions using Apex Central. This centralized visibility and management solution provides a single, integrated interface to manage, monitor, and report across multiple layers of security–delivered as a SaaS solution by Trend Micro Apex Central™ as a Service, or as an on-premises solution by Trend Micro Apex Central. Customizable dashboards provide the visibility and situational awareness that equip you to rapidly assess status, identify threats, and respond to incidents. User-based visibility (based on active directory integration) allows you to see what is happening across all endpoints, devices owned by your users as well as their email and web traffic. This enables you to review policy status and make changes across everything the user touches.



Features

Feature parity between SaaS (Apex Central as a Service) and on-premises (Apex Central).

- Continuously monitor and rapidly understand your security posture, identify threats and respond to incidents with up-to-the-minute situational awareness across your environment. In addition, when an attack makes its way in, you have the ability to investigate where it has spread.
- Intuitive, customizable interface gives you visibility across all security layers and users and lets you drill down to the specific information you are looking for.
- Security dashboards allow instant triage by giving administrators the ability to prioritize critical threat types, critical users or critical endpoints, so they can take action on the most pressing issues first.
- Configurable dashboards and reports, ad-hoc queries, and alerts give you the actionable information you need to ensure protection and compliance.
- Integration with your security operations center (SOC) is easily achieved through integration with leading SIEM solutions.
- Predefined reporting templates and customizable SQL reporting facilitates compliance with internal IT audit requirements and regulations.

Benefits

- **Reduces risks:** Ensures security insight and control.
- **Lowers costs:** Simplifies security management.
- **Minimizes complexity:** Creates an integrated, centrally managed security framework with unified defense function.

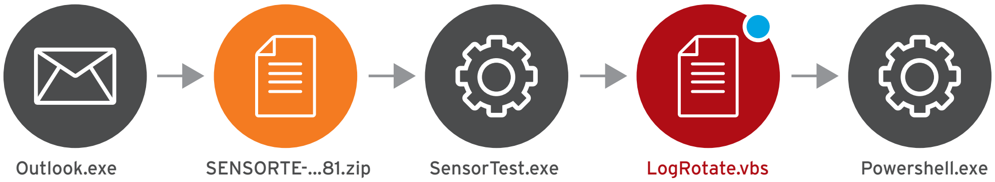
Endpoint Detection and Response

Endpoint detection and response (EDR) enables fast and reliable analysis of complex attacks, for example by root-cause or patient-zero investigations. Leading analyst firms like ESG Research are forecasting an 88% increase in detection and response spending over the 18 months, especially on solutions that include more than just the endpoint.[2] Solutions that combine endpoint protection with EDR will prove especially popular. Apex One already includes a number of advanced EDR features that can be expanded to a complete solution. It also delivers the ability to extend detection and response beyond the endpoint—XDR—with the same deployed solution. Simply leverage additional Trend Micro solutions for email, servers, cloud, and/or network, and realize the benefits of visibility and investigation across multiple environments.

Benefits

- Significantly easier handling through automation and integration.
- Context-aware investigations and faster responses for endpoints.
- Recording and detailed reporting of system-level activities.
- Detection and analysis of complex threat indicators, such as fileless attacks.
- Multi-level scans across endpoints using search criteria such as OpenIoC, YARA, and suspicious objects.
- Expand easily beyond the endpoint to XDR with the same deployed solution connecting to new Trend Micro security solutions.

Root Cause Analysis



Cloud Sandboxing

Trend Micro Apex One and Trend Micro Apex One™ as a Service provides additional security—through optional cloud sandboxing for automated, detailed simulations, and analysis of potentially dangerous file attachments—in a secure virtual environment hosted by Trend Micro. Cloud Sandboxing requires a separate paid license.

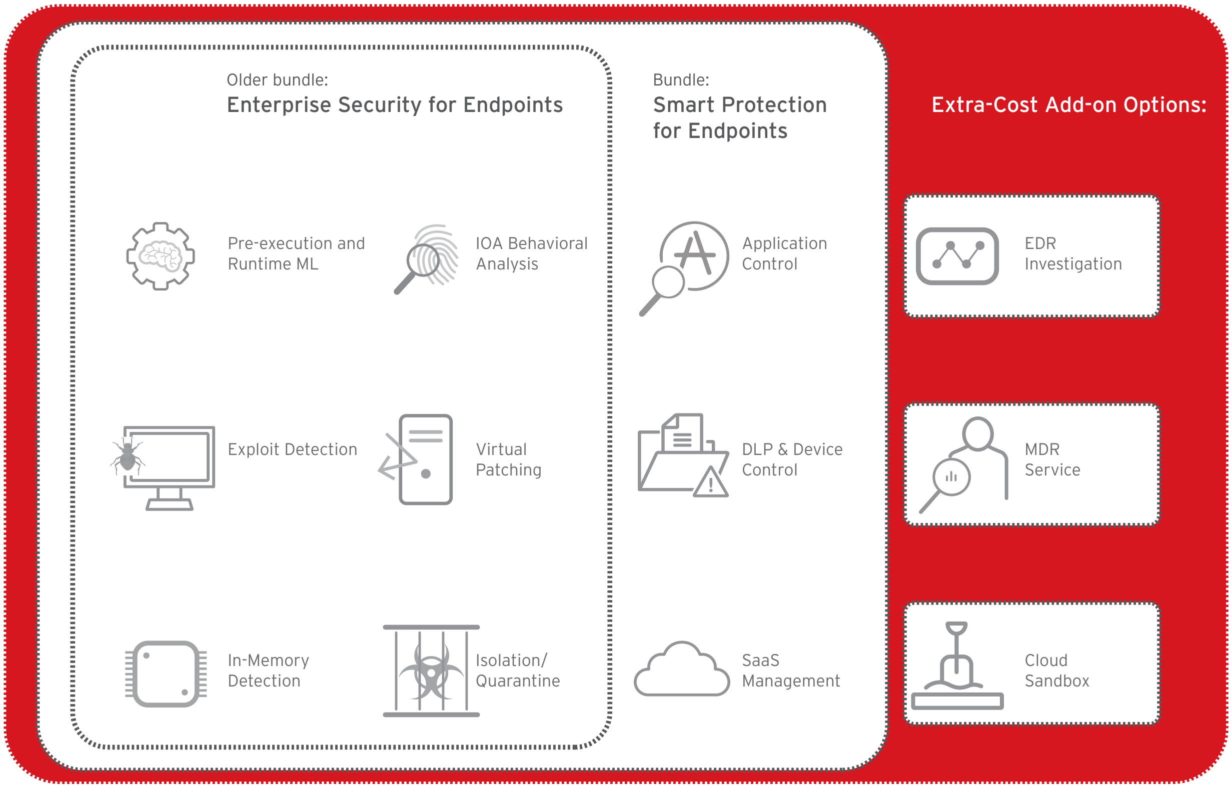
Managed Detection and Response (MDR) Services*

EDR and MDR are available for all suites that include Apex One.

*See the Service and Support section in this document for information on this service.

[2] ESG 2019: Beyond EDR: Natively Correlating and Analyzing Telemetry from Endpoint, Network, Email, and Cloud

Apex One: A convergent agent



Older bundle:
Enterprise Security for Endpoints

Pre-execution and Runtime ML

IOA Behavioral Analysis

Exploit Detection

Virtual Patching

In-Memory Detection

Isolation/ Quarantine

Bundle:
Smart Protection for Endpoints

Application Control

DLP & Device Control

SaaS Management

Extra-Cost Add-on Options:

EDR Investigation

MDR Service

Cloud Sandbox

Email and Collaboration Security

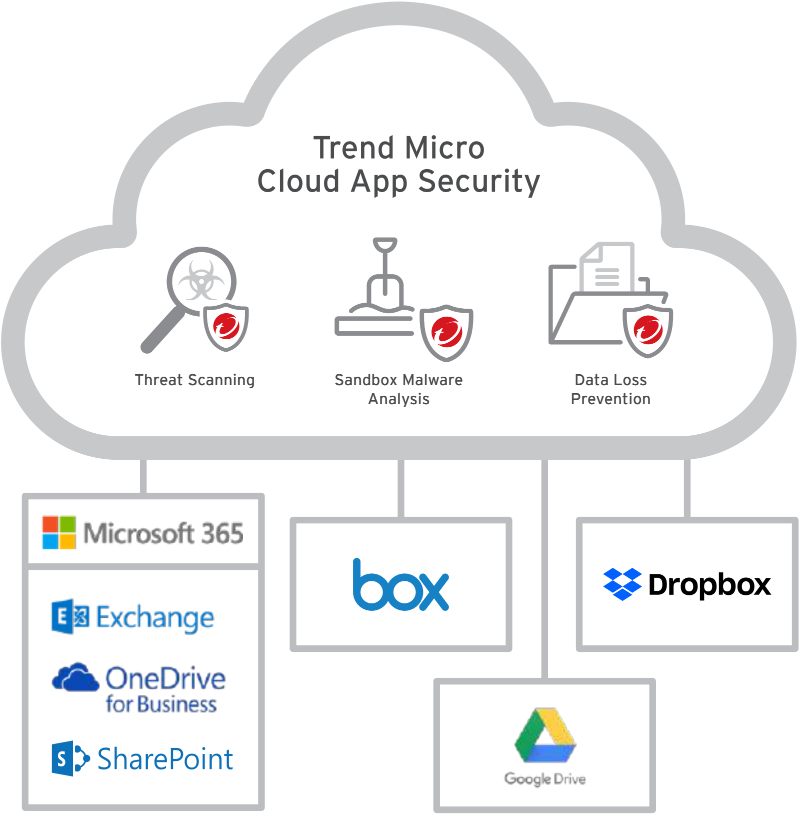
Cloud App Security for Microsoft 365

Cloud App Security extends Microsoft 365, Box, Dropbox, Google Drive, SharePoint Online and OneDrive for Business protection by adding important control mechanisms to detect and defend against data breaches and targeted attacks and maintain compliance. These include:

- Sandbox malware analysis: Identifies zero-day malware and malicious code hidden in Office and PDF documents, for example.
- Data Loss Prevention: Improves control and visibility when exchanging sensitive data.

Benefits

- Extends the built-in security features with sandbox malware analysis and DLP for Box, Dropbox, Google Drive, Exchange Online, SharePoint Online, and OneDrive for Business.
- Minimizes latency impact by assessing the risk of files before sandbox malware analysis.
- Provides document exploit detection.
- APIs (direct cloud-to-cloud connection) eliminate the need to set up a web proxy or change the MX record to reroute email.



Trend Micro™ Email Security™ Standard

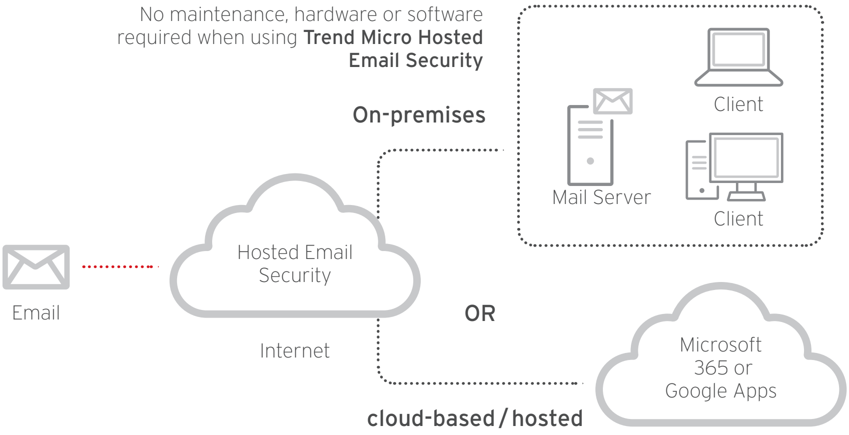
This cloud-based, no-maintenance-required solution delivers continuously updated protection to stop spam and malware before they reach the network.

- Protection against targeted and social engineering attacks.
- Sandbox analysis in the cloud.
- Email encryption using identity based encryption technology.
- Helps you reclaim productivity and bandwidth.

Trend Micro™ Email Security Advanced

Our advanced service, Email Security Advanced, gives you continuously updated protection against BEC, ransomware, spam, and advanced targeted attacks, plus enterprise-grade features.

- Email continuity, allowing users to send/receive email during an email service outage.
- Customizable reporting.
- External log sharing directly to security information and event management (SIEM).


No maintenance, hardware or software required when using **Trend Micro Hosted Email Security**
On-premises
Client
Mail Server
Client
Email
Hosted Email Security
Internet
OR
Microsoft 365 or Google Apps
cloud-based / hosted

Comparison Table: Trend Micro Email Security

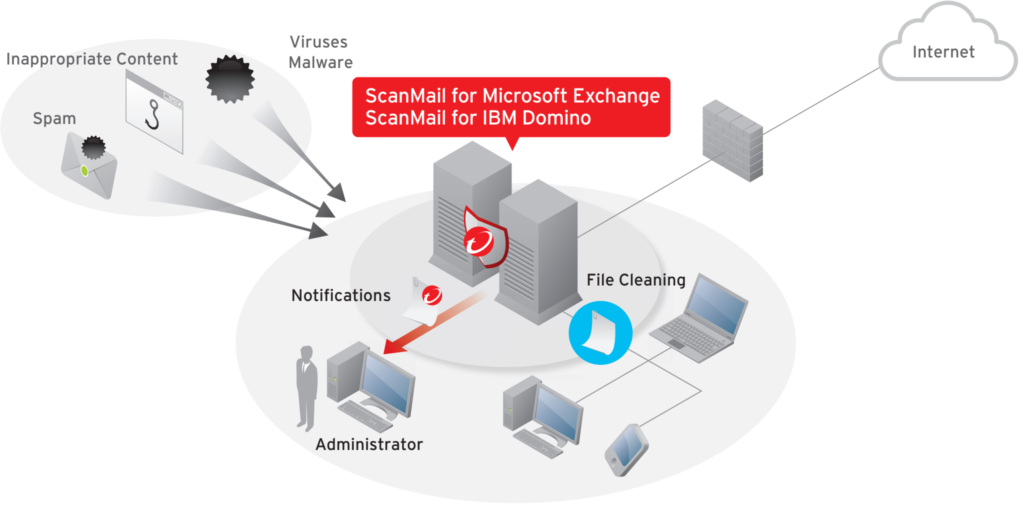
Capability	Standard	Advanced
Email sender analysis and authentication by SPF, DKIM, and DMARC	Yes	Yes
Protection: Known threats (spam, malware, malicious URLs, and graymail)	Yes	Yes
Protection: Unknown malware detection	Exploit detection, predictive machine learning	Exploit detection, predictive machine 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

Trend Micro™ ScanMail™ for Microsoft® Exchange®

ScanMail Suite for Microsoft Exchange delivers leading content security, plus innovative email and web reputation technologies, to protect your data from theft and accidental loss. ScanMail for Microsoft Exchange detects targeted email attacks using exploit detection and sandboxing as part of the Trend Micro Network Defense solution for protection.

Benefits

- Microsoft Exchange Server integration and optimization.
- Anti-spam, anti-malware, and zero-day protection.
- Flexible content filtering.
- Unique web reputation.
- Email reputation (optional).
- Integrated data loss prevention protects your sensitive data.
- Part of the Connected Threat Defense strategy (sandbox integration, suspicious object subscription).
- Predictive machine learning.
- URL time-of-click protection.
- Trend Micro™ Writing Style DNA.



Trend Micro™ ScanMail™ for IBM® Domino

Stop viruses, spyware, spam, phishing, and inappropriate content at your mail server—the central security point for inspecting inbound and internal mail—with ScanMail Suite for IBM Domino. If the solution is integrated into the Trend Micro™ Deep Discovery™ Analyzer, it works to block targeted email attacks.

