

Mobile Threat Defense Checklist

Empowering organizations against mobile threats

WHITE PAPER



TABLE OF CONTENTS

Introduction	04
Chapter 1: Threats against mobile devices	07
Malware and malicious apps/websites	07
Mobile ransomware	08
Unsecured Wi-Fi networks	09
Phishing	10
Advanced jailbreaking and rooting techniques	10
Insider threats	11
Quick measures to keep the threats against mobile devices in check	12
Chapter 2: Endpoint protection	14
Anti-malware and Anti-virus software	15
Secure containers	15
Device and app control policies	16
Chapter 3: Detection, awareness and training	17
Real-time monitoring	17
Incident response plan	18
Detect and respond to potential security incidents	18
Chapter 4: Data encryption	19
Data encryption on mobile devices	19

Device-level and application-level encryption	20
Chapter 5: App management	21
App whitelisting and blacklisting	22
App security testing and vulnerability scanning	22
Chapter 6: Network security	23
Network security measures	24
Wi-Fi security measures	24
Secure web gateway	25
Network access control	26
Chapter 7: Hexnode amping up your mobile threat defense strategy	27
App security	27
Data loss prevention (DLP)	28
Content filtering	28
Web security	29
Device security	29
Network security	30
Compliance	30
Conclusion	31



Introduction

The consequences of a successful mobile attack can be devastating, including data breaches, financial loss and damage to an organization's reputation. Therefore, it is crucial for organizations to adopt a comprehensive mobile threat defense strategy.

Mobile devices have become an essential tool for staying connected and productive, both personally and professionally. We use them for everything from social media and entertainment to banking and business operations. They offer unparalleled convenience, allowing us to access information, communicate with others and work from virtually anywhere. However, with the increasing reliance on mobile devices, they have also become an attractive target for cybercriminals. Mobile devices are particularly vulnerable to a wide range of cyber threats, including malware, phishing attacks and network intrusions.

A mobile threat defense mechanism provides a systematic approach to securing mobile devices and minimizing the risk of cyberattacks. By implementing a strong mobile threat defense mechanism, organizations can protect their sensitive data and maintain the trust of their customers. The mobile threat defense mechanism should address three key areas:

- Connectivity
- Management
- Security

Organizations must ensure that their mobile devices are connected securely and efficiently to the corporate network. A secure and reliable network infrastructure is critical to protecting against network-based attacks.

Mobile device management is also a crucial aspect of a mobile threat defense strategy. Organizations must have robust management policies and procedures in place to monitor and control access to their mobile devices. They should also implement security controls to prevent unauthorized access and data leakage.

Finally, security is the most crucial aspect of a mobile threat defense mechanism. Organizations must have a proactive approach to identifying and mitigating mobile-related cyber threats. They should implement endpoint protection solutions that provide real-time threat detection and response capabilities. Additionally, they should train their employees on the best practices for mobile device security and ensure that their mobile devices are updated with the latest security patches. By addressing each of these areas, organizations can significantly reduce the risk of mobile-related cyberattacks and protect their sensitive data.

What is meant by mobile threat defense ?

Mobile Threat Defense (MTD) is a security solution that protects mobile devices from various threats, including malware, phishing, and network-based attacks. In the context of Unified Endpoint Management (UEM), MTD is a critical component of securing and managing mobile devices. UEM solutions provide a unified approach to managing and securing all endpoint devices, including mobile devices, laptops, and desktops, from a single console. MTD is integrated with UEM solutions to provide comprehensive mobile device management and security.

With MTD, UEM administrators can:

- Monitor and manage mobile devices
- Enforce security policies
- Protect against mobile threats

MTD provides visibility into:

- Device and application behavior
- Detection of suspicious activity indicating security threats

MTD solutions offer automated responses to detected threats, including:

- Quarantining a device
- Blocking a malicious app

MTD solutions provide threat intelligence, such as:

- Information about emerging threats or vulnerabilities
- Proactive protection for mobile devices by enabling UEM administrators to respond preemptively.

Why is mobile threat defense important ?

Mobile threat defense solutions help organizations protect their mobile devices from a wide range of threats, including malware, phishing, network attacks, device and OS exploits, and more. These solutions use various techniques such as behavioral analysis, machine learning, and artificial intelligence to detect and prevent mobile threats in real time.

By implementing mobile threat defense, organizations can:

- Ensure the security of their mobile devices and data
- Prevent unauthorized access to corporate networks
- Maintain compliance with industry regulations
- Avoid the financial and reputational damage that can result from a mobile security breach.

1

Threats against mobile devices



The threat landscape for mobile devices is constantly evolving, with attackers developing new and sophisticated techniques to exploit vulnerabilities in mobile devices and operating systems.

