ManageEngine

Improving Endpoint Security using ManageEngine's **Endpoint Management Solutions**

Table of **Contents**

1.Introduction 03

2. What is endpoint security? Why is it critical? 04

3. Potential challenges and threats faced by enterprises 05

- 3.1 Data theft 05
- 3.2 Identity theft 05
- 3.3 Distributed denial-of-service attacks 06
- 3.4 Remote code execution 06
- 3.5 Watering hole attacks 06

4. How do ManageEngine's solutions ensure endpoint security? 07

- 4.1 Tackling vulnerabilities through automated patching 09
- 4.2 Restricting blacklisted applications using inventory management 09
- 4.3 Tracking critical applications using system health reports 10
- 4.4 Antivirus software deployment and virus de nition updates 11
- 4.5 Achieving USB port security using con guration settings 11
- 4.6 Security standards: HIPAA and PCI DSS 12
- 4.7 Securing roaming users' endpoints through a forwarding server 14
- 4.8 Secure remote troubleshooting using encryption 14
- 4.9 Preventing interception attacks through SSL certi cates 15
- 4.10 Security con gurations 15
- 4.11 Data leak prevention in case of device loss or theft 19
- 4.12 Securing corporate email 19
- 4.13 Securing distribution and viewing of content 19
- 4.14 Preventing device misuse 19

5. Summary 20

6. Endpoint management and security solutions - Products catalogue 20

1.Introduction

In terms of cyberattacks, 2017 saw some of the worst threats yet. After WannaCry hit 150 countries in May, another ransomware variant named NotPetya struck; in total, at least 300,000 computers were affected by these two attacks. Later in the year, Equifax saw 145 million consumers' data get compromised—the most expensive breach in recent times. All of these cyberattacks had one thing in common: slackened endpoint security practices.

