Citrix XenMobile Service Security
# Table of contents

- Introduction .................................................. 4
  - Cloud Benefits ............................................. 5
  - Cloud Security ............................................ 5
  - Security Concerns .......................................... 6
- Overview .......................................................... 7
- XenMobile Service ............................................ 8
  - Architecture ................................................ 8
  - Environment Security ...................................... 9
    - Logical Security ........................................ 9
    - Access controls ......................................... 10
    - Data access controls .................................. 10
    - Network access controls ............................... 10
    - Operating system access controls .................. 11
    - Change control and business continuity .......... 11
  - Personnel security ........................................ 12
  - Compliance .................................................. 13
    - Data Encryption ......................................... 13
    - Physical Security ...................................... 13
  - UEM .............................................................. 14
    - Enrollment ............................................... 14
    - Authentication ......................................... 15
    - Client Management ..................................... 16
- Citrix Cloud .................................................... 17
  - Services ..................................................... 18
  - Benefits ...................................................... 19
  - Cloud Connector ........................................... 20
**Table of contents**

Cloud Platform Provider .................................................. 22
  Microsoft Azure .......................................................... 22
    Azure Transparent Data Encryption ............................... 23
    Azure Security Center ............................................... 24
    Azure Active Directory (AAD) ...................................... 24
  Network Security Groups .............................................. 24
  Availability Sets ....................................................... 25
  Physical Security ....................................................... 25
  Azure Portal ............................................................. 25
  Azure Activity Logs ................................................... 25
Amazon Web Services ..................................................... 26
  Resource Locations .................................................... 26
  Domain Controllers ..................................................... 27
  NetScaler Gateway ...................................................... 27
Data .............................................................................. 28
  Exchange ...................................................................... 28
  Intranet Web Sites ....................................................... 28
  ShareFile StorageZones .................................................. 28
XenMobile Client ............................................................ 29
  Device Security ............................................................ 29
App Security .................................................................... 30
  MDX Container .............................................................. 30
  Partners Container Solutions ........................................... 32
  Productivity Apps .......................................................... 32
Network Security ............................................................ 34
Summary ........................................................................ 35
About the Authors and Contributors .................................. 35
Introduction

Enterprises are moving to Citrix Workspace to support their digital transformation efforts to utilize its breadth of services in a consolidated and secure environment. The Citrix Workspace simplifies the management of information systems by centralizing management while unifying applications, data and desktops into a digital workspace.

Enterprise are under attack and protecting their digital workspace is an essential requirement. Citrix has been helping the largest companies in the world secure their apps and data for nearly three decades. Security is a fundamental part of all Citrix technology and a primary consideration in the solutions we deliver to our customers.

Citrix Workspace secures customer environments in four key ways:
• by centralizing and enclaving applications and data
• ensuring data is protected when shared or distributed
• controlling who has access to data and resources
• by bringing IT together for application and data-specific security.

XenMobile Service is the Unified Endpoint Management (UEM) component of Citrix Workspace based in Citrix Cloud that securely manages Enterprise apps and data on mobile endpoints. As enterprises continue to find benefits in and use cases for moving IT systems and workloads to the cloud there’s increasing focus on validating and verifying the security underpinning cloud services to ensure protection of critical data.
Cloud Benefits

Customers are moving to XenMobile Service to take advantage of many benefits of being hosted in the cloud including:

Efficiencies

- New features and bug fixes availability prior to on-premises version
- Common management dashboard alongside all Citrix Cloud services
- Easy and reliable access to the service anytime, anywhere

Time

- Assisted web-based on-boarding process can have the XenMobile service up and running in a matter of hours
- Refocus IT staff time on other projects with upgrades and many operational management tasks offloaded by Citrix Cloud Ops
- Peace of mind with 99.9% uptime SLA

Financial

- Reduced infrastructure to implement and maintain
- Predictable budget with elastic pay-as-you-go SaaS subscription (Opex vs. Capex)
- Reduced subscription cost when Workspace Services are packaged together

Cloud Security

XenMobile Service has built a large customer base some of which started their environments in the cloud. Others have moved to the cloud with the Citrix seamless XenMobile Migration Service which requires no reenrollment and is unique in the industry. XenMobile Service is designed to secure our customer’s mobility environments. Nevertheless, moving mission critical systems to the cloud is a significant change for many enterprises. They need to reevaluate the trust that they built up in their on-premises infrastructure, processes, and procedures over years of operations.

Citrix considers it paramount to detail the security behind XenMobile Service to ensure the continued trust we’ve developed with our customers over decades. In this white paper we will review the security landscape, give an overview of the components that comprise XenMobile Service, and discuss the elements of each component that collectively form its security framework to protect customer environments.
Security Concerns

There are many cost, operational, and functional benefits of moving to the cloud that vary by industry, yet irrespective of the vertical enterprises all need to ensure their apps and data are secure. A few areas of primary concern that are top of mind for CIOs often come up in studies, surveys and customer conversations:

1. **Data Loss or Leakage** – they fear the potential dissemination, deletion, or corruption of their data by unauthorized parties while it is at rest or in transit.
   Some contemporary examples include ransomware holding valuable intellectual property hostage; a man-in-the-middle breach eavesdropping on the transfer of personal data in violation of the General Data Protection Regulation (GDPR); or illegal transfer of sensitive data out of country borders in violation of the Federal Information Security Management Act (FISMA).
   You will learn how XenMobile Service architecture, design, controls, host environment, operational roles, polices, and procedures collectively mitigate the risk of data loss or leakage.