As mobile devices continue to be an integral part of daily life and work, attackers are increasingly targeting them to steal sensitive data, disrupt operations, and gain unauthorized access to corporate networks. Some of the major threats faced by the mobile devices deployed in a corporate setup are listed here...

Malware and malicious apps/websites

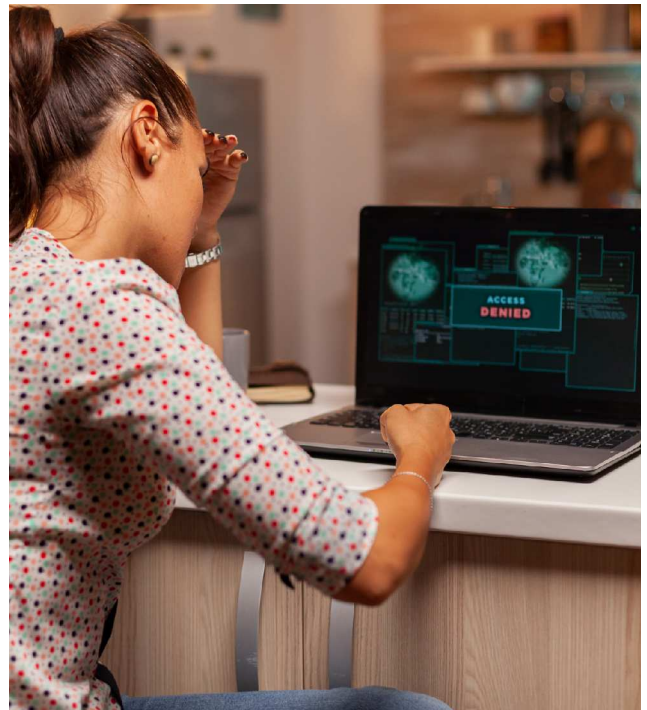
Malware and malicious apps/websites pose serious security risks to mobile devices in corporate environments. Malware, including viruses, worms, and Trojan horses, can infiltrate devices through various channels such as malicious apps, websites, or email attachments. Users may accidentally click on dangerous links or download malicious apps from unreliable sources, which can cause infections.

Attackers get unauthorized access to sensitive data for goals like financial fraud, identity theft, or espionage by employing techniques including Remote Access Trojans (RATs), backdoor entry, exploit kits and social engineering.

Malicious websites and apps can also be dangerous since they pose as their legitimate equivalents to fool users into downloading them or providing sensitive information. These programs might be infected with malware, spyware, or adware, jeopardizing user privacy and data security. Adware slows down device performance with unwanted pop-ups and adverts, while spyware tracks user activities and records passwords and credit card information. Vigilance, robust antivirus software, regular updates, cautious app and link usage, and user education are essential to mitigate these threats and safeguard mobile devices, sensitive data, and user privacy in enterprise environments.

Mobile ransomware

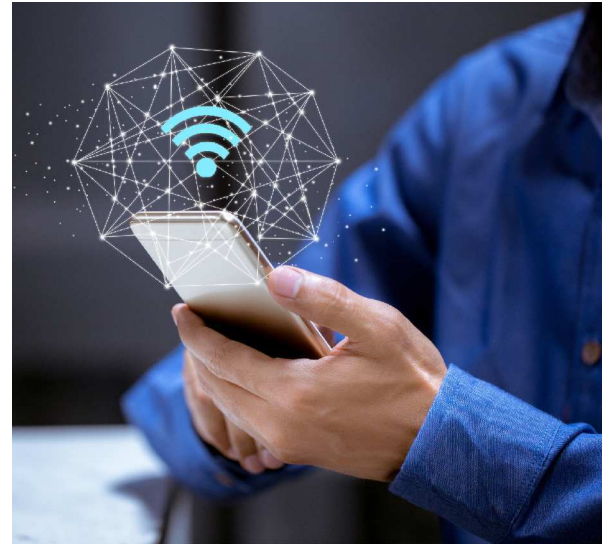
Mobile ransomware is a type of malware that encrypts files on a mobile device, making them inaccessible to the user, and then demands a ransom in exchange for the decryption key. Ransomware can spread through various channels, such as malicious apps or websites, phishing attacks, or infected email attachments. Once a device is infected, the ransomware can encrypt files, rendering them unusable, and demand a ransom in exchange for decryption. Mobile ransomware uses sophisticated encryption algorithms to lock files and prevent unauthorized access. The encryption keys used by ransomware are usually unique and can be difficult to crack without the correct decryption key. Ransomware can target various types of files, including documents, images, videos, and music, and can cause significant damage to personal and corporate data.



