Trend Micro™

APEX ONE™

Automatic, insightful, all-in-one endpoint security from the trusted leader

The threat landscape used to be black and white – you kept the bad stuff out and the good stuff in. Now it's harder to tell the good from the bad, and traditional signature-based antivirus approaches alone are a weak defense against ransomware and unknown threats, which often slip through. Next-generation technologies help with some threats but is in no way foolproof, and adding multiple anti-malware tools on a single endpoint results in too many products that don't work together. To complicate matters your users are increasingly accessing corporate resources from a variety of locations and devices, and even services in the cloud. You need endpoint security that is smart, optimized, and connected, from a proven vendor you can trust.

Trend Micro™ Apex One™ uses a blend of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint. It constantly learns, adapts, and automatically shares threat intelligence across your environment.

This blend of protection is delivered via an architecture that uses endpoint resources more effectively and ultimately outperforms the competition on CPU and network utilization, giving you:

- Automatic detection and response against an ever-growing variety of threats, including fileless and ransomware
- Insightful investigative capabilities and centralized visibility across the network by using an advanced EDR and MDR toolset, strong SIEM integration, and an open API set
- An all-in-one lightweight agent with deployment flexibility through both software as a service (SaaS) and on-premises options

Apex One™ is a critical component of our **Smart Protection Suites** that delivers gateway and endpoint protection capabilities like application control, intrusion prevention (vulnerability protection), Trend Micro™ Endpoint Encryption™, Data Loss Prevention™ (DLP), and more, in one compelling package. Additional Trend Micro solutions extend your investigative capabilities with endpoint detection and response (EDR). All of this modern threat security technology is made simple for your organization with central visibility, management, and reporting.

YOU CAN HAVE IT ALL

- **Advanced malware and ransomware protection:** Defends endpoints–on or off the corporate network–against malware, trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like cryptomalware and fileless malware.
- **Detection and response capabilities:** Advanced detection and response capabilities are included with Apex One™. An optional investigation tool, Trend Micro Endpoint Sensor, and our managed detection response (MDR) service are available as add-ons.
- **The industry's most timely virtual patching:** Apex One™ Vulnerability Protection™ virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable.
- **Connected threat defense:** Apex One™ integrates with other security products locally on your network and also via Trend Micro's global cloud threat intelligence to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection and reducing the spread of malware.
- **Centralized visibility and control:** When deployed with Trend Micro™ Apex Central™, multiple capabilities can be managed through a single console to provide central visibility and control across all functions.
- **Mobile security integration:** Integrate Trend Micro™ Mobile Security™ and Apex One™ by using Apex Central™ to centralize security management and policy deployment across all endpoints. Mobile Security includes mobile device threat protection, mobile app management, mobile device management (MDM), and data protection.
- **Available on-premises or as a service:** Apex One™ can be deployed on site in your network or is available as a service, with full product parity between the two deployment options.

Protection Points

- Physical endpoints
- Virtualized endpoints (add-on)
- Windows PCs and servers
- Mac computers
- Point of sale (POS) and ATM endpoints

Threat Protection

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory and browser attacks)
- File reputation
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Data Loss Prevention
- Device control
- Good file check
- Sandbox and breach detection integration
- Detection and response
- Endpoint Encryption
- Vulnerability Protection

See how we stack up

KEY BUSINESS ISSUES

* Too many malware and ransomware threats getting through

* Need one solution to protect against all known and unknown threats on PC endpoints, Macs, and VDI

* Endpoint security solutions that don't talk to each other, lengthens time to protection and increase the management burden

* Risks of users working remotely, and sharing information in new ways via the cloud, etc.