2. **Availability** – backup failure, data storage corruption, data center failure, admin error, or natural disasters can all cause outages and costly downtime.
   You will discover how cloud-based XenMobile Service elements like appliance clustering, NetScaler high availability, and a host of resource availability features ensure high uptime backed by robust SLAs.
   You will also learn how an experienced operations team, thoroughly vetted by Citrix, manage XenMobile Service in the cloud.

3. **Identity** – as the use of mobile endpoints and cloud hosted services grow enterprises have been challenged to find a ubiquitous identify solution to keep pace. Single factor domain authentication is unacceptable, beyond the sanctity of the corporate network, on unknown networks with uncertain security threats.
   Citrix Identity Platform coupled with Microsoft Azure Active Directory (AAD) provide powerful, flexible identity options, and are the basis for enrollment, authentication, and identity administration for XenMobile Service.

Through the course of detailing the security foundation of the XenMobile Service we will uncover how it addresses these concerns and more. Security conscious Enterprise decision makers will see how they may meet their UEM needs and trust their apps and data with XenMobile Service.
Overview

The goal of this white paper is to detail the key security elements of XenMobile Service for security practitioners to reference when evaluating, migrating to, or utilizing it as their UEM provider. XenMobile Service is an aggregate of several components that together provide flexibility, user experience and security to manage any endpoint, anytime, and anywhere. We will describe the secure elements of each component in subsequent sections of the document.

- **XenMobile Service** – is the XenMobile engine to provide Unified Endpoint Management of XenMobile Clients in the cloud.
- **Citrix Cloud** - Citrix Cloud is the hub that orchestrates access to and interaction between essential elements.
- **Cloud Platform Provider (CPP)** – We host our services primarily in Microsoft Azure, although we also use and support other cloud vendors, such as Amazon Web Service (AWS).
- **Resource Location(s)** – is the location(s) with the customer domain Active Directory presence, resources like SharePoint sites and backend databases.
- **XenMobile Client** – is the mobile endpoint that is managed by XenMobile.
XenMobile Service

XenMobile Service is the hub responsible for coordinating mobility management functions with the XenMobile Client including enrollment, authentication, and delivery of apps, data, and UEM policies.

Architecture

The XenMobile Service facilitates all the UEM activities for managed mobile endpoints. It relies on the Citrix Cloud environment, utilizes CPP functionality, and works in conjunction with customer Resource Locations(s) along with on-premises NetScaler Gateway(s).

The service requires a limited set of inbound ports, yet accesses a variety of outbound ports to utilize standard mobile services. Each XenMobile Service customer uses dedicated public IP addresses, protected by a firewall for ingress traffic with restricted security groups which allow required service ports only.

Customer devices enroll over HTTPS on a specific URL assigned to the front-end instance. Only two Internet-accessible IP ports are required for device enrollment and ongoing mobile device communication with the XenMobile Service. (TCP 443, 8443), while TCP port 4443 is used for administration.

For more information on ports utilized by XenMobile Service see port requirements.
Environmental Security

XenMobile Service environment security is composed of a variety of layers, processes, and procedures including Logical security, Access controls, Data access controls, Network access controls, Operating system access controls, Change control and business continuity, and Personnel security.

Logical Security

System security is governed by a comprehensive policy maintained by the Director of Cloud Security Operations. It is reviewed bi-annually by leadership. XenMobile Service infrastructure is monitored on a 24/7 basis with support available on a 24/7/365 basis. Currently, support level response for all service-related requests is within 24 hours. In the event of a security incident the Cloud Operations Team notifies the Director of Incident Management (DIM) who in turn directs the Cloud Operations Team response.

Citrix has internal processes for code review and patching systems for known security vulnerabilities as they are identified. All scheduled maintenance activities, including deploying service patches to the XenMobile Service production infrastructure, are communicated to customers.
Access controls

A limited set of authorized personnel, with a need to know, have access to these business-critical production systems. If additional access is required for a specific situation, approval by the operations director must be obtained, and it is granted on a temporary basis.

Access requires individual accounts and authentication keys that would only be distributed to a limited number of operations personnel who require access for support responsibilities. All system passwords are hashed. Policies are in place to remove access for user IDs that are no longer valid. A formal audit is conducted periodically.

All systems related to the XenMobile Service are classified as business critical. Database systems that store customer data records are further secured in a different network security zone, e.g., isolated internal network, separated by a firewall and with a limited amount of application and personnel access.

Data access controls

All customer data is viewed as business critical and access is limited to authorized personnel who have a need to know or must access this information as part of a support role. No customer financial information is stored in XenMobile Service business-critical systems and all customer payment information is processed out of band.

Workstations are secured with two factor authentication. All employees must sign confidentiality agreements that require protection of customer data. XenMobile Service customer data will be maintained for the duration of the service contract. All customer detail data is transmitted via secure, encrypted channels.

Network access controls

Firewall filtering occurs at the Internet routing layer and the web, application and database layers. Firewalls are configured in a default deny-all mode; only the ports necessary to run the XenMobile Service are open. Firewall configurations are relatively static after the initial implementation. These configurations are audited on a periodic basis.

Customer data and system related administration information that traverses the Internet is protected in a HTTPS or SSH connection, both of which are secure channels. Access to systems is currently documented in the system access logs, which are only available to operational personnel.
Operating system access controls

All XenMobile Service production systems are built with the Citrix provided image with any default accounts removed. All XenMobile Service systems are built with operating system images that allow only ports specifically required for the service application to operate properly.

The Cloud Operations team is responsible for ensuring that all XenMobile Service systems are updated with the appropriate security patches. These patches are applied on a periodic basis once their criticality and XenMobile Service exposure is evaluated. XenMobile Service application software has code reviewed internally with all design changes reviewed and approved by appropriate leadership.

All user level sessions to the XenMobile Service application through the XenMobile Service management console have a timeout value with session expiration. All user access activity is logged, including failed attempts. Accounts are locked after a specified number of failed attempts. User accounts are removed upon termination of the account. In addition, a periodic review the status of all production accounts is completed from an auditing perspective.

Change control and business continuity

Data is redundantly stored in multiple physical locations as part of normal operation of XenMobile Service production services. In case of failure, automated processes move customer data traffic away from the affected area. Disaster recovery for customer data stored within the XenMobile Service database is provided by cross-region replication and backup. XenMobile Services are deployed in an N+1 configuration, such that in the event of a datacenter failure, there will be sufficient capacity to enable traffic to be load balanced to the remaining datacenter locations. Citrix performs monthly Disaster Recovery drills for all our cloud hosted services.

All equipment used for the XenMobile Service is in accordance with Citrix recommended specifications. Currently, no XenMobile Service hardware or software is scheduled for EOL or EOS. The XenMobile Service operations director is responsible for incident response for any service related outages and incidents. Incident response processes are documented and distributed to all personnel that may be involved and impacted by these situations.

Patches are currently deployed on an as needed basis based on the criticality of the vulnerability and exposure to the XenMobile Service. All service upgrades to the XenMobile Service live environment are first implemented in a pre-production test environment. All changes to the production environment are made under the review of the operations director and are logged. All changes to the XenMobile Service production systems are recorded in an update tracking tool, including the success/failure of updates.
Citrix follows coding best practices, including performing internal code reviews which are conducted for all XenMobile Service production releases as part of the development process. A formal testing release process is followed to ensure that no untested or unauthorized code is released to the XenMobile Service production infrastructure. A combination of internal employee test accounts/devices and system generated “test” data is used to test all releases on the pre-production network prior to rollout to the XenMobile Service production environment.

**Personnel security**

Comprehensive background checks of employees are conducted prior to hiring. All employees sign a confidentiality or non-disclosure agreement as part of their terms and conditions of employment. Contractors are required to undergo the same level of background checks as Citrix employees, either from their staffing agency or as part of the standard hiring process.

All XenMobile Service datacenters have physical and personnel access controls over the removal of any data from the XenMobile Service environment. When contracting with vendors that process or retain sensitive data, Citrix requires that provisions for protection of personal and confidential information be specified in the contract language. Vendors are required to agree with the Citrix Technical and Organizational Security Measures, or materially similar terms.

As part of the new hire orientation process where systems access is granted and accounts are enabled, the Citrix IT organization provides training on security access and guidelines for all Citrix employees. Security awareness training applies to all business-critical information and customer data regardless of whether it is on site at a Citrix location or off site. Citrix has a culture of open communication where employees are encouraged to raise issues to senior management without the need to go directly through their manager.

All Citrix employees are expected to protect sensitive company materials. All parties who access XenMobile Service business critical data are subject to confidentiality agreements and company security policies. Access controls and audit logging are employed for XenMobile Service production systems to ensure compliance. Citrix employees have signed a confidentiality employment agreement that specifies disciplinary measures, including termination, if employees fail to adhere to the conditions of the agreement.

An employee’s direct manager is responsible for collecting all company assets when the person leaves the company. A notification process alerts appropriate Human Resources and Information Technology staff to ensure that all relevant system account access is rescinded and data is removed from the collected equipment before being reused. All Citrix employees are required to sign an acknowledgement that they understand and agree to comply with company policies regarding protection of company data and other responsibilities of being a Citrix employee.
Compliance

Citrix Cloud Platform Providers Azure and AWS have a variety of compliance certifications.

For more information see:
Azure Compliance Offerings
AWS Compliance Programs

Data Encryption

XenMobile Service utilizes a variety of methods to ensure data is encrypted at rest and in transit.

XenMobile Service - Data Encryption

<table>
<thead>
<tr>
<th>Data</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data at rest – iOS device</td>
<td>• AES 256 bit encryption</td>
</tr>
<tr>
<td>Data at rest – Android device</td>
<td>• AES 256 bit encryption</td>
</tr>
<tr>
<td>Data at rest - Cloud</td>
<td>• Data in the database is encrypted using Transparent Data Encryption.</td>
</tr>
<tr>
<td></td>
<td>• Dedicated instance model prevents accidental co-mingling of customer data</td>
</tr>
<tr>
<td></td>
<td>• Strict firewall rules protect data in our cloud</td>
</tr>
<tr>
<td></td>
<td>• Role-based access controls (RBAC) are in place to ensure the security principle of “least-privilege” for access to production environments.</td>
</tr>
<tr>
<td></td>
<td>• Passwords and other sensitive data in the DB are further encrypted.</td>
</tr>
<tr>
<td>Data in transit</td>
<td>• Access to Citrix Cloud (Policy and Traffic flows): TLS</td>
</tr>
<tr>
<td></td>
<td>• Access to Enterprise systems:</td>
</tr>
<tr>
<td></td>
<td>• Data access over TLS 1.1+ via NS Gateway (micro VPN)</td>
</tr>
<tr>
<td></td>
<td>• AD/PKI access over TLS 1.1+ via Cloud Connector</td>
</tr>
</tbody>
</table>

Diagram 5: XenMobile Service Data Encryption

Physical Security

Customer instances are provisioned in the datacenter location of their preference, typically the one closest to the majority of users. Customer data never leaves the region where it was provisioned which may consist of multiple data centers integrated for high availability. (e.g. data for customer instances provisioned in the United States would never leave the US).

Each XenMobile Service customer database is isolated to prevent cross-customer communication with other tenants. Citrix CPP’s have access controls that limit physical access to XenMobile Service servers and have procedures to limit access to authorized personnel.

Citrix leverages CPP shared responsibility models and rely on their Physical Security policies. Physical access to Citrix CPP data centers is strictly controlled and authorized staff must be authenticated to access data center floors.

For more information see:
Azure data center’s physical security
AWS data center’s physical security
**UEM**

Unified Endpoint Management is the core functionality provided by XenMobile Service. It securely manages apps, data, and endpoints. It has broad platform support including iOS, Android, Windows 10, macOS, all Android Enterprise modes, Chrome Enterprise, tvOS, Citrix's Workspace Hub and others. For more information see the [XenMobile Platform Matrix](#).

For more information on the overall UEM functionality it provides including Mobile Device Management (MDM), Mobile App Management (MAM), Mobile Content Management (MCM), and Client Management Tool (CMT) functionality see [XenMobile UEM](#).

Some of the essential aspects of securely managing endpoints that it provides include enrollment, authentication, and client management.

**Enrollment**

Enrollment is the first phase of mobility management that identifies a user’s authorization to have their device managed, and it maps a user’s identity to their device which is essential to all other endpoint management activity. XenMobile supports several ways for users to assert their identity and obtain authorization to enroll a device such as through direct domain authentication, or through a one-time enrollment code, per user, distributed by email or other means to name a couple.

During enrollment, a device certificate is installed on the user’s device, using a certificate signing request (CSR) that is generated uniquely for that device. How the certificate is generated and delivered varies by platform. A built-in XenMobile Service certificate authority (CA) generates the device certificate. Certificates issued by the built-in CA use RSA 2048-bit keys and SHA-256. Once a device is enrolled, future management communication between the device and XenMobile Service is conducted over mutually authenticated Transport Layer Security (TLS) connections, using the device certificate for client authentication.

During device enrollment, XenMobile Service creates an internal binding between the user identity obtained through an LDAP query to the domain, via Cloud Connector (see the Citrix Cloud section for more information) and the device identity in the certificate that was installed on the device as part of the enrollment. Once enrolled apps and device security settings may be “pushed” to the device (e.g. using APNS for iOS), or apps may be made available within the XenMobile Store, for users to manually subscribe to and install.

For more information see [Enrollment Modes](#).
Authentication

The XenMobile Client initiates authentication with the XenMobile Service to validate the user context where authorized apps and policies need to be presented. XenMobile Service supports several single and multi-factor authentication options (depending on the platform).

- **Domain(LDAP)** - you can configure a connection in XenMobile to one or more directories, such as Active Directory that are compliant with the Lightweight Directory Access Protocol (LDAP). This is a commonly used method to provide single sign-on (SSO). It supports Citrix PIN (a numeric passcode configurable as part of Client Properties settings) with Active Directory password caching while still providing the security of complex passwords on enrollment, password expiration, and account lockout.

- **Client Certificate** – XenMobile Service can deliver a client certificate to a device for use in authentication. XenMobile Service is aware of the user identity from the binding done initially during enrollment and uses this information to interact with the configured enterprise Public key infrastructure (PKI) entity to generate the user certificate.

- **Domain(LDAP) + Client Certificate** - this configuration offers the best combination of security and user experience, with the best SSO possibilities coupled with security provided by two-factor authentication via NetScaler.

- **Domain(LDAP) + Token** – XenMobile Service also supports requiring users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol in conjunction with NetScaler.

- **Azure Active Directory** – configuring AAD as your identity provider (IDP) lets users enroll in XenMobile using their Azure credentials.

- **Derived Credentials** - Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card.

For more information see XenMobile Service Authentication, Certificates, Domain Authentication, Client Certificate Authentication, AAD as IDP, and Derived Credentials.
Client Management
XenMobile Service plays a central role in managing the client and securing it throughout its managed lifecycle. It can report on device and app activity and take a variety of actions as needed to secure them operationally.

Reporting
XenMobile Service includes several reports to help monitor security events and analyze trends.

- **Inactive Devices** - includes a list of devices that have not had any activity for a configurable number of days
- **Jailbroken/Rooted Devices** - lists jailbroken iOS devices and rooted Android devices
- **Terms & Conditions** - lists users who have accepted and declined Terms and Conditions agreements
- **Top 10 Apps: Failed Deployment** - lists top 10 apps by failed deployment
- **Blacklisted Apps by Device & User** - lists users with blacklisted apps on their devices

Device Management
XenMobile can initiate several security actions through the admin console, by automated actions such as based on user’s state in the domain, or by the user himself or herself via the self-help portal.

- **Lock (/Unlock)** - locks the device (provided a device passcode has been set).
- **Selective Wipe** - unenrolls the device and removes enrollment settings on the client.
- **Revoke** – similar outcome to selective wipe, yet additionally requires the XM admin to reauthorize it before it can reenroll.
- **Full Wipe** – MDM level command, that wipes enterprise information off the device while doing a factor reset on the device.
- **Locate** – on supported platforms reports the last known device GPS coordinates.
- **App Wipe** – removes MDX app (occurs on app checking / use).
- **App Lock** - locks MDX app (occurs on app checking / use).
Citrix Cloud

Citrix Cloud is a cloud management platform that allows organizations to provide workspaces to end users through a single management plane that delivers unified and reliable access to apps and data. It is the backbone that unifies the management of Citrix cloud services like XenMobile Service.
Services

It combines a breath of Citrix Workspace services all managed through a common console, that share common secured enterprise communication paths, and are accessible behind a unified Citrix Identity solution. Key services include:

- **XenMobile Service** – (as discussed in more detail in this white paper) provides Unified Endpoint Management including comprehensive enterprise mobility management (EMM), mobile device management (MDM), mobile application management (MAM), and enterprise-grade productivity apps on BYO or corporate devices.

- **XenApp and XenDesktop Service** – Deliver secure access to virtual Windows, Linux, and web apps and desktops. Manage apps and desktops centrally across multiple resource locations while maintaining a great end user experience.

- **Smart Tools** – The easy on-ramp to Citrix Cloud services, Smart Tools works with both Citrix perpetual licenses and other Citrix subscription services; in the cloud or on-premises. A collection of easily consumable services empowers Citrix Administrators to easily optimize Citrix sites by proactively checking the health of running systems and keeping costs under control with on-demand scaling.

- **XenApp Secure Browser** – Protects enterprises from browser-based attacks by isolating browsing from the enterprise network.Delivers secure remote access to web applications from the cloud with zero endpoint configuration.

- **App Layering** – Packages any Windows app as a portable virtual disk with a normal install and delivers it anywhere without further installations. It may be updated, combined with other layers, rolled back, or retired just as easily.


- **XenDesktop Essentials** – Accelerates Windows 10 Enterprise migration with the power of XenDesktop and Microsoft Azure. Purchased on the Azure Marketplace.

- **ShareFile Service** – Provides secure access to files and data from any device, across any infrastructure. Controls how and where you store your data while meeting mobility and collaboration needs of employees and the data security requirements of the enterprise.

- **NetScaler Gateway Service** – Utilizes the most secure ways to deliver virtual apps and desktops with a cloud-based offering that is simple to deploy and manage. Ensures the availability of Citrix Cloud services and provides the best user experience on any device, under any network condition.
• **NetScaler Web App Security Service** – Protects web applications and infrastructure from cyber-attacks using security tools like signatures, blacklisted and whitelisted URLs/applications, and IP Reputation. Keeps historical retention capabilities for easy operations and incident analysis.

• **NetScaler Management and Analytics Service** – Gains end-to-end visibility and control of application infrastructure across multiple clouds. Using application and network data, provides view summaries and detailed analytics to allow for faster troubleshooting, proactive performance management, and security-threat management.

**Benefits**

Citrix manages the control plane in the cloud which provides several benefits. This helps provide a consistent user experience through a single, unified console/login, with all Workspace services integrated into a common launch point. It also carries the benefit of automatic updates whereby all updates including functionality, security patches, or otherwise are implemented in a timely manner seamlessly by operations staff.

Customers also benefit from the flexibility of being able to store their data such as intellectual property and personal data according to their business and security requirements wherever they need it. This includes the advantages of better security, compliance, and data sovereignty.
Cloud Connector

Cloud Connector provides connectivity between the cloud and the customer’s resource location. It’s designed to operate within your company’s current security restrictions. It does not operate as a VPN, rather all connections are egress (port 443 only). It requires access to a limited set of domain names, used by XenMobile Service, to be reachable outbound to function properly. For more information see Internet Connectivity Requirements.

It is a collection of purpose built micro provider services hosted on a Windows Server(s). Two used by XenMobile Service include:

- **AD Provider** - used for discovering Active Directory (AD) domains that the Cloud Connector host trusts and for performing specific queries to AD (enumerate users, groups, search for group memberships, authenticate users etc.).

- **Web Relay** - enables integration of enterprise web-services (PKI server or StoreFront) with XenMobile Service.

It’s invoked by API calls to Citrix Cloud secured by a service key. The key is per-connector and limited to customer scope. Key rotation is done on a periodic basis by Citrix, but can also be updated by Cloud Operations by request for example if there was a change in key customer personnel.

It supports High Availability and it is recommended to install 2+ per resource location.
Cloud Connector is evergreen and updates automatically ensuring all updates, especially any security related ones are implemented rapidly and seamlessly, with no downtime and no customer intervention. Updates are implemented to customer using a “canary” approach which statistically mitigates the risk of any anomalies being deployed. Also, connector instances are updated one at a time and additional upgrades are halted if a connector verification fails after upgrade. This virtually eliminates the possibility of Cloud Connector related downtime and reinforces the fact that Citrix Cloud and XenMobile Service are designed to ensure availability.

Diagram 10: Resource Locations

Diagram 11: Cloud Connector Canary Process
Cloud Platform Provider

Citrix relies on our CPP shared responsibility models for hosting aspects such as physical security, yet there are certain platform logical security features utilized by Citrix to enhance overall protection. Amazon Web Services (AWS) has been a reliable secure Citrix Platform Provider for XenMobile Service several years. We also host our services in Microsoft Azure and is currently the default location for new customers. Microsoft Azure, and its security related features utilized by XenMobile Service, will be the focus of the CPP section.

Microsoft Azure

Microsoft Azure has a comprehensive approach to protect cloud infrastructure needed to run hyper-scale global services. Microsoft cloud infrastructure includes hardware, software, networks, and administrative and operations staff, in addition to the physical data centers.

Before Internet traffic can get to the Azure virtual networks, there are two layers of security inherent to the Azure platform which all Azure hosted services benefit from:

1. DDoS protection is a layer of the Azure physical network that protects the Azure platform itself from large-scale Internet-based attacks.
2. The Public IP addresses are configurable to determine which traffic is passed in, and how and where it's translated on to the virtual network.
Beyond those layers services may incorporate additional layers of protection:

3. Virtual Network Isolation – applies boundaries to traffic through virtual networks and prevents unwanted communication with resources.

4. Network Security Groups (NSG) and User Defined Routing (UDR) – implement access control lists (ACLs) to limit hosted based access, and control communication paths by defining custom routing tables, respectively.

5. Network Virtual Appliances - firewalls, load balancers, and IDS/IPSes available on the Azure Marketplace may be implemented at virtual network security boundaries.

For more information see Microsoft cloud services and network security, and Azure security overview.

**Azure Transparent Data Encryption**

The Azure SQL data at rest is encrypted using Azure SQL Database Transparent Data Encryption (TDE). It performs real-time encryption and decryption of the database activity including backups, and transaction log files. The entire database is encrypted using a symmetric key. We further encrypt sensitive data using secret keys generated on the XenMobile Service.

For more information see Transparent data encryption for SQL Database and Data Warehouse.
Azure Security Center

Azure Security Center uses Microsoft's real-time intelligence to protect deployments from internal or external threats. It provides support for configuring and deploying security policies, through the Azure console, for resources and automates threat detection through machine learning.

For more information see What is Azure Security Center.

Azure Active Directory (AAD)

Azure Active Directory (Azure AD) is Microsoft’s multi-tenant, cloud based directory and identity management service. It includes directory services, advanced identity governance, and application access management. It also includes the ability to create and manage access control policies.

For more information see What is Azure Active Directory.

Network Security Groups

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). They can be attached to subnets, or network interfaces (NIC). The former applies to all VMs on the subnet, while the later pertains to one specific VM.

For more information see Filter network traffic with network security groups.
Availability Sets

Availability sets ensure that the VMs deployed on Azure are distributed across multiple isolated hardware nodes in a cluster which ensures that if a hardware or software fails, only a sub-set of VMs are impacted, and that the overall solution remains available and operational.

For more information see Availability Sets.

Physical Security

Windows Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24 x 7 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These data centers comply with industry standards for physical security and reliability and they are managed, monitored, and administered by Microsoft operations personnel.

For more information see Microsoft Cloud Platform.

Azure Portal

Azure Portal gives access to the user interface to managed Azure environments. While it provides a rich set of capabilities with multiple access and management capabilities this flexibility can add significant risk to a cloud deployment. Use of secure dedicated workstations for developing and managing infrastructure is Mandatory to avoid introducing unpredictable threat vectors such as web browsing (for example, watering hole attacks) or email (for example, social engineering and phishing).

For more information see Microsoft Azure portal.

Azure Activity Logs

Azure Activity Logs are subscription logs that provides insight into subscription-level events that have occurred in Azure. They include information such as Azure Resource Manager operational data to updates on Service Health events. The XenMobile Service Operations team utilizes these logs for monitoring and analysis, such as to follow an audit trail for non-automated actions.

For more information see Monitor Subscription Activity with the Azure Activity Log.
Amazon Web Services
To obtain more information on the AWS Cloud Platform see https://aws.amazon.com/

Resource Locations

Resource Locations contain the resources required to deliver services to subscribers. They utilize NetScaler Gateway to access resources such as ShareFile StorageZones, Exchange, Intranet Web sites, or SharePoint sites. For XenMobile Service the Resource Location(s) may be hosted in flexible locations. XenMobile Service embraces Hybrid cloud by supporting apps and data, based in Resource Locations, hosted in either public or private clouds.
Domain Controllers
The Microsoft Active Directory domain is a key on-premises resource. It is integrated with Citrix Cloud by Cloud Connector servers. Any LDAP queries to look up domain objects and attributes happen securely over the connectors. During the first-time use configuration, the domain entry is automatically populated as part of the XenMobile Service LDAP configuration.

NetScaler Gateway
NetScaler Gateway is the Citrix scalable solution to securely provide remote access and manage delivery of apps and data. It is a market leading gateway and includes a variety of features to secure Citrix customer environments such as multi-factor authentication, DDOS protection, access control, and traffic monitoring.

It is utilized both in the XenMobile Service and in customer Resource Locations. The former handles control traffic, while the latter handles data traffic and is the basis for establishment of proprietary per-app VPN sessions called “micro-VPNs” used by apps integrated with the XenMobile SDK.

For more information see NetScaler Gateway Product Documentation.

Micro-VPN
Micro-VPN brings the remote access capabilities of Citrix NetScaler Gateway to mobile devices via apps integrated with the XenMobile SDK. It is an on-demand application VPN connection that is initiated by Secure Hub on mobile devices to access corporate network sites or resources.

Secure Hub is launchpad for the Citrix XenMobile experience on iOS and Android devices (while others rely on OS functions) During the enrollment process, upon successful user authentication, NetScaler creates a Micro-VPN session and Secure Hub fetches the client-side configuration settings for the session, including split DNS, split tunnel, and the internal network IP address ranges that should be tunneled.

Micro-VPN is now also integrated with the Intune SDK and the Intune Managed Browser For more information see XenMobile Integration with Microsoft EMS/Intune.
Data

Exchange
On-premises Exchange that provides email, personal information management and messaging services to users may be securely proxied by NetScaler. It securely provides access to those services by managing traffic flow to components, depending on the version, such as Exchange 2016 Edge Transport, and Mailbox Server including the mail database, and Client Access roles. Citrix Secure Mail is an enterprise mobile email solution which in turn uses micro-VPN to transport ActiveSync session to synchronize data with Exchange mailboxes. (Find more regarding Secure Mail in the XenMobile Client section)

For more information regarding how to secure and scale Exchange with NetScaler see Deploying NetScaler with Microsoft Exchange 2016.

Intranet Web Sites
Intranet web sites hosted in Resource Locations such as company Html sites, or SharePoint sites may be accessed securely and seamlessly using the XenMobile managed browser Secure Web and micro-VPN (Find more regarding Secure Web in the XenMobile Client section). Depending on the platform full or per-app VPN tunnels using OS functionality or dedicated clients like Citrix VPN may also be configured by XenMobile Service and provide full access to those internal corporate web sites, behind the DMZ/(s).