Once a device is infected with ransomware, the attacker can demand a ransom payment to provide the decryption key. Ransomware attacks can be costly and can cause significant disruptions to business operations. Payment of the ransom does not guarantee that the files will be decrypted, and the attacker may demand additional payments or use the same encryption keys to attack other devices.

Unsecured Wi-Fi networks

Unsecured Wi-Fi networks are a significant security risk for mobile devices. When a mobile device connects to an unsecured Wi-Fi network, an attacker can easily intercept any data transmitted over that network. This can include sensitive information such as login credentials, financial information, and other confidential data. Hackers can use various techniques to intercept data transmitted over unsecured Wi-Fi networks. Some of the techniques commonly used by attackers to exploit vulnerabilities in mobile devices and unsecured Wi-Fi networks are:



1. Eavesdropping:

- Monitoring network traffic to capture data transmitted between the mobile device and the network.
- Utilizing tools like packet sniffers or network analyzers for eavesdropping purposes.

2. Spoofing:

- Creating a fake access point that imitates a legitimate Wi-Fi network.
- When a mobile device connects to the fake access point, the attacker can intercept transmitted data.
- Tools such as wireless adapters or software can be employed for spoofing attacks.

3. Man-in-the-Middle (MitM) Attacks:

- Attackers position themselves between the mobile device and the target network.
- Intercepting data transmitted over unsecured Wi-Fi networks.
- Difficult to detect and enables stealing sensitive data or injecting malicious code into legitimate traffic.

Phishing

Phishing attacks are a common threat to mobile devices and involve tricking users into providing sensitive information through fake emails, text messages, or websites. Attackers can use various social engineering techniques to create convincing phishing emails or websites that appear to be legitimate but are, in reality, designed to steal sensitive information.

One technique used in phishing attacks is the creation of fake websites that mimic legitimate websites, such as banking or e-commerce websites. These websites look like the real thing, with similar logos, color schemes, and page layouts. The user is then tricked into entering sensitive information such as login credentials, credit card details, or other confidential information, which is then captured by the attacker. Phishing attacks also make use of social engineering. This involves manipulating users into revealing sensitive information.

Attackers may send fake emails or text messages that appear to be from a trusted source, such as a bank or other financial institution. The message may contain a link to a fake website or may request that the user provide sensitive information such as a password or credit card details. The user is then tricked into providing this information, which is captured by the attacker.

Advanced jailbreaking and rooting techniques

Jailbreaking is the process of removing software restrictions imposed by the manufacturer or carrier on iOS devices while rooting is the process of gaining administrative access to Android devices. Advanced jailbreaking and rooting techniques involve exploiting vulnerabilities in the bootloader, kernel, or OS to bypass security mechanisms and gain full control over the device.

1. Bootloader exploits:

Bootloader exploits involve taking advantage of vulnerabilities in the bootloader, which is the first program that runs when the device is turned on. By exploiting these vulnerabilities, attackers can gain full access to the device's memory and install a custom recovery or boot image.

2. Kernel exploits:

Kernel exploits involve exploiting vulnerabilities in the kernel, which is the core component of the operating system that manages system resources and provides a layer of protection between apps and the hardware. By exploiting these vulnerabilities, attackers can gain administrative access to the device, allowing them to install malware, spyware, or other malicious software.

3. Operating system vulnerabilities:

OS vulnerabilities are weaknesses in the operating system. Buffer overflows, code injection, or privilege escalation vulnerabilities are some common vulnerabilities that can have drastic repercussions if exploited.

- Buffer overflow attacks exploit memory vulnerabilities to execute malicious code or take control of the device.
- Memory leaks occur when apps or processes fail to free memory, leading to unstable devices or unauthorized data access.
- Code injection inserts malicious code into a legitimate app or system process, allowing attackers to execute code or take control of the device.
- Privilege escalation exploits OS or app vulnerabilities to gain administrative privileges and install malware, spyware, or other malicious software. By exploiting these vulnerabilities, attackers can gain system-level privileges. These privileges allow them to bypass security mechanisms and gain full control over the device.

Once a device has been jailbroken or rooted, attackers can easily install malware, spyware, or other malicious software that can steal sensitive data, spy on users, or disrupt operations.

Insider threats

Insider threats refer to the risk of unauthorized access, disclosure, or misuse of sensitive data by employees or contractors who have legitimate access to an organization's mobile devices. Insider threats can occur intentionally, such as when employees or contractors steal sensitive data for personal gain or sell it to third parties. Alternatively, insider threats can occur unintentionally, such as when employees or contractors accidentally expose sensitive data due to negligence or lack of awareness of cybersecurity risks. Insider threats can be particularly difficult to detect and prevent, as they often involve legitimate access to mobile devices and corporate data.

