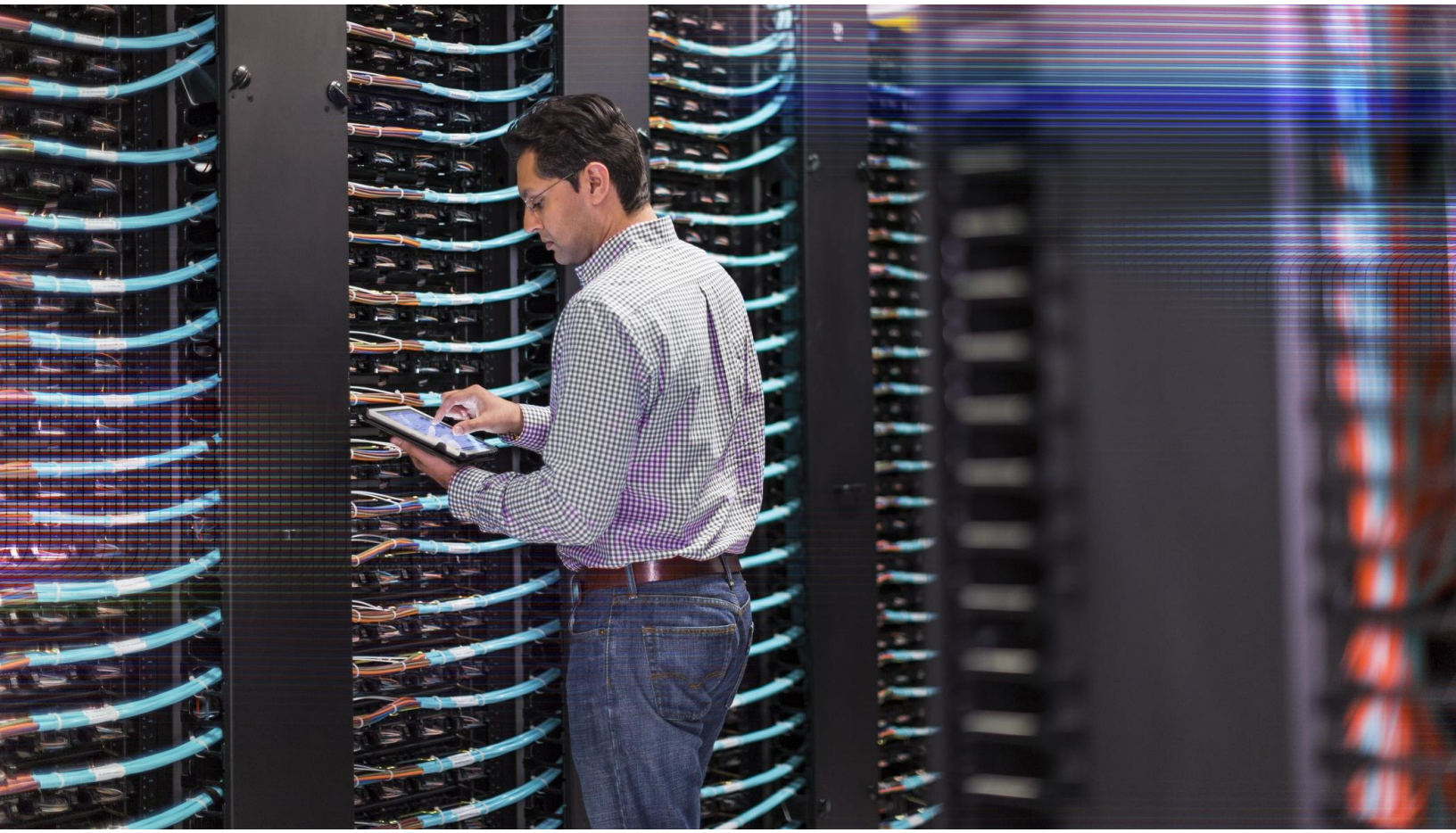


Getting Started with Citrix XenApp and XenDesktop Security

Security guidance for Citrix Deployments

This document is based on Citrix XenApp and XenDesktop 7.6 Long Term Service Release. However, the guidance and the principles are relevant to most releases. Where release-specific details are included, these are highlighted.

CITRIX®

Table of Contents

Last updated: 18 March 2016

Introduction

Citrix products offer a wide range of features and capabilities to help secure applications and data within Citrix XenApp and XenDesktop deployments. These features and capabilities are particularly important when deploying Citrix XenApp and XenDesktop in government, finance and health sector environments, where security is an essential consideration and often a regulated requirement.