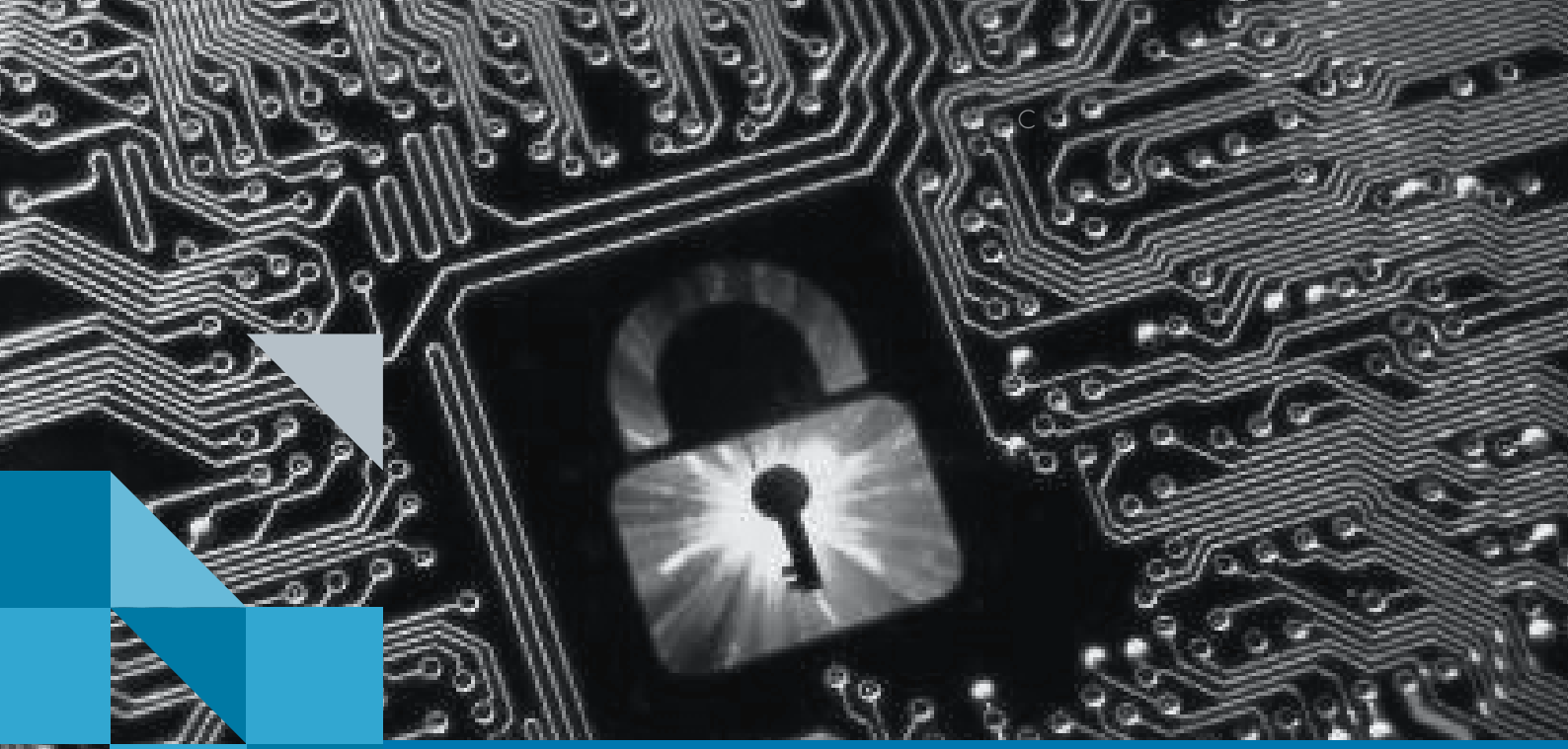
If victims' machines had been up-to-date with the latest patches, chances are they would have been spared from these attacks. While hackers always seem to find a way to sneak past security defenses, the best way to protect your organization is to invest in the right endpoint security solution for your network. ManageEngine offers multiple endpoint management solutions, including Desktop Central and Mobile Device Manager Plus, to take care of all the endpoints connected to your network. Both integrated endpoint security and management solutions offer an array of security features, ensuring complete endpoint security for your network.

Ransomware victims

150 countries

300,000 computers

145 million consumers



2.What is **endpoint security?** Why is it **critical?**

An endpoint is any device connected to a network: laptops, desktops, tablets, mobile devices, etc. Endpoints are connected to other devices within an enterprise network, as well as the external network of the internet. That means endpoints can be plagued with both internal and external security threats.

Endpoint security is all about achieving secure communication among all computers within a network as well as outside systems, without succumbing to vulnerabilities and data breaches. Gartner predicts that by 2020, 99 percent of all cyberattacks will occur via known vulnerabilities. This guide lists some of these vulnerabilities and how ManageEngine's endpoint management solutions can resolve your enterprise's endpoint security concerns.

3.Potential challenges and **threats faced by enterprises**

There are several types of security threats: malware—like ransomware and trojans—data theft, identity theft, etc. The motives behind cyberattacks vary—they may aim to monetarily exploit a company, ruin an enterprise's reputation, or gain access to confidential data—but all cyberattacks exploit one vulnerability or another.

3.1 Data Theft

Data theft happens when an attacker gains access to confidential corporate data. Data disclosure in a public forum can result in serious monetary losses, not to mention damage to a brand's reputation.

3.2 Identity theft

Identity theft can be dubbed an elevation of privilege, especially when a miscreant elevates their access privilege to gain unauthenticated access to confidential data.

3.3 Distributed denial-of-service attacks

In a distributed denial-of-service (DDoS) attack, an internal or external attacker inundates a network with an enormous amount of malicious data packets, which results in more traffic than the network can handle. This causes a temporary interruption or suspension of service. The hacker may demand a ransom for restoration of services. For organizations like hospitals, where digital health records, data sharing, and network-enabled medical devices are crucial, a temporary service interruption is enough to cause serious damage.