Benefits

- Leading anti-malware, anti-spyware, anti-spam, anti-phishing, zero-day protection.
- Innovative Web Reputation technology.
- Flexible content filtering.

Trend Micro™ Deep Discovery™ Email Inspector

Designed to quickly detect advanced malware that usually bypasses traditional security defenses and infiltrates sensitive data and intellectual property. Machine learning, specialized detection engines, password extraction, and custom sandbox analysis detect and prevent breaches.

Gateway Security

Trend Micro™ Web Security

Protects against cyber threats before they reach your users. It uses cross-generational defense techniques to catch known and unknown threats, giving you visibility and access control on unsanctioned cloud applications for each of your users. Our unique deployment model provides you with the flexibility to deploy gateways on-premises, in the cloud, or both—protecting your users no matter where they are. One cloud-based management console simplifies your workload, letting you set up policy, manage users, and access reporting across a single pane of glass.

Benefits

- **Delivers superior protection—any device, anywhere:** Trend Micro Web Security stops threats directly in the cloud before they get to your endpoints.
- **Cloud application access control:** This powerful capability allows you to configure access control on unsanctioned cloud apps for different users or user groups within a defined schedule, boosting your organization's security and productivity.
- **Flexible deployment options to fit your needs:** Cloud-based deployment for all users, including onsite, branch offices, and remote/mobile users, eliminates the expense and resource drain associated with backhauling traffic or managing multiple separate on-premises secure web gateways.
- **Single, centralized management console**: This single pane of glass lets you to manage centralized and unified policies across both on-premises and cloud-based deployment instances.

Features

- Gateway anti-malware and HTTPS decryption.
- Web Reputation with correlated threat data
- URL filtering and categorization
- Cloud DLP (Data Loss Prevention)

Comparison Table: Trend Micro Web Security

Capability	Standard	Advanced
On-premises proxy, cloud proxy, or both	Yes	Yes
Authentication (on-premises AD, Microsoft Azure AD, Okta, ADFS)	Yes	Yes
SSL inspection/HTTPS decryption	Yes	Yes
Real-time reporting, logging, audit logs	Yes	Yes
Role-based access control	No	Yes
Syslog for exporting logs	No	Yes
URL filtering and application control	Yes	Yes
Anti-malware and web reputation service	Yes	Yes
Predictive machine learning (PML) for unknown malware	No	Yes
Cloud sandboxing for unknown malware after PML	No	Yes
Data loss prevention with 240+ global templates	No	Yes
Cloud app access control for 30,000 apps	No	Yes
Cloud service filters block personal account access to sanctioned apps	No	Yes

THE ART OF CYBERSECURITY

CYBERSECURITY CAN BE BEAUTIFUL

Automated Hybrid Cloud Workload Protection via APIs Over Time by Jindrich Karasek

06 HYBRID CLOUD SECURITY

With an exploding set of cloud infrastructure services and an increasing number of stakeholders involved in infrastructure and security decisions, the cloud has formed the perfect storm for security.

In order to gain the benefits of the cloud and meet business objectives, Trend Micro cloud security is designed to be less complex. Business requirements and DevOps processes demand faster application delivery, however, if you increase the speed of delivery, everything else must follow suit. For example, compliance, which changes based on industry, geography, and infrastructure, as well as protecting against evolving and increasingly sophisticated threat vectors.

Trend Micro is able to provide powerful security solutions, allowing you to leverage all of the benefits and efficiencies the cloud offers your business.

Cloud Security

Trend Micro Cloud One™

A security services platform for cloud builders, Cloud One delivers the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity. By considering your cloud projects and objectives holistically, Cloud One is able to provide powerful security, while you leverage all of the benefits and efficiencies the cloud offers your business. Comprised of multiple services designed to meet specific cloud security needs, Cloud One gives you the flexibility to solve your challenges today, and the innovation to evolve with your cloud services in the future.

Benefits

Automated. Security as code lets your DevOps teams bake security into their build pipeline to release continuously and frequently. With built-in automation, including automated discovery and deployment, quick-start templates, and our Automation Center, secure your environment and meet compliance requirements quickly.

Flexible. Builder's choice. Security for your hybrid cloud, multi-cloud, and multi-service environments, as well as protection for any vintage of application delivery—with broad platform support.

All-in-one solution. One platform that has the breadth, depth, and innovation required to meet and manage your cloud security needs today and in the future.

Cloud One provides solutions for:

Cloud migration

Automates the discovery and protection of public, private, and virtual cloud environments, while also protecting the network layer. This provides flexibility and simplicity in securing the cloud throughout the migration and expansion process. Gain increased visibility and consistent security throughout your cloud environments, with the most security controls and integrations within your existing toolsets.

DevOps

Cloud One provides automated protection for your applications, which can be built into your CI/CD pipeline. Identify and resolve security issues sooner, as well as improve delivery time for DevOps teams. Simply set it and forget it, and focus on what you do best building great applications.

Containers

Delivers cloud-native security optimized to protect and scale across environments, baking security into your CI/CD pipeline. Build secure, ship fast, and run anywhere with automated security for your containers from the software-build pipeline to runtime, with container image scanning, as well as protection for your Kubernetes®, and Docker platform.

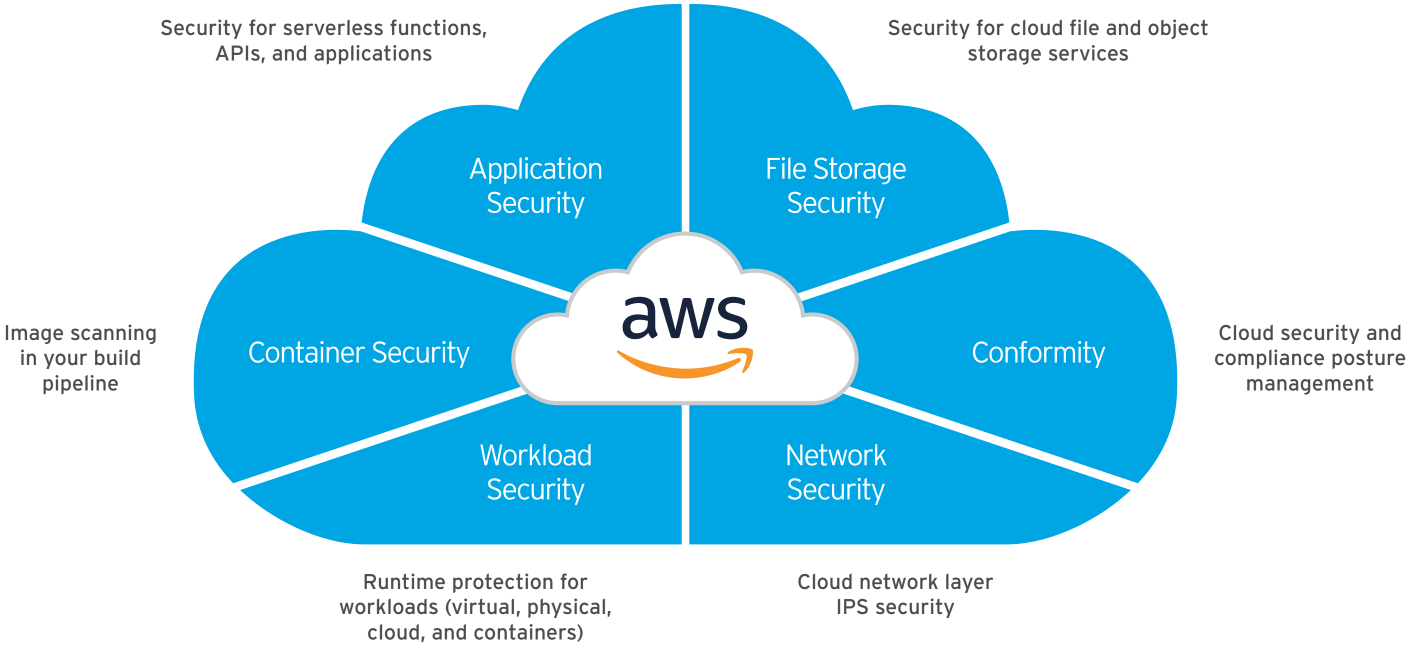
Serverless

Provides protection for your serverless applications against exploits, which can harm your systems, data, and business. Built for speedy deployment, with minimal impact on development streams and performance, simply add to your app with two lines of code.

Data center

Enables the operational efficiency required to support your modern data center. Integrating with the fabric of your physical and virtualized environments, Cloud One delivers fewer agents and automatic discovery and deployment of security. What's more, by consolidating security tools with a comprehensive set of capabilities, you can better detect, protect, and respond to vulnerabilities, malware, and unauthorized system changes.

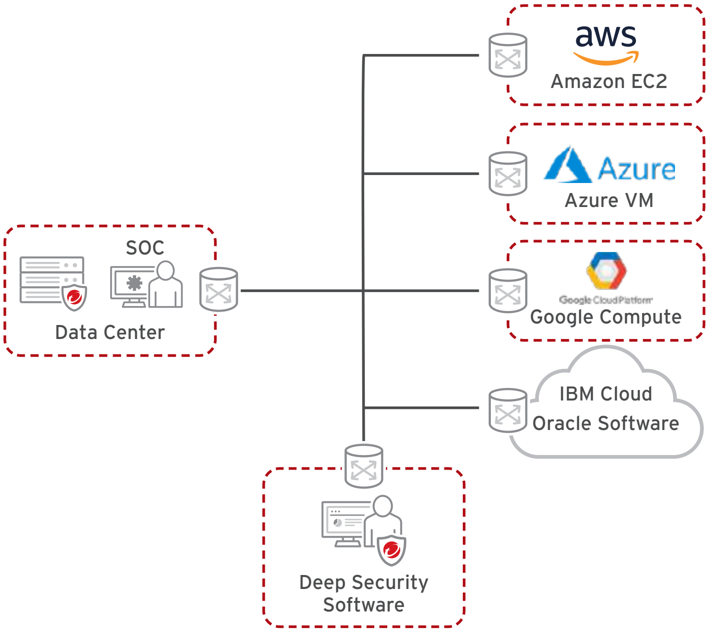
Cloud One includes the following services:


Security for serverless functions, APIs, and applications
Security for cloud file and object storage services
Application Security
File Storage Security
Image scanning in your build pipeline
Container Security
aws
Conformity
Cloud security and compliance posture management
Workload Security
Network Security
Runtime protection for workloads (virtual, physical, cloud, and containers)
Cloud network layer IPS security

Data Center Security

Trend Micro™ Deep Security™ Software

Trend Micro Deep Security Software offers a comprehensive server security platform designed for physical and virtualized data centers. Powered by XGen™ security, Deep Security provides a layered approach to server security. It protects against zero-day attacks, secures servers against ransomware attacks, and detects compromised data. Tightly integrated modules easily expand the platform to ensure server, application, and data security in your data center, helping to ensure compliance. By flexibly choosing modules, you can custom-tailor your security solution to your needs with any combination of agent-based or VMWare® NSX-based agentless protection, including anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, application control, and log inspection. This results in an adaptive and efficient server security platform that protects business-critical enterprise applications and data from breaches and business disruptions without expensive emergency patching.



Key Business Issues

- **Automated protection** Save time and resources with automated security policy across your hybrid environments, such as data center and cloud, as you migrate or create new workloads.
- **Unified security** Deploy and consolidate security across your physical, virtual, multi-cloud, and container environments with a single agent and platform.
- **Security for the CI/CD pipeline** API-first, developer-friendly tools to help you ensure that security controls are baked into DevOps processes.
- **Accelerate compliance** Demonstrate compliance with a number of regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.

Key Advantages

- **Protect your critical servers and applications** with advanced security controls, including an intrusion prevention system (IPS), integrity monitoring, machine learning, application control, and more.
- **Detect and block threats** in real time, with minimal performance impact.
- **Detect and block unauthorized software execution** with multi-platform application control.
- **Shield known and unknown vulnerabilities** in web, enterprise applications, and operating systems through an IPS.
- **Advanced threat detection and remediation** of suspicious objects through sandbox analysis.
- **Send alerts and trigger proactive prevention** upon the detection of suspicious or malicious activity.
- **Secure end-of-support systems** with virtual patches delivered via an IPS, ensuring legacy systems stay protected from existing and future threats.
- **Track website credibility** and protect users from infected sites with web reputation threat intelligence from Trend Micro's global domain reputation database.
- **Identify and block** botnet and targeted attack C&C communications.
- **Secure against the latest threats** using threat intelligence from the Trend Micro Smart Protection Network, powered by Trend Micro's market-leading threat research.

Trend Micro™ Deep Security™ Smart Check–Container Image Security

Trend Micro Deep Security Smart Check–Container Image Security delivers automated build-time and registry-image scanning with detection for malware, vulnerabilities, secrets, and policy compliance. This is designed to secure images earlier in the CI/CD pipeline without negatively impacting the ability for DevOps teams to continuously deliver production-ready applications and meet the needs of the business.

Key Advantages

Prevent exploits prior to runtime

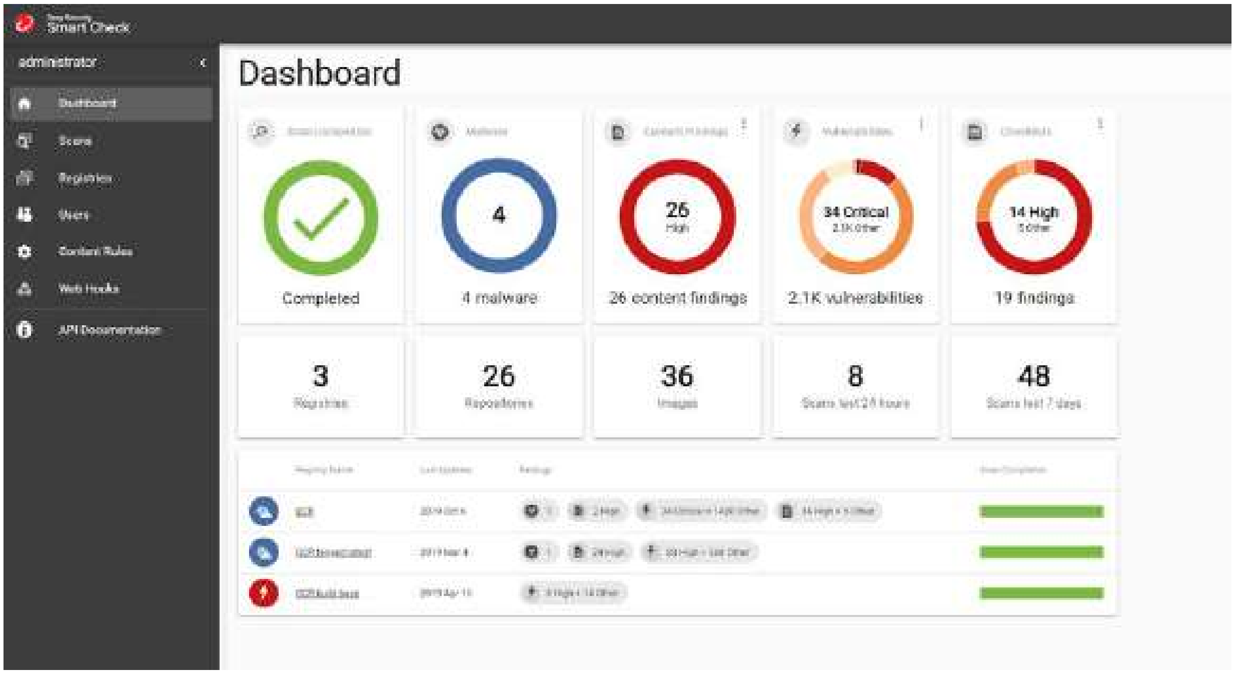
Protect against malware, vulnerabilities, and secrets with build-time and registry scanning of Docker® images. Ensure threats are detected before applications are deployed.

