Citrix Endpoint Management
Security Overview

Understanding the technology used by CEM to deliver comprehensive, end-to-end security.
Citrix Endpoint Management Security Overview

Understanding the technology used by CEM to deliver comprehensive, end-to-end security.

Mobility initiatives are a top priority for I.T. organizations. More employees than ever are demanding access to applications and data that help them achieve maximum productivity outside the office. But satisfying mobility requirements are becoming more challenging as employee expectations continue rising.

Today, employees want access to all their apps from any mobile device, including their devices. Modern mobile apps have expanded beyond conventional tools and use cases, such as mobile email. They now include Windows, web, and native mobile apps, delivered both from the cloud as well as the company datacenter. These apps are also being distributed broadly across different locations and mobile endpoints.

Allowing users to access all their apps and data from untrusted devices and unpredictable locations raises security concerns for I.T. The Citrix Secure Digital Workspace offers the most complete and integrated solution to enable people to access their apps, desktops and data from anywhere securely. And only a Citrix Workspace provides you a comprehensive choice of devices, cloud, and network, streamlined for I.T. control and simple, secure access for users. Endpoint Management is the cornerstone of mobility management in the Citrix Secure Digital Workspace. This white paper will help mobile technologists understand critical mobility requirements concerning security. It also explains the technology used by Endpoint Management to deliver comprehensive, end-to-end mobile protection.
The evolution of mobile management

Enterprises initially turned to **Mobile Device Management (MDM)** solutions to manage their devices. MDM not only centralized device management, but it also gave I.T. the ability to perform remote configurations and updates, and efficiently deliver applications and data to mobile endpoints. MDM helped I.T. organizations overcome early bring-your-own-device (BYOD) challenges, such as onboarding and large-scale management.

**Mobile Application Management (MAM)** emerged soon after MDM and focused on securing and managing applications as individual components. MAM offers a similar set of policies and user experience management as MDM, but at a different application level rather than the device level. Since then, MAM has expanded to encompass app-level control of secured Micro VPN, inter-container communication, and secure containers.

MAM has also gained in popularity as a standalone (**MAM-only**) alternative to MDM for enterprises that want to roll out **Bring Your Own Device (BYOD)** policies. Employees are becoming increasingly resistant to enrolling to corporate MDM environments because of user privacy concerns and putting their personal information at risk to an accidental or deliberate wipe by I.T.

**Unified Endpoint Management (UEM)** has recently emerged as an approach to securing and controlling desktop computers, laptops, smartphones, and tablets, in a connected, cohesive manner from a single console. Unified endpoint management typically relies on the mobile device management (MDM) application program interfaces (APIs) in desktop and mobile operating systems.

Of course, an EMM/UEM solution alone is not enough to ensure the success of mobile initiatives. I.T. organizations still need the right network infrastructure in place to ensure that applications and data are delivered across different devices securely, while also addressing performance, management, and scale requirements. This includes protecting data on-premises, in transit, and on mobile devices.

Standard network infrastructure components and management tools used for mobile initiatives include:

- Firewalls
- Enterprise Proxies
- VPNs
- Wi-Fi networks
- Application management/push technology
- Monitoring products
- Intrusion Detection System
- Workflow automation
- Policy management

An EMM/UEM solution also benefits from the evaluation of business needs, user needs, and work/life considerations. Many organizations are using their mobile initiatives to re-think the way they provide all I.T. services to end-users. They are now implementing public/private clouds, application/desktop virtualization, application layer firewalls/network gateways, security assertion markup language (SAML), and certificate services to assist and secure service delivery.
Enterprise Mobility Management (EMM)/Unified Endpoint Management (UEM) functionality of the Citrix Secure Digital Workspace is a crucial component of a reasonable General Data Protection Regulation (GDPR) compliance program:

- Citrix Workspace allows enterprises to establish a clear boundary between personal and business data on the device. I.T. doesn’t have access or visibility to personal content on the device, such as personal email or photos. Personal data is critical to the data minimization as well as the integrity and confidentiality principle of GDPR.

- Citrix Workspace gives I.T. visibility into which devices and apps are accessing business services. In the case of a data breach, the I.T. administrator can navigate through audit logging to identify what actions took place leading up to the compromise and what, if any, actions I.T. took as a result. Audit logging provides a clear record of any unauthorized access to business services and supports the GDPR principle of integrity and confidentiality, as well as of accountability. Citrix’s solution enables I.T. to:
  - Manage inventory – Identify authorized and unauthorized devices and apps
  - Allow applications – Establish a subset of applications that are authorized to run on a device and access business services
  - Protect access – Allow only authorized users, devices, and apps to access business services, whether on-premises or in the cloud
  - Provide audit logging – Monitor administrative actions and business data flows

- Citrix Workspace allows the I.T. administrator to protect the device from security threats, which is vital for the principle of integrity and confidentiality, as well as of accountability. Citrix’s solution enables the I.T. administrator to enforce compliance:
  - Apply appropriate security configurations and policies to the devices and applications
  - Actively Monitor the security compliance of the endpoint and applications, including attacks on the integrity of the operating system to jailbreak or root the device
  - Take remediation actions if the device or application is out of compliance via automated actions

Citrix mobility solution—Endpoint Management

Citrix Endpoint Management (CEM) provides comprehensive, end-to-end security, and delivers the full breadth of UEM capabilities along with an engaging user experience.

CEM leverages the enterprise-proven knowledge and technologies of Citrix and the platforms to provide a complete, integrated, and scalable solution for delivering apps and data to any device while maintaining security and a high-performance end-user experience from any location.

In the sections that follow, we will discuss critical components that enable security without compromising the user experience.
Citrix Endpoint Management Service

The CEM Service is the central hub for managing devices in Citrix Cloud. Citrix offers a single console for management of devices, apps, and data.

Mobile Device Management (MDM)

MDM allows you to manage mobile devices, set mobile policies and compliance rules, and gain visibility to the mobile network. It also provides control over mobile apps and data and shields your internal network from mobile threats. With a “one-click” dashboard, simple administrative console, and real-time integration with Microsoft Active Directory and other enterprise infrastructure such as public key infrastructure (PKI), Endpoint Management simplifies the management of mobile devices. CEM can be used to manage Android, iOS/iPadOS, MacOS, Windows 10, Chrome Books, and other devices like Workspace Hub.

Mobile Application Management (MAM)

Citrix Endpoint Management provides the industry’s most comprehensive set of MAM capabilities to secure information at the application level. CEM MAM capabilities allow you to protect enterprise apps and data with policy-based controls, such as restricting access to authorized users, automatic account de-provisioning for terminated employees, and remote wipe for data and apps stored on lost devices.

CEM takes advantage of platform security capabilities to provide a secure BYO experience to users. Google’s Android Enterprise Work Profiles is an excellent example of leveraging the platform to create a separation of work and personal data on the device and only allow management of the work profile to the organization.

With CEM MAM, you can provide the following benefits for each application type:

• Centralized user account creation and management for applications
• A unified enterprise app store to enable the publishing and distribution of Android-, iOS-, and Windows Phone-based applications for authorized users to download and install on mobile devices
• Access to virtual Windows applications and desktops with seamless SSO (no redundant prompts for credentials)
• Centralized policy controls to secure applications and data, with easy removal of user accounts, erase and lock of Citrix-delivered applications and data, and consolidated auditing and reporting of application access.

Endpoint Management MAM also includes the Citrix MDX app container technology:

• Mobile applications can have their network access controls managed by the solution to ensure network connections are routed appropriately thru secure SSL channels (MicroVPN) based on application, domain name, etc.
• Isolation from other user-owned apps on mobile devices is also available. Each application may receive its dedicated SSL encrypted tunnel that can only be leveraged by that application
• Applications inherit all MDX security features, including SSO, secure inter-app communication, information/data containment, restrictions based on device states
Endpoint management security details

Application authentication controls

Each application under management retrieves its policy check-in times from the Secure Hub application. The applications will then verify timers across each application/resource on the device.

When a user is successfully authenticated, an application-specific key is generated with an associated expiration time applied. This key further encrypts and protects access to any user-based certificate delivered to the MDX framework.

This key is validated and stored in memory to encrypt/decrypt data for that specific application in the secure vault. When the key expires, the app will obtain a new key based on current authentication status and policy.

FIPS 140-2 compliance (Available on-premises only)

The Federal Information Processing Standard (FIPS), issued by the U.S. National Institute of Standards and Technologies (NIST), specifies the security requirements for cryptographic modules used in security systems. FIPS 140-2 is the second version of this standard.

Endpoint Management release v10 has achieved broad end-to-end FIPS 140-2 compliance. Data-at-rest and transit cryptographic operations are using FIPS-certified cryptographic modules.

Endpoint Management MDX overview

Device data at rest—at a glance

<table>
<thead>
<tr>
<th>Platform</th>
<th>Location</th>
<th>Strength</th>
<th>Key Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>MDX Applications</td>
<td>AES-256</td>
<td>Citrix Secure Vault</td>
</tr>
<tr>
<td>Android</td>
<td>MDX Applications</td>
<td>AES-256</td>
<td>Citrix Secure Vault</td>
</tr>
</tbody>
</table>
How is my data protected at rest?

Most employees today do their best to protect company interests. But the stress of work and the need for productivity can drive employees to make bad decisions. This situation often arises in the form of users leveraging applications and cloud storage systems that are not under company control, or who copy/paste sensitive content to unprotected email systems. These applications make the mobile end-user experience more productive, but raise the risk of losing control of the data. At the opposite end of the spectrum are malicious users who may be attempting to steal company assets. Regardless of the motive, I.T. needs tools to protect company property.

Considerations:

- **Control copy/paste:** MDX can prevent copy/paste or only allow it to happen across company-wrapped applications resulting in a separation of company/private data.

- **Restrict open-in:** Controls are available so that opening documents can only be occur within company-wrapped applications. When an employee receives an email with an attachment, all personal apps on the device with the ability to open the document will be made unavailable. Only company-approved apps will be able to perform this function. Links to websites can also be enabled to only open within a secure browser. (Administrators can set specific exceptions to this policy when needed, such as for Office 365 mobile applications.)

Data containment has been outlined below in a functional diagram:

On iOS platforms, Endpoint Management leverages strong platform-specific FIPS-validated cryptographic services and libraries such as keychain. OpenSSL is also well known for providing FIPS-validated modules for a variety of platforms, further securing data in motion as well as certificates needed to manage and enroll devices. CEM uses our proprietary secure vault for storing sensitive data in the keychain and leverages the platform device encryption for everything else. There are MAM controls at the app level that check for compliance to validate device encryption is enabled at every app launch. These MAM controls are a part of the Encryption Management feature.
Secure vault

Secure Vault is a strong encryption layer that is used by Secure Hub, and other Citrix MDX/MAM SDK enabled applications to persist their sensitive data, such as passwords and encryption keys on the device.

CEM stores sensitive data in the secure vault of platform-native stores such as the iOS keychain. The data persisted in secure vault include Active Directory username/password, pkcs12 (certificate/private-key) and its protection password, key material, pasteboard encryption key, SAML token, STA ticket, and Citrix PIN history.

Platform security

Apple and Google both provide a comprehensive security architecture that has improved greatly with each version release. iOS and Android both provide certified FIPS140-2 data protection and use a hardware-based secure enclave for encrypting all files written to disk. Encryption keys are always stored in the secure enclave, and keys never leave the enclave.

Both platforms also provide app sandboxes that don't allow other applications from gaining access to the app data. If applications follow the best practice guidelines and save data only to the app sandbox, there is no way to access that data from other 3rd party rogue applications.

iOS provides an MDM policy for supervised devices to enforce USB restricted mode. Enforcing USB restricted mode does not allow devices to be plugged into debuggers for access.

For more information about device encryption, refer to Apple's and Google's security guides.

Android Enterprise

Android Enterprise is the modern management platform with in-built security that protects the device from different layers:

**Hardware backed security:** Includes features like Verified Boot, Trusted Execution Environment (TEE), Keystore, Tamper-resistant hardware support.

- **Verified Boot** verifies the system software before running it, each boot stage is cryptographically signed, and every phase of the boot process verifies the integrity of the next phase before executing code.

- **TEE** makes sure that untrusted code is separated from the most security-critical tasks like lock screen, biometrics, DRM, etc.

**O.S. level security:** Includes features that maintain the device integrity protecting the device from running a tampered or compromised operating system. One key feature there is:

- **App sandboxing:** Android runs all apps in a sandbox preventing malicious apps from impacting other apps or system components. By default, apps cannot interact with each other and have limited access to the O.S.

**User and data privacy:** Starting Android 9, followed by 10 and 11, the O.S. had added many features to protect end-user privacy from limiting background access to device sensors, restriction information gathered from Wifi-scans, and so on.
Application Security

Safety Net attestation is a set of anti-abuse API’s that Secure Hub leverages to assess the integrity of the device. This information can then be used to set up device compliance checks to protect corporate data.

Safety Net Verify Apps API allows Secure Hub to interact programmatically with Google Play to check if there are known potentially harmful apps installed on the device.

Managed Google Play: Content marketplace for Android Enterprise, allows users to browse public and private apps approved by the organization and enables the admin to pick and choose the apps that will be available to the end-user in the work environment.

Data protection (Encryption)

Starting Android 6 encryption is mandatory on all devices; there are two forms of encryption:

File-based: Storage areas are encrypted with different keys available since Android 7. There are two kinds of storage locations for apps:

Device Encrypted (D.E.) storage: Available once the device boots and before the user enters the credentials. Protected by hardware secret and software running in Trusted Execution Environment.

Credentials Encrypted (C.E.) storage: Available only after the user has unlocked the device. C.E. storage keys can only be derived after unlocking the device, with protection against brute force attacks in hardware.

Most of the apps store data in C.E., but apps like alarms and even Secure Hub can take advantage of D.E. storage.

Full disk encryption: Available on devices running Android 5.0-9.0. Encodes all user data using a single encryption key.

Citrix Endpoint Management has a passcode policy that enforces passcode on BYOD and corporate devices. Additionally, in MAM only mode MDX policies restrict app access if no passcode is present on the device.

For additional details, please follow the Android Security Whitepaper.

Android Enterprise on Citrix Endpoint Management

Two main modes can manage Android devices:

BYOD: This mode is meant for the end-user using their personal device to access corporate apps and data. When a user enrolls in this mode, Citrix Secure Hub creates a separate user space on the device known as “Work Profile.” This space is completed separately from the Personal space (where personal app and data are present). Secure Hub will be in the Work Profile and communicate with the CEM server/Play EMM API’s to deliver apps and policies.

App/data protection on work profile: The user only has access to apps approved by the organization via Managed Play, and since there is a clear separation of Work and Personal, malicious apps from the personal side cannot impact work apps and data.

CEM has policies that prevent users from copying data from work to the personal side of the device. There are additional protections against screenshot, camera, contacts & calendar sharing, etc. that can be applied based on preference.
Application permissions: Through CEM policies, admins can control which apps can have access to camera, gallery, location, microphone, etc. This enables admins to prevent certain apps from having access to device hardware.

Security: CEM provides multiple security actions that can be applied to the Work profile in case of a security issue. You can wipe the work profile—which deletes all the work apps and data from the device. You can lock the work profile—which would prevent access to the work profile.

Fully managed: This mode is for corporate-owned devices that mainly meant for work but could be used for personal purposes as well. In this mode, there is no work / personal separation. The admins have control over most of the device level policies. This mode requires a factory reset, and Secure Hub can be pushed on the device to enroll via Zero Touch, NFC, QR Code, or DPC identifier (afw#xenmobile). Secure Hub enrolls the device in the Fully Managed mode.

This mode is further broken down based on use-cases:

- Device Owner: Corporate use case
- Corporate Owned Single Use (COSU): Kiosk/Shared Device user case
- Fully Managed with Work Profile (COPE)/Enhanced Work Profile: Corporate and Personal use case. Note COPE is changing to Enhanced Work Profile in Android 11. This mode removes certain security policies like Factory Reset, Passcode Reset, and App inventory due to user privacy since the device is used for personal purposes.

App/data protection: The user only has access to apps approved by the organization via Managed Play and do not access to Personal play store to download other apps. Policies also protect from side loading. Since all apps go thru the admin approval process, the device is inherently protected from malicious apps.

CEM has policies that further prevent data leakage from the device from blocking the camera, Bluetooth, USB file transfer, NFC, etc.

Application permissions: Through CEM policies, admins can control which apps can have access to camera, gallery, location, microphone, etc. This enables admins to prevent certain apps from having access to device hardware.

Security: CEM provides multiple security actions that can be applied to a Full Managed device in case of a security issue. You can fully wipe the device, lock the device, reset the passcode. As mentioned above—Corporate devices used for personal purposes would not have all the security actions available.
High-level architecture:

Android Enterprise with Citrix Endpoint Management

CEM connects with Google via PlayEMM APIs to bind CEM as the EMM provider, to provide app store approvals, and to publish private app publishing via an embedded Google iFrame.

Secure Hub, which is the Device Policy Controller (DPC), will also connect via Play EMM API’s to create managed Google play accounts at enrollment and fetch the approved apps from Managed Play.

Device policies are fetched by Secure Hub from the CEM server and delivered to the device.

Remote lock and wipe

Certain security features such as remote lock and wipe both rely on the device receiving instructions from a server. If a device is lost or stolen and put into airplane mode before such an instruction is received, this could prevent corporate data from being destroyed. MDX protects against this situation with a device-side “Kill Pill” feature which causes the container to lock or erase itself if it hasn’t been able to successfully connect to CEM Server within a configurable interval (Max Offline Timer).
How is my data protected in transit?

**MicroVPN**

MicroVPN capabilities are a core feature of the MDX framework, granting secure access to enterprise resources for several functions including:

- Application access
- Intranet access
- Mail access (Negating the need for ActiveSync to be exposed directly on the firewall perimeter)

MicroVPN tunnels are specific per application and encrypted to protect from other device communication or other MicroVPN communication. In addition to these security features, MicroVPN also offers data optimization techniques including compression algorithms to ensure that only minimal data is transferred in minimal time, improving user experience—a key success factor in mobile project success.

The following diagram outlines a typical network call established as part of the MDX policy definition within the CEM Server. Although the CEM Server defines the usage of a MicroVPN, the Citrix Gateway will ultimately determine the path the client takes once it hits the gateway.

**Encryption level for TLS session**

The encryption level for a TLS session can be defined on the Citrix Gateway but is typically AES-256.
Device/server verification

Endpoint Management employs strong two-factor authentication to prevent possible attacks. Multiple levels of digital certificates form the foundation of the Endpoint Management security infrastructure. A device certificate is issued during the enrollment process and required for communications between the device and Endpoint Management Servers. Citrix also supports user identification certificates in addition to device certificates.

Jailbreak status is also validated before enrollment. On iOS, enrollment starts with a device certificate request using the Simple Certificate Enrollment Protocol (SCEP) via the built-in MDM capabilities embedded in the iOS operating system. Device certificates are signed and issued by an embedded Endpoint Management Certificate Authority (C.A.). These certificates are used during communication to ensure that the device is what it says it is. From this point forward, basic device management is performed by authenticating the client with the appropriate client, certificate-based handshakes. Client certificates are generated by a 3rd-party trusted C.A., such as when customers already have a PKI deployment in place. Endpoint Management supports the most popular commercial C.A. services, such as Microsoft, Symantec, RSA, and OpenTrustCA.

Android Enterprise enrollment is initiated via the Secure Hub app published on Google Play. Basic user authentication is performed, as explained above. The device is evaluated for rooted status using the Google attestation APIs and then authenticated. Once this process completes, certificates are then exchanged. These certificates are passed from this point forward to authenticate the client to the CEM service.

All data and certificates/private keys locally stored on the device are encrypted using AES-256 encryption in Citrix secure vault or a strong platform-native service such as iOS keychain.

Operational security features

Endpoint Management offers a full set of features to assist with day-to-day or operational security management of mobile devices, applications, and data. Operations teams get the control they need to enroll users, manage and wipe devices (or selectively wipe corporate apps and data), and to automate actions such as notifications and device compliance flagging. They can also maintain app and data integrity through advanced auditing capabilities and ensure the protection of sensitive corporate assets with multi-layered DDoS protection.

Enrollment

There are basic differences between iOS and other managed platforms for enrollment concerning the process of joining a device to the managed service. These are mostly due to the documentation and API’s offered by the device manufacturer.

Some optional enrollment controls within Endpoint Management MDM provide a balance between security and usability. These include a username (locally created or in Active Directory) in addition to one or more of the following 2nd factors:
Additionally, each device enrollment may have the following attributes associated with it:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity Time</td>
<td>How long the enrollment invitation is valid</td>
</tr>
<tr>
<td>Device Binding</td>
<td>To which device Serial/IMEI/UDID is this invitation bound</td>
</tr>
</tbody>
</table>

Alternatively, a SAML token may be used as a credential to pass validity from a SAML server such as Active Directory Federated Services (ADFS).

**Initial enrollment flow diagrams**

The following sections describe initial enrollment using iOS as an example. Android enrollment is very similar.

**MDM enrollment**

Enrollment is usually end-user driven, as part of either a reactive download from a device platform app store, or as part of notification generation at the server-side.
After downloading the Secure Hub Application, the user is prompted to enter a username or email address used to authenticate within the service.

The domain portion of the entered email address is compared with the Endpoint Management AutoDiscovery Service (ADS) to determine whether auto-population of the server address, port, and additional security parameters is possible. If not, the user is prompted to enter a valid server address.

The Endpoint Management AutoDiscovery Service also facilitates Certificate Pinning, which provides Secure Hub with a certificate. It can then compare with the certificate provided to it by Endpoint Management Server. If the certificate provided by Endpoint Management Server doesn't match the certificate provided by ADS, then enrollment is not allowed to proceed. Certificate Pinning is a key feature to block man in the middle (MITM) attacks.

The Endpoint Management enrollment service is checked for availability, and the user is authenticated against Endpoint Management, which also confirms that the device has not been revoked previously. Endpoint Management will validate the user is valid against the configured Active Directory (or a valid IDP via Citrix Identity Platform). At this point, the user will need a supplied password and/or PIN identified by the enrollment type on the server.

After successful authentication, optional terms and conditions are presented. If a user fails to comply, they are not allowed to continue enrollment.

At enrollment, a certificate is generated and installed on the client, which will represent the user for future MDM sessions. Once SCEP is complete, Endpoint Management instructs the APNS to notify the device to use this certificate to connect into the standard 443 connection port to complete the enrollment, run the initial MDM session, collect inventory, etc.

**Post enrollment (Day-to-day connectivity)**

Day-to-day management takes place in one of the four scenarios below:

- **Scheduled deployment**: where a deployment task is delayed until a specific time
- **Scheduled in bound check-in**: by default every 6 hours for IOS
- **Ad hoc task**: such as right-click lock/wipe/locate, activated by a console administrator
- **Web service call**
All events are triggered via an Apple Push Notification instructing the device to connect inbound over port 443. Apple Push Notification Service (APNS) is an Apple-specific notification method and service for secure notification of both “connect” events for MDM as well as general device notifications (e.g. message popups). APNS ensures only valid messages get pushed to devices, and that all MDM activity is associated with a server-installed certificate that is co-signed by the MDM provider.

When a device connects inbound to Endpoint Management Server, it presents a valid certificate containing the user I.D. of the device. This ID is used by the Active Directory “Bind User” function to check three attributes:

- Active Directory Group Membership
- User account is not disabled
- Active Directory attributes of the user (e.g. email address)

Optional security measures include the support of secure LDAP, where a certificate is used as an additional authentication to support the lookup process of the Active Directory bind user.

**Remote data wipe**

The safety net for data loss prevention is the ability to initiate the removal of data from a remote device.

Wipe functionality is available at multiple levels, including:

- Selective (corporate wipe)
- Full wipe (device reset)
- MAM Container wipe

And can be initiated in the following ways:

- Administrator initiated (subject to role approval within console)
- User-initiated (as part of the self-help functionality)
- Automated (as part of automated actions, described below)
- Automated based on device inability to contact the server (Kill Pill)
- As part of some other process initiated via web service

**Application execution prevention**

On supported platforms, Endpoint Management can permit or block applications and processes. This prevents both the installation and execution of unauthorized tasks. Typical use cases include preventing access to public application stores, restricting personal or social applications, or simply preventing configuration changes. This is achieved with a task watcher embedded within Secure Hub that can prevent interaction with any unauthorized execution.

**Automated actions**

Endpoint Management provides automated actions that protect and inform both users and the security administrator in the event of an issue. An automated action can be used as an engine to perform a task or tasks should the device or user state change.
A typical example:

**IF User no longer employed with company (disabled in A.D.), THEN selective wipe the device.**

This example automates the un-enrollment process and drives security based on existing best practices. This process should remove user access to company systems, and also remove company apps, cloud systems (SFDC, etc.) along with SSO credentials, etc.

These actions may be combined and can result in notifications, blocking, flagging as out of compliance, or wiping. The enterprise has the flexibility to make this choice. With the typical needs understood, let’s examine how to secure enrollment and MDM components.

**Auditing capability**

Endpoint Management leverages audit trails for server-based activity. Key user information obtained from gateway components, including the time of access, I.P. address, and device data.

**Citrix Gateway**

Rich audit trails are recorded both on the appliance and streamed to configured external log collection servers.

**Endpoint Management Service**

Endpoint Management does not (by default) expire audit trails and information from the database. Endpoint Management also provides different levels of server logging and verbose logging if needed during troubleshooting exercises. No data is shown in log files; however, log files will contain useful information such as logon user I.D., with password information excluded. Many device policy violations—such as jailbreak, unmanaged device, location perimeter violation, or location disabling—can be configured to generate automatic alerts. Application, device, and user login events are all recorded in audit logs. Different levels of log and audit info, warnings, and errors can all be configured on a per-module basis. This information is available for access by sending log files to a system log (Syslog) server.

**Ensuring denial of service protection**

**Citrix Gateway**

All logon input fields are protected against standard security threats. DDoS protections defend against malicious clients.

**Endpoint Management Service**

Security penetration testing is done to identify and remediate attack vectors. Additional app firewalling is possible via NetScaler.

**PKI integration and distribution**

Endpoint Management can make certificate requests to external certificate service providers such as Microsoft, Entrust, Intercede, or RSA via web enrollment to enable certificate-based authentication for WIFI, VPN, and Exchange ActiveSync profiles. The end game is to provide controlled, authenticated access to the network resources—but only for devices that are compliant with
company security and compliance requirements. Certificates can provide access to network resources without the need for user interaction or serve as a second authentication factor.

This can be done by acting as a client and requesting certificates on behalf of users with enrolled devices or configuring the device to communicate directly with the C.A. using Simple Certificate Enrollment Protocol (SCEP). Certificate revocation and renewal are also supported, driving a balance between security and usability.

**Summary**

Citrix Endpoint Management is the key to managing personal devices in a corporate setting at scale—without impacting the user experience and without inflating costs or introducing security risks.

Citrix Endpoint Management delivers the powerful end-to-end EMM solution you need. By combining the essential features of MDM and MAM, Endpoint Management gives you complete control over mobile apps and data, centralizes mobile device and user management, and shields your network from mobile threats.

The Endpoint Management solution—with integrated Citrix products—enables secure remote access to applications. Citrix Secure Hub provides a comprehensive set of mobile productivity apps, while Citrix NetScaler Gateway fortifies the network and lets I.T. control how users access their applications and data.

Endpoint Management uses a broad range of technologies and standards—including authentication, encryption, containers, policies, passwords, certificates, and micro VPNs—to provide enterprise-class data protection and compliance in key mobility use cases, allowing you to protect data:

- At rest
- In transit

In addition, Endpoint Management lets you manage ongoing operational scenarios, including user and device enrollment, remote data wipe, and auditing.

Citrix delivers a single integrated EMM solution to manage mobile devices, mobile apps, desktops, and desktop applications. This integrated approach helps I.T. further reduce costs by leveraging the same architecture, hardware, and devices for end-to-end application and data delivery. Endpoint Management facilitates positive user experiences that improve productivity and help eliminate shadow I.T. while ensuring employee privacy and providing enterprise-grade protection for the corporate data and assets that matter most.