GitHub, a web-based hosting service for programmers, was recently hacked by a huge influx of traffic. This is touted to be the largest DDoS attack yet.

3.4 Remote code execution

With this type of vulnerability, a hacker can gain access to a network device and remotely execute malicious code. This code could corrupt the internal functioning of the affected application, negatively impacting the environment in which the application or software is used. Several applications, including Windows Defender and Adobe Flash Player, have been exploited using remote code execution in the past.

Sometimes, attackers can bypass security controls and execute a crafted application on a targeted system. Once they've infiltrated a system, they can access its inherent security features to carry out further attacks; for example, malicious content could cause unsuspecting websites to run harmful adware.

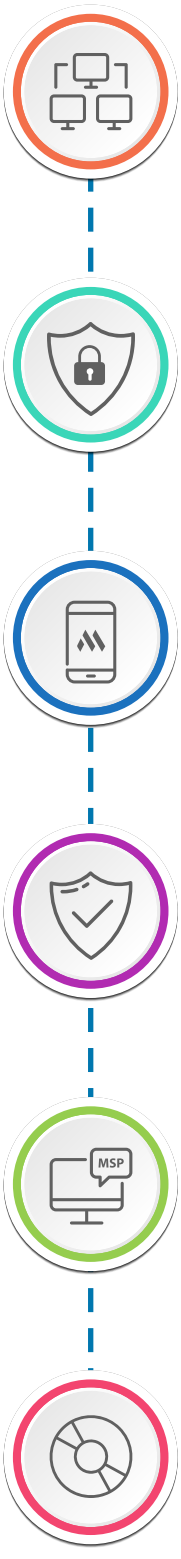
3.5 Watering hole attack

In a watering hole attack, hackers target a specific group of end users, usually by infecting the websites that particular group visits. For example, hackers might target a group of employees from a specific enterprise using a public Wi-Fi network or visiting websites outside of the corporate network. If firewall settings aren't configured properly, an attacker can gain access to an entire network once an affected user is back on the enterprise's network, even if just one user's laptop is affected.

4. ManageEngine's **endpoint security solutions**

Let's take a look at how you can tackle these vulnerabilities using ManageEngine's endpoint security capabilities.

Solutions for managing mobile devices and desktop computers



Desktop Central

Unified endpoint management.

Patch Manager Plus

Automated patch management for Windows, Mac, Linux & 3rd party applications.

Mobile-Device Manager Plus

Enterprise mobility management.

Patch Connect Plus

Third party patch management using SCCM.

Desktop Central MSP

Unified Endpoint management and RMM for Managed Service Providers.

OS Deployer

OS imaging and deployment software.

4.1 Automated patching

When security researchers discover vulnerabilities, vendors quickly develop and release the necessary hotfixes. If computers aren't up to date with the latest patches and hotfixes, it opens up an opportunity for hackers to exploit these vulnerabilities. But for IT admins, the question remains: Which endpoints should you patch first? How do you apply patches without interrupting business processes? Desktop Central helps you answer these questions.

Manually patching a network with just a few computers is relatively easy. But if your network has more than 50 endpoints, manual patching is tedious. Downloading non-OS security updates can be especially demanding. Using Desktop Central's regularly updated patch database, you can patch all your systems within one day after a patch is released (which almost comes as an unmentioned service level agreement. Desktop Central also offers automated patching which periodically scans your systems for missing patches, as well as flexible deployment policies so you can rest assured that all critically severe patches are applied as soon as they're available.

4.2 Blacklisting software using inventory management

Every organization should maintain a list of prohibited software and blacklist any applications that aren't required for work. Commonly blacklisted software, including gaming, social networking, and media streaming applications, can not only affect productivity, but also potentially bring malicious content that can harm endpoints into your network.