Attackers can use various techniques to exploit insider access, such as installing malicious apps or software, using social engineering techniques to trick other employees into revealing sensitive information or sharing login credentials with unauthorized individuals.

Apart from all these threats, there is also the threat of someone losing or stealing corporate devices. A lost or stolen device poses the risk of exposing sensitive data to unauthorized access. Attackers can gain access to the data stored on the device through various means, such as bypassing device locks, exploiting vulnerabilities in the device's software, or using specialized tools to extract data from the device's memory.

Quick measures to keep the threats against mobile devices in check

There are many ways to prevent and mitigate the threats against mobile devices. These include:

- **Keep software up to date**

Mobile device manufacturers and software vendors regularly release security updates that fix or at least fill in the loops made by known vulnerabilities. Keeping the device's operating system and all installed applications up to date with the latest patches and updates is a helpful measure in combatting the threats against mobile devices.

- **Use strong passwords and authentication**

Two-factor authentication adds an extra layer of security to login processes by requiring users to provide a second form of identification, such as a code sent to their phone or a biometric scan. Strong passwords that are difficult to guess, along with two-factor authentication (2FA) and biometric authentication, can help protect devices from unauthorized access.

- **Implement encryption**

Encryption can protect sensitive data stored on mobile devices from unauthorized access. Implementing full-disk encryption or encrypting individual files can help prevent data breaches. Encryption is a lifesaver in case of lost or stolen devices to prevent data abuse.

- **Secure Wi-Fi networks**

Secure Wi-Fi networks with strong encryption and authentication mechanisms. Avoid public Wi-Fi networks as far as possible.

- **Use Mobile Device Management (MDM) and Unified Endpoint Management (UEM) solutions**

MDM and UEM solutions can manage and secure mobile devices. These solutions can enforce security policies, remotely wipe devices, and also track devices.

- **Educate employees on safe mobile device practices**

Educating employees on safe mobile device practices such as not downloading unknown apps, avoiding public Wi-Fi networks and suspicious websites, and not sharing sensitive information over unsecured channels can help prevent security incidents.

Understanding the threat landscape for mobile devices is just the first step toward setting up a defense against mobile devices. And the best step forward is to ask ourselves a few questions that help us set up our line of defense against these threats. Mobile threat defense is a multi-faceted setup with interlinks to everything from endpoint protection, data encryption, app management, and network security to detection, awareness, and training. Amp up your organization's mobile threat defense by understanding these different segments and ticking away the checklist presented.

2

Endpoint protection

A person in a dark blue suit and grey tie is holding a tablet. Overlaid on the image is a digital shield icon with a keyhole in the center, surrounded by binary code (0s and 1s). The shield is enclosed in a white rectangular frame. There are also some faint digital interface elements like 'A1' and a blue dot with a line extending from it.

A comprehensive endpoint security solution protects mobile devices against various threats such as malware, phishing attacks, and network intrusions.

As mobile devices have become prevalent in the workplace, cybercriminals target them to gain unauthorized access or steal valuable information. To counter these threats, endpoint security solutions offer a range of features. Anti-malware and anti-virus software safeguard against malicious software, while secure web gateways filter internet traffic for potential threats. Network access control ensures that only authorized devices can connect to the network. Secure containers create isolated environments to separate personal and corporate data, preventing unauthorized access. Device and application control allow administrators to define policies regarding device usage and application permissions.

These features work together to provide multi-layered protection, covering various types of mobile threats like malware, phishing, data leakage, and device compromise. By implementing robust endpoint security measures, organizations can mitigate risks, maintain the integrity of their mobile devices, and safeguard sensitive corporate data.

Have you installed anti-malware and anti-virus software on all mobile devices in your organization ?

The use of anti-malware and anti-virus software is one of the essential elements of mobile endpoint security. This software assists in defending mobile devices from a variety of dangers, such as viruses, malware, and spyware. Due to the fact that they usually lack the same level of built-in security protection compared to traditional computers, mobile devices are particularly prone to these dangers. This makes them a desirable target for cybercriminals wanting to take advantage of flaws and steal private information.

Organizations can greatly lower the risk of cyberattacks and data breaches by installing and routinely updating anti-malware and anti-virus software on all mobile devices. These software solutions work by actively scanning the device's files, applications, and network connections to detect and eliminate dangerous malware. They employ a comprehensive database of known malware signatures and behavioral patterns to identify potential threats.

Additionally, anti-malware and anti-virus software can restrict the download and installation of potentially harmful apps on mobile devices. They utilize app reputation services and behavioral analysis techniques to identify suspicious or malicious applications, preventing them from being installed on the devices.

