IBM Endpoint Manager for Core Protection

Device control and endpoint protection designed to guard against malware and loss of sensitive data

Highlights

- Delivers real-time endpoint protection against viruses, Trojan horses, spyware, rootkits and other malware
- Protects with methods including file and web reputation, behavior monitoring, personal firewall, data loss prevention and device control
- Enforces security policies using integrated data loss prevention and device control
- Provides virtualization awareness to reduce resource contention issues on virtual infrastructures
- Leverages industry-leading IBM and Trend Micro technologies with a single-console management infrastructure

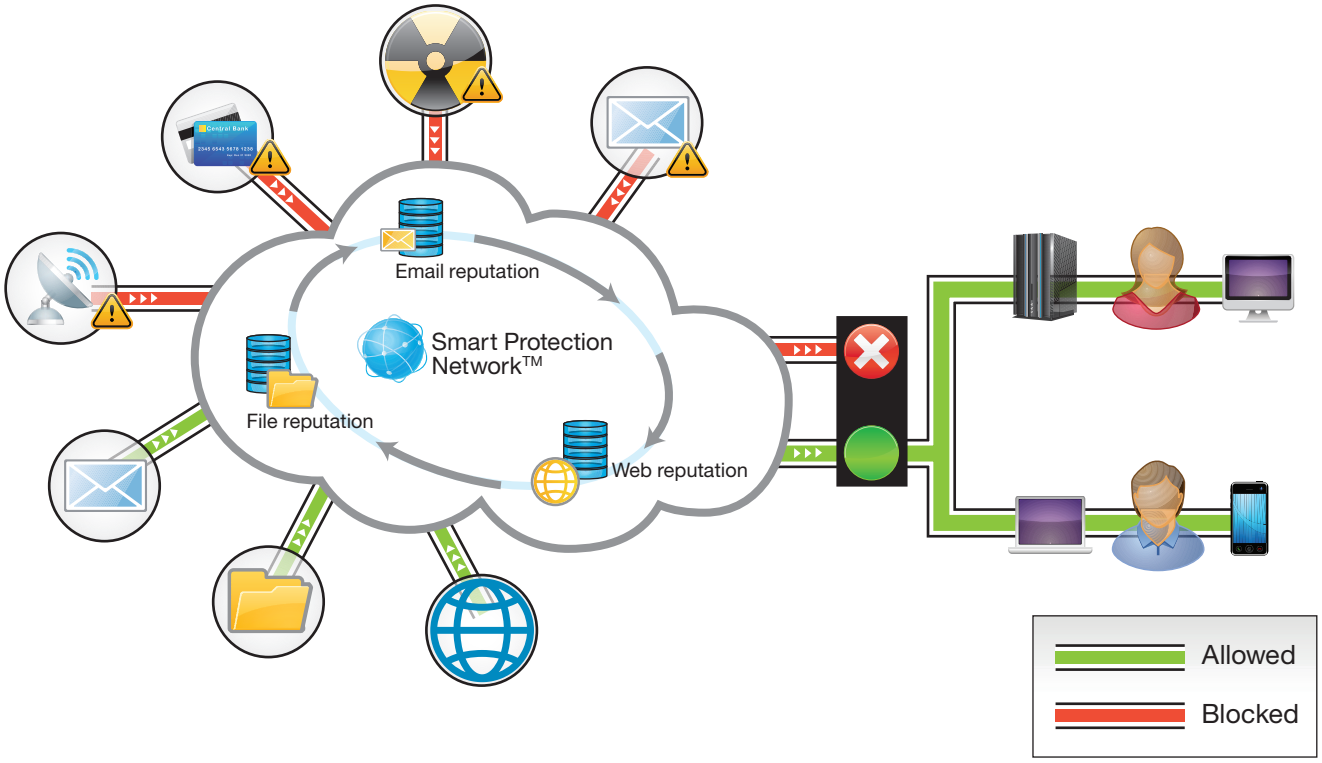
While the ever-increasing volume and frequency of malware attacks pose ongoing challenges for protecting endpoints and preventing the loss of sensitive corporate data, these are not the only dangers. The speed of attacks has increased significantly, which enables attackers to take advantage of exploits immediately after discovery. In addition, intentional or inadvertent data losses occur daily due to poor enforcement or lack of awareness of existing data security policies.

Organizations are typically careful to implement measures to protect themselves from attack and data loss, but these measures often can be part of the problem, as they create complex layers of sprawling point products that cannot respond quickly enough.

IBM Endpoint Manager for Core Protection provides IT organizations with an automated and easy-to-use solution to ensure protection of sensitive data and guard against malware before it can exploit vulnerabilities. From a single console, it provides protection functions such as malware detection and removal, file and web reputation, personal firewall, data loss prevention and device control.

Enhanced protection for distributed endpoints

This IBM solution protects physical and virtual endpoints from damage caused by viruses, Trojan horses, worms, spyware, rootkits, web threats and their new variants. It reduces the business disruptions that can result from endpoint infection, identity theft, data loss, network downtime, lost productivity and compliance violations.



IBM Endpoint Manager for Core Protection stops threats before they arrive by checking files, URLs and emails for malicious potential in real time.

IBM Endpoint Manager for Core Protection cross-references threat information with a large, cloud-based database created by Trend Micro and continuously updated via Trend Micro's Smart Protection Network™ for Windows endpoints. The solution checks files and URLs against this database for malicious potential in real time, in addition to delivering anti-malware protection to Mac and Windows endpoints as needed.

IBM Endpoint Manager for Core Protection provides security for both fixed, network-connected endpoints and roaming, Internet-connected endpoints. Constant, agent-based monitoring proves to be an effective way to combat the extreme vulnerability of roaming endpoints. A laptop used in an airport, for example, can receive anywhere, anytime, cloud-based protection from threats lurking on websites it visits or files it receives.

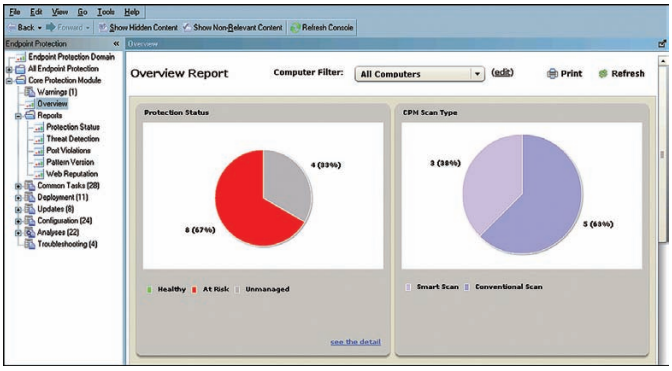
Safer, smarter protection designed to reduce risk

Key to the solution's success is its ability to work at multiple levels of threat protection, including stopping threats even before they arrive. IBM Endpoint Manager for Core

Protection, for example, can scan URLs in email messages, check them against databases of known threats and block access if appropriate. Such front-line measures build on other capabilities that protect infrastructure and endpoints against attacks as they are delivered. The result is that in recent tests, the combined capabilities of IBM Endpoint Manager for Core Protection capture 100 percent of threats, while the next highest scoring competing solution captured only 77 percent.*

These capabilities include:

- **Superior malware protection:** The solution guards against the full range of malware and scans POP3 email and Microsoft Outlook folders for threats. It automatically cleans endpoints of malware, including rootkits, spyware, processes and registry entries that are hidden or locked. Performance improvements significantly speed on-demand scanning and system start-up times.
- **Data loss prevention:** An optional data protection add-on component delivers integrated data loss prevention capabilities deployed using the same single console and single agent infrastructure. Integrated data loss protection enables organizations to enforce security policies in a manner that allows users to access sensitive data for their jobs but not misuse or lose that data, and to leverage predefined templates to help comply with data privacy regulations. Multichannel monitoring and enforcement can block or allow data being copied to or sent to a variety of delivery channels. These can include email, printers, CD/DVD, network drives and USB storage. The monitoring and enforcement measures can provide configurable response actions to instances that involve data matching specific patterns (such as credit card or social insurance numbers), predefined lists of confidential keywords or file attributes including file name, size or type.
- **Granular device control:** Included with the data protection add-on component, granular device control monitors and controls physical ports on endpoints and can enable or disable these ports based on device type and content-aware scanning restrictions. Additional protections can be applied to restrict removable USB storage device access based on the vendor, model and serial number of the device.
- **File reputation:** Querying up-to-the second data in a cloud-based database (a private cloud implementation delivered by Trend Micro is also supported), this feature can determine the safety of a file and prevent users from opening infected documents. It reduces both the amount of management effort required and the impact of protection on endpoint performance while providing immediate protection on or off the network.
- **Web reputation:** This feature automatically determines the safety of millions of dynamically-rated websites to protect endpoints against web-based malware, data theft, lost productivity and reputation damage. It provides real-time protection regardless of connection type, and can improve web performance with its cloud-based synchronization.
- **Behavior monitoring:** The solution identifies suspicious system activities such as the use of flash memory to change the registry. If triggered by such an event, this feature can block execution to prevent potentially damaging activities.



An innovative graphical user interface allows administrators to easily understand their protection status and identify endpoints that are at risk.

Simplified endpoint management with enhanced visibility

From a single console, IBM Endpoint Manager for Core Protection can enhance management with complete visibility to all endpoints. It simplifies and centralizes management for physical and virtual endpoints and supports task delegation with granular, role-based administration.

Utilizing the IBM Endpoint Manager infrastructure delivers increased protection through policy enforcement to ensure that antivirus services are always installed, running and up to date. Organizations can realize operational efficiencies with the centralized single console, and lower management and distribution server costs with the tremendous scalability provided by the IBM solution.

Security that fits the organization

IBM Endpoint Manager fits the needs of growing and evolving endpoint environments. Forward-looking technologies such as desktop virtualization and cloud-based services that enhance speed and simplify deployments while reducing operational load are significant features of the solution.

- **Virtualization awareness:** For initiatives transitioning desktops and laptops to virtual machines, the IBM solution provides protection by automatically recognizing whether an agent is on a physical or virtual endpoint. If virtual, it takes steps to avoid problems such as "antivirus storms" in which scans running concurrently on large numbers of machines can bring networks and endpoints to a halt. Instead, the solution serializes scans and updates to prevent conflicts. It also shortens scan times by white-listing base images and previously scanned content. IBM Endpoint Manager for Core Protection integrates with the organization's existing virtualization solutions, including Citrix XenDesktop and VMware View to enhance return on investment for ongoing virtualization projects.
- **Lightweight footprint:** IBM Endpoint Manager for Core Protection liberates resources with cloud-based capabilities for both security deployment and management. In a conventional solution, the large signature updates required to keep up with the growing numbers of threats can lengthen deployment, overburden endpoints and impact user productivity. With the IBM solution, signatures remain in the cloud, reducing the burden on individual endpoints.

The smart way to deliver endpoint protection

In today's interconnected, instrumented and intelligent world, where the complexity of endpoint management and the importance of security are constantly on the rise, IBM Endpoint Manager for Core Protection delivers up-to-the-minute endpoint visibility and protection. This easy-to-use solution can detect and remove the full range of malware before it exploits endpoint vulnerabilities, through protection functions such as file and web reputation. Additionally, integrated data loss prevention and granular device control help protect against data breaches and meet compliance objectives while controlling operating costs.

Organizations can realize significant value by deploying additional products from the IBM Endpoint Manager family, beyond IBM Endpoint Manager for Core Protection. For example, malware attacks typically target unpatched vulnerabilities. IBM Endpoint Manager provides comprehensive patch management capabilities for delivering patches from a full range of operating system and application vendors to distributed endpoints. This capability can shorten times for delivery of patches and updates with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks.

And the broader IBM Endpoint Manager solution addresses the convergence of system management and security requirements by delivering capabilities for vulnerability management, security configuration management, asset discovery, inventory,

software distribution, operating system deployment, software usage analysis, compliance reporting and more. The single IBM Endpoint Manager console is used to manage all of these capabilities, including those provided by IBM Endpoint Manager for Core Protection. This comprehensive solution provides a holistic view of the organization's endpoint security posture.

IBM Endpoint Manager for Core Protection at a glance

Server requirements:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Console requirements:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Supported platforms for the agent:

- Microsoft Windows, including XP, 2003, Vista, 2008, 2008 R2, 7, Embedded POSReady 2009
- Mac OS X.

Virtualization Support:

- Microsoft Virtual Server, Windows Server, Hyper-V Server
- VMware ESX/ESXi Server, Workstation and Workstation ACE, vCenter, View
- Citrix XenDesktop, XenServer, XenApp

For more information

To learn more about IBM IBM Endpoint Manager for Core Protection, contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com**/tivoli/endpoint

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

© Copyright IBM Corporation 2012

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2012

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information provided in this document is distributed "as is" without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

Please Recycle

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

* "Trend Micro Enterprise Endpoint Comparative Report," AV-Test, January 2011. http://us.trendmicro.com/us/trendwatch/core-technologies/competitive-benchmarks/avtest/

Tivoli® software

TID14081-USEN-02