Trend Micro™

CONTROL MANAGER™

Centralized Policy Management and Visibility for Data and Threat Protection

In today's sophisticated threat landscape, advanced attacks leverage multiple threat vectors, crossing user endpoints, applications, web, and email. You need to manage multiple layers of security to ensure the best possible security posture for your organization. And with the transition to cloud-based IT delivery models, you need to manage security across on-premises, cloud, and hybrid deployment environments.

Consistent security management will help you bridge the IT silos that often separate layers of protection and deployment models. This type of centralized approach improves visibility and protection, reduces complexity, and eliminates redundant and repetitive tasks in security administration—all of which make your organization more secure, and your life easier.

Trend Micro Control Manager centralized management solution provides a single, integrated interface to manage, monitor, and report across multiple layers of security, as well as across all deployment models. Customizable data displays provide the visibility and situational awareness that equip you to rapidly assess status, identify threats, and respond to incidents. User-based visibility enables you to see what is happening across all endpoints owned by your users, enabling you to review policy status and make changes across everything the user touches.

And if you do experience a threat outbreak, you'll have complete visibility across your environment to track how threats have spread. With a better understanding of security events, you're more likely to prevent them from reoccurring. Direct links to the Trend Micro Threat Connect database deliver actionable threat intelligence, which allows you to explore the complex relationships between malware instances, creators, and deployment methods.

Trend Micro products supported by Control Manager

Cloud and Data Center
- Deep Security

Custom Defense
- Deep Discovery Inspector
- Deep Discovery Analyzer
- Deep Discovery Endpoint Sensor
- Deep Discovery Email Inspector

Complete User Protection
- OfficeScan™
- Worry-Free™ Business Security
- Endpoint Encryption
- Endpoint Application Control
- Security for MAC
- Vulnerability Protection
- Data Loss Prevention
- Mobile Security
- InterScan™ Messaging Security
- ScanMail™
- Hosted Email Security
- PortalProtect
- InterScan™ Web Security

KEY ADVANTAGES

Simple, Enterprise-wide Visibility and Continuous Monitoring

Continuously monitor and rapidly understand your security posture, identify threats, and respond to incidents with up-to-the-minute situational awareness across your environment. And 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 data displays and reports, ad hoc queries, and alerts give you the actionable information you need to ensure protection and compliance

- Quick start with predefined reporting templates facilitate compliance with internal IT audit requirements

Connected Threat Defense for Better Protection

Integrate security management and analysis across multiple layers of protection—critical to defending against advanced threats that exploit multiple threat vectors.

- Consistent policy enforcement uses a single central console to configure and manage threat and data protection across multiple protection points: endpoint, mobility, messaging, collaboration, web, cloud, and data center; in addition to Deep Discovery for breach detection

- Connected Threat Defense enables Control Manager to retrieve suspicious objects from Deep Discovery when it detects a new threat locally, and deliver rapid response (real-time signature updates) to endpoints, enabling faster time-to-protection and reducing the spread of malware

- Comprehensive threat response and investigator enable you to look back in time to identify where a threat has spread in your organization and discover the full context, timeline, and extent of the attack so that you can rapidly respond to compromises

- Direct links to our Threat Connect database give you access to actionable threat intelligence. This includes rich correlated threat data describing characteristic behaviors like network activities and system modifications, along with global and system- and industry-specific impacts

- The Trend Micro knowledge base provides suggestions for remediation and prevention

User-based Visibility

Visibility of multiple security layers, whether deployed on-premise or in the cloud, means you don't have to hop from console to console to ensure that protection is properly defined across the enterprise.

- Streamlined security administration allows you to manage threat and data protection for endpoint, mobility, messaging, collaboration, and web all through a single consolidated interface

- Your central view lets you easily manage security across all device types so that you can deploy and review policy status for any endpoints owned by a given user, whether desktop or mobile

SYSTEMS REQUIREMENTS

SERVER HARDWARE REQUIREMENTS
• At least 2.3 GHz Intel™ Core™ i5 or compatible CPU; AMD™ 64 processor; Intel 64 processor
• 4 GB RAM (8 GB recommended)
• 20 GB Minimum 40 GB Recommended

SOFTWARE REQUIREMENTS
Operating system
• Microsoft™ Windows™ Server 2008 Standard/Enterprise Edition R1/R2
• Windows Server 2008 Web Edition R1/R2, Standard Edition with/without SP1 (R2) (WoW 64-bit)
• Windows Server 2012 Standard Edition (64-bit)
• Windows Server 2012 (R2) Enterprise Edition (64-bit) with/without SP1
Web Console
• Microsoft™ IIS 6.0 (for 2003 platform)
• IIS 7.0 (for 2008 platform)
• ISS 7.5 (for 2008 R2 platform)
Database Software
• Microsoft™ SQL Server 2005 Express SP4
• SQL Server 2005 Standard/Enterprise (including 64-bit) SP4
• SQL Server 2008 Express
• SQL Server 2008 (R2)
• SQL Server 2008 Standard/Enterprise (including 64-bit)
• SQL Server 2012
• SQL Server 2014
• SQL Server 2014 Express
Virtualization Support
Control Manager provides support for virtual platforms that are supported by the installed operating system

Key Benefits

- **Simplifies administration** with central console for security and data policies

- **Improves data protection** by managing integrated DLP across the IT infrastructure with re-usable policy templates

- **Reduces risk** with consolidated updates and security alerts and connected threat defense to share information among security layers

- **Increases visibility** with easy access to critical data

- **Lowers security management costs** by saving time and reducing IT workload

TREND MICRO™

Securing Your Journey to the Cloud