Protection optimized for DevOps

Implement frictionless security early in the CI/CD workflow with security as code and automated protection that won't slow down your DevOps processes.

Full life cycle container protection

Trend Micro provides leading runtime protection, complementing Smart Check–Container Image Security for full life cycle container security.

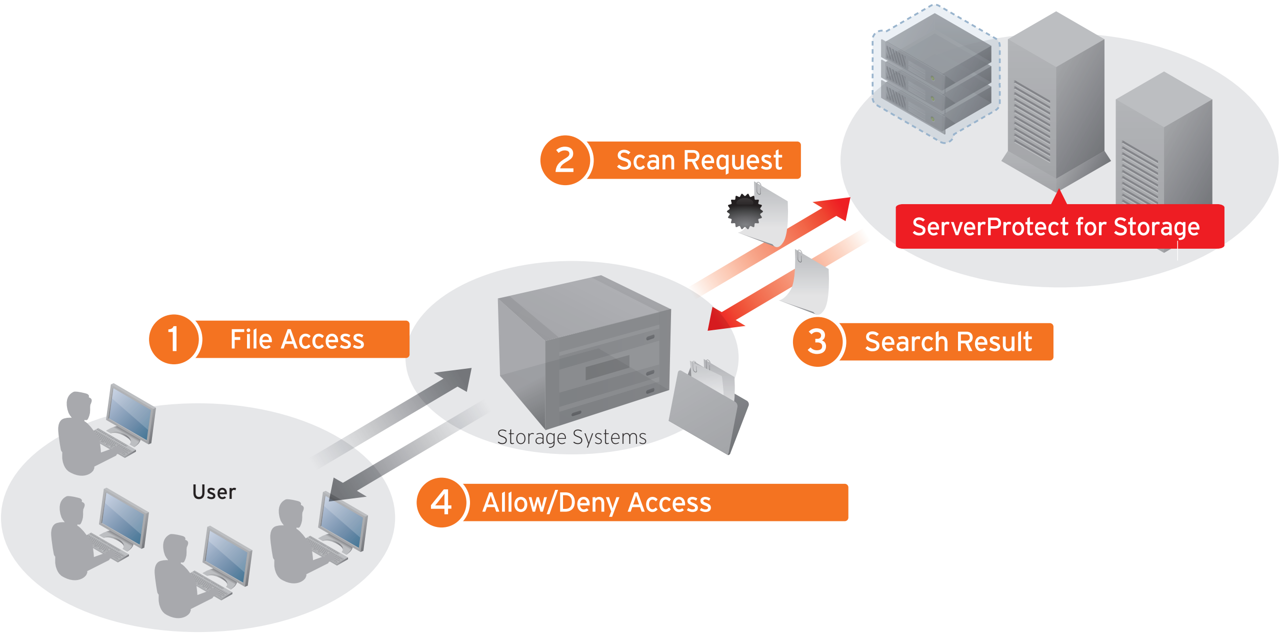


Storage Security

Trend Micro™ ServerProtect™ for Storage

Trend Micro ServerProtect for Storage—the industry's most reliable, high-performing security solution for storage platforms—safeguards your file storage systems by detecting and removing malware and spyware in real time.

- Tight integration with EMC® Celerra®, NetApp, Hitachi Data Systems, IBM, HPE, and other storage systems.
- Enables real-time, high-performance malware scanning with minimal impact on servers and no impact on end users.
- Also supports malware scanning via iCAP protocol.



THE ART OF CYBERSECURITY

CYBERSECURITY CAN BE BEAUTIFUL

Threats Detected & Blocked Globally Over Time
by Daniel Beauchamp

07 NETWORK DEFENSE

Complex networks

The enterprise boundary is gone, with networks extending far beyond the traditional LANs and WANs. Wi-fi, remote access, connected branch offices, and the cloud are giving enterprises more flexibility and productivity. Today there are more points to protect than ever, so how do you evolve your network security to go beyond perimeter defenses and also detect lateral movement within networks?

Through strong integration between intrusion prevention solutions (IPS) and advanced threat protection (including sandboxing), Trend Micro provides a blend of cross-generational techniques and advanced threat detection to maximize protection of your networks and go beyond known and unknown.

Network Threat Detection

Trend Micro™ Deep Discovery™ is a family of advanced threat protection products that enables companies to detect, analyze, and respond to today's stealthy, targeted attacks. Powered by XGen™ security, Deep Discovery blends specialized detection engines, custom sandboxing, and global threat intelligence from the Trend Micro Smart Protection Network, for the highest detection rate possible against attacks that are invisible to standard security products. Deployed individually or as an integrated solution, Deep Discovery works with Trend Micro and third-party products to provide advanced threat protection across your company.

- **Protection against attacks:** Unique threat detection technologies discover attacks before the damage is done.
- **Intelligence for a rapid response:** Deep Discovery and global threat intelligence drive a rapid and effective response.
- **Integration of your defenses:** Deep Discovery integrates with your Trend Micro and third-party security tools to successfully prevent targeted attacks.
- **Protection from integrated threats:** Trend Micro™ TippingPoint™ Intrusion Prevention System (IPS) and Trend Micro™ Deep Discovery™ Advanced threat protection work closely together to deliver integrated detection and prevention of known, unknown, and undisclosed threats.

Advanced Threat Protection

Increasingly, organizations are facing stealthy targeted attacks in their networks. Often custom designed to penetrate standard defenses, these attacks are poised to monetize intellectual property and customer information or to encrypt essential data for ransom.

Trend Micro Deep Discovery protects against targeted attacks, advanced threats, and ransomware, giving you the power to detect, analyze, and respond to today's stealthy attacks in real time.

Trend Micro™ Deep Discovery™ Analyzer

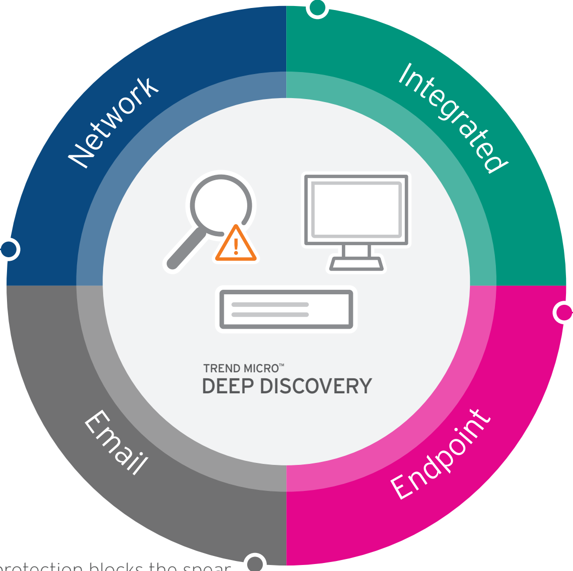
Trend Micro Deep Discovery Analyzer is an open custom sandbox analysis server that enhances the malware detection capabilities of all your security products. The Analyzer supports out-of- the-box integration with many Trend Micro products, manual sample submission, and an open web services interface to allow any product or process to submit samples and obtain results. It can extend existing Deep Discovery products by adding a high-availability, clustered sandbox analysis farm.

Trend Micro™ Deep Discovery™ Network Analytics

Deep Discovery Network Analytics provides deeper insight into an attack. Leveraging Deep Discovery Inspector as advanced persistent threat (APT) detection and network metadata collection points, Deep Discovery Network Analytics utilizes expert rules to correlate and connect threat detection events against network access events, presenting threat investigators with complete view of the attack life cycle.

Trend Micro™ Deep Discovery™ Analyzer as a Service

Deep Discovery Analyzer as a Service is an add- on for the virtual Deep Discovery Inspector. It provides cloud sandboxing capabilities and is especially well-suited for smaller environments that require a virtual solution and cloud-based sandboxing to provide protection from advanced threats and targeted attacks.

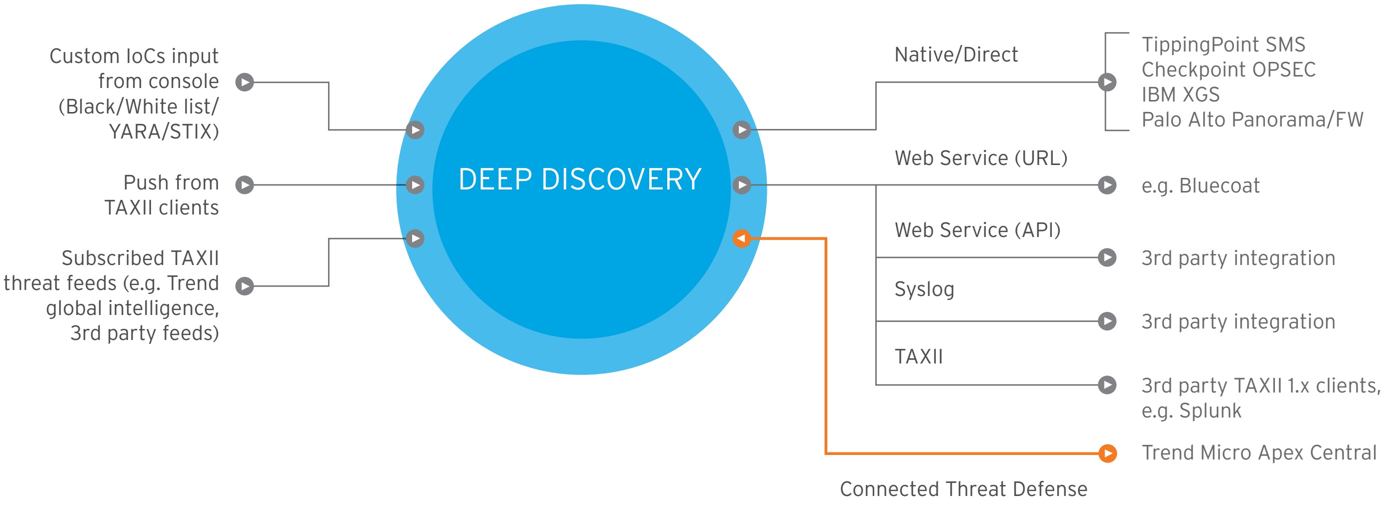


Integrated custom sandboxing analysis extends the capabilities of Trend Micro and third-party security products

360-degree detection identifies advanced attacks across your network

Detailed endpoint activity tracking enables rapid analysis of the nature and extent of an attack

Dedicated protection blocks the spear phishing emails that cybercriminals use to initiate targeted attacks



Features

- **Inspection of network content:** Monitor all traffic across physical and virtual network segments, all network ports and over 100 network protocols to identify targeted attacks, advanced threats and ransomware.
- **Extensive detection techniques:** Utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware and attacker behavior.
- **Custom sandbox analysis:** Use virtual images that are tuned to precisely match an organization's system configurations, drivers, installed applications, and language versions.
- **Flexible deployment:** Deep Discovery Analyzer can be deployed as a standalone sandbox or alongside a larger Deep Discovery deployment to add additional sandbox capacity.
- **Advanced detection:** Methods such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly.
- **Threat intelligence:** Correlate and share advanced threat intelligence using standards-based formats and transports like STIX/TAXII and YARA.
- **Threat analytics:** Greater visibility into an attack, helping you priorities the threats and show just how the threat breached the network, where it went from there and who else has been impacted by the attack.
- **Integration:** Deep Discovery is built to work with Trend Micro products as well as third-party products.

Trend Micro™ Deep Discovery™ Inspector

Trend Micro Deep Discovery Inspector is a network appliance that monitors network traffic across all ports and more than 100 protocols and applications. Using specialized detection engines and custom sandboxing, it identifies the malware, command and control (C&C) communications and activities signaling an attempted attack. The results of the sandbox analysis aid your rapid response and are automatically shared with your other security products to block further attacks.

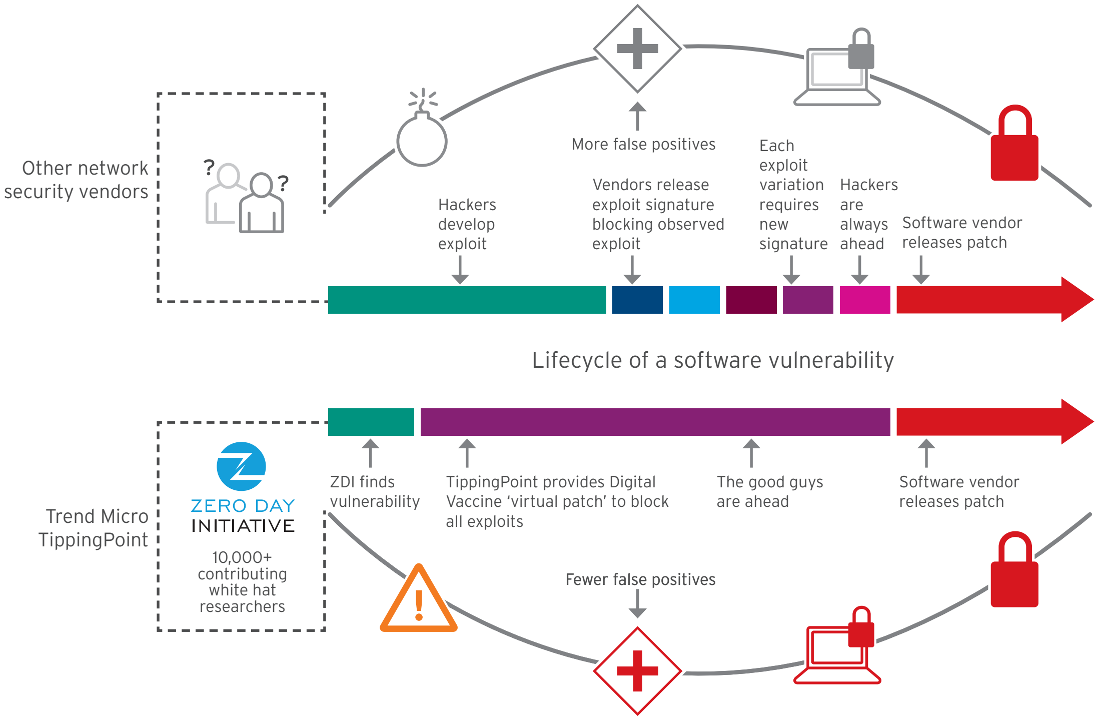
Next-Generation Intrusion Prevention

Trend Micro™ TippingPoint™–Next-Generation Intrusion Prevention System

TippingPoint Threat Protection System (TPS) a network security platform. Powered by XGen™ security, it offers comprehensive threat protection against vulnerabilities, blocks exploits, and fights known and zero-day attacks with high accuracy. TPS provides industry-leading coverage across different threat vectors from advanced threats like malware and phishing with extreme flexibility and high performance. The TPS uses a combination of technologies, including deep packet inspection, threat reputation, URL reputation, and advanced malware analysis on a flow-by-flow basis to detect and prevent attacks on the network.

The platform enables enterprises to take a proactive approach to security to provide comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks, and zero power high availability (ZPHA). In addition, TPS can be provisioned using redundant links in a transparent active-active or active-passive high availability (HA) mode.