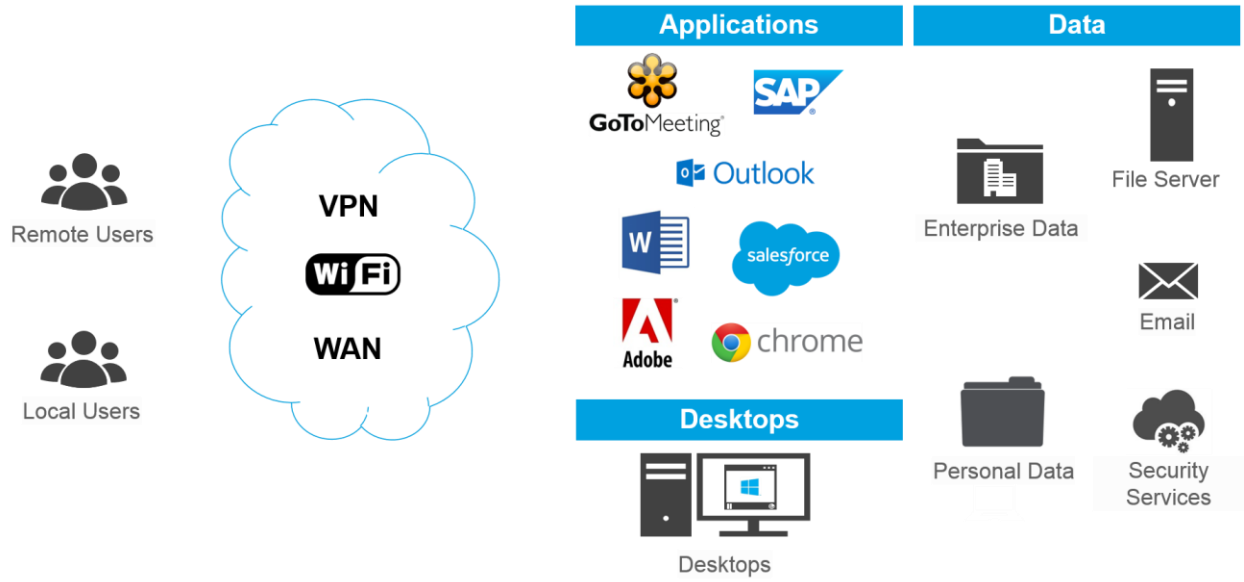
This document provides an overview and guidance regarding configuring Citrix environments to mitigate security threats and to comply with security standards.

Further documentation is available to support the guidance in this document, providing examples and use cases. See Finding more information. You can also consult your local Citrix representatives for advice regarding your deployments and updates.

Scope and use cases

Citrix offers solutions and associated licensing models for deployments managed and hosted by the customer (on the customer's premises), or deployments managed in the cloud. This document provides security guidance for solutions deployed on customer premises, rather than cloud deployments.

The primary use case for this document is a deployment that allows local and remote users to access published resources (desktops and applications) managed and hosted on the customer's premises.



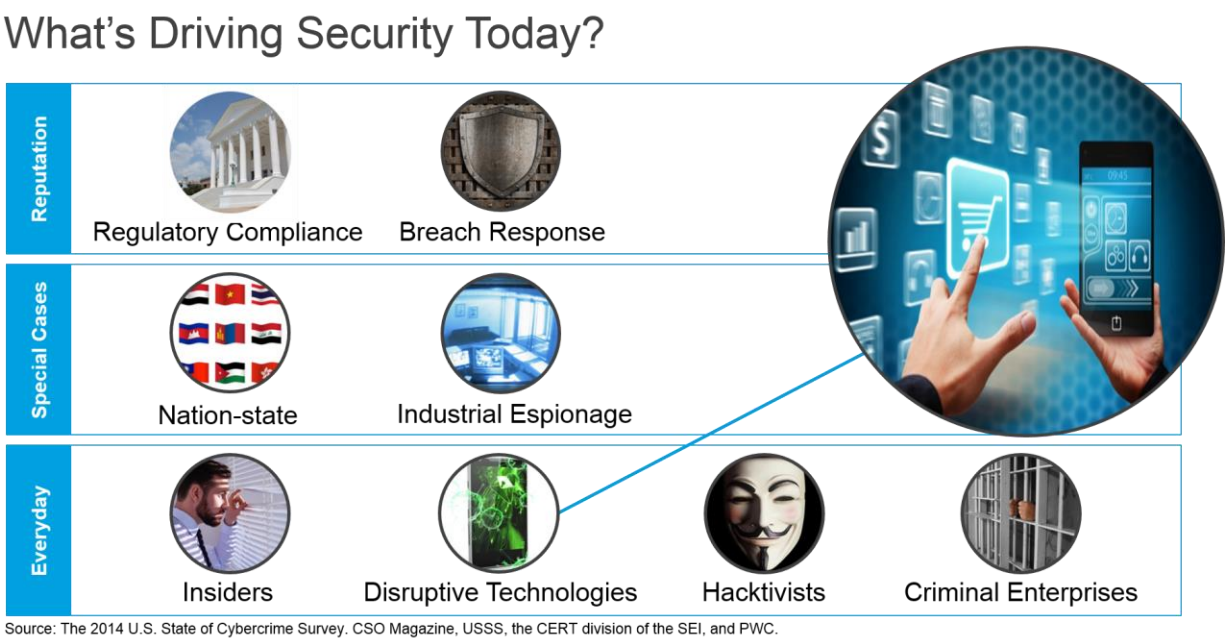
This document is based on XenApp and XenDesktop 7.6 Long Term Service Release. However, the guidance and the principles are relevant to most releases. Where release-specific details are included, these are highlighted. For more information regarding the Long Term Service Release, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6/xad-whats-new/long-term-service-release.html