Regular software updates are crucial as they ensure that the anti-malware and anti-virus software has the latest threat definitions and security patches to effectively combat evolving threats. This proactive approach helps organizations maintain a robust security posture and protect sensitive data from unauthorized access.

Have you implemented secure containers to protect sensitive data and prevent unauthorized access on mobile devices ?

Secure containers are virtualized environments that segregate sensitive information and software from the rest of the system, adding an extra degree of security against unauthorized access. Businesses may protect critical data even if a device is lost, stolen, or corrupted by creating a secure container for corporate data and applications.

Sensitive company data, such as private documents and intellectual property, can be safely stored and accessed in secure containers. These containers also offer robust encryption to guarantee the security of data while it is in transit and at rest. Secure containers also help to retain user privacy while safeguarding organizational data since they enable the separation of personal and corporate data.

Have you implemented device and app control policies to secure sensitive data and restrict unauthorized access ?


Device control rules give IT managers the power to control the functioning of mobile devices and guarantee that users follow the company's security guidelines. By enabling features like encryption, passcode protection, and the deactivation of unused devices, they can customize devices to fit particular security requirements. With this method, users are unable to alter the device's security settings, and devices are always kept secure.



Application control policies give IT managers the power to govern which apps are installed on mobile devices. With this strategy, users are prevented from installing unauthorized or malicious applications and only authorized applications are loaded on mobile devices. Application control policies can prevent applications from running if they are not approved, preventing sensitive data from being exposed or stolen.

3

Detection, awareness and training



By taking a holistic approach to mobile threat defense, organizations can significantly reduce the risk of cyberattacks and protect their sensitive data from compromise.

The mobile threat landscape is constantly evolving, and organizations must be proactive in detecting and responding to threats to their mobile devices. To do this, they require an effective detection and response strategy that combines real-time monitoring, incident response capabilities, and advanced threat intelligence. Nevertheless, spotting risks and taking action are insufficient.

Have you implemented real-time monitoring for mobile device security incidents ?

Real-time monitoring is crucial for mobile threat defense because it enables IT administrators to spot and act swiftly on possible security events on mobile devices. Through this, administrators can identify and take action in response to abnormalities and patterns that point to a security breach or danger.

It uses machine learning and artificial intelligence to swiftly spot dangerous trends while analyzing enormous amounts of data.

Real-time monitoring can be also integrated with other Mobile Threat Defense solutions, such endpoint protection and network access control, to provide a holistic approach to mobile security. This will enable the detection and response to threats while restricting unauthorized access to important data and apps.

Have you established an incident response plan to mitigate the damage caused by mobile-related security incidents ?

A well-defined plan can assist IT administrators in responding promptly and limiting damage in the case of a security issue. An incident response plan should have clearly defined roles and duties, clear communication channels and a step-by-step procedure for managing security issues. It should also include instructions on how to analyze the incident, control it, find the cause, and take corrective action to stop similar incidents from happening in the future.

IT administrators should guarantee that they are well-prepared to respond to mobile-related security issues and can minimize the harm caused by such incidents to ensure endpoint security by creating an incident response strategy.

Have you set up real-time monitoring to detect and respond to potential security incidents on mobile devices ?

Employee awareness of potential risks associated with mobile devices and an understanding of the significance of using them safely depend on adequate user education and training. Password security, recognizing and reporting suspicious activity and the best ways to access and store sensitive data on mobile devices must all be addressed in training sessions.

Organizations can enhance their mobile threat defense systems and lower the possibility of security events caused by human error by educating employees about the risks and proposed practices for mobile device security.



4

Data encryption



Data encryption involves the use of algorithms to convert sensitive data into a format that is unreadable and unusable without the correct decryption key. This ensures that even if an attacker gains access to the data, they cannot read or use it.

Mobile devices are highly convenient and enable us to access and process data on-the-go. However, with this convenience comes a heightened risk of sensitive data being accessed or stolen by unauthorized individuals or malicious software. This is why data encryption is crucial for mobile security. Encryption can be applied to various forms of data, such as emails, messages, documents, and stored data on devices or cloud services.

Have you implemented data encryption on mobile devices to protect sensitive data ?

Sensitive data, including private business information, financial data, and personally identifiable information (PII), is frequently stored on mobile devices. One of the best ways to safeguard sensitive data from potential attacks is encryption. Even if a device is

lost, stolen, or compromised, it helps preserve data confidentiality and lowers the risk of data breaches.

Organizations can also prevent unauthorized access and guarantee that data is secure even in the event of a security compromise by encrypting data while it is at rest and in transit. Organizations can use encryption to help them comply with legal requirements for data protection. To ensure that data is kept secure, it is crucial to adopt robust encryption algorithms and key management procedures.