Software vulnerability lifecycle

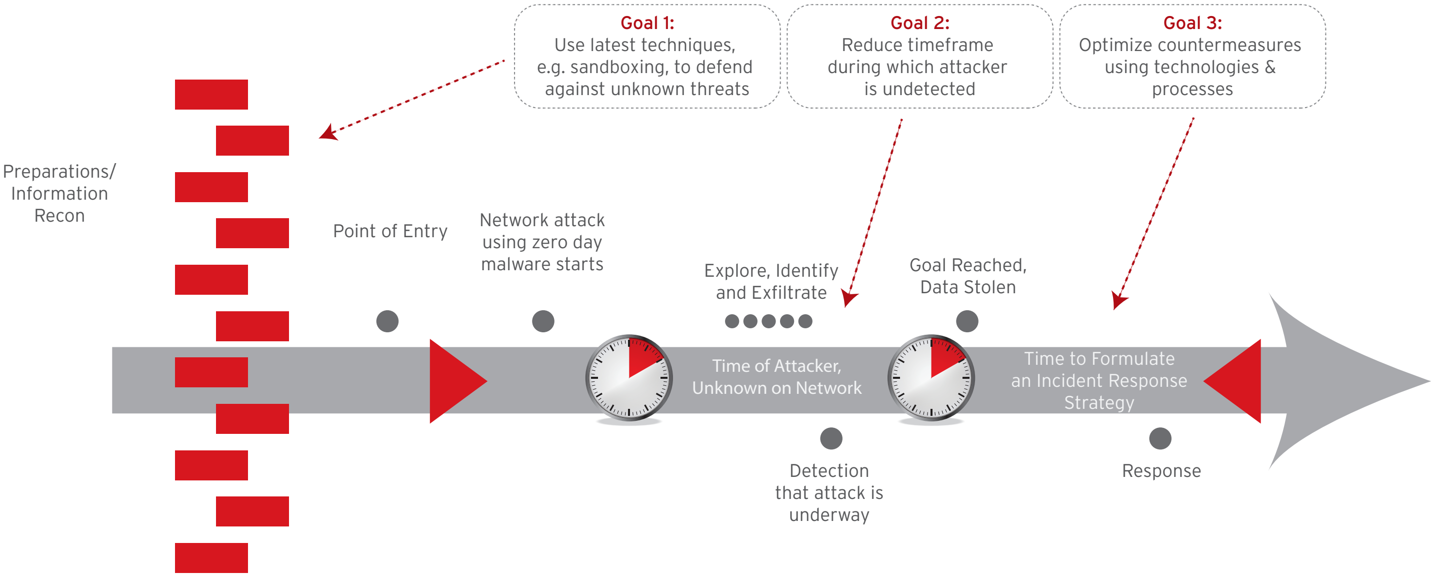

Other network security vendors
?
?
More false positives
Hackers develop exploit
Vendors release exploit signature blocking observed exploit
Each exploit variation requires new signature
Hackers are always ahead
Software vendor releases patch
Lifecycle of a software vulnerability
Trend Micro TippingPoint
ZERO DAY INITIATIVE
10,000+ contributing white hat researchers
ZDI finds vulnerability
TippingPoint provides Digital Vaccine 'virtual patch' to block all exploits
The good guys are ahead
Software vendor releases patch
Fewer false positives

Features

- **On-box SSL inspection:** Sophisticated and targeted attacks are increasingly using encryption to evade detection. TPS reduces security blind spots created by encrypted traffic with on-box SSL inspection.
- **Performance scalability:** The increase in data center consolidation and proliferation of cloud environments requires security solutions that can scale as network demands increase.
- **Flexible licensing model:** Easily scale performance and security requirements with pay-as-you-grow approach and flexible licenses that can be reassigned across TPS deployments without changing network infrastructure.
- **Real-time machine learning:** Many security threats are short-lived and constantly evolving, at times limiting the effectiveness of traditional signature-and hash-based detection mechanisms. TPS uses statistical models developed with machine learning techniques to deliver the ability to detect and mitigate threats in real time.
- **Enterprise Vulnerability Remediation (eVR):** Quickly remediate vulnerabilities by integrating third-party vulnerability assessments with the TippingPoint product portfolio. Customers can pull in information from various vulnerability management and incident response vendors (Rapid7, Qualys, Tenable), map Common Vulnerabilities and Exposures (CVEs) to TippingPoint Digital Vaccine® filters and take action accordingly.
- **Advanced threat analysis:** Extend protection from unknown threats through integration with Deep Discovery Analyzer. TPS pre-filters known threats, forwards potential threats for automated sandbox analysis and remediates in real time upon confirmation of malicious content.
- **High availability:** Ideal for inline deployment, TPS has multiple fault-tolerant features including hot swappable power supplies, watchdog timers to continuously monitor security and management engines, built-in inspection bypass and zero power high availability (ZPHA). In addition, TPS can be provisioned using redundant links in a transparent active-active or active-passive high availability (HA) mode.
- **Integrated advanced threat prevention:** TPS integrates with Trend Micro Deep Discovery Advanced threat detection solutions, rated as the most effective and "recommended" breach detection system by leading test labs and customers.
- **Asymmetric traffic inspection:** Traffic asymmetry is widespread and pervasive throughout enterprise and data center networks. Enterprises must overcome challenges from both flow and routing asymmetry to be able to fully protect their networks. TPS by default inspects all types of traffic, including asymmetric traffic, and applies security policies to ensure comprehensive protection.
- **Agility and flexibility:** TPS embraces software-defined network protection by deploying IPS as a service. TPS also protects virtualized applications from within your virtualized infrastructure (VMware, KVM). Editing network security policies, configuring elements, and deploying network security policy across the entire infrastructure, whether physical or virtual.
- **Best-in-class threat intelligence:** Exclusive access to vulnerability information from the Zero Day Initiative (ZDI) protects customers from undisclosed and zero-day threats. ZDI is the largest vendor-agnostic bug bounty program, with 1,045 vulnerabilities published in 2019, with customers using Trend Micro TippingPoint protected an average of 81 days ahead of a vulnerability being patched by affected vendors[3].
- **Virtual patching:** Virtual patching provides a powerful and scalable frontline defense mechanism that protects networks from known threats and relies on vulnerability-based filters to provide an effective barrier from all attempts to exploit a particular vulnerability at the network level rather than the end user level. This helps enterprises gain control of their patch management strategy with pre-emptive coverage between the discovery of a vulnerability and the availability.
- **Support for a broad set of traffic types:** TPS platform supports a wide variety of traffic types and protocols. It provides uncompromising IPv6/v4 simultaneous payload inspection and support for related tunneling variants (6in4 and 6in6). It also supports inspection of IPv6/v4 traffic with VLAN and MPLS tags, mobile IPv4 traffic, GRE and GTP (GPRS tunneling) and jumbo frames. This breadth of coverage gives IT and security administrators the flexibility to deploy its protection wherever it is needed.
- **Centralized management:** Trend Micro™ TippingPoint™ Security Management System (SMS) delivers a unified policy and element management graphical user interface that provides a single mechanism for monitoring operational information.

[3] http://cms.ipressroom.com.s3.amazonaws.com/365/files/202003/IGOO_ZDI_Infographic_200305US.pdf

Software vulnerability lifecycle


Goal 1:
Use latest techniques, e.g. sandboxing, to defend against unknown threats
Goal 2:
Reduce timeframe during which attacker is undetected
Goal 3:
Optimize countermeasures using technologies & processes
Preparations/ Information Recon
Point of Entry
Network attack using zero day malware starts
Explore, Identify and Exfiltrate
Goal Reached, Data Stolen
Time of Attacker, Unknown on Network
Time to Formulate an Incident Response Strategy
Detection that attack is underway
Response

Benefits

- **Pre-emptive threat prevention:** TPS deployed inline has the ability to inspect and block all directions of traffic (inbound, outbound, and lateral) in real time to protect against known, unknown, and undisclosed vulnerabilities.
- **Threat insight and prioritization:** Visibility and insight is crucial to making the best security policy decisions. TPS delivers complete visibility across your network and provides the insight and context needed to measure and drive threat prioritization.
- **Real-time enforcement and remediation:** Defend the network, from the edge to the data center and to the cloud, with real-time, inline enforcement and automated remediation of vulnerable systems. TPS achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The Trend Micro™ TippingPoint™ Threat Suppression Engine (TSE) architecture performs high-speed inline deep packet traffic inspection, and the purpose-built appliance's modular design enables the convergence of additional security services.
- **Operational simplicity:** With flexible deployment options that are easy to set up and manage through a centralized management interface, TPS provides immediate and ongoing threat protection with out-of-the-box recommended settings.

TPS Tech Specifications

Features	440T (TPNN0291)	2200T (TPNN0292)	8200TX (TPNN0090)	8400TX (TPNN0091)
Supported IPS Inspection Throughput	250 Mbps/500 Mbps/1 Gbps	1 Gbps/2 Gbps	3/5/10/15/20/30/40 Gbps	3/5/10/15/20/30/40 Gbps
SSL Inspection	Not Available	500 Mbps	2 Gbps (2K keys SHA-256)	2 Gbps (2K keys SHA-256)
Latency	< 100 microseconds	< 100 microseconds	< 40 microseconds	< 40 microseconds
Security Contexts	750,000	2,500,000	10,000,000	10,000,000
Concurrent Sessions	1,000,000	10,000,000	120,000,000	120,000,000
New Connections per second	70,000	115,000	650,000	650,000
Form Factor	1U	2U	1U	2U
Weight	6.93 kg (15.28 pounds)	11.91 kg (26.26 pounds)	14.5 kg (max. including IOMs) 13.2 kg (w/ blank IOMs)	22.7 kg (max. including IOMs) 18.8 kg (w/ blank IOMs)
Dimensions (W x D x H)	16.78 in. (W) x 17.3 in. (D) x 1.72 in. (H) 42.62 cm x 45.00 cm x 4.40 cm	16.77 in. (W) x 18.70 in. (D) x 3.46 in. (H) 42.60 cm x 47.50 cm x 8.80 cm	16.78 in. (W) x 17.3 in. (D) x 1.72 in. (H) 42.62 cm x 45.00 cm x 4.40 cm	16.77 in. (W) x 18.70 in. (D) x 3.46 in. (H) 42.60 cm x 47.50 cm x 8.80 cm
Management Ports	1 out-of-band-RJ-45 (10/100/1000), 1 RJ-45 serial, Manageable			
Management Interface	Security Management System (SMS), Local Web Console, Command line, SNMPv2c, SNMPv3 (TippingPoint MIB available)			
Network Connectivity	8 RJ-45 ports (10/100/1000) with integrated bypass support 1 RJ-45 high availability port (10/100/1000)	8 RJ-45 ports (10/100/1000) with integrated bypass support, 8 x 1G SFP 4 x 10G SFP+ 1 RJ-45 high availability port (10/100/1000), Support for external ZPHA for SFP/SFP+	2x IOM Slots, Mix/Match: 6-Segment 1GE Copper 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Copper Bypass 2-Segment 1GE SR/LR Fibre Bypass 2-Segment 10GE SR/LR Fibre Bypass	4x IOM Slots, Mix/Match: 6-Segment 1GE Copper 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Copper Bypass 2-Segment 1GE SR/LR Fibre Bypass 2-Segment 10GE SR/LR Fibre Bypass
On-box Storage	8GB CFast Drive (Hot-Swappable)		32GB 1.8" SSD Module (Hot-Swappable)	
Voltage	100 to 240 VAC, 50 to 60 Hz		100 to 240 VAC/-40 to -60 VDC	
Current (max. fused power)	4-2 A	12-6 A	12/6 Amps AC, 24/16 Amps DC	
Max. power consumption	250 W (853 BTU/hour)	493 W (1,682 BTU/hour)	750 W (2,557 BTU/hour)	
Power supply	Single fixed	Dual/redundant, hot swappable	Dual/redundant, hot swappable	
Operating temperature	0°C to 40°C (32°F to 104°F)			
Operating relative humidity	5% to 95% non-condensing			
Non-operating/storage temperature	-20°C to 70°C			
Non-operating/storage relative humidity	5% to 95% non-condensing			
Altitude	Up to 3,048 m			
Safety	UL 60950-1, IEC 60950-1, EN 60950-1, CSA 22.2 60950-1, ROHS Compliance			
EMC	Class A, FCC, VCCI, KC, EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2, EN61000-3-3, CE Marking			

XDR: Cross-Layer Detection and Response

Trend Micro™ XDR offer detection and response across multiple security layers, including email, endpoints, servers, cloud workloads, and networks.

Trend Micro XDR allows for broader visibility and expert security analytics, leading to more detections and an earlier, faster response. Users can respond more effectively to threats, minimizing the severity and scope of a breach.

Advantages

AI and Expert Security Analytics

Built-in threat expertise and global threat intelligence to detect more:

- Combine threat and detection data from your environment with Trend Micro's global threat intelligence in the Trend Micro Smart Protection Network for richer, more meaningful alerts.
- More context means faster detection and higher fidelity alerts.
- Optimal AI and big data analytics provide you with a deeper understanding of data collected from Trend Micro's intelligent sensors.
- Gain the power that only humans can bring to bear with new expert detection rules based on what from Trend Micro threat experts are finding in the wild.

Beyond the Endpoint

Detect and respond to threats across multiple layers and gain greater context to understand better:

- Automatically correlate data from sensors from native Trend Micro solutions that collect detection and activity data across email, networks, endpoints, and servers, eliminating manual steps.
- Activity that may not seem suspicious on its own suddenly becomes a high-priority alert, allowing you to contain its impact faster.
- Contain threats more easily, assess the impact, and action the response across email, endpoints, servers, cloud workloads, and networks.

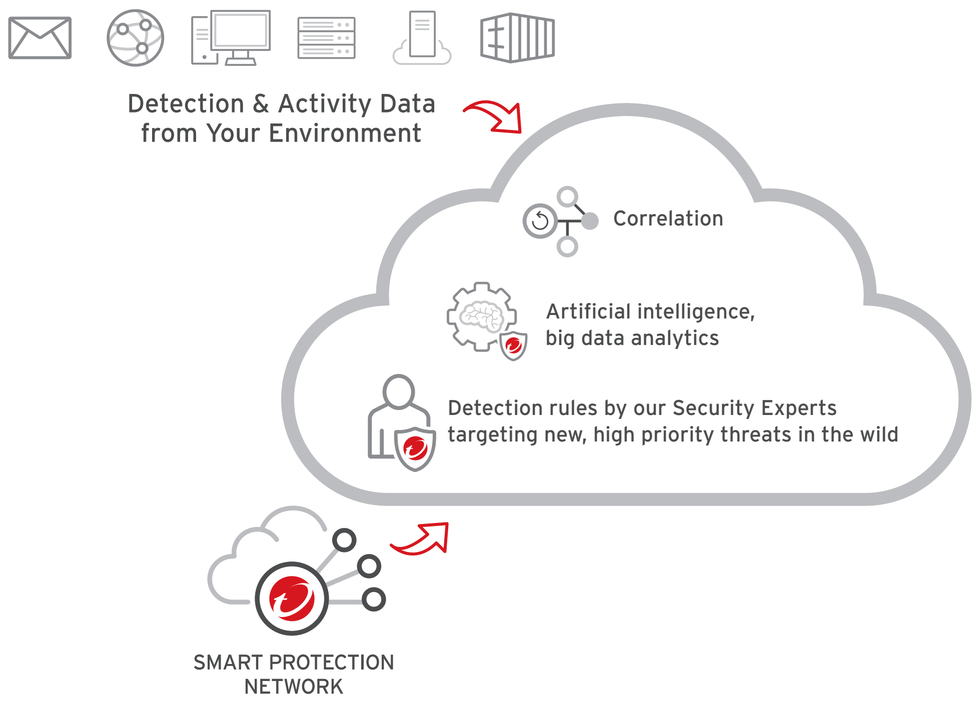
Complete Visibility

One platform to respond faster with less resources:

- ONE source of prioritized alerts based on one expert alert schema to interpret data in a standard and meaningful way.
- ONE consolidated view to uncover events and the attack path across security layers.
- ONE source for guided investigations to understand the impact and identify the path to resolution.