Desktop Central allows you to blacklist certain software and prevent those applications from being downloaded or installed from the internet. You can also configure alerts for any new software or hardware that comes into your network, helping you track any undesirable assets. To blacklist apps in Desktop Central:

- Perform an inventory scan to generate a list of all applications in your network.
- Mark any applications that need to be blacklisted.
- Detect blacklisted software that is currently in use on any computers and mobile devices.
- Automatically uninstall blacklisted software.
- Notify admins and users whenever prohibited software is removed.
- Generate reports on prohibited software.

Any undesirable software that isn't already present in your network can also be blocked using Desktop Central's Block Executable feature.

4.3 Tracking critical applications using system health reports

You can define vulnerability levels for systems in your network based on how many and what kinds of patches an endpoint is missing. For instance, you can mark a machine (or group of workstations) as "highly vulnerable" if it's missing just one critical patch, and "vulnerable" if it's missing a certain number of important patches. That way you can attend to the highly vulnerable systems first and ensure they're secure.

Desktop Central also has a dedicated Critical Vulnerabilities tab in its console, where you can find any missing critical patches that need to be deployed right away. If you need more granular information, you can check the system health of computers and find out which computers need immediate attention, then deploy the missing patches in bulk.

4.4 Antivirus software deployment and virus definition updates

With Desktop Central's Software Deployment feature, you can distribute and deploy McAfee's popular antivirus and endpoint security software throughout your network. Best of all, you can silently install McAfee's antivirus software without user intervention, ensuring all your network's endpoints are secure.

Of course, there's a lot more to network security management than just installing antivirus software. You need to regularly track and update antivirus software to detect upcoming vulnerabilities. Antivirus software vendors like Symantec, Microsoft (Windows Defender), and McAfee roll out virus definition updates frequently. It can be tedious to update these definitions every time they're released.

Desktop Central makes life easier by automating virus definition updates. The Automated Patch Deployment options help you schedule daily, weekly, or monthly system scans for virus definition updates depending on your organization's needs. Once scanning is complete, you can also specify an appropriate action to be performed based on the scan results. The auto-update process goes a step further by allowing you to configure email notifications about the scan status. Throughout the process, Desktop Central also tracks bandwidth utilization.

4.5 Achieving USB port security using configuration settings

Granting USB access to all users may lead to misuse of official data, resulting in data theft; there's also the risk of a compromised USB device potentially infecting workstations throughout your network. All things considered, you need to block USB devices judiciously.

Control USB devices using Desktop Central's USB configuration settings. Grant users access to use USB ports concerning mice, keyboards, CD drives, printers, and other portable devices. In certain cases, users may need exemptions from USB restrictions. Since user privilege configurations override computer configurations, you can configure a user's privileges to give them USB access on a computer whose ports are blocked. Read more about USB security on our **blog**.

4.6 Security standards and compliance regulations

HIPAA compliance for healthcare organizations

The Health Insurance Portability and Accountability Act (HIPAA) is focused on securing patients' health information. HIPAA requires that all healthcare organizations dealing with sensitive patient data establish a security management process to protect patients' confidential data from attempted unauthorized access, use, disclosure, or interference.

Desktop Central helps enterprises achieve HIPAA compliance by tracking file and folder access and the type of action (read, write, or modify) performed on confidential information. All together, Desktop Central helps organizations comply with the following HIPAA clauses:

- Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- Implement policies and procedures to prevent, detect, contain, and correct security violations. (Unauthorized changes).
- Implement procedures for monitoring log-in attempts and reporting discrepancies.
- Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

PCI DSS compliance for financial organizations

The Payment Card Industry Data Security Standard (PCI DSS) was developed to enhance cardholders' data security. PCI DSS requires all payment processing entities, like merchants, processors, issuers, acquirers, and service providers, to adhere to a set of requirements concerning the protection of cardholders' data and what's known as sensitive authentication data (SAD).