Have you implemented device-level and application-level encryption to ensure data privacy and confidentiality ?

Application-level encryption targets applications that may contain sensitive data, whereas device-level encryption secures the entire device by encrypting all data stored in it. By combining both encryption techniques, organizations can create a layered defense against potential security breaches and safeguard their private data.

5

App management



Data leaks, unauthorized access and malware infections are a few examples of the security concerns that mobile applications can pose.

With the increasing use of mobile devices in the workplace, organizations face a significant challenge in managing and securing the numerous applications used by employees on their devices. As part of their overall Mobile Threat Defense system, organizations must establish a successful app management strategy to handle these threats.

App management involves a range of activities, including app selection, deployment, monitoring, and control. It is crucial to make sure that only authorized applications are used on mobile devices and that they are consistently updated to the most recent versions.

Monitoring potential security vulnerabilities and ensuring that the right policies are in place to reduce risks are other important components of effective app management. Businesses can accomplish this through a variety of techniques, like mobile application management (MAM) solutions, which enable administrators to control and safeguard mobile apps.

Have you implemented app whitelisting and blacklisting to prevent the installation of unauthorized or malicious apps ?

App whitelisting allows only authorized applications to be installed on mobile devices, while app blacklisting prevents the installation of unauthorized or malicious apps. The danger of data breaches, malware infections, and other cyberattacks can be decreased by applying these policies, which allow IT managers to make sure that only reputable apps are loaded on mobile devices.

Have you implemented app security testing and vulnerability scanning to identify and remediate security weaknesses in mobile apps ?

Organizations can detect weaknesses in their mobile apps and take corrective action to reduce the risk of data breaches and other cyber threats by conducting comprehensive security evaluations. This can include utilizing secure coding practices, carrying out routine security updates, and adopting app shielding methods to safeguard sensitive data. Organizations can make sure that their mobile apps are secure and do not pose a risk to their sensitive data and systems by conducting app security testing and vulnerability scanning.

In addition to these, the organization should also manage app configurations and permissions. This involves controlling and enforcing app permissions to limit access to sensitive data and reduce vulnerabilities. Secure app deployment and self-service app catalogs are also important. They ensure that only authorized apps are deployed, minimizing the risk of downloading malicious applications. Regular security evaluations and updates are essential to identify and remediate weaknesses in mobile apps. By implementing these measures, organizations can maintain a secure mobile environment and protect sensitive data.

6

Network security

A man in a dark blue suit and red tie is holding a white tablet. Overlaid on the image are various network security icons: a padlock, a Wi-Fi symbol, an envelope, a house, a person, and a server rack. A central circular graphic features a padlock icon surrounded by circuit-like lines.

Cybercriminals can attack mobile devices and compromise the sensitive data they hold and access by taking advantage of flaws in the network architecture.

Network security is a key component of mobile threat defense as businesses are relying more and more on mobile devices for operations. The risk of network-based attacks rises as mobile devices are more closely tied to business networks and cloud services.

To ensure the security of mobile devices, organizations need to implement an effective network security plan that addresses both internal and external threats. This plan should encompass various measures to prevent unauthorized access, identify potential dangers, and promptly respond to them. Additionally, it is essential to safeguard the network infrastructure from malicious activities that may target mobile devices.

Organizations should establish a robust defense against network-based threats targeting mobile devices. This holistic approach helps safeguard sensitive data, maintain business continuity, and preserve the trust of customers and stakeholders in an increasingly mobile-centric operational landscape.

Have you implemented network security measures such as VPN and SSL to protect data in transit ?

To ensure the security of data in transit on mobile devices, network security mechanisms like Secure Sockets Layer (SSL) and Virtual Private Network (VPN) must be implemented. While SSL makes sure that data is protected and secure when delivered over the internet, VPNs offer secure and encrypted connections to distant networks.



Organizations can prevent sensitive data from being intercepted and guarantee that it is transmitted confidentially and securely by putting these safeguards in place. Given that mobile devices are frequently used outside of a secure network perimeter and that their data is more susceptible to being intercepted and compromised, this is an essential element of network security for the defense against mobile threats.

Have you implemented Wi-Fi security measures such as WPA2 encryption and certificate-based authentication to secure wireless networks ?

Network security for mobile threat protection must include the deployment of Wi-Fi security measures. Wireless networks can be protected against illegal access and data eavesdropping by employing WPA2 encryption and certificate-based authentication.

Wireless communication is well protected by WPA2 encryption, and certificate-based authentication makes sure that only approved devices can access the network. These precautions help to keep your network secure by preventing data loss, theft, and unauthorized access to critical information.

