Trend Micro™

ENDPOINT APPLICATION CONTROL

Prevents Unwanted and Unknown Applications from Executing

Organizations are becoming increasingly aware that traditional signature-based antivirus approaches do not provide adequate defense against modern threats and targeted attacks. This is exacerbated by the hundreds of thousands of new malicious software applications being rolled out daily, making it extremely difficult to protect against all potential threats. Without proper protection, you risk losing private company data that resides on endpoints. In addition, the machines can be used as a springboard for malicious threats to enter the network. This increases the need to safeguard data and machines against both inadvertent end-user behavior or unauthorized infiltration and the resulting execution of new unwanted or malicious applications.

Trend Micro Endpoint 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 Trend Micro™ Control Manager™.

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)

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™)
- Integrates with Trend Micro User Protection to complement antivirus, host intrusion prevention, data loss prevention, mobile security, and more

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 Control Manager
- Easily deployed using existing OfficeScan endpoint security or other third-party deployment tools
- 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

KEY BENEFITS

- Protects against users or machines executing malicious software

- Further simplifies deployment when used with OfficeScan

- Provides advanced features for centralized enforcement of corporate policies with Control Manager

- Utilizes extensive categorized application catalog (analyzed and correlated threat data from billions of files in the Trend Micro Smart Protection Network)

- Employs dynamic policies to allow users to install valid applications based on many reputation-based variables such as prevalence, regional usage, and maturity

PLATFORM ARCHITECTURE

Trend Micro Endpoint Application Control can scale up to 20,000 users per server and further with a cluster of servers or multiple servers managed by Control Manager. As an on-premises software application, Endpoint Application Control integrates with other Trend Micro threat protection solutions to enhance overall malware protection. Two components are required:

- Server installs on supported Windows platforms and is managed through a web-browser
- Agent installs on supported Windows platforms

SYSTEMS REQUIREMENTS

MINIMUM RECOMMENDED SERVER REQUIREMENTS

Server Operating Systems:
- Microsoft Windows Server 2008 and 2008 R2 (x86/x64)
- Microsoft Windows Server 2012 and 2012 R2 (x86/x64)
- Microsoft Windows Server 2016 (x86/x64)
- (Optional) IIS v7.0 or higher with these modules: CGI, ISAPI, ISAPI Extensions

Server Platform:
- Processor: Intel XEON E5-2695 v3 generation or higher generation
- Memory: 8GB is minimum and 16GB is recommended
- Disk Space: 500 GB of free disk space

MINIMUM RECOMMENDED AGENT REQUIREMENTS

Agent Operating System:
- Windows (x86/x64) XP Editions
- Windows (x86/x64) Vista Editions
- Windows (x86/x64) 7 Editions
- Windows (x86/x64) 8, 8.1 Editions
- Windows (x86/x64) 10 Editions
- Microsoft Windows (x86/x64) Server 2003, 2003 R2
- Microsoft Windows (x86/x64) Server 2008, 2008 R2
- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2016
- Windows Embedded Enterprise, POSReady 2009, POSReady 7, XPe, Standard 2009, Standard 7

Agent Platform:
- Processor: 300 MHz Intel Pentium or equivalent
- Memory: 512 MB RAM
- Disk Space: 350 MB

Detailed requirements are available here:
http://docs.trendmicro.com/en-us/enterprise/endpoint-application-control/requirements.aspx

User Protection

Endpoint Application Control is part of the Trend Micro™ Smart Protection Suites™. These interconnected, multi-layered security suites protect your users and their data regardless of the device they use, or where they are working. The Smart Protection Suites combine the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. And, you can manage users across multiple threat vectors from a single management console that gives you complete user-based visibility of the security of your environment.

Trend Micro Control Manager

This centralized security management console ensures consistent security management and complete visibility, policy management, 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. Control Manager also provides 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.

TREND MICRO

Securing Your Journey to the Cloud