ShareFile StorageZones
ShareFile Enterprise is a Citrix cloud-based content collaboration platform that allows users to easily collaborate and exchange documents securely. The ShareFile StorageZone, which securely stores enterprise files, may be hosted as a customer-managed StorageZone in the resource location of choice; on-premises; in a customer-managed cloud location; or in a ShareFile cloud-based StorageZone.

StorageZones Connectors to existing on-premises repositories such as network file shares, or SharePoint Server stores can integrate with XenMobile Service and operate without the management plane, with reduced functionality (e.g. no sharing). In this configuration the MDX ShareFile app authenticates through Secure Hub and the NetScaler Gateway with the ShareFile StorageZone Controller using Kerberos or NTLM, after which the StorageZone Controller authenticates to the repository using AD impersonation for the user.

For more information see ShareFile use with XenMobile, and the ShareFile Enterprise Security White Paper.
XenMobile Client communicates directly with both the XenMobile Service and Resource Location. The former manages the endpoint with activities including enrollment, coordinating authentication, pushing policies, populating the store with available apps, and pushing apps for installation. Once installed, apps access Resource Locations to obtain client data such as to obtain email from on-premises Exchange, surf web data on intranet SharePoint sites, or load files from ShareFile on-premises StorageZones.

**Device Security**

**Mobile Threat Defense (MTD)**

Gartner defines the Mobile Threat Defense solutions market as products that protect organizations from threats on mobile platforms, including iOS, Android and Windows 10 at one or more levels: “Device behavioral anomalies, Vulnerability assessments, Network security, or App scans.” - *Gartner*

XenMobile integrates with many of the leading MTD solution providers including Symantec, Wandera, and Checkpoint. Based on input from MTD solutions XenMobile can set device compliance and act on *Automated Actions* defined according to security policies.

**Jailbreak detection**

XenMobile has a proprietary mechanism to detect whether a device has been jailbroken, making it susceptible to vulnerabilities. It verifies its status during enrollment and at regular intervals throughout the device management lifecycle. Upon detection a variety of actions may be initiated such as notifying an admin, blocking apps, selective wipe, etc.
OS Update
When vulnerabilities are identified in platforms OS vendors develop patches to fix them. Verifying the viability of those updates and applying them is a critical step to ensuring endpoint security. XenMobile administrators have the ability to control OS updates for most platforms that support it. Some allow deployment from private servers, others via the cloud, and most have many other features to schedule and verify updates are applied.

Device Policy
XenMobile Service integrates with broad platform MDM interfaces to enable and configure security features through device policy. It can configure host firewalls, enable malware protection provided by the OS, require encryption, or restrict feature use such as network protocols, peripherals, or the use of apps or data in an unsecure manner.
For more information see Device Policies.

App Security
MDX Container
MDX is a Citrix app container technology that enhances the mobile endpoint experience and supports secure deployment and management of apps with XenMobile policies and settings. MDX includes micro-VPN technology.

If a MDX app needs to access the network, and the MDX policy is configured to tunnel network traffic via the Resource Location’s NetScaler Gateway, then the MDX framework checks to see if a NetScaler Gateway micro-VPN session cookie is cached. If not, the MDX app prompts Secure Hub to initiate NetScaler Gateway login and then return control to the MDX app.

Apps enabled with MDX technology include over 70 policies to manage and secure the app and data it processes. Key app protection polices areas include:

- **Authentication** – such as requiring an app passcode, or specifying an alternative NetScaler Gateway to enforce multi-factor authentication.
- **Access** – such as timers that specific the length of time an authentication token is valid.
- **Encryption** – such as requiring device database and keychain encryption (iOS only).
- **App Interaction** – control copy and paste, open-in, or allowed URLs.
- **App Restrictions** – allow or block device functions like camera, microphone, or location services.
- **App Network Access** – specifying micro-VPN, per-app VPN use, or require http proxy server and include settings.
• **App Logs** – specify level of detail, and parameters like how long to store each

• **App Geofencing** – specify restricted use coordinates.

• **Secure Mail** – includes a variety of Secure Mail settings such as mail server, ability to export contacts, or email marking classifications.

• **Secure Web** – also includes a variety of settings such as allowed or blocked URLs, preloaded bookmarks, or URL whitelists.

For more information see [MDX Policies at a glance](#).

**MDX Timers**

MDX policies control the authentication experience of the individual app. Each application can have the following settings:

• **Reauthentication timer** – Dictates how frequently the user needs to authenticate to continue using the app. If the current time less the time of the last successful authentication exceeds the admin specified value, then an appropriate authentication prompt is displayed by switching to Secure Hub. Timer checks occur when the app is started, or brought to the foreground (typically by user action).

• **Authentication type** – The authentication prompt is controlled by the type of authentication configured. Offline only prompts for Secure PIN or AD password, according to configuration. The PIN or password is validated against a salted password hash value stored on the device. (This is updated upon each successful network authentication when AD password is used for offline authentication.) The password hash function is based on PBKDF2 (RFC 2898) using HMAC SHA-256 with iterations and a strong random salt input.

• **Offline period** – This setting controls how long the app can continue to operate offline, without a network authentication to NetScaler Gateway. For an application such as Secure Mail this setting allows the user to continue to interact with the app (i.e.: read and compose mails) even when network access is not available. At the end of this offline lease period, the app enters the lock state and will not be accessible to the user until network authentication to NetScaler Gateway and MDX policy refresh from XenMobile Service has occurred.
Partners Container Solutions
In addition to MDX XenMobile integrates with several partner App Container solutions.

Samsung Knox
Samsung Knox is a containerization framework that allows corporate apps and data to be securely isolated from personal apps and data. It uses hardware for encryption. XenMobile integrates with Samsung Knox to manage and deliver apps, data, and policies to the secure container. For more information on the capabilities XenMobile and Knox provide see Deliver secure mobile productivity with XenMobile KNOX Edition for MDM.

Android Enterprise
With Android Enterprise Google has enabled the ability to install Work profiles using default encryption, with enhanced SELinux security enforcement and multi-user support. Android Enterprise makes provisions for a Device policy controller (DPO) to manage the work profile by apply restrictions, settings, and handle app delivery. As an approved DPO XenMobile Service, manages business policies and apps, via a secure private app store. For more information on the capabilities XenMobile and Android Enterprise provide see “Leading the move to an app-centric, mobile-first world”.

Microsoft EMS/Intune
The XenMobile Integration with Microsoft EMS/ Intune includes several capabilities. A couple key app security features include; XenMobile SDK and micro-VPN integrated with Intune SDK and supported natively in the Microsoft Intune Managed browser; and Intune App protection polices available in Citrix Secure Mail allowing secure data transfer between it, Office 365, and Intune enabled apps. For more information on the capabilities the XenMobile and Intune provide see “XenMobile Integration with Microsoft EMS/ Intune”.

Productivity Apps
Citrix-developed XenMobile Apps, like Secure Mail, Secure Web and ShareFile, support MDX and provide a suite of productivity and communication tools within the XenMobile Service environment that are secured by company policies.

Secure Mail
Citrix Secure Mail is a MDX enabled enterprise mobile email solution which in turn uses micro-VPN to transport ActiveSync session to synchronize data with Exchange mailboxes. It also includes a variety of Enterprise security features such as:
- **EMS/Intune & Office 365 App Protection** – secure data transfer with Office 365 and Intune enabled apps through XenMobile integration with EMS/Intune described above.

- **Microsoft IRM support** - support messages protected with Microsoft Information Rights Management (IRM), subject to the configured IRM policy.

- **Email security classifications** - enables users to specify security classifications and dissemination limiting markers (DLM) when sending emails.

- **S/MIME** - supports Secure/Multipurpose Internet Mail Extensions (S/MIME) enabling users to sign and encrypt messages for greater security.

- **XenMobile Mail Manager** – uses Exchange Active Sync (EAS) messaging protocol to control email access based on device compliance.

### Secure Web

Citrix Secure Web is an Enterprise grade browser that provides secure access to internet and intranet destinations according to IT policy. It includes many security features such as the ability to prohibit use (in MAM mode) if an attempt is made to run it on a jailbroken device. It can be configured to block sites known to propagate malware, or block the popups to prevent “drive by” variants of malware that “live” in browser sessions without infecting the OS. It can preload bookmarks and make the address bar read-only so users can only go to specific sites.

It also includes URL Whitelist/Blacklist that are invoked when users select links within the body of emails in Secure Mail to direct specific URLs to use Secure Web to use the mobile devices’ native browser depending on security requirement. That intranet traffic directed to Secure Web utilizes micro-VPN and it may be configured to directed to a web proxy to filter sites. It can also parse PAC file rules and send the proxy server information to NetScaler Gateway.

### ShareFile

ShareFile is a cloud based collaboration, and enterprise file sync and sharing service that lets users exchange information easily and securely. ShareFile gives users a variety of access options for Android and iOS platforms. It is fully integrated with XenMobile from provisioning and deployment to single sign-on and secure file sharing.

ShareFile includes a broad variety of features to secure data including information rights management (IRM), data leak protection (DLP), and several StorageZone options to securely host data on-premises as required.

For more information see [XenMobile Apps](#).
Network Security
Smart Access

Smart Access provides the ability to control access to HDX apps on managed endpoints. HDX apps, configured in XenApp and XenDesktop with Smart Access, may be denied the ability to launch on out-of-compliance devices which is set through automated actions configured by admins according to security policy. XenMobile communicates the status of the devices to StoreFront using a signed, encrypted tag. StoreFront then allows or denies access based on the access control policy of the app.

Network Access Control (NAC)

XenMobile includes the ability to limit per-app VPN access based on device compliance status for iOS endpoints. Working in conjunction with NetScaler, during the VPN setup process, a NetScaler authentication action consults XenMobile to determine status and subsequently permits or denies access. Device compliance status is set through automated actions configured by admins according to security policy.

Network Restrictions

XenMobile includes a variety of device and app layer network restrictions, depending on the platform, such as specifying the WiFi SSID a device must join and setting the access point security configuration parameters, blocking the use of the device as a personal hotspot, or configuring http proxy setting a device is required to use.
Summary
In this white paper we reviewed the security landscape, gave an overview of the components that comprise XenMobile Service, and discussed the elements of each component that collectively form its security framework and protect customer environments. It is critical to Citrix to continue to operate XenMobile Service with the highest level of security diligently to ensure the continued trust of our customers.

About the Authors and Contributors
Matthew Brooks is a Sr. Technical Marketing Manager

Special thanks to the reviewers of this Security Whitepaper:
Terry Duchastel is Sr. Principal SW Engineer
Ashish Gujarathi is a Distinguished Engineer
Tarkan Kocoglu is Sr. Director Technical Marketing
Florin Lazurca is a Sr. Technical Marketing Manager
Justin Maeder is a Product Manager
Amandeep Nagra is a Sr. Product Marketing Manager
Joey Peloquin is Director, Cloud SecOps, Information Security
Rob Sanders is Sr. Technical Marketing Manager
Martin Zugec is a Principal Technical Marketing Manager
Jiun Hong is a Product Marketing Specialist