WPA2 encryption encrypts the data transmitted between mobile devices and the network, ensuring that sensitive information remains confidential and cannot be intercepted or deciphered by unauthorized entities. This encryption mechanism significantly reduces the risk of data loss, theft, and unauthorized access to critical information.

Have you implemented a secure web gateway to block malicious websites and prevent phishing attacks on mobile devices ?

A crucial part of endpoint security for mobile devices is secure web gateways. They are designed to stop malicious attacks by denying access to websites that are known to host malware or phishing scams. For real-time threat identification and blocking, these gateways often combine signature-based and behavior-based detection techniques.

- **Signature-based detection**

involves comparing website characteristics against a database of known malicious signatures. If a website matches a known signature, access is denied, preventing potential harm.

- **Behavior-based detection**

is used to identify suspicious patterns or activities on websites. This technique analyzes website behavior, such as unexpected redirects, malicious JavaScript, or hidden form fields, to identify potential phishing attempts or malware distribution. By proactively analyzing website behavior, secure web gateways can block access to malicious websites even if they have not yet been identified through signature-based detection.

Organizations can drastically lower the chance that mobile devices will be infected with malware or fall prey to phishing scams by utilizing a secure online gateway. This can help safeguard private information and prevent expensive data breaches.

It is essential for IT administrators to guarantee that all mobile devices have access to a secure web gateway, and that the gateway is set up correctly and is updated with the most recent threat intelligence. It can also be ensured that the gateway is offering appropriate protection against new threats by conducting regular testing and monitoring of its efficiency.

Organizations should have a secure web gateway in addition to educating staff about the value of safe web browsing habits and teaching them on how to spot and avoid phishing scams and harmful websites. This can assist in lowering the danger of endpoint security breaches on mobile devices even further.

Have you set up network access control to ensure that only authorized devices can access your organization's network ?


Network access control involves implementing policies and tools to ensure that only authorized devices can access an organization's network. Organizations can lower the risk of data breaches by managing network access.

Network access control typically involves a combination of technologies and policies. For example, IT administrators may use firewalls, virtual private networks (VPNs), and authentication tools to control access to the network. Policies may also be implemented to limit access to certain resources or applications based on the user's role within the organization.

In addition to network access control, organizations adopt zero-trust network security principles, treating every device and user as potentially untrusted. This approach requires continuous authentication, authorization, and verification throughout the network, enhancing security. It leverages techniques like multi-factor authentication, device health checks, and granular access controls based on user roles. By adopting a zero-trust approach, organizations ensure only trusted devices access sensitive resources, even beyond the network perimeter.

Identification and blocking of unauthorized devices are advantages of network access control, especially for mobile devices. Policies should be established based on the principle of least privilege, granting minimal access required for job duties. Access controls, multi-factor authentication, and encryption further enhance mobile device security, preventing data loss and unauthorized access.

7



Hexnode amping up your mobile threat defense strategy

By leveraging Hexnode's MTD features and capabilities, organizations can mitigate risks associated with mobile threats, maintain data privacy, and safeguard their devices and users from various security vulnerabilities.

Hexnode offers a comprehensive set of mobile threat defense (MTD) capabilities and features that are designed to protect devices and data from various mobile threats. These capabilities and features ensure the security and integrity of mobile devices within an organization. Here's a breakdown of Hexnode's MTD capabilities:

App security

Hexnode enables administrators to manage all apps on devices, including both corporate and personal apps. This includes the ability to block, uninstall, and restrict app usage. Administrators can block malicious or inappropriate apps, uninstall unnecessary apps, and set restrictions on app usage based on time or location. Hexnode's app sandboxing feature creates a secure environment by isolating corporate and personal apps from each other and the operating system. This isolation prevents malware infections from spreading between apps or affecting the device's operating system, enhancing overall device security.

Data loss prevention (DLP)

Hexnode's DLP feature helps prevent data leakage by setting policies and controls to prevent sensitive data from being shared or leaked. Administrators can define rules to block or monitor the transfer of sensitive data, such as personally identifiable information (PII), preventing potential data breaches.

- **Data access policies:** Hexnode allows administrators to define data access policies that restrict or control the sharing of sensitive data. These policies can prevent data from being transferred to unauthorized apps, cloud services, or external storage devices.
- **Copy-paste restrictions:** Hexnode enables administrators to restrict the copy-paste functionality on devices, preventing users from copying sensitive data from managed apps and pasting it into unmanaged or unauthorized apps.
- **App whitelisting and blacklisting:** Hexnode enables administrators to whitelist approved apps and blacklist unauthorized or risky apps. This helps ensure that sensitive data is only accessed and shared through trusted and secure applications, reducing the risk of data leakage.
- **Encryption enforcement:** Hexnode supports encryption enforcement on devices, ensuring that sensitive data stored on devices or transmitted over networks is properly encrypted. This helps protect the data even if the device is lost or stolen.
- **Geofencing:** Hexnode allows administrators to define geofences i.e. virtual boundaries based on geographic locations. With geofencing, administrators can enforce data access policies, restricting access to sensitive data when devices are outside authorized locations.