* IT efficiency reduced when advanced threat and data protection don't integrate

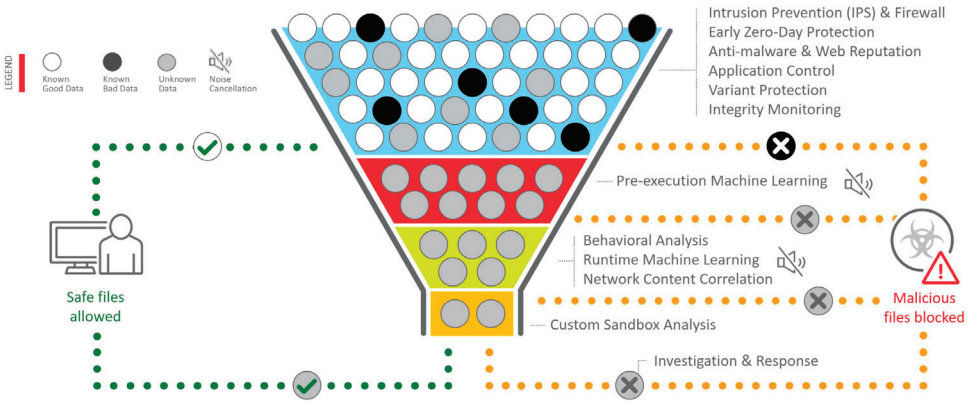
* Difficulty correlating and prioritizing all alerts coming through

Trend Micro User Protection solution is powered by XGen™, a smart, optimized, and connected security approach.

ADVANTAGES

Maximum XGen™ security

- Infuses high-fidelity machine learning with other advanced detection techniques for the broadest protection against ransomware and advanced attacks.



- Progressively filters out threats using the most efficient technique for maximum detection without false positives.
- Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.
- Trend Micro is the first to infuse high-fidelity machine learning which uniquely analyzes files not only before execution but also during runtime for more accurate detection.
- Noise cancellation techniques like census and whitelist checking at each layer reduce false positives.
- Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks.
- Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, and even recovers lost files if necessary.

Minimal Impact

Reduce user impact and management costs

- Apex One™ as a Service (only available from Smart Protection Suites) allows you to deploy and manage Apex One™ from our cloud-based service and offers full feature parity with the on-premises option.
- This lightweight and optimized agent uses the right detection technique at the right time to ensure minimal impact on devices and networks.
- Comprehensive central view of endpoint status lets you get visibility to security risks quickly.
- Automatic sharing of threat intelligence across security layers enables protection from emerging threats across the whole organization.
- Enable off-premises compliance and protection with the Edge relay that enables employees to work outside the corporate network and still connect to Apex One™ without a VPN.
- Customizable dashboards to fit different administration responsibilities.
- 24/7 support means that if a problem arises, Trend Micro is there to resolve it quickly.

Proven Security Partner

Trend Micro has a history of constant innovation to provide the most effective and efficient security technologies. We are always looking ahead to develop the technology needed to fight tomorrow's ever-changing threats.

- Thirty years of security innovation.
- Protects over 155 million endpoints.
- Trusted by 45 of the top 50 global corporations.
- Trend Micro positioned as one of only three Leaders amongst a field of 21 vendors in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.

Click here to learn more

> "With a network like ours, spread across the entire country, being able to secure mobile and desktop devices under one platform simplifies the security for our network and improves our team's productivity."

Greg Bell,
IT director, DCI Donor Services

CUSTOMIZE YOUR ENDPOINT PROTECTION

Apex One™ gives you the freedom to add additional security models and broaden protection. Choose from a range of advanced capabilities designed to efficiently satisfy your organization's needs:

Data Loss Prevention (DLP)

Trend Micro™ Apex One™ DLP™ minimizes the complexity and cost of data security by integrating DLP functionality directly into your existing Trend Micro endpoint solution. Quickly and easily gain visibility and control of your sensitive data and prevent data loss via USB, email, software as a service applications, web, mobile devices, and cloud storage. Leverage built-in regional and industry-specific templates to simplify deployment and comply with regional guidelines and regulations. Apex One™ DLP™ allows you to deploy data security for a fraction of the cost and time of traditional enterprise DLP solutions.