Desktop Central addresses the following requirements of PCI DSS:

- Building and maintaining secure network systems.
- Protecting cardholders' sensitive data through encryption.
- Employing a vulnerability management program.
- Implementing a strong access control.
- Regularly monitoring and testing networks.
- Maintaining an information security policy.

4.7 Securing roaming users' endpoints through a forwarding server

Sales and marketing personnel often have to travel as part of their work. Like any end user, traveling employees' assets can be at threat at various levels: using corrupted USB sticks, connecting to seemingly harmless Wi-Fi networks, falling prey to infectious websites, etc. All employees' laptops and mobile devices should be up-to-date and free from vulnerabilities, which means endpoint management software must be able to manage endpoints that are disconnected from the office network, too.

Desktop Central can secure roaming users' endpoints; you can also manage computers in remote offices (including those used at home) with Desktop Central installed in your local office. Employees that are away from the central office network are grouped under a default common remote office, with their agents actively contacting Desktop Central through a distribution server/forwarding server.

4.8 Securing remote troubleshooting using encryption

IT administrators often collaborate with other technicians to remotely troubleshoot endpoints. However, since remote access can be abused, Desktop Central allows you to grant appropriate read/write access to desired technicians. The remote desktop sharing mechanism supports remote login to any desktop on the network from a user account that has remote control privileges. Files are transferred across domains and workgroups in a fast, reliable, and secure manner, aided by strong AES-256 encryption.

Technicians can also black out users' screens during remote sessions to protect any sensitive information that they need to access or enter to troubleshoot the issue. Remote troubleshooting sessions can also be recorded to prevent unauthorized access.

4.9 Preventing interception attacks through SSL certificates

Desktop Central has secure agent-server communication via HTTPS, which helps you keep your network safe from intercepting attacks from hackers. You can also install an SSL certificate to encrypt agent-server communication and keep messages from being intercepted by a third party.

4.10 Security configurations

Security configurations like firewall settings and security policies help protect Windows machines from various security threats. With Desktop Central, you can:

- Configure security policies.
- Set up alerts for expiring passwords.
- Configure legal notices to alert end users about company privacy policies.
- Enable a firewall and configure firewall exceptions on Windows machines to prevent unauthorized access.

Extending its security capabilities to mobile devices, Desktop Central's mobile device management feature—as well as ManageEngine's Mobile Device Manager Plus—allow you to secure access to your corporate resources by:

- Configuring, distributing, and enforcing security policies on mobile devices.
- Ensuring that devices are compliant with company policies.
- Detecting and reporting jailbroken and rooted devices.

Registry key configurations

When the Meltdown and Spectre processor flaws were first addressed in the initial weeks of 2018, some patches for these vulnerabilities caused users to run into the blue screen of death. At that time, Microsoft required that all third-party antivirus vendors confirm compatibility with its CPU fixes and then set a registry key in their antivirus products to certify compatibility. Without the key being set, Microsoft's security update wouldn't install. As a workaround, admins could tweak certain registry keys to make their antivirus software compatible with the updates. Desktop Central's registry key configurations can help in situations like these.

Password alerts

You can also set alerts in Desktop Central that warn users a certain number of days before their computer password expires. Alerts can also prompt a user when they run out of disk space. If need be, you can create or overwrite important legal notices which are displayed during system startup.

Firewall configurations

Desktop Central also helps you control unwanted traffic in your network by configuring firewall settings, including opening certain ports. This can help control a DDoS attack by regulating data traffic.

Custom script configurations

In the summer of 2017, malware called Fireball automatically added extensions to victims' browsers to redirect their browsers to a fake search engine filled with adware and other malicious content. Desktop Central had a workaround for this particular cyberattack using custom script configurations.

Browser Security configuration

Browser security management is a vital part of IT administration, which broadly involves managing browser settings and ensuring a secured browsing for users. Browser configurations in Desktop Central allow you to

- Enable proxies to verify authentic communication from browsers
- Restrict potentially harmful websites from users' access
- Disable password cache preventing misuse
- Restrict non-secure downloads by disabling auto-downloads

Permission Management

You can manage the access to files, folders, registries by granting/revoking permission to specific users using Desktop Central's configurations. This helps restrict undesirable file actions.