Content filtering

Hexnode allows content filtering, ensuring that devices access only appropriate and safe content. Administrators can block websites and apps, and restrict file downloads. This helps prevent users from accessing malicious websites, inappropriate apps, or downloading potentially harmful files.

- **Web content filtering:** Hexnode enables administrators to implement web content filtering policies, allowing them to block access to specific websites or categories of websites. This feature helps prevent users from accessing malicious or inappropriate websites, reducing the risk of malware infections and maintaining a secure browsing environment.

- **URL filtering:** Hexnode supports URL filtering, where administrators can define policies to block or allow specific URLs or URL patterns. This feature allows organizations to control access to websites based on their URLs, ensuring that users adhere to browsing guidelines and avoiding potentially risky or non-compliant websites.
- **Media and content whitelisting/blacklisting:** Hexnode allows administrators to create whitelists and blacklists for media and content. Whitelisting ensures that only approved media or content sources are accessible while blacklisting prevents access to specific media or content sources that are deemed inappropriate or unsafe.
- **App restrictions:** Hexnode allows administrators to control app usage by blocking or restricting access to specific apps. This feature ensures that only approved and work-related applications are accessible on devices, minimizing distractions and potential security risks associated with unauthorized app usage.
- **Safe search enforcement:** Hexnode enables administrators to enforce safe search settings on search engines. This feature ensures that search results are filtered for explicit or inappropriate content, providing a safer browsing experience and reducing the risk of accessing harmful or offensive material.

Web security

Hexnode's web security feature safeguards users from malicious websites. It enables administrators to block access to known malicious websites, preventing users from inadvertently visiting sites that could infect devices with malware. Hexnode's web filtering capabilities are designed to help protect devices from malicious websites and phishing scams.

Device security

Hexnode's device security features provide a range of protective measures. Remote wipe enables administrators to erase all data on a device remotely, ensuring sensitive information does not fall into the wrong hands if a device is lost or stolen. The remote lock allows administrators to remotely lock devices, rendering them unusable until unlocked. Password policy enforcement ensures that devices are protected with strong passcodes, reducing the risk of unauthorized access.

Network security

Hexnode helps secure networks by allowing administrators to block access to specific websites and apps. It also supports the creation of Virtual Private Networks (VPNs) to ensure secure data transmission. Administrators can block access to websites with malicious content or those that are not suitable for work purposes. VPNs encrypt data during transmission, safeguarding it from potential threats.

- **VPN configuration:** Hexnode supports the configuration of Virtual Private Networks (VPNs) on devices. This feature enables secure data transmission by encrypting network traffic, thus protecting sensitive information from potential eavesdropping or interception.
- **Wi-Fi configuration:** Hexnode enables administrators to configure Wi-Fi settings on devices, including connecting to trusted networks and blocking access to insecure or unauthorized networks. This feature helps ensure that devices connect to secure and authorized networks, minimizing the risk of data exposure or unauthorized access.
- **Firewall configuration:** Hexnode enables administrators to configure device firewalls to control incoming and outgoing network traffic. This feature adds an extra layer of protection by allowing administrators to define rules and block potentially harmful network connections.

Compliance

Hexnode assists organizations in complying with regulations and industry standards. It offers features such as data encryption and device usage tracking. Data encryption protects sensitive information stored on devices, ensuring compliance with data protection regulations. Device usage tracking helps monitor and enforce policies to ensure that devices are used appropriately for work-related purposes.



Conclusion

From real-time threat detection to anti-malware protection, network security, app security, web filtering, and device encryption, Hexnode provides a complete set of mobile threat defense capabilities that are designed to meet the needs of modern organizations.

There is no denying the fact that mobile threat defense is a critical aspect of enterprise security, as mobile devices have become an integral part of the modern workplace. With the rise of mobile devices and the growing sophistication of mobile threats, it is more important than ever for organizations to take a proactive approach to mobile threat defense.

Implementing a robust mobile threat defense solution like Hexnode helps organizations secure their mobile devices and protect sensitive data. However, maintaining vigilance and staying updated on the latest mobile threats is crucial. By staying informed and maintaining a strong security posture, organizations can keep their mobile devices and data secure. Mobile threat defense is an ongoing process that requires a combination of technology, best practices, and a commitment to security. Partnering with a trusted mobile security provider like Hexnode ensures that mobile devices and data remain secure against advanced threats.