Benefits

- AI and expert security analytics correlate data from customer environments and Trend Micro's global threat intelligence to deliver fewer, higher-fidelity alerts.
- Provides a broader perspective and a better context to identify threats more easily and contain them more effectively.
- Complete visibility through a single console for one source of prioritized, optimized alerts supported with guided investigation.


Detection & Activity Data
from Your Environment
Correlation
Artificial intelligence,
big data analytics
Detection rules by our Security Experts
targeting new, high priority threats in the wild
SMART PROTECTION
NETWORK

Managed XDR

Trend Micro™ Managed XDR provides a service for continuously monitoring security-related endpoint and network data. Using artificial intelligence (AI) and machine learning, alerts can be prioritized according to their level of severity. Managed XDR helps organizations detect threats that may previously have been identified as "grey alerts" by themselves. Trend Micro threat researchers investigate further to determine the extent and spread of the attack through a detailed root cause analysis (RCA), working with customers to provide a detailed response plan.

Trend Micro Managed XDR service offers you:

- Around the clock monitoring and investigation of alerts.
- Big data correlation of events, alerts, and network data to identify potential advanced attacks.
- Proactive threat hunting as needed to validate dynamically evolving zero-day threats.
- Access to an advanced team of security experts skilled in investigating advanced threats, determining the severity of any incidents and providing actionable threat remediation plans.
- Root cause analysis to provide an understanding of how the attack was initiated and spread and which devices were affected.
- Access to industry-leading protection and network intrusion detection platforms.
- Experts available 24/7 without increasing staff costs, to help assist companies who typically lack the staff for dedicated threat hunting.

09 SECURITY FOR SMALL AND MEDIUM BUSINESSES

Trend Micro™ Worry-Free™

Worry-Free security is specially designed for small to medium-sized businesses, offering advanced protection for desktops, servers, mobile devices, and emails. You can choose from two different variants to find the best security solutions for your customers.

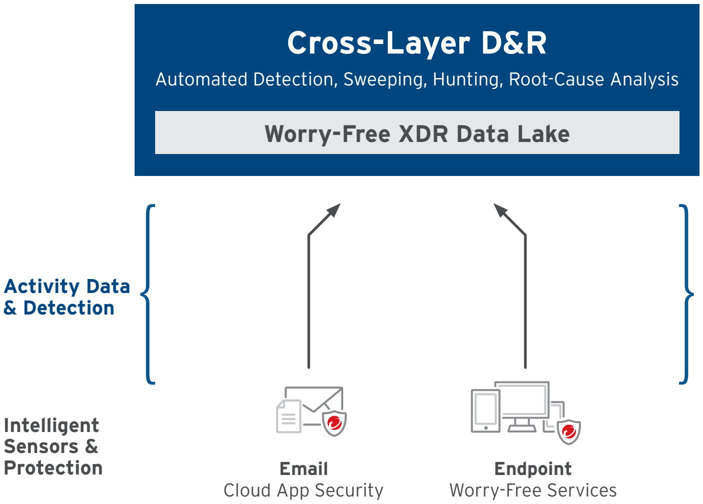
Trend Micro™ Worry-Free™ Services/ Services Advanced

Since users remain the biggest security vulnerability, your customers should prevent threats from even reaching their users. Worry-Free gives you protection against advanced malware and ransomware. On or off the corporate network, your endpoints are protected against malware, Trojans, worms, spyware, ransomware, and new variants as they emerge. Worry-Free Advanced protects email, web applications, and file sharing services – and filters URLs by blocking access to inappropriate websites. Spam is blocked and phishing and social engineering attacks are staved off, so your employees don't have to worry about security problems and can focus on their work.

To save your customers time and resources, Worry-Free Services Advanced is hosted and maintained by Trend Micro and combines the features of Worry-Free Services to protect devices, Hosted Email Security to protect emails, and Cloud App Security to protect Microsoft 365® email, OneDrive, SharePoint Online, Google Drive, Dropbox, and Box.

Trend Micro™ Worry-Free™ XDR

The Worry-Free XDR bundle provides detection and response capabilities across email and endpoints to help you discover and respond to targeted attacks more effectively.


Cross-Layer D&R
Automated Detection, Sweeping, Hunting, Root-Cause Analysis
Worry-Free XDR Data Lake
Activity Data & Detection
Intelligent Sensors & Protection
Email
Cloud App Security
Endpoint
Worry-Free Services

What Worry-Free can do for you

	Worry-Free Services	Worry-Free Services Advanced	Worry-Free XDR	Worry-Free with Co-Managed XDR*
100% SaaS Complete SaaS solution with no servers to install or maintain, ever	✓	✓	✓	✓
Endpoint Security Secures Windows (desktops and servers), Mac, iOS, and Android devices by infusing high-fidelity machine learning into a blend of threat protection techniques for the broadest protection against ransomware and advanced attacks	✓	✓	✓	✓
Email Security • Secures Microsoft Exchange, Microsoft 365, Gmail and any other email solution in real time • Stops targeted attacks, spam, phishing, viruses, spyware, and inappropriate content from impacting your business • Includes our latest business email compromise and credential phishing protection capabilities	✓	✓	✓	✓
Collaboration Security Protects online collaboration tools from unknown threats and secures company data from intentional and accidental loss	✓	✓	✓	✓
Cross-Layer Detection and Response (XDR) • Detection, response, and investigation capabilities within a single agent, across email and endpoints • Automated root cause analysis, including recommended step-by-step actions, allows quick mitigation • Advanced threat detection by cloud sandboxing included	✓	✓	✓	✓
Managed Detection and Response (MDR) *For MSP only • Trend Micro security analysts provides 24/7 critical alerting & monitoring • Incident investigation and cross-customer analysis for MSP's customer base • Provides recommendations or authorized actions	✓	✓	✓	✓

Trend Micro Cloud Edge™

A unified threat management (UTM) solution that combines a physical appliance with an industry-unique cloud scanning function. Trend Micro Cloud Edge provides maximum protection that is managed natively from the cloud, providing zero-touch deployment, multi-tenant management, and complete control of your customers' security in one central location.

UTM as a service for managed service providers (MSP)

Purpose Built for Managed Service Providers (MSPs)

- With our unique, pay-as-you-go MSP pricing model, there are no upfront costs and no term commitments.
- Trend Micro™ Cloud Edge™ integrates with existing tools and processes for maximum efficiency and optimal security.

Better Performance

- Combines a physical appliance with an industry-unique cloud scanning function for maximum performance and protection.
- Benefit from a next-generation, on-premises unified threat management appliance plus the convenience of Security as a Service.

Superior Management

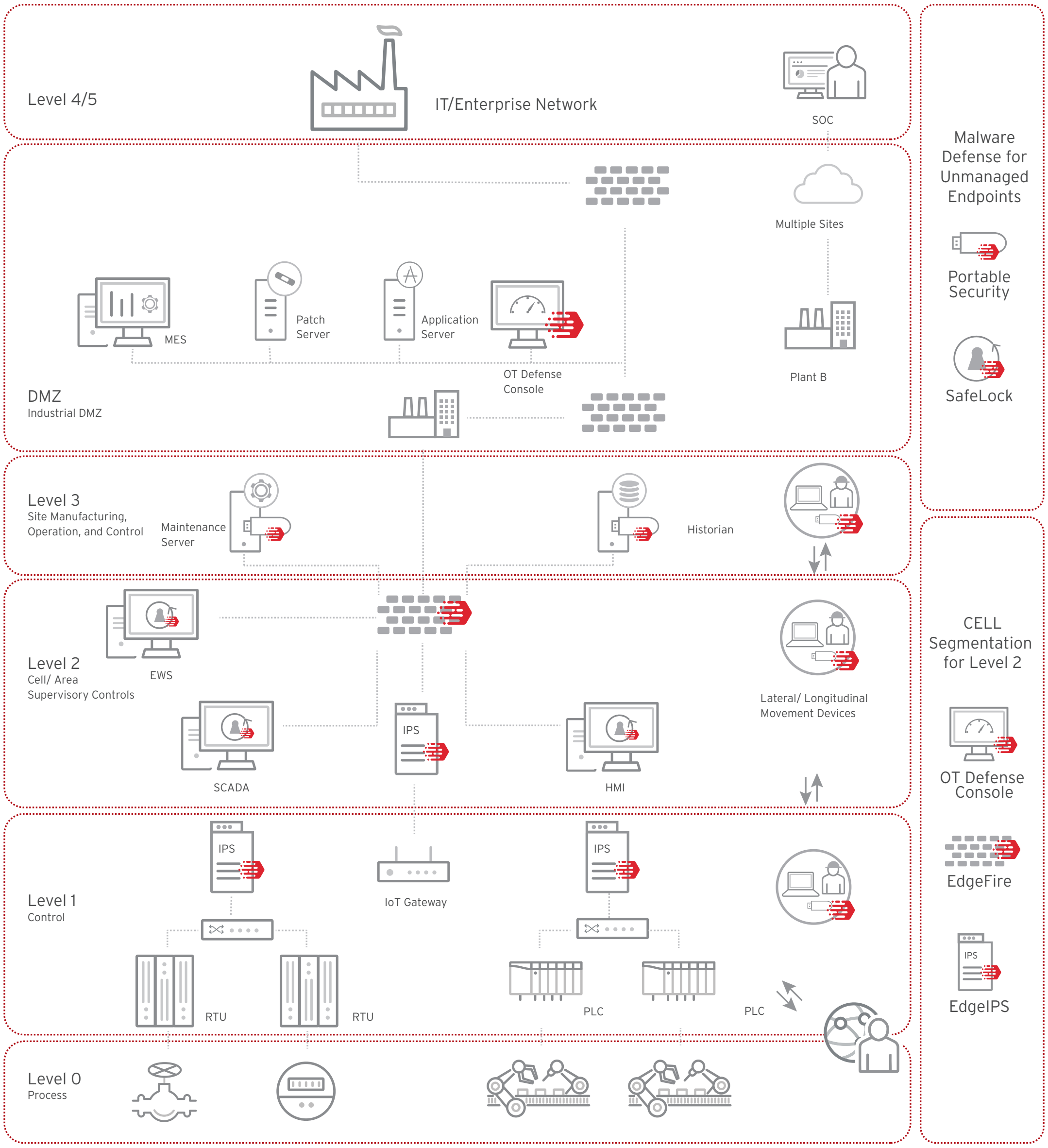
- Protection managed natively from the cloud provides zero-touch deployment, multi-tenant management, and complete control of your customers' security in one central location.
- Simple deployment and user-friendly management allow you to maintain security without compromising on performance.

10 INDUSTRIAL IOT SOLUTIONS

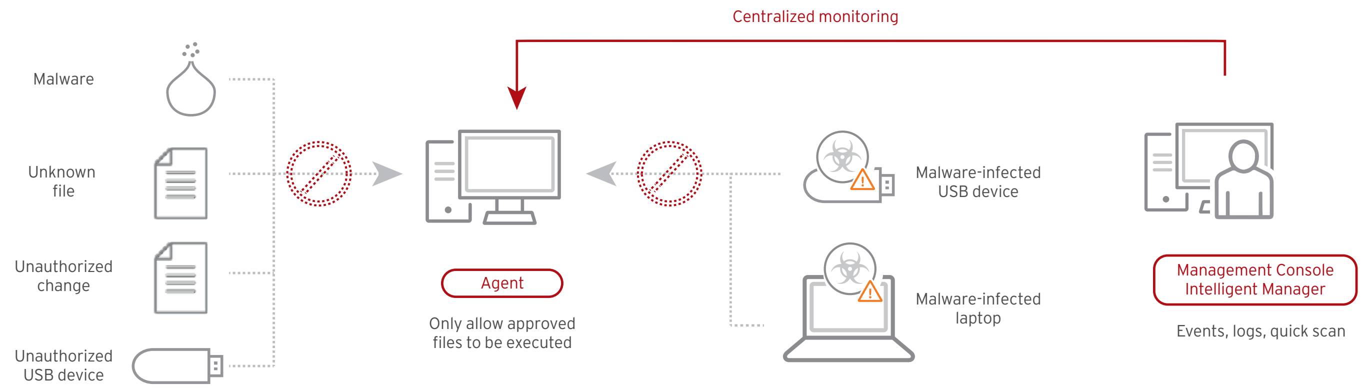
Industrial control systems (ICS) vulnerabilities are easy to exploit and are being attacked in ever-increasing numbers. In addition, many of these ICS systems include out-of-date equipment developed at a time when cybersecurity was not yet a serious issue. Therefore, these devices are particularly vulnerable to modern cyber threats. Installing patches and updates to address vulnerabilities can be very cumbersome. These complex environments span multiple layers, each of which needs to be protected. Traditionally, it remains unclear where the security responsibility for combining these levels lies. In the industrial environment, there are more and more security violations and incidents that could not only lead to operational disruptions, but could even endanger lives.

TXOne Networks

TXOne Networks provide solutions to address security vulnerabilities common in industrial environments. In doing so, TXOne Networks satisfies the needs of both critical infrastructure manufacturers and operators in order to develop the best approach with the greatest practicality. The result is a tailor-made technology that goes beyond conventional safety tools and assess complex challenges. Because ICS environments consist of multiple tiers and includes devices with different operating systems, TXOne Networks provides optimized network and endpoint-based products for real-time protection of OT networks and mission-critical devices.



Trend Micro™ Safe Lock™



Production, healthcare, and energy companies today face a growing number of cyber threats targeting ICS, industrial IoT devices, and embedded devices. Systems that use components of older operating systems are particularly vulnerable. They most likely don't match the current patch state and contain vulnerabilities that attackers can exploit. A lockdown can control the use of system resources and the execution of applications while limiting them to the minimum required for operation. Safe Lock protects against threats by effectively blocking the execution of malware even without signature files.

Benefits

- Minimal impact on performance
- Security solutions for industrial environments
- Easy deployment and maintenance
- Protection of older operating systems
- Security for mission-critical devices

Functions

- Agent application whitelisting
- USB device whitelisting
- Maintenance mode
- Write-protection integrity
- Monitoring protection against fileless attacks
- Protection against exploits
- Management of shared lists
- Pre-scan (malware verification during installation)
- Role-based administration
- Logging

Management Console (Intelligent Manager)

- Central monitoring notification
- Account management quick scan (checks files blocked by agent)
- Root-cause analysis
- Syslog forwarding
- Central management of trusted applications

Trend Micro™ Portable Security™ 3

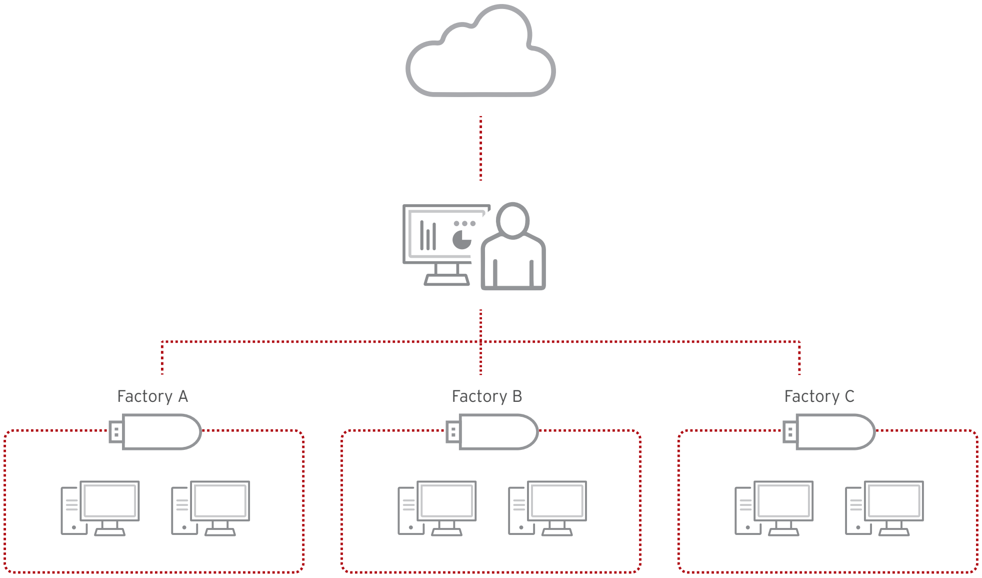
Trend Micro Portable Security 3 provides a solution for malware-scanning and removal in environments that include standalone and systems that are not networked, but allow data exchange via USB sticks, DVDs, and other ways. This portable tool can be connected to Windows or Linux-based devices via a USB port to detect malware and remove it (if necessary) without any software installation. When a scan is performed, colored LEDs indicate whether malware has been found or removed or if further investigation is required. In addition, Trend Micro Portable Security 3 collects important asset information during the scan, increasing the transparency of operational technology (OT) and eliminating undocumented Shadow OT. A centralized management program allows you to create policies and the investigation of scan logs for multiple Trend Micro Portable Security 3 tools and different locations, so that security responsibility provides a holistic overview of all endpoint devices. In addition, scan configurations can be transferred remotely or physically to multiple tools in different locations.

