Proactive response to today’s advanced persistent threats

IBM Endpoint Manager: Comprehensive strategies for mitigating risk
Introduction
There is no fail-safe in today’s digital world. Incidents will occur, both unintentional and malicious. To mitigate damage and organizational impact, the agile organization will respond quickly. To mitigate risks before damage occurs, an organization can maintain a continuous high state of security, ensure that all computing endpoints are in compliance, automate actions to shorten response time and enact measures to control infections with quarantine until remediation is complete.

Achieving this level of agility, however, requires pervasive real-time visibility and control over all endpoints, not only to identify deviations from policies but also to quickly return the environment to stability. An effective response system must also manage remote devices—on or off the network—running heterogeneous operating systems. It must scale to meet growing network demands. It must combine speed, accurate detection and high-quality remediation techniques in the face of threats that are faster, more sophisticated and more difficult to prevent.

Answering threats with a rapid, effective response
In today’s interconnected, instrumented and intelligent world, where organizations are more globally distributed, more complex and more mobile than ever before, both the importance of security and the challenges of endpoint protection are constantly on the rise. With today’s advanced persistent threats growing stealthier, more dynamic and more damaging, the need for an effective, high-performance response system has never been greater.

At one time, the lag between the discovery of a vulnerability and the release of exploit code was measured in months. Then it shrank to weeks—then days. Today, the ability to target previously unknown vulnerabilities or unleash new ways to exploit known vulnerabilities (known as “zero-day” attacks) can be as short as a few hours. In many cases, cyber criminals no longer need to discover system and application vulnerabilities on their own. They simply wait until vulnerability information is made public by security researchers and software vendors. The information is then used to develop code to exploit the vulnerability faster than organizations can respond.

IBM® Endpoint Manager, built on IBM BigFix® technology, helps organizations maintain continuous compliance to prevent threats, and includes additional capabilities to quickly respond to security incidents and mitigate their impact. Powered by an intelligent agent architecture, Endpoint Manager delivers real-time visibility and control to arm IT operations with near zero-day protection across heterogeneous environments and wherever laptops roam. It includes leading analytics capabilities that provide insights for hardening the infrastructure against attacks to the network, servers and endpoints.
An attack and infection on the organization’s technology infrastructure—especially a fast, unexpected zero-day attack—can lead to significant losses in revenue, user productivity, customer relationships and market reputation. The answer to this danger lies in maintaining a continuous high state of security to prevent attacks when possible, and a high-performance incident response system that matches the speed of these increased attacks and increasingly sophisticated attackers.

Endpoint Manager can provide that continuous compliance and rapid response. The Endpoint Manager intelligent agent continually assesses compliance with policies, automates remediation and immediately notifies the centralized management console of a change in status. This approach gives organizations up-to-the-minute endpoint visibility and control, and quickly identifies and remediates endpoint security exposures and risks. Its analytics capabilities provide insight and reporting to meet compliance regulations and IT security objectives.

Endpoint Manager helps organizations respond quickly to today’s threats with:

- **Blazing speed:** Whether applying a patch to repair a newly discovered vulnerability on hundreds of thousands of endpoints or changing the configuration of a system so that it is compliant with standards, Endpoint Manager can affect organization-wide change within minutes. With Endpoint Manager, assessment and analysis are conducted on the endpoint itself—which increases the speed of discovery, software delivery and validation. Less communication is required between the management server and endpoint, increasing speed and reducing the amount of network bandwidth consumed.

- **Exceptional accuracy:** Endpoint Manager can accurately interrogate any aspect of an endpoint and provide a real-time view into problems that exist in the environment. By doing so, it enables organizations to discover issues quickly and it provides an additional layer of defense when traditional security defenses either fail completely or provide fixes too late to prevent an incident. The solution’s centralized management console provides a single, granular view for comprehensive visibility and control across distributed global networks. Operators can perform remedial actions in minutes—and receive immediate validation that the action has completed successfully.

- **Quality of control:** As viruses, worms and botnets make configuration changes on a computer, these “stealthy” exploits often go unnoticed by traditional security approaches such as anti-virus and anti-spyware. But with granular visibility into endpoint properties, Endpoint Manager enables organizations to see these changes and automate remedial action to maintain compliance. Similarly, Endpoint Manager can discover applications installed in its infrastructure. When a piece of malicious code attempts to install unauthorized applications, Endpoint Manager has the ability to identify that behavior in real time and automatically remediate it.

- **Cloud-based protection:** Endpoint Manager can provide security for fixed, network-connected endpoints and roaming, Internet-connected endpoints faster than waiting for a vendor’s mass-distribution of signature files. Endpoint Manager cross-references threat information against a large, cloud-based database to assess the malicious potential of files and URLs in real time, and delivers anti-malware protection to endpoints as needed. 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.
Network self-quarantine: Endpoint Manager can automatically assess endpoints against required compliance configurations—and if an endpoint is found to be out of compliance, the solution can configure the endpoint so that it is placed in network quarantine until compliance is achieved. Endpoint Manager retains management access to the endpoint, but all other access is disabled.

Getting a virus attack under control—quickly

A year after suffering through a major attack from an Internet-based worm—requiring four hours per system to repair at a total cost of USD1.6 million—a major university implemented Endpoint Manager as a better defense from the next attack.

When the next set of worms affected the university, only about two percent of more than 12,000 computers running Endpoint Manager were compromised. These infected systems were quickly and automatically repaired at minimal inconvenience to their owners. Of the other 8,000 computers that were not running Endpoint Manager, more than 15 percent became infected and required a great deal of work to repair.

Protecting today’s complex, distributed organization

As many organizations now go global, their network infrastructures often struggle to keep up. Many infrastructures run over low-bandwidth, high-latency networks. Poor visibility and long lag times translate to poor currency of data and increased risk. IT does not know the state of computing devices, whether a device has been exploited or, after software delivery, whether a fix has been implemented on an endpoint. Furthermore, cyber criminals have learned to take advantage of corporate reliance on email and the web—simple actions like opening an email attachment or clicking a web link can result in lost confidential data, damaged infrastructure or a ruined reputation.

In addition, many organizations own multitudes of legacy systems and must manage assets running on a variety of platforms. While some may consider a heterogeneous infrastructure to be a good defensive security strategy, it complicates the ability to effectively manage and secure endpoints. And as infrastructures expand, the challenge of managing and securing a growing number of endpoints increases proportionally.

Endpoint Manager is designed to give organizations the capabilities they need to manage and protect complex, heterogeneous environments:

- Optimized management of remote and mobile devices: The distributed, intelligent agent architecture of Endpoint Manager enables the continual discovery and assessment of roaming laptops no matter where they are. Any system running the solution’s agent can act as a relay—a communication point for policies and remediation—and any publicly routable relay can assess and ensure configuration compliance on endpoints that are connected to the Internet. Because each agent has a local copy of the policy, the relay can send any policy changes directly to the endpoint as long as the relay is connected to the Internet.
Continuous compliance: Endpoint Manager comes with best-practice checklists that can be used “out of the box” to assess compliance. The intelligent agent provides continuous policy enforcement and endpoint protection, whether or not the endpoint is connected to the corporate network. As soon as an endpoint configuration is modified, the agent can detect if this behavior is noncompliant and can automatically perform the necessary tasks to bring the endpoint back into a compliant state. It then notifies the management server of this activity. The result is constant protection against exploits regardless of where an endpoint roams.

Multiplatform support: The multiplatform support of Endpoint Manager simplifies administration of heterogeneous environments—including those with legacy systems and applications. The Endpoint Manager solution supports environments running multiple generations of Microsoft Windows as well as UNIX, Linux and Mac operating systems—including in virtualized environments.

Mitigating vulnerabilities before an exploit: Endpoint Manager has the ability to touch any registry key, file, service or component that sits on the endpoint. It also can manage any application or service that sits on the endpoint. If the IT staff needs to know what’s inside a registry key, they can use Endpoint Manager to query the environment and get an accurate response in minutes. An endpoint that is offline when the query is sent will respond to the policy once the endpoint is Internet routable.

Security information and event management integration: Endpoint Manager vulnerability information enriches the IBM Security QRadar® vulnerability database, resulting in more accurate risk and offense correlation and improved compliance reporting. QRadar solutions and Endpoint Manager together provide continuous monitoring, compliance enforcement, remediation and reporting; advanced endpoint, network, security event and vulnerability correlation; and “risky” device identification and remediation.

Data loss prevention (DLP) support: Endpoint Manager helps improve data protection capabilities while controlling operational costs. DLP policies can be created and applied to limit or prevent the transmission of digital assets through common transmission channels, such as email, and help secure data on devices that leave the premises. Endpoint Manager regulates access to external storage devices and network resources to help prevent data loss, which, combined with file scanning, helps guard against security risks. Predefined templates can be used to identify, monitor and optionally block the transmission of sensitive data such as credit card numbers.

Rapid time to protection: Endpoint Manager can manage up to 250,000 endpoints over highly distributed, highly complex network infrastructures from a single management server. And because endpoints themselves perform the assessment and policy enforcement, the organization does not need to invest in and manage a huge endpoint management server infrastructure. Regardless of network size or complexity, Endpoint Manager can be implemented quickly, typically in a matter of hours.
Anti-virus vendor migration at Concord Hospital

Anti-virus vendor migrations can often leave an organization exposed during the transition. Utilizing the automation capabilities in Endpoint Manager, Concord Hospital was able to migrate without disruption or exposure, achieving improved performance at the same time.

The removal and installation took an average of five to ten minutes per machine, with full scans taking between 30 and 60 minutes. Implementation was nearly invisible—no users placed help-desk calls during the rollout phase. After the rollout, workstation usability scores increased from one to seven on a 10-point scale. The dispersion of definition updates and full manual scans that formerly crippled many workstations can now be implemented so rapidly that they go virtually unnoticed.

Ensuring rapid incident response

Even in the most securely managed environments, incidents will happen. Beyond providing the capabilities to help organizations maintain a continuous high level of security and effectively prepare for an incident, Endpoint Manager offers specific remediation functionality to mitigate damage and return endpoints to stability as quickly as possible when an incident occurs.

Historical visibility into the state of compliance can be a particularly powerful tool to discover a past status that led to an issue. An organization that was the victim of a cyber attack, for example, can examine its compliance status at the time of the attack to discover where vulnerabilities existed. This ability to drill down into specific details of both compliant and noncompliant endpoints can help identify critical gaps and provide insights that can be used to bring endpoints into compliance and strengthen the overall security posture of the organization.

The following examples show how Endpoint Manager can be used for incident response:

- **Disabling ActiveX controls or DLLs being exploited:** Endpoint Manager can quickly deploy policies that shut down an exploited control or dynamic-link library (DLL) as soon as a vulnerability is identified—limiting the damage from a potential attack even before a vendor's fix is available. When a zero-day exploit is discovered, the solution can execute policies that turn manual remediation steps provided by the vendor into automated policies to help identify whether endpoints are potentially vulnerable and then mitigate problems.

- **Migrating from one technical control to another:** Replacing an anti-virus solution due to high cost or ineffectiveness can often be a challenge. Additionally, there is the potential risk that endpoints will be exposed during the migration. Endpoint Manager allows an organization to easily and safely remove a solution in as little as a day. It also helps install products from a new vendor. In either operation, the solution's speed helps shrink the window of vulnerability to attack.
Quickly updating endpoint protection controls: Endpoint Manager can ensure that endpoint security clients are always running and that virus signatures are updated. Closed-loop verification ensures that updates and other changes are completed, including Internet-enabled verification for endpoints disconnected from the network. An organization can also use Endpoint Manager to turn off services—for example, closing open Telnet ports—that expose the system to vulnerabilities.

Migrating to a new browser en masse: A browser exploit can expose the organization to risk by allowing remote attackers to execute arbitrary code when users access certain websites. With Endpoint Manager, organizations have the flexibility to move to another browser—and even large infrastructures can accomplish the migration in days.

Discovering and cleaning up malware that cannot be removed: To combat a malware attack, Endpoint Manager can raise IPSec firewall rules to quarantine infected systems from the rest of the network. Allowing outgoing communication only to a remediation server allows IT staff to build policy definitions that identify what impact the virus is having. IT staff can also look at other endpoints to see if they exhibit that behavior, and quarantine those that do. Once a fix is available, Endpoint Manager can ensure that endpoints are disinfected and stay up to date.

Key solution components

Key high-performance incident response solutions in the Endpoint Manager portfolio are:

- **IBM Endpoint Manager for Security and Compliance:** Provides continuous IT security configuration enforcement and remediation, plus leading analytics capabilities to collect and archive automated security check results. Provides a variety of views on compliance status and security exposure, from high-level aggregate roll-up views, to the identification of hot spots, to drill-downs for detailed information.

- **IBM Endpoint Manager for Core Protection:** Detects and removes malware before it can exploit vulnerabilities. Cross-references threat information with a large, continuously updated cloud-based database. Checks files and URLs against this database for malicious potential in real time, and delivers anti-malware protection to Mac and Windows endpoints as needed.
Conclusion

IBM Endpoint Manager helps organizations maintain continuous compliance to prevent threats, as well as analytics capabilities to harden the infrastructure against attacks. Its intelligent agent technology provides multiple layers of security and helps discover anomalous behavior in real time. Administrators can target those systems that are affected with specific actions tailored for an exact type of endpoint configuration or user type. Endpoint Manager brings pervasive, real-time visibility, automated remediation and global scalability to the incident response process. This allows organizations to protect endpoints no matter where they are located, how they are connected or whether they are on or off the network, while minimizing the impact of exploits to the network, endpoints and end users.

For more information

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

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.