APEX ONE™ DLP™ ON ENDPOINTS

- **Strengthens Data Protection and Control**
  - Empowers IT to restrict the use of USB drives, USB attached mobile devices, CD/DVD writers, cloud storage, and other removable media with granular device control and DLP policies.
  - Enables cloud storage with DLP enforcement of file encryption as well as SaaS application usage with DLP for Microsoft® Office 365®.
  - Detects and reacts to improper data use based on keywords, regular expressions, and file attributes.
  - Educates employees on corporate data usage policies through alerts, blocking or soft-blocking, and reporting.
- **Supports Compliance**
  - Simplifies regulatory compliance with out-of-the-box compliance templates.
  - Speeds audits and enforcement with forensic data capture and real-time reporting.
  - Provides regional specific templates and data protection options, helping customers comply with data protection guidelines such as GDPR, PCI/DSS, HIPAA, GLBA, SB-1386, and US PII.
- **Streamlines Administration, Lowers Costs**
  - Improves visibility and control with a fully-integrated, centrally-managed solution
  - Reduces resource demand and performance impact with a single agent for endpoint security, device control, and content DLP.

Advantages of Apex One™ DLP™

- **Protect your data—today**

Deploy DLP immediately and gain visibility and control of your data right away

- **Lower DLP costs**

Save on deployment and maintenance costs compared to traditional DLP

- **Protect privacy**

Identify, monitor, and prevent data loss—on or off network

- **Comply with regulations**

Implement controls for protection, visibility, and enforcement

- **Educate users**

Notify employees of risky behavior or enforce user controls if necessary

- **Central Point of Visibility and Control**
  - Trend Micro™ Apex Central™ provides a convenient, centralized security management console that consolidates policy, events, and reporting, across multiple DLP solutions.
  - Apex Central™ also includes access to threat statistics from the Trend Micro™ Smart Protection Network™, cloud-based security infrastructure. Administrators gain insight into both the global threat landscape and the protective power of Trend Micro security in their own environments.
- **Protect Data at Rest, In Use, and In Motion**
  - Data at rest with wide coverage of file types.

✓ Apex One™ DLP™ can recognize and process over 300 file types, including most email and office productivity applications, programming languages, graphics, engineering files, and compressed or archived files. Discovery capabilities scan the endpoint, file server, mail store, Microsoft© SharePoint© Portal Server repository, including SaaS applications and cloud storage, to see where compliance data is located.

- Data in motion control points

✓ Apex One™ DLP™ gives you visibility and control of data in motion—whether it's in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP.

- Data in use control points

✓ Apex One™ DLP™ provides visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen.

- **Data Identifiers**
  - In addition to templates, Apex One™ DLP™ includes a granular list of truly international identifiers to identify specific data by patterns, formulas, positioning, and more. Identifiers can also be created from scratch.
- **Complete User Protection**
  - Apex One™ DLP™ is part of Trend Micro Complete User Protection, a multi-layer solution which provides the broadest range of interconnected threat and data protection across endpoints, email and collaboration, web, cloud storage, SaaS applications, and mobile devices.
- **DLP Policies and Reporting**
  - Managed through the administrative console of the host application. In cases where more than one DLP solution is deployed, policies and reporting can be consolidated to a single console through Trend Micro Apex Central™.

Security for Mac Module provides a layer of protection for Apple Mac clients on your network by preventing them from accessing malicious sites and distributing malware—even if the malware is not targeted at Mac OS X.

- Reduces exposure to web-based threats, including fast-spreading 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.

Virtual Desktop Infrastructure (VDI) Module lets you consolidate your endpoint security into one solution for both physical and virtual desktops.

- Recognizes whether an agent is on a physical or virtual endpoint and optimizes protection and performance for its specific environment.
- Serializes scans and updates, and whitelists base images and previously scanned content to preserve the host resources.

Endpoint Encryption Option ensures data privacy by encrypting data stored on your endpoints—including PCs, Macs, DVDs, and USB drives, which can easily be lost or stolen. Trend Micro™ Endpoint Encryption provides the data security you need with full-disk encryption, folder and file encryption, and removable media encryption.

- Automates data management with self-encrypting hard drives.
- Encrypts data in specific files, shared folders, removable media.
- Sets granular policies for device control and data management.
- Manages Microsoft Bitlocker and Apple FileVault

VULNERABILITY PROTECTION OPTION

Backed by world-class vulnerability research, Apex One™ security's virtual patching delivers the most-timely vulnerability protection in the industry across a variety of endpoints, including point of sale (POS) and Internet of things devices (IoT), and devices with end-of-support (EOS) operating systems.

Stop zero-day threats immediately on your physical and virtual desktops and laptops—on and off the network.