Benefits

- No installation required
- Easy operation
- Works across multiple platforms
- Eliminates Shadow OT
- Centralized management

Features

- Deletion or quarantine of malicious files
- Multiple options for malware scanning
- Current updates for malware signatures
- Supports on-demand and boot scans status
- Display via LED
- Integrated self-protection
- Integrated scan logs
- Supports Windows and Linux
- Collects asset information
- Supports case in file and folder names on Windows



TXOne EdgeIPS™

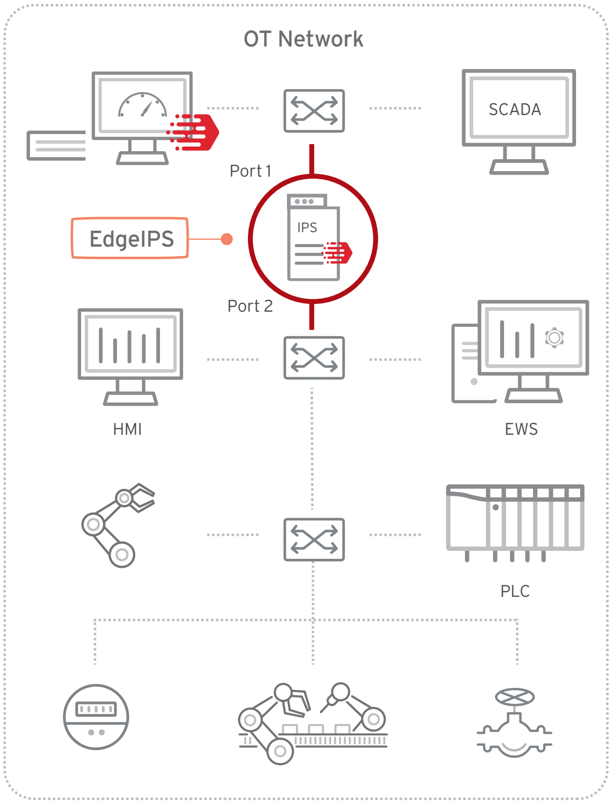
EdgeIPS protects business-critical machines, individual cells/ systems, as well as small production zones and supports uninterrupted production line operations. This solution enables reliable OT visibility, OT protocol filtering, and inline or offline functionality. EdgeIPS is specially developed to integrate into the network without disturbing the existing configuration. Industrial environments usually include tools and devices that were not designed to be connected to a modern company network. This provides reliable security which does not necessitate changes to the manually configured network topology. EdgeIPS ensures visibility and protection of legacy systems and devices without a patch, which forms the backbone of the production line and ensures uninterrupted operations.

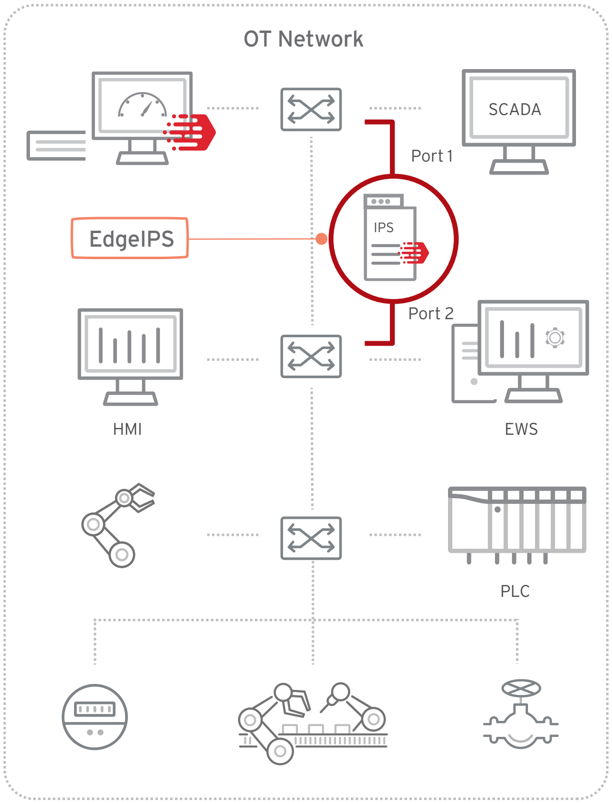
Advantages

- Minimizes time spent on configuration, maintenance, and administration
- Can be deployed at any location
- Increases the visibility and reliability of business-critical systems
- Does not require changes to network topology

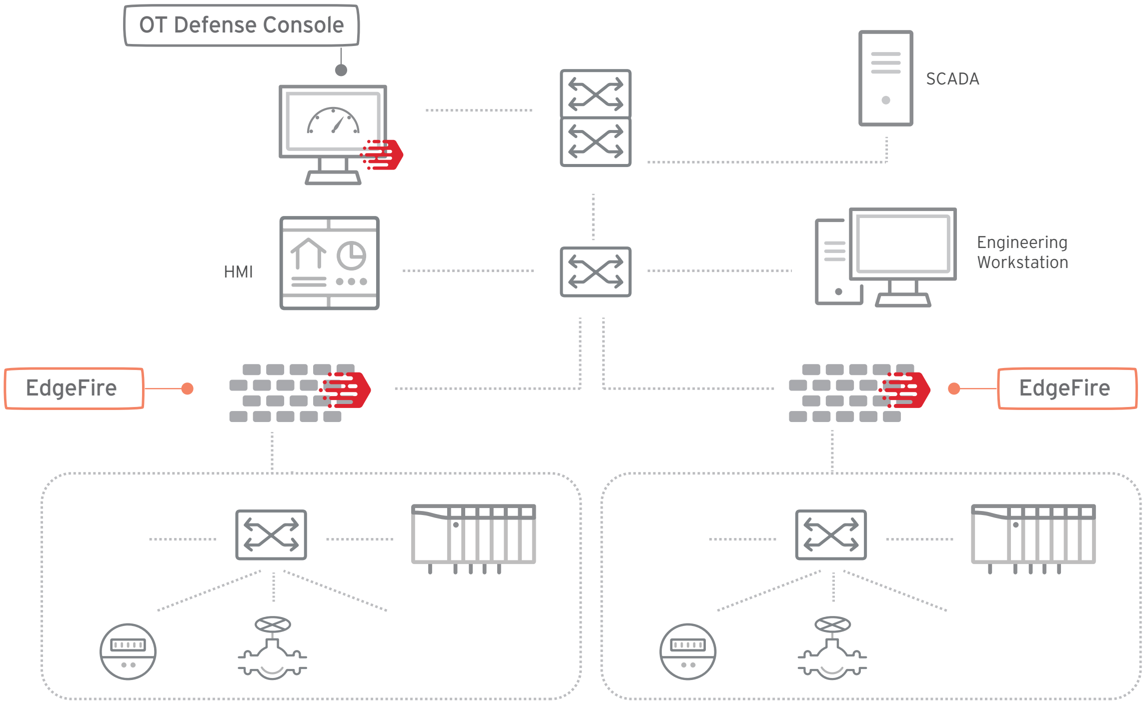
Features

- Visibility of network traffic
- OT protocol whitelisting controls for mission-critical systems
- Improved visibility of the Shadow OT through integration of IT and OT networks
- Signature-based virtual patching
- Switches between two flexible modes (monitor and protect)
- Uninterrupted operation in the event of network hardware failures
- Supports a wide range of industrial protocols
- Leading threat information and analysis
- Easy management centralization





TXOne EdgeFire™



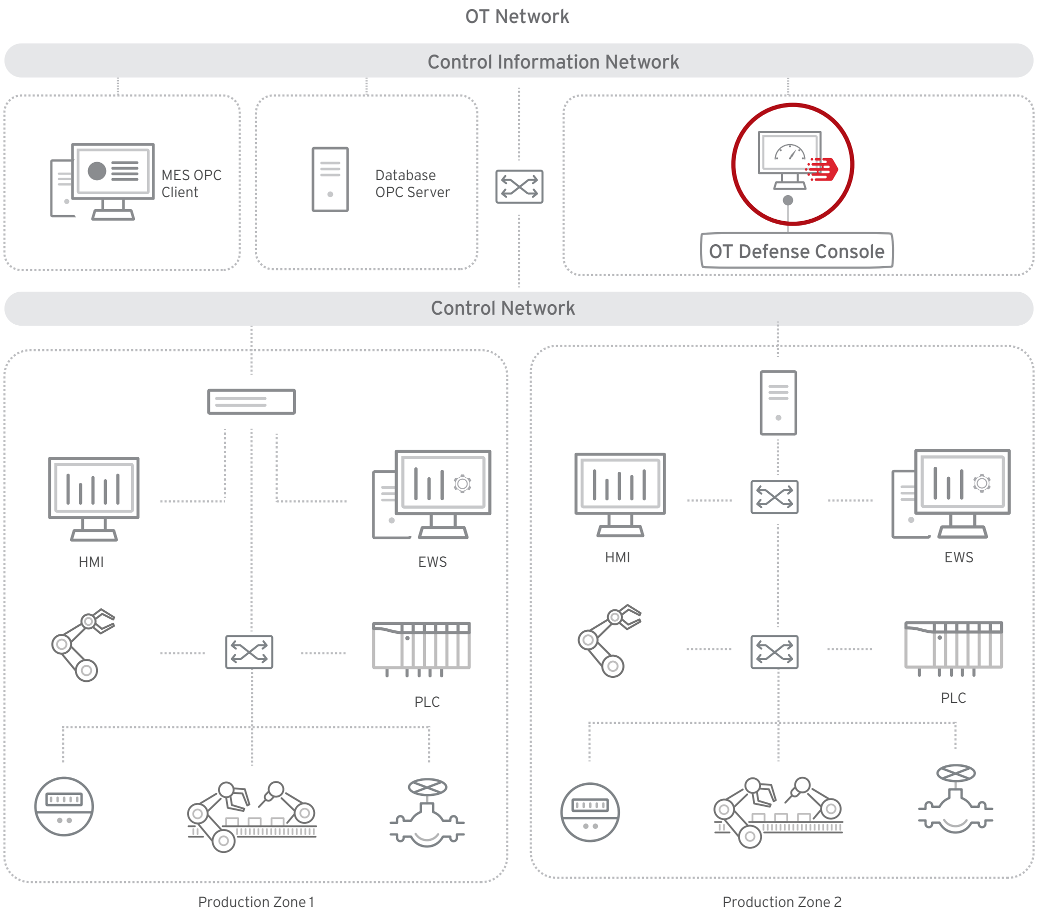
Due to the ever increasing integration of information and operational technology, the defense against threats must become an intuitive component. In traditional industrial environments, information technology (IT) and operational technology (OT) are usually operated separately from one another—each with its own network, maintenance team, goals, and requirements. In addition, industrial environments are made up of tools and devices that are not designed to connect to a corporate network. This makes the timely provision of security patches and updates extremely difficult. With EdgeFire Next-Generation Firewall, companies can optimize the effectiveness of their cyber defense.

Advantages

- Reliable firewall offers security, stability, and comfort
- Detects and blocks the spread of threats using unique hardware
- Offers full visibility into Shadow OT

Features

- OT protocol filter controls for mission-critical machines
- Improved visibility into Shadow OT through integration of IT and OT networks
- Signature-based virtual patching
- Switches between two flexible modes (monitor and protect)
- Supports a wide range of industrial protocols
- Leading threat information and analysis
- Flexible segmentation and isolation
- Centralized management



OT Defense Console

The manufacturing industry and critical sectors, such as oil and gas, mining, chemicals, energy, and defense have had to cope with crippling cyberattacks in recent years. Protecting infrastructure against threats is central to any operational technology (OT) environment. This poses a challenge for traditional IT security management because proprietary SCADA/ ICS networks and devices are often used that are both business-critical and highly sensitive. Industrial plants also require remote access by the manufacturer in order to receive prompt support. This further increases the complexity of OT network security. With the OT Defense Console (ODC), companies can achieve complete OT visibility and, if necessary, make immediate adjustments to ensure the smooth operation of the production line.

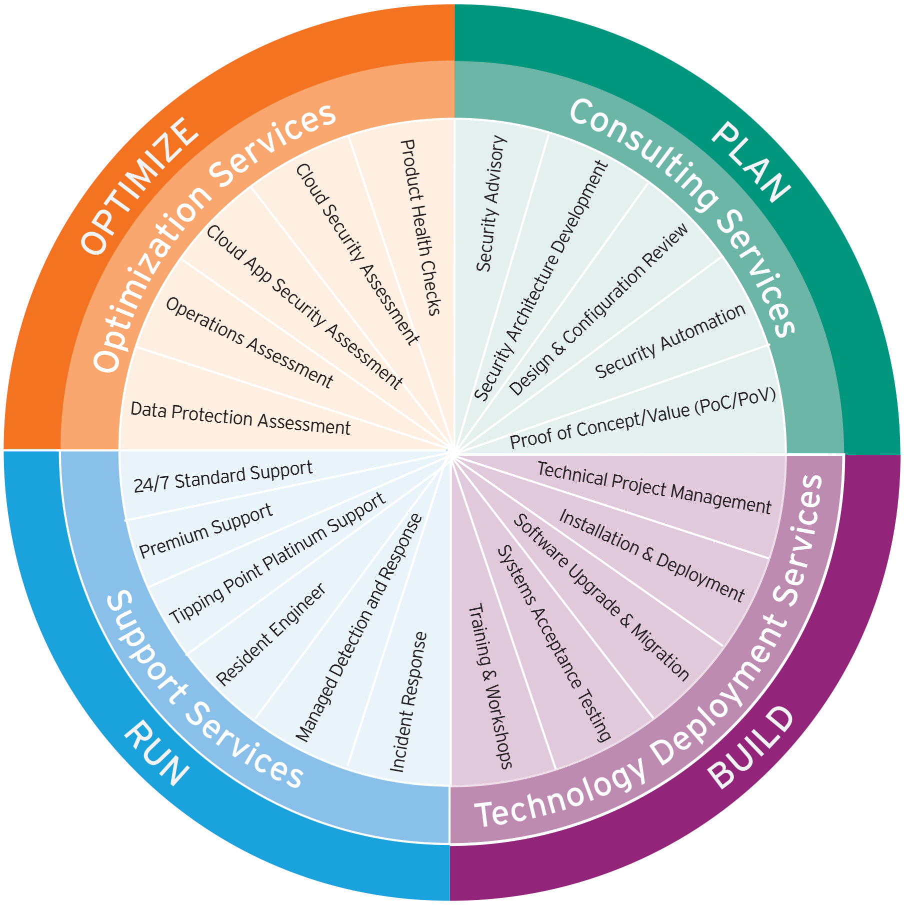
Advantages

- Designed for industry standard reliability, security, and flexibility
- Full visibility of large OT networks
- Improves usability and interconnectivity

Features

- Organization of all information with the ODC dashboard
- Overview of the cyber environment
- Easily manage large amounts of network nodes
- IPS and policy enforcement by group
- Convenient pattern and firmware updates
- Log view and query
- Form factor: Hardware or virtual appliance

11 SERVICE AND SUPPORT



PLAN
Consulting Services
Security Advisory
Security Architecture Development
Design & Configuration Review
Security Automation
Proof of Concept/Value (PoC/PoV)
BUILD
Technology Deployment Services
Technical Project Management
Installation & Deployment
Software Upgrade & Migration
Systems Acceptance Testing
Training & Workshops
RUN
Support Services
24/7 Standard Support
Premium Support
Tipping Point Platinum Support
Resident Engineer
Managed Detection and Response
Incident Response
OPTIMIZE
Optimization Services
Data Protection Assessment
Operations Assessment
Cloud App Security Assessment
Cloud Security Assessment
Product Health Checks

Services

With a global Service and Support Network, Trend Micro is uniquely positioned to support domestic and international customers with growing demands in IT security. Our services are based on traditional methods and allow you to use Trend Micro products and solutions to their full potential and protect your investments in the long term. Our services cover the complete life cycle of our solutions, from consultancy services (PLAN), supporting deployment (BUILD) and operation (RUN), to services aimed at optimizing the implementation of our solutions, increasing security levels and reducing administrative costs (OPTIMIZE).