Audience

This document is designed to meet the needs of security specialists, systems integrators and consultants responsible for designing, deploying and securing Citrix deployments.

Security challenges and trends

In recent years, there have been many high profile cases of security breaches and attacks. There is no sign of this relenting, endorsing the need to consider security at the design stage, to continuously monitor and respond to security threats and to adapt and harden the environment accordingly.



It is of course essential to protect sensitive data and intellectual property. Security is becoming more complex with the increase in remote working and a highly mobile workforce, including adoption of bring your own device (BOYD) work styles. The result is more unmanaged and/or unknown devices accessing resources.

Security complexity increases with the emergence and use of more types of devices (including mobile devices, tablets and internet-enabled devices) and additional network types (such as 3G/4G, Wi-Fi and Bluetooth).

Monitoring, identifying and responding to security breaches is a significant challenge and essential to ensure business continuity and security of resources.

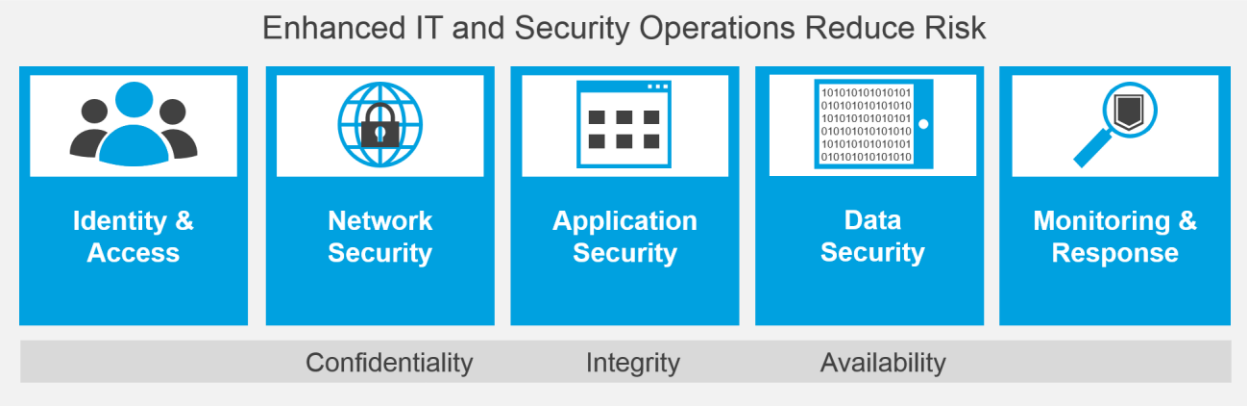
Additionally, many sectors insist on certain accreditation or security compliance. For example, to deploy Citrix products within US Federal environments, the deployment must be FIPS compliant.

Citrix products offer substantial security features and options to help safeguard sensitive data and intellectual property, ensure business continuity, and help organizations comply with security standards. This document provides guidance and recommendations to help you design and manage your Citrix deployment.

The Citrix Ready Marketplace includes an extensive list of verified products, trusted solutions, and enterprise-enabled apps. See www.citrix.com/ready

Security considerations in XenApp and XenDesktop deployments

There are various security considerations when designing and deploying Citrix XenApp and XenDesktop. This diagram shows key security areas and deployment options that help assure confidentiality, integrity and availability of resources.



To ensure security, integrity and business continuity, you need to determine your IT governance, risk management and compliance strategy. Your strategy should include security risk assessments, procedures, process, training and awareness.

The integrity and confidentiality of data is essential. Appropriate encryption, segmentation of users and access to resources, and managing the location of data, helps provide compliance that is more consistent, enforceