How Endpoint Management Secures Organizations

Mechdyne IT Services

Mechdyne
ENABLING DISCOVERY

What is Endpoint Management?

Endpoint Management (EM) is a way for organizations to outsource the ongoing administration of device security, monthly deployment of Windows, and select third-party application patches across laptops, desktops, and servers.

EM offers layers of protection that keep servers and devices secure against online threats. In 2019, there were over 7.9 billion records exposed from data breaches. 2019 saw an increase over 2018, and 2018 over 2017. The trend will only continue. Businesses, universities, and governments are being relentlessly targeted by attacks. An effective EM program adds multiple layers of cybersecurity to organizations' systems and networks, helping to minimize attack vectors that could leave them vulnerable.

How does Endpoint Management protect a business?

While no solution is completely fool-proof, adding layers makes attackers' work that much more difficult, and hardens systems against possible threats or infections.

Below are various cybersecurity protection layers, available through an EM program, that an organization should have in place:

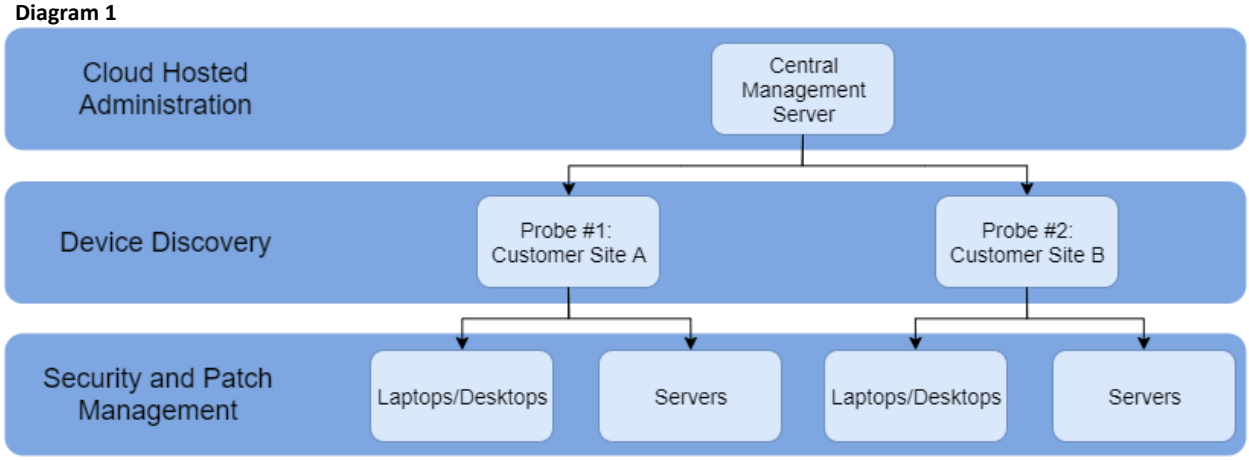
- **Anti-Malware** – detecting and blocking malware threats before they have a chance to inflict damage to devices. This feature makes a distinction between an "infected file" and a "suspected file" based on the confidence that it has detected a security threat.
- **Behavioral Analysis** – examining the behavior of a file and determining if the file may be a threat.
- **Network traffic scans** – providing data protection for email and user web browsing in real time, and scanning various types of network traffic for potential security threats.
- **Content Control** – providing a way to restrict what users can access and send over the Internet.
- **Anti-Phishing** – preventing external attempts to obtain sensitive information such as credit card numbers or account information from a bank for malicious reasons.
- **Firewall** – controlling access to network resources, network services, and to the Internet by specified applications.
- **Disk Encryption** – protecting the contents of computer hard disks, especially laptops, from being compromised in the event a device is lost or stolen.
- **Endpoint Document Backup** – versioned, encrypted archive of user's important data files to safeguard against loss from corruption, a successful ransomware attack or the device being lost or stolen.

How it works

As noted above, EM protects devices by orchestrating the deployment of security patches, reducing the attack opportunities, and keeping endpoints secure with anti-virus, network packet inspection, content control, and firewalls. But how does EM actually achieve this?

Endpoint Management works by deploying probe software, as seen in Diagram 1, to select devices in an organization's environment. It is important that the collection of probes deployed will be able to "scan" the entirety of the network to reduce gaps in protection. A single, comprehensive EM solution can perform all these activities. Finding a good tool will take research but the main advantage is that management of all elements is done through a single interface.

Diagram 1



On a scheduled basis, the probes poll all of the devices attached to the network and report back to the Central Management Server (CMS) with a collection of statistics. Devices discovered on the network are then mapped and categorized into laptops/desktops, servers, and "other". Only laptops/desktops and servers are targeted for automated installation of an administrative agent and protective software. The "other" category may refer to various types of network appliances (switches, routers, firewalls, or remote management controllers), printers, or even mobile devices (which would fall under a mobile device management solution and not Endpoint Management).

The CMS then takes over the role of telling the devices, through the administration agent, when to run anti-virus scans, update definitions, deploy application patches and reboot.

Once the network has been mapped, the other layers of cybersecurity cover all of the devices to keep the organization safe and secure. As an added benefit, the EM solution can also back up end-user documents and securely store data within an encrypted cloud-based vault for on-demand recovery.

Why organizations need EM

All of this might sound good, but is EM really necessary? Don't patches already come out for Windows and other applications? What if an organization already has anti-virus software?

Microsoft Windows patches and other application vendors do put out patches regularly and users may receive the notifications that they need to install updates and restart. How many users do this right away? How many users do this within a week? How many users put this off indefinitely because they want to be "reminded later"? According to several research studies, nearly 60% of all security breaches involve "unpatched" vulnerabilities. That is a staggering percentage and keenly highlights the importance of routine IT administrative and management practices as absolutely essential for mitigating threats. EM's scheduled and automatic patching helps keeps all machines compliant and up-to-date. This eliminates worries around updating – individual users are no longer in charge, so IT groups know the patches have been implemented across the network(s).

Anti-virus and patch management are only part of a cybersecurity solution. Windows comes with a firewall, but this alone cannot stop threats. Adding layers like network traffic scans, behavioral analysis, anti-phishing, disk encryption, and document backup complement the other pieces to create a stronger shield for a more secure organization. Each one of these pieces protects organizations from different attack vectors.

Besides patching and security layers, organizations that outsource their EM activities save on headcount and infrastructure costs. Members of the IT department also have more time to focus on strategic projects and growth, rather than maintenance/patching. Such focus generates higher returns for the business.

As outlined above, the device discovery and data collection happen automatically, on a scheduled basis. The solution scales according to the needs of the organization as devices and servers are added and removed from the network. EM also eases vendor communication since all of these services come from one source.

Should this type of management be a priority?

To answer this question, there are other questions that need to be answered first such as:

- Is the organization prepared in the event of a disaster? *More than 77% of organizations surveyed responded they have no Cybersecurity Incident Response Plan.*
- How much downtime can an organization afford if a breach occurs?
- What happens, for example, if a car is broken into and a work device is stolen? How secure is the data backup currently?
- What is the value and/or sensitivity of the data being secured? What would happen if that data was accessed?

Secure backup is another layer of EM protection. Theft or loss leaves critical information vulnerable. And not all threats are man-made; natural disasters destroy offices and equipment. These real threats can be prevented by backing up data in offsite secure vaults.

The backup data is stored within an encrypted, offsite vault managed by the provider, so if any system becomes compromised, the data can be recovered without losing any valuable information it may contain. This dramatically improves the opportunity for an organization to get back up and running quickly.

Cybersecurity Gaps

Cybersecurity is consistently a top concern for business leaders. As more users and devices are connected to networks, the likelihood of a breach increases. As IT teams' task lists grow, their focus can shy away from critical projects like cybersecurity. Solar Winds, a Mechdyne IT services partner, identified 7 pitfalls many IT groups inadvertently fall into that expose organizations to threats. They are:

1. Inconsistency in cybersecurity enforcement
2. Negligence in user awareness training
3. Shortsightedness in the application of cybersecurity technologies
4. Complacency in vulnerability reporting
5. Inflexibility in adaptation after a breach
6. Stagnation in the application of key prevention techniques
7. Lethargy around detection and response

Alone any one of these can be a large gap in cybersecurity but having multiple leaves massive vulnerabilities in the environment. Endpoint Management of devices and servers can alleviate many of these issues.

1. **Inconsistency in cybersecurity enforcement**
   IT environments are in a constant state of change - user onboarding and offboarding, software application updates and changes, new devices being added. All of these changes require some type of cybersecurity support. EM helps to alleviate that strain. The automatic network scanning identifies new devices and adds them to the index. Off-boarded devices will drop out of the list. The list can also act as another checkpoint to make sure that an off-boarded machine has been removed. The system also ensures that all devices and servers are up-to-date with any security updates and patches. When a machine fails to update, notifications can be automatically sent.
2. **Negligence in user awareness training**
   This layer of cybersecurity is critical; most breaches occur when a user unknowingly allows an attack into the system. While EM cannot directly address the training of users, it can help identify users who may need more training. If the user consistently chooses 'remind me later' about patching, they may need to be shown why the patching is so important. When new machines are added to the system, EM will identify batches of users who need to go through initial/onboarding trainings.
3. **Shortsightedness in the application of cybersecurity technologies**
   Cyber threats evolve as current best practices and technology improve. Not staying up-to-date on technologies leaves an organization vulnerable. Working with an IT services provider about EM keeps the organization looking ahead. Cybersecurity service offerings must be up-to-date to be effective. While the tools that are part of the system today add

layers of protection to organizations, they will not be effective forever. The procedures and software used within the service offering must continue to adapt as well. See the comparison of current and Next-Gen programs below to see how the management tools are evolving.

4. **Complacency in vulnerability reporting**
   Data reporting and analysis are critical, especially when it comes to cybersecurity. Improvement plans can be developed when an organization knows where its vulnerabilities and gaps exist. Without that knowledge, organizations are guessing at best, or doing nothing at all. EM regularly reports on device and server patching. Organizations using the service are able to see when the patch occurred, what machines completed the update, and what machines had issues or still need to be updated. Once this information is in-hand, the IT team can then take the next steps to resolve the issues and identify potential gaps.

5. **Inflexibility in adaptation after a breach**
   While EM works to protect organizations from breaches, threats come from many directions and a layered security approach is needed. If a breach does occur, EM's reporting can verify the security patches and updates recently enacted in the environment. EM also enables the IT team to make widespread updates to all of the machines on the network. Breaches are a constant threat, especially following a successful attack. Quickly adapting and increasing security measures is critical in the aftermath of a breach. EM enables the IT team to rapidly implement changes to laptops, desktops, and servers. As noted in #4, the reporting from EM is also critical to understanding the environment and what is happening.

6. **Stagnation in application of key prevention techniques**
   While not able to directly assist with tasks like restricting local or domain administrative rights or application whitelisting, EM removes items from IT team task lists. IT teams can focus on projects that increase the security of the entire organization when they don't have to worry about patching schedules or patching individual machines. Disk encryption, as a data security measure, increasingly impacts IT teams, and their priority lists, as more mobile and laptop devices are added to organizations' environments. Encryption is a critical security procedure that protects trade secrets and other vital business data as more users switch to mobile computing (laptops) and travel with their work.

7. **Lethargy around detection and response**
   Early detection is perhaps the most important preventative technique. The longer it takes to detect and respond to a threat, the more damage occurs and remediation costs rise. If threats and breaches are caught early, both damage and costs can be contained. EM leverages next-gen behavioral analysis, heuristics, and machine learning to detect and stop threats before widespread infection. Next-gen endpoint detection and response (EDR) utilizes pre-execution programs to "test" files, downloads, and programs before they fully execute in the system. If the program determines there is a threat, it is quarantined. The combination of services contained within EM reduces detection and response times, which directly lower threat damage and costs.

How Endpoint Management Stops Threats

As noted above, EM has many features that add cybersecurity layers to an IT environment. Anti-phishing, content control, network traffic scanning, patching and firewalls all help to secure points from threats. But what happens when a threat gets past one of these layers?

Examining one particular Endpoint Management solution, SolarWinds N-Central, shows the differences between current cybersecurity solutions and what the next generation of solutions can do. Security Manager AV Defender (AVD) is a current solution and the next-generation solution is known as an Endpoint Detection & Response (EDR) solution. These programs work in tandem to protect endpoints and servers from threats that have bypassed the other cybersecurity layers. See Table 1 below for a breakdown of features between the two programs.

Table 1

Program Features	AVD	EDR
Bit Locker Encryption Control	X	
Anti-Phishing	X	
Content Control	X	
Anti-ransomware Scan Vaccine	X	
Network Traffic Scanning	X	
Software Firewall	X	X
Malware Detection Using Heuristics	X	X
Threat Behavioral Analysis	X	X
Pre-Execution Program Analysis		X
Machine learning / AI enabled threat detection		X
Enhanced quarantine (“Disconnect from Network”)		X
Automatic file rollback (Windows OS only)		X

EDR may be the next generation of cybersecurity solutions, but Security Manager has many features that the current version of EDR program does not. Disk encryption management, anti-phishing, content control, anti-ransomware (using Scan Vaccine) and network traffic scanning all protect endpoints. Scan Vaccine is a tool that can protect against known and possible future versions of crypto-ransomware families such as CTB-Locker, Locky, and TeslaCrypt. The vaccine works by exploiting flaws in how the ransomware spreads and halting it. These features make current solutions, like Security Manager AV Defender, critical to a cybersecurity program. However, EDR is the future.

EDR uses machine learning and artificial intelligence (AI) to protect from new kinds of threats. Current anti-malware programs use definitions and established patterns to identify and stop threats. When new types of threats develop, it takes time for these systems to catch up. Any time spent unprotected could mean a successful breach. EDR utilizes eight AI engines that analyze multiple data points to identify threats and determine if a response is necessary before letting executable files or processes operate within a system. By using machine learning, EDR can determine how to best respond to threats and adjust responses over time. With the AI data stored locally on the endpoint, EDR does not rely upon access to the Internet or wait for signature file updates to keep a device safe from new and emerging threats. The program determines if the file or application is a threat and quarantines it, or clears it and lets it open and

operate like normal. Also supported are enhanced quarantine measures that can disconnect a device from the network to prevent the risk of a local infection from spreading to other endpoints or servers. Additionally, on Windows OS systems, EDR allows for automatically replacing compromised files with their last known healthy version. The most comprehensive real-time protection against known and unknown threats necessitates both AVD and EDR working in parallel to create layers of protection.

We have seen success using these types of systems together. In November 2019, one client saw over 1,550 attacks. 95% were blocked completely from entering the endpoint or system. Of the remaining 5%, 2% were deleted or quarantined and 3% remain harmlessly present. Harmlessly present means that the file is identified, but not active and not causing harm. The most frequent example is a malicious email in a spam or deleted folder. If a user were to open the file, the real-time protection would activate to neutralize the threat.

Looking Ahead – Where is Endpoint Management and Business Security Heading?

Cyber-attacks and security measures will always have an "arms race" sort of relationship. A better security measure will develop, and then a new threat will develop to circumvent the new defense. So what new security measures will we see in the near future?

Machine Learning and AI

These leading-edge technologies will continue to develop and improve. Advanced heuristics (strategies derived from previous experiences with similar problems) will eventually replace traditional anti-virus and anti-malware programs and systems. With the ability to rapidly learn and adapt, they will be one of the main ways that new threats are detected and blocked.

Automation

Security through automation will continue to evolve to better include policy-driven protection such as allowing/blocking USB access or endpoint traffic, enhanced quarantine measures, automated recovery responses, and real-time reporting and notification.

Hardware Improvements

New system components, like Trusted Platform Module (TPM) chips, are continually being developed. This embeds additional security into each machine and endpoints through on-the-fly, hardware-based, data encryption, and secure boot. Secure boot's role is to ensure that critical software hasn't been tampered with and that only the trusted operating system loads on startup.

User Awareness Programs

Hardware and software improvements will never be enough. People will always be the #1 way threats are introduced to environments. While they have no malicious intent, people can be fooled into allowing someone with nefarious intent to access their IT systems. To fight this, a strong user awareness program should teach users what to look out for, what to do when they suspect something is wrong, and test the users to confirm they are following best practices.

About Mechdyne IT Services

Our 100% US-based IT professionals offer a full range of IT support services including an ITIL best-practices-driven service desk that enables end-users to get back to work quickly and improve the businesses for which they work. Mechdyne IT Services is a business unit of Mechdyne Corporation, a global technology leader creating distinctive electronic, software, and service solutions that enable discovery.

For more information, please visit mechdyne.com/it-and-audiovisual-services.