The Trend Micro Service and Support Network spans the globe, with Trend Micro represented on every continent by experts in all of our products and services. Our support services are based on four global support centers (Centers of Excellence, [CoE]) that provide round-the-clock, top-quality support for your business-critical environments. As well as our Trend Micro technical specialists, our certified Professional Services partners are always ready to assist with delivery services in particular.

Consulting Services

Technology's short innovation cycles and the ever-changing threat landscape have given rise to various new approaches to IT security. In this highly competitive market, investment decisions must be weighed, made, and acted on quickly. Our Consulting Services give you access to the knowledge and experience of our technical experts to help you achieve your business goals.

Trend Micro's consultants plan and design your security infrastructure in close cooperation with your IT team:

- After a detailed assessment, experienced experts support your difficult, technical challenges with future-proof solutions. You'll be given a security architecture specifically tailored towards your needs and that maximizes the effectiveness of Trend Micro solutions.
- We demonstrate the advantages of Trend Micro solutions in a test environment using proofs of concept (PoC) and proofs of value (PoV). Our experts will demonstrate and explain functions based on your requirements, so that you can see concrete results even before you go ahead with a full-scale implementation.

Technology Deployment Services

Our Deployment Services help ensure that the implementation of your new products or upgrades of existing solutions in your IT infrastructure go off without a hitch, so you can enjoy maximum return on investment. Our team analyzes your network and system environment according to your performance requirements and security strategies. Trend Micro consultants work with you to create an implementation plan based on traditional methods. After the approval of the implementation plan, the solution is executed in accordance with your change management policies. The implementation generally ends with an acceptance test, which verifies the functionality of the features of the solution in your environment.

Training

Our comprehensive training program helps you to get to know and expand your knowledge surrounding the installation, configuration and administration of your selected Trend Micro solutions. Our courses are delivered by experienced trainers in authorized training centers (ATC) or in collaboration with our training partners. As well as theoretical teaching, they include laboratory tutorials, where the theoretical content is immediately put to practice. The courses cover our complete product portfolio and range from endpoint, email, and collaboration security training—through cloud and server security to protection from targeted attacks. Our training helps you make the best use of our products, reduce your administrative activities, improve vulnerability management in the company, and increase the company's overall protection.

Support

Trend Micro offers you comprehensive support services, which are typically provided by our support centers around the globe.

Support Offerings

What you can expect from Trend Micro Support Services	Standard Support*	Premium Support	Tipping Point Platinum Support
Telephone support	Around the clock (24/7)	Around the clock (24/7)	Around the clock (24/7)
Dedicated contacts	3	6	
Product upgrades and updates, and DV for TippingPoint	✓	✓	✓
Telephone, email, and web-based support	✓	✓	✓
Access to Customer Service Engineers (CSE)	✓	✓	✓
Suspicious file analysis (via Premium Support Connection)	✓	✓	
Installation and upgrade support	✓	✓	✓
Assignment of named Customer Service Manager (CSM)		✓	
Assignment of named Technical Account Manager (TAM)			✓
Priority case handling		✓	✓
TippingPoint hardware RMA	NBD shipment		NBD shipment
Advanced implementation services			✓
Advanced TippingPoint training			✓
On-going security assessments and recommendations		✓	✓
Regular conference calls		monthly	weekly
Number of regions		1	

*Trend Micro Standard Support is included with active maintenance agreements for all business products (see www.trendmicro.com/severitydefinitions).

For details on support, please see the Technical Support Guide at https://esupport.trendmicro.com/

Standard 24/7 Support

Trend Micro Standard Support includes access to customer service engineers and a highly-trained team of support specialists with years of experience dealing with daily security challenges. Customer Service Engineers assist you with urgent issues such as diagnosing and eliminating problems by email, phone, chat, or a web portal. Our specialists have deep security expertise as well as access to the Trend Micro global technical ecosystem and tools that help address the range of security concerns including content, data center, and risk management. Trend Micro Standard Support is included with active maintenance agreements for all business products. Outside of business hours, round-the-clock support is only for critical cases (see www.trendmicro.com/severitydefinitions).

Customer Service Engineer

Trend Micro Customer Service Engineers are dedicated to staying on top of the continually evolving threat landscape. They dedicate at least 25% of their time to developing their personal knowledge base—attending internal and external trainings, completing hands on product-readiness exercises, and researching new security threats. Trend Micro Customer Service Engineers are trained to deal with today's IT challenges, including data center modernization using cloud, multi-cloud, and container environments, as well as targeted attacks that are putting your valuable information at risk.

Trend Micro™ Premium Support

Continuously assessing and managing your security is a real challenge—especially as targeted attacks and other threats arrive on breakthrough technologies like mobile and cloud. We know how difficult it is to continually secure and protect your data and infrastructure against new threats. Trend Micro Premium Support provides you with expert resources to give you the personalized solutions you need to stay protected. A personalized Customer Service Manager (CSM) will help you implement your security in the way that is most effective for your business. These security experts are thoroughly trained to provide prompt guidance on threat response, planning, preparedness, and solution optimization. Customer Service Managers focus on your environment, business processes, and security posture to make sure you receive the highest return on your security investment. They are your champions inside Trend Micro.

Trend Micro Premium Support includes:

- Optimized implementation of your Trend Micro security solution for the best possible protection of your particular environment.
- Real-time advice on current security threats and risks that help you avoid infections and targeted attacks and prevent loss of intellectual property and other data.
- Periodic health checks to ensure ongoing protection against data loss and business interruption.
- Expert consultation on your particular security issues. This will help you save time and money by avoiding the cost of researching security options and by implementing only optimal solutions.
- Regular security planning meetings with your management teams to ensure you get the most out of your security systems and can prioritize security investments based on your needs and objectives. Your Customer Service Manager will provide a detailed evaluation of your security profile, looking at where the gaps reside and how you can best fill them.

Customer Service Manager

Customer Service Managers are committed to collaborating closely with your team to deliver highly responsive, personalized service and protection. They focus on your business to deliver operations strategies to best fit your environment. Your Customer Service Manager works alongside you to help address the most challenging aspects of security, improve your security profile across technologies, processes, and people, and configure your Trend Micro security solutions to achieve optimized IT service levels.

TippingPoint Platinum Support

TippingPoint Platinum Support is the best choice for customers who exclusively use TippingPoint products for comprehensive threat protection against vulnerabilities in their IT infrastructure. A dedicated Technical Account Manager (TAM) specialized in TippingPoint products gives you prompt and accurate solutions to issues and acts as your direct contact for your tailored support services.

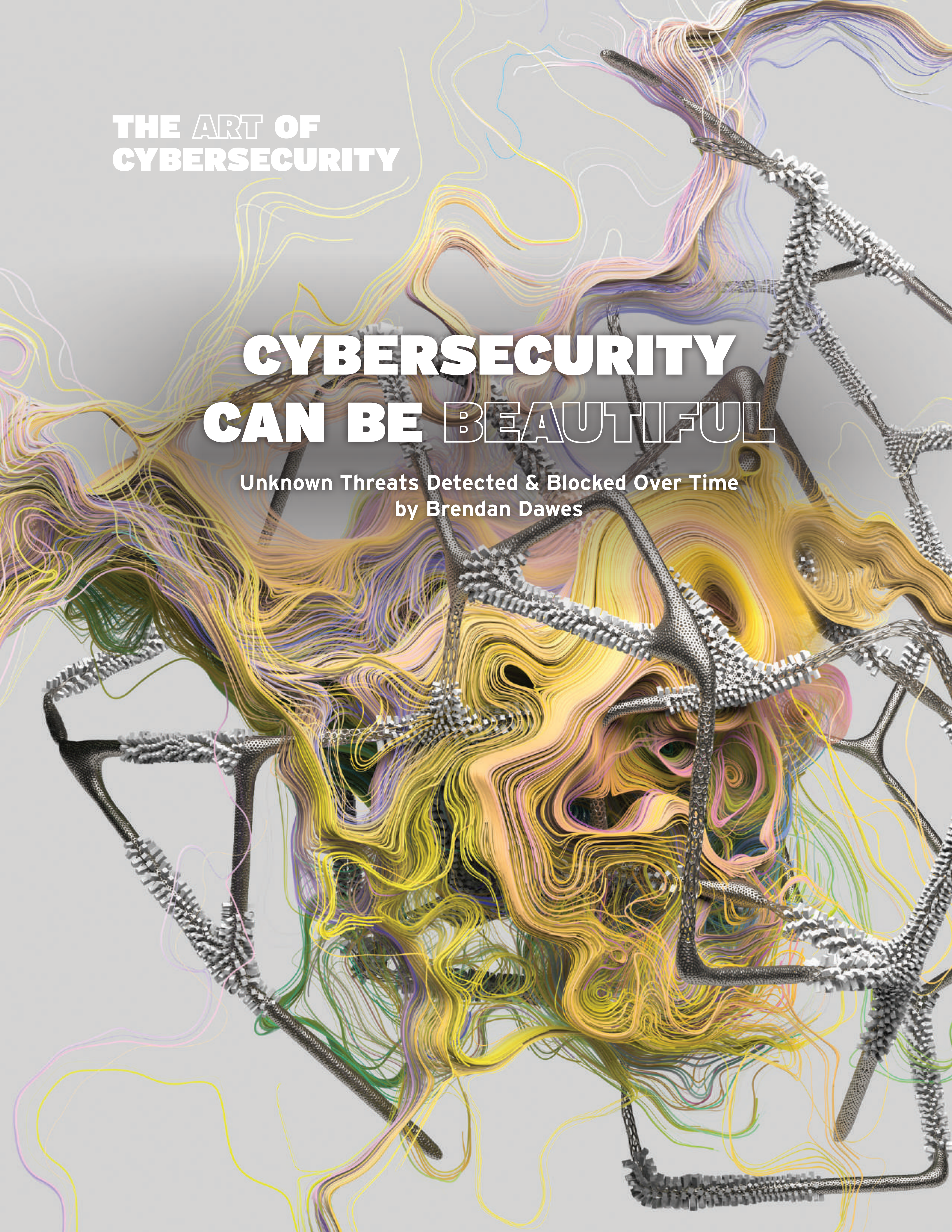
In addition to a dedicated point of contact, TippingPoint Platinum Support also includes the following services:

- Onsite Advanced Training for up to 12 participants per year. The foundation for this training is a standard training course that Trend Micro tailors to the customer's specific needs.
- Advanced Implementation Services (AIS) for up to 10 days per year. For example, this can be used to configure and deploy additional TippingPoint appliances or plan and execute a migration. This service can be rendered remotely or on-site, depending on the particular project requirements.
- Custom Digital Vaccine. Customers will have varying filter requirements which may be driven by legacy applications, unique network architectures, or systems deployments and internal security policies. Trend Micro researches, develops, tests and delivers up to five custom DV filters per year based on customer specification.

Technical Account Manager

The Technical Account Manager (TAM) collaborates closely with your team as a dedicated point of contact for all issues relating to your TippingPoint infrastructure. Keeping up to date on the customer's current network and security infrastructure is essential to assisting in troubleshooting and diagnosis, whether remotely or onsite. Open issues, upcoming projects, and the current status of support cases are discussed in weekly conference calls. The Technical Account Manager can also perform up to two deployment reviews per year.

CYBERSECURITY CAN BE BEAUTIFUL



Unknown Threats Detected & Blocked Over Time
by Brendan Dawes

12 LICENSING GUIDELINES

Licensing Small and Medium Business (SMB) Products

Trend Micro SMB products are available with a minimum of five users, with the following exceptions:

- Worry-Free Services, which is available with a minimum of two users.
- Trend Micro Worry-Free products, where a license is required for the total number of clients and servers. Every virtual machine on which a Worry-Free solution is installed is included. Between 5 and 250 users can be licensed.

Example

Company X wants to use Worry-Free Advanced to protect its network. The company has 5 servers and 40 PC seats, as well as 30 employees. Licenses are required for 45 users.

Licensing Enterprise Products

Every user who has access to a device that can, directly or indirectly, access servers that protect network traffic or data stored on the servers using the installed Trend Micro software requires a license. This also applies to the use of one device by several employees at different times. The basis for calculating the number of licenses required may be, for example, the number of personalized email accounts. The number of servers on which the product is installed is not relevant here.

Example 1

Company X purchases a security solution for 400 personalized email accounts on the Microsoft Exchange mail server. It purchases Trend Micro™ ScanMail™ for Microsoft® Exchange® for 400 users.

(Aliases such as info@trendmicro.com, sales@trendmicro.com etc. are not personalized mailboxes.)

Example 2

Company Y purchases Trend Micro Enterprise Security for Endpoints as a security solution for its clients. The number of licenses required depends on the number of users to be protected, rather than the number of laptops, workstations, or servers in use. The company wants to protect 100 employees, who use a total of 120 PCs and laptops. Licenses are required for 100 users.

Deep Security: Licenses are required for the number of (virtual) desktops/servers installed. CPU-based licensing is possible as an alternative. Each workload in public cloud environments must be licensed.

Example

Company X wants to use Deep Security to protect its four ESX servers, each with two CPUs. Five virtual machines are used per server. Therefore, 20 virtual machines are licensed.

Cloud One Workload Security: The prepaid annual subscription includes all security modules. The one-year subscription protects a specified number of AWS instances. The price per instance is independent of the size of the instance.

Cloud One Workload Security can alternatively be charged on a pay-as-you-go, usage-based model starting at USD 0.01/hour. The pricing for usage-based billing does take the size of the instance into account.

Trend Micro Enterprise products are available with a minimum of 26 users with the following exceptions:

Smart Protection Suites (Endpoint and Complete)
Minimum of 101 users

Endpoint Sensor as a Service and Sandbox as a Service
Minimum of 25 users

XDR and Managed XDR Services
Minimum of 500 users

For Deep Discovery and TippingPoint requests, please contact our sales team at: us_info@trendmicro.com

Licensing support services

For Premium Support services, please contact our sales team at: us_info@trendmicro.com for an individual quote.

New purchase

New purchasers are customers that are purchasing their first Trend Micro license, or that are purchasing a certain product for the first time. The date of purchase is considered the start date of the license. The duration of the license is always one year. If a multi-year licensing agreement is signed, the first year is regarded as a new purchase. The following years are regarded as extensions.

Additional seats

An extended license refers to the purchase of additional "users" by customers that already have a valid license for a specific product. Extended licenses have a validity period of 12 months, which begins on the day of delivery. A license upgrade may provide the customer with a higher license scale and thus a lower per-license fee. There are always three steps in the calculation of an extended license:

Step 1:

The number of new users is added to the number of existing users.

Step 2:

The increase of the number of licenses is based on the price of one license of the total volume.

Step 3:

To align the maintenance period expiration dates of the old and new licenses, the duration of the existing licenses must be extended.

Maintenance renewal

In order to keep usage rights for a Trend Micro product, a year-long maintenance renewal must be purchased before the license validity period expires. Maintenance for 12 months is included in the purchase price for the first installation year (new purchase). Maintenance includes software upgrades, scan engine and pattern file updates, as well as access to our 24/7 standard support. Thereafter, the maintenance fee is equal to 30% of the current list price for 12 months (35% for Worry-Free solutions; for exceptions, see "Maintenance Renewals for Services").

When a license is extended, the new validity period begins the day after the expiry of the previous license. This also applies where the customer extends their license after the expiry of the previous license.

Example

The license ends on July 7th.

Maintenance renewals for services/subscriptions

Trend Micro services are based on an annual usage fee of 100% of the current list price: There is therefore no maintenance renewal in the traditional sense. This applies to the Smart Protection Suites or Worry-Free Services, for example.

Cross-upgrades

A cross-upgrade indicates a customer's change from one Trend Micro product or suite to another suite. Trend Micro products already in use and under maintenance agreements can be credited at their license volume. Existing maintenance of the individual product(s) expires and is renewed for 12 months upon purchase of the product bundle.

Cross-grades

In a cross-grade, a customer changes from one existing platform to another, e.g. from Trend Micro™ ScanMail™ for Exchange to Trend Micro ScanMail for IBM Domino. In this case, the start and expiry dates of the original license remain the same. There is no change of fee of the current list price.

Discounts

Government discount (eGovernment) up to 30% applicable to national or local authorities, cities, counties, offices, administrations, community hospitals, organizations of which 50% or more belongs to said institutions, as well as statutory bodies.

Academic discount (NGO/NPO) up to 40%

Applicable to all non-government/non-profit organizations, state or state-approved general education, or vocational schools or colleges, state-approved institutions of adult education, as well as non-commercial institutions (churches and faith-based organizations, societies with proof of their non-profit nature such as the Red Cross, IOC, UNICEF, etc.).

Competitive Discount

Trend Micro grants a discount if one or more fee-incurring and comparable competitor products are replaced. The proof of license for the existing competitor product must be present at the time of ordering at the latest.

Evaluation licenses

Every license can be tested for 30 days at no cost. To download an evaluation license, go to www.trendmicro.com. Please contact us if your customer needs an evaluation key for a longer period.

Merging corporate licenses

Licenses of two corporate companies can be merged or changed during a maintenance alignment (matching products with the same expiration date). This has to be discussed with a Trend Micro employee.

The corporate company losing its licenses by transferring them to the corporation needs to declare its consent in written form.

Other

Trend Micro licensing is based on the "Global Business Software and Appliance Agreement": www.trendmicro.com/en_us/about/legal.html?modal=en-english-global-business-software-appliance-agreementpdf#t4

For large clients individual provisions that differ from those described here may be considered. Subject to change.

13 ANALYST OPINIONS, INDUSTRY TESTING, AND CUSTOMER REFERENCES

We have been named a leader in endpoint security, cloud workload security, email security, and enterprise detection and response. We also have the most advanced threat intelligence network in the world, our Trend Micro Smart Protection Network, which is continually enhanced by big data analytics and machine learning and is bolstered by hundreds of Trend Micro security experts and the Zero Day Initiative (ZDI).

Cross Solution

Mitre Att&ck APT29 test

In this testing, MITRE took on the persona of APT29, a threat group that has been attributed to the Russian government and has operated since at least 2008. As a first-time participant in the MITRE ATT&CK evaluation, we are proud to have ranked among the top tier of EDR vendors for our detection rates—showing a great balance of detection capabilities across the full attack chain.

https://resources.trendmicro.com/MITRE-Attack-Evaluations.html

Trend Micro has been named a Leader in The Forrester Wave™: Enterprise Detection and Response, Q1 2020

"Trend Micro delivers XDR functionality that can be impactful today."

User Protection

Trend Micro named a leader once again in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms.[4]

Trend Micro has been positioned by Gartner as the Leader in every Magic Quadrant for Endpoint Protection Platforms and Magic Quadrant for Enterprise Antivirus since 2002.[5]

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trend Micro is named a leader in The Forrester Wave™: Endpoint Security Suites, Q3 2019.[6]

"Trend Micro continues to offer the most complete endpoint security solution."

"Their endpoint security offerings span the full gamut of threat prevention and detection, with market-leading capabilities in both categories."[7]

Trend Micro name a Leader in the Forrester Wave, Enterprise Email Security, Q2 2019[8]

"As one of the pioneers of email security, Trend Micro has a long history of protecting inboxes and delivering innovations like writing style DNA, for preventing email impersonation, and Computer Vision detection, for detecting fake login sites."

[4] Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 2019

[5] https://www.trendmicro.com/en_au/about/newsroom/press-releases/2019/20190828-trend-micro-positioned-as-a-leader-again-in-gartner-magic-quadrant-for-endpoint-protection-platforms.html

[6] https://resources.trendmicro.com/Forrester-Endpoint-Leadership-Report.html

[7] The Forrester Wave™: Endpoint Security Suite, Q3 2019

[8] The Forrester Wave™: Enterprise Email Security, Q2 2019

Hybrid Cloud Security

IDC
Analyze the Future

Trend Micro has been ranked #1 in Cloud Workload Security Market Share[9]

Gartner®

Trend Micro has determined we meet all 8 of 8 core capabilities for hybrid cloud workload protection.[10]

FORRESTER®

Trend Micro named a Leader in the Forrester Wave: Cloud Workload Security[11]

Global Threat Research

IHS Markit®

The Trend Micro Zero Day Initiative (ZDI) is the leader in global vulnerability research.[13]

[9] IDC Market Share Report for Cloud Workload Security, Q4 2019

[10] https://resources.trendmicro.com/2018-EU-BE-Gartner_CWPP.html

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[11] Forrester Wave: Cloud Workload Security, Q4 2019

[13] Research from the National Institutes of Standards and Technology (NIST) National Vulnerability Database (NVD)

Success Stories

RICOH USA

Solutions:

- Trend Micro™ OfficeScan™
- Trend Micro Deep Security

CLUBCORP USA

Solutions:

- Managed detection and response services (Trend Micro™ MDR)
- Endpoint detection and response (EDR)
- Trend Micro Apex One as a Service
- Trend Micro Cloud App Security
- Trend Micro™ Control Manager™
- Trend Micro Deep Security

NASA

Solution:

- Trend Micro Deep Security

CARHARTT

Solutions:

- Trend Micro™ Smart Protection™ Complete
- Trend Micro™ OfficeScan™ XG
- Trend Micro Cloud App Security
- Trend Micro Data Loss Prevention
- Trend Micro Control Manager
- Trend Micro Deep Security

ESSILOR OF AMERICA

Solution:

- Trend Micro Deep Security

LIVE NATION

Solutions:

- Trend Micro Smart Protection Suites
- Trend Micro OfficeScan
- Trend Micro Deep Security
- Trend Micro Cloud App Security
- Trend Micro Deep Discovery

DHR HEALTH

Solutions:

- Trend Micro™ Deep Discovery™ Family
- Trend Micro Smart Protection Complete
- Trend Micro Deep Security
- Trend Micro ScanMail for Exchange
- Trend Micro Apex One
- Trend Micro Apex Central
- Trend Micro Hosted Email Security
- Trend Micro™ Mobile Security for Enterprises

COMMUNITY NATIONAL BANK

Solutions:

- Trend Micro Smart Protection Suites
- Trend Micro OfficeScan
- Trend Micro™ InterScan™ Messaging Security
- Trend Micro Deep Discovery Analyzer
- Trend Micro Control Manager

COLLIN COUNTY

Solutions:

- Trend Micro OfficeScan
- Trend Micro Control Manager
- Trend Micro™ InterScan Messaging Security Virtual Appliance™

UNIVERSITY OF FLORIDA AT SHANDS

Solutions:

- Trend Micro Smart Protection Suites
- Trend Micro OfficeScan
- Trend Micro InterScan Messaging Security
- Trend Micro™ InterScan Messaging Security Virtual Appliance™
- Trend Micro ScanMail
- Trend Micro Control Manager
- Trend Micro Data Loss Prevention
- Trend Micro Deep Discovery
- Trend Micro Deep Security
- Trend Micro Premium Support Services

DATA BANK

Solution:

- Trend Micro™ TippingPoint™ 8400TX Threat Protection System

MEDIMPACT

Solutions:

- Trend Micro TippingPoint
- Trend Micro Deep Discovery Inspector
- Trend Micro Deep Discovery Analyzer
- Trend Micro Deep Security
- Trend Micro Apex One™ as a Service
- Trend Micro Apex Central
- Trend Micro™ Endpoint Sensor
- Trend Micro Cloud App Security
- Trend Micro™ Cloud Email Gateway Services

14 CONTACTS AND OTHER

Online registration (Customer Licensing Portal)

Trend Micro distributes product licenses with a registration key (RK), which is used to set up an account and register a product. After registration, the user must activate the software using an activation code (AC). This allows you to access the Trend Micro™ ActiveUpdate Server and download updated pattern files.

The registration of the Trend Micro product is your responsibility or the responsibility of your commissioned reseller.

Online registration enables the activation of a newly purchased product, the extension of an existing product, or the merging of box products. The following link brings you to the English online registration page: https://tm.login.trendmicro.com

Trials–beta program–download center–technical documentation

You are able to test the newest Trend Micro software solutions at any time. There is the opportunity to take part in beta testing and programs.

Find out more at: http://beta.trendmicro.com

You can also use the Trend Micro Update Centre to download Test and Demo software from the Trend Micro website. You typically have 30 days to trial your desired software. After the free trial period, you can purchase the license or end the evaluation period. For individual trial queries please contact your reseller. Find out more at: http://downloadcenter.trendmicro.com

Technical documentation such as administrator's guides, installation guides, system requirements, readmes are available at: http://docs.trendmicro.com

Trend Micro contacts

Technical Support Team–Find general support information, including the Download Center and Support Database under >>> "Support" in the main menu at www.trendmicro.com

To open a support case: http://esupport.trendmicro.com/srf/SRFMain.aspx

Contact Trend Micro free of charge*

For a complete, always up-to-date overview of Trend Micro success stories and references, please see: www.trendmicro.com

USA: 1-888-977-4200
Email: us_info@trendmicro.com

*Free on a landline in the respective country.
Charge for calls from mobile phones may vary.

www.trendmicro.com

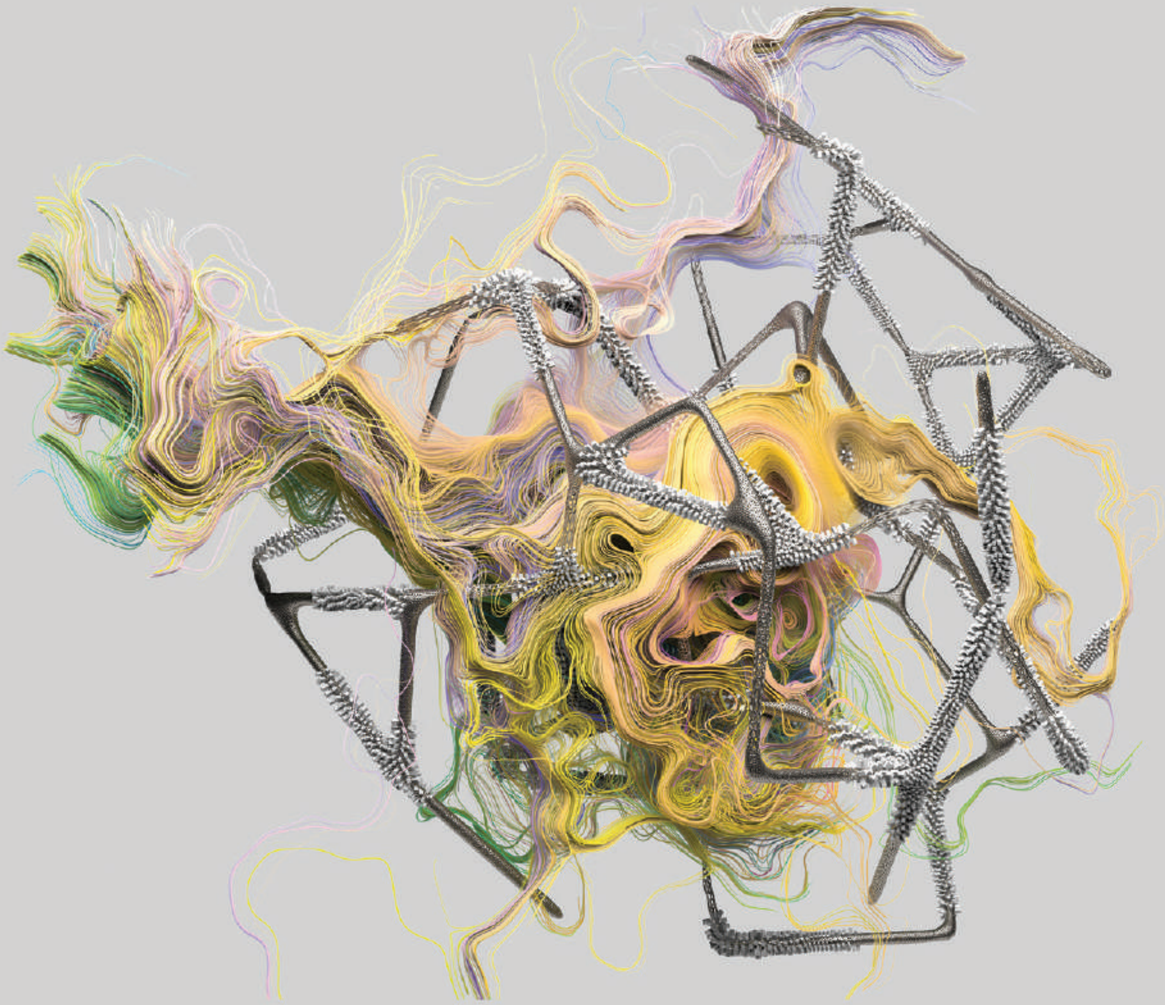
Data Privacy

At Trend Micro, your privacy is important to us. With the introduction of GDPR, our focus on security and data protection continues to be a top priority across the globe. You can find out more about our data privacy policies and information on how our products and SaaS solutions use data on our web site at: https://www.trendmicro.com/en_ca/about/legal.html

THE ART OF
CYBERSECURITY

CYBERSECURITY CAN BE BEAUTIFUL

Infrastructure Shifts and Early Protection by Trend Micro
by Andy Gilmore



TREND MICRO U.S.A. HEADQUARTERS

Trend Micro Incorporated
225 East John Carpenter Freeway, Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900
Toll-free: (888) 762-8736

This Trend Micro Product Guide is based on information available as of July 4, 2020.

www.trendmicro.com