Trend Micro™ Vulnerability Protection, along with Trend Micro's portfolio of endpoint capabilities extend protection to critical platforms, including legacy operating systems such as Microsoft® Windows® XP.

- **Defends Against Advanced Threats**
  - Blocks known and unknown vulnerability exploits before patches are deployed.
  - Protects end of support and legacy operating systems, for which patches may never be provided.
  - Automatically assesses and recommends required virtual patches for your specific environment.
  - Dynamically adjusts security configuration based on the location of an endpoint.
  - Protects endpoints with minimal impact on network throughput, performance, or user productivity.
  - Shields endpoints against unwanted network traffic with multiple protection layers.
  - Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance.
- **Removes Bad Data from Business-Critical Traffic**
  - Applies control filters to alert/block specific traffic such as instant messaging and media streaming.
  - Uses deep packet inspection to identify content that may harm the application layer.
  - Filters forbidden network traffic and ensures allowed traffic through stateful inspection.
- **Provides Earlier Protection**
  - Provides protection before patches are deployed and often before patches are available.
  - Shields operating system and common applications from known and unknown attacks.
  - Detects malicious traffic that hides by using supported protocols over non-standard ports.
  - Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection.
  - Prevents networking backdoors from penetrating into the corporate network.
  - Blocks all known exploits with intrusion prevention signatures.
  - Defends custom and legacy applications using custom filters that block user-defined parameters.
- **Deploys and Manages with Your Existing Infrastructure**
  - Preserves endpoint performance with lightweight agent architecture.
  - Simply and easily deploys with existing endpoint security solutions.
  - Increases convenience of implementing granular control with simplified dashboard and user-based visibility with the management console.
  - Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information.
  - Provides logging integration with popular SIEM tools.
  - Simplifies deployment and management by by using the Apex One™ single agent, with centralized visibility and control Reduces the need to patch and reboot immediately causing unnecessary downtime on systems

SOFTWARE

Protection Points

- Endpoints
- Threat Protection
- Vulnerability exploits
- Denial of service attacks
- Illegitimate network traffic
- Web threats

KEY BENEFITS

- Eliminates risk exposure due to missing patches
- Extends the life of legacy and end-of-support operating systems like Windows XP
- Reduces down-time for recovery with incremental protection against zero-day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints

ENDPOINT APPLICATION CONTROL

Trend Micro Apex One™ Application Control™ allows you to enhance your defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on your corporate endpoints. With a combination of flexible, dynamic policies, whitelisting and blacklisting capabilities, as well as an extensive application catalog, this easy-to-manage solution significantly reduces your endpoint attack exposure. For even greater insight into threats; user-based visibility and policy management are available in the local administration console or in the centrally-managed Apex Central™. Apex Central™ also extends visibility and control across on-premises, cloud, and hybrid deployment models. Gain access to actionable threat intelligence with Trend Micro's connected threat defense from a local sandbox or the Trend Micro Smart Protection Network which uses global threat intelligence to deliver real-time security from the cloud, blocking threats before they reach you.

KEY FEATURES

Enhanced protection defends against malware, targeted attacks, and zero-day threats

- Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).
- Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network.
- Interconnects with additional layers of security to better correlate threat data and stop more threats more often.
- Leverages application data analyzed and correlated from over 1+ billion good file records (Trend Micro Smart Protection Network).
- Complements security like antivirus, host intrusion prevention, data loss prevention, and mobile protection, all integrated with Apex One™.

Simplified management speeds protection

- Increases convenience of implementing granular control with a customizable dashboard and management console.
- Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application.
- Provides greater insight into threat outbreaks with user-based visibility, policy management, and log aggregation. Enables reporting across multiple layers of Trend Micro security solutions through Apex Central™.
- Categorizes the applications and provides regular updates to simplify administration using Trend Micro's Certified Safe Software Service.

In-depth whitelisting and blacklisting blocks unknown and unwanted applications

- Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting.
- Contains broad coverage of pre-categorized applications that can be easily selected from Trend Micro's application catalog (with regular updates).
- Ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change.
- Features roll-your-own application whitelisting and blacklisting for in-house and unlisted applications.
- Delivers unparalleled breadth of applications and good file data.

Compliance with internal IT policies helps reduce legal and financial liabilities

- Limits application usage to a specific list of applications supported by data loss prevention (DLP) products for specific users or endpoints.
- Collects and limits application usage for software licensing compliance.
- Features system lockdown to harden end-user systems by preventing new applications from being executed.

SOFTWARE

Protection Points

- Endpoints
- Servers
- Embedded and point of sale (POS) devices

THREAT PROTECTION

- Vulnerability exploits
- Malicious applications (executables, DLLs, device drivers, Windows® store apps, and others)

ENDPOINT SENSOR OPTION

- Provides context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls enable you to:
- Record detailed system-level activities
- Perform multi-level search across endpoints using rich-search criteria such as OpenIOC, Yara, and suspicious objects.
- Detect and analyze advanced threat indicators such as fileless attacks.
- Rapidly respond before sensitive data is lost.

TREND MICRO APEX CENTRAL MODULE

This centralized security management console ensures consistent security management and complete visibility and reporting across multiple layers of interconnected security from Trend Micro. It also extends visibility and control across on-premises, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administration. Apex Central™ also provides access to actionable threat intelligence from the Trend Micro Smart Protection Network, which uses global threat intelligence to deliver real-time security from the cloud, blocking threats before they reach you.

> "My first objective was to get rid of the heavy overhead that the previous endpoint solution was putting on our systems, my second objective was to introduce security that really worked. Since we replaced the previous solution, we can see that Trend Micro has stopped the infections."
>
> Bruce Jamieson,
> Network Systems Manager
> A&W Food Services of Canada

MINIMUM RECOMMENDED AGENT REQUIREMENTS

Agent Operating System:

- Windows XP (SP3) (x86) Editions
- Windows XP (SP2) (x64) (Professional Edition)
- Windows 7 (with/without SP1) (x86/x64) Editions
- Windows 8 and 8.1 (x86/x64) Editions
- Windows 10 (32-bit and 64-bit)
- Windows 10 IoT Embedded
- Windows Server 2003 (SP2) and 2003 R2 (x86/x64) Editions
- Windows Compute Cluster Server 2003 (Active/Passive)
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (x86/x64) Editions
- Windows Server 2008 (SP2) (x86/x64) and 2008 R2 (SP1) (x64) Editions
- Windows Storage Server 2008 (SP2) (x86/x64) and Storage Server 2008 R2 (x64) Editions
- Windows HPC Server 2008 and HPC Server 2008 R2 (x86/x64) Editions
- Windows Server 2008/2008 R2 Failover Clusters (Active/Passive)
- Windows MultiPoint Server 2010 and 2011 (x64)
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows Storage Server 2012 and 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Server 2012 Failover Clusters (x64)
- Windows Server 2016 (x64) Editions
- Windows XP Embedded Standard (SP1/SP2/SP3) (x86)
- Windows Embedded Standard 2009 (x86)
- Windows Embedded POSReady 2009 (x86), Embedded POSReady 7 (x86/x64)
- Windows 7 Embedded (x86/x64) (SP1)
- Windows 8 and 8.1 Embedded (x86/x64) Editions

Agent Platform:

- Processor: 300 MHz Intel Pentium or equivalent (Windows XP, 2003, 7, 8, 8.1, 10 family)
- 1.0 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent (Windows Vista, Windows Embedded POS, Windows 2008 (x86) family)
- 1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent (Windows 2008 (x64), Windows 2016 family)
- Memory: 256 MB minimum (512 MB recommended) with at least 100 MB exclusively for Apex One™ (Windows XP, 2003, Windows Embedded POSready 2009 family)
- 512 MB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One™ (Windows 2008, 2010, 2011, 2012 family)
- 1.0 GB minimum (1.5 GB recommended) with at least 100 MB exclusively for Apex One™ (Windows Vista family)
- 1.0 GB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One™ (Windows 7 (x86), 8 (x86), 8.1 (x86), Windows Embedded POSReady 7 family)
- 1.5 GB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One™ (Windows 7 (x64), 8 (x64), 8.1 (x64) family)
- Disk Space: 650 MB minimum

Detailed requirements are available online at **docs.trendmicro.com**

TREND MICRO™

Securing Your Journey to the Cloud