Certificates management:

Using Desktop Central, you can install the security certificates specifying the certificate store and give a password to it.

Restricting device functionality

Every industry operates a bit differently, but in general an employee's level of corporate data access depends on their role within the organization. You can configure mobile devices using Desktop Central/Mobile Device Manager Plus to ensure that the right person gets access to the right data. Assign role-based device usage permissions in a matter of seconds with Desktop Central's mobile device management feature.

Restricting jailbroken mobile devices

Jailbreaking iOS devices and rooting Android devices might give owners a sense of freedom since many device restrictions and limitations are dismissed. However, there is a downside to this: security restrictions that were initially protecting the device are circumvented, thereby exposing the device to a whole new world of security threats. Security threats are amplified at an enterprise level, especially when corporate data is being accessed from rooted or jailbroken devices. With Desktop Central's reporting feature, you can restrict jailbroken and rooted devices from accessing corporate resources, preventing sensitive data leaks.

ManageEngine's Mobile device management capabilities

4.11 Data leak prevention in case of device loss or theft

Mobile devices, being small and portable, are commonly misplaced and an easy target for theft. If a mobile device goes missing, it's crucial to secure the data residing on the device, especially if it's sensitive to your enterprise. With Mobile Device Manager Plus, you can locate a lost device, securely and completely wipe the entire device, or selectively wipe only the corporate data.

4.12 Securing corporate email

Email is the most basic form of communication used by enterprises, and mobile devices are becoming the preferred way to access corporate email. Email security is critical, especially in high-risk industries like healthcare and defense, where sensitive information is exchanged via email. You can containerize emails on mobile to prevent misuse of data exchanged over email. Allow only enterprise-approved accounts on managed mobile devices to access corporate email, along with managed access to Exchange ActiveSync.

4.13 Securing distribution and viewing of content

In addition to securing email, your enterprise might be faced with needing to securely share content amongst employees as well. For example, Human Resources might need to share sensitive policy documents with employees. Using mobile content management feature, you can share sensitive files with ease.

4.14 Securing distribution and viewing of content

In certain sectors such as hospitality and retail, enterprises provide corporate devices to employees for a single purpose like inventory management or front-end sales. When employees only need a few apps to perform their required task, Mobile Device Manager Plus's configurations can prevent them from misusing their devices.

ManageEngine's endpoint management solutions don't just protect confidential data from security breaches, they also add a layer of accountability to endpoint management.

5 Summary

From automated patching to security configurations, ManageEngine's Endpoint management solutions help address all your endpoint security concerns proactively. ManageEngine's endpoint management solutions are capable of handling desktop, laptop and mobile device security so you can breathe easy. While Desktop Central comes bundled with a multitude of endpoint management features and security solutions, ManageEngine also offers standalone solutions for specific facets of endpoint management. ManageEngine, known for its high-utility IT management solutions, offers the following endpoint management solutions. You can try any of them in your network for one month, completely free.

Product Catalogue

ManageEngine's endpoint security solutions

Product	Description	30 day free trial
Desktop Central	Unified endpoint security solution for all sizes of enterprises	
Patch Manager Plus	Exclusive patching solution against vulnerabilities	
Mobile-Device Manager Plus	Enterprise mobile security solution for any number of employees	
Patch Connect Plus	SCCM add-on for patching third-party applications	
Desktop Central MSP	Endpoint security solution for managed service providers	
OS Deployer	OS deployment and disk imaging solution	

ManageEngine

ManageEngine offers real-time IT management tools that empower IT administration teams to meet their organizations' needs for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises including more than 60 percent of the Fortune 500-rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure: networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corporation Pvt. Limited with offices in the United States, United Kingdom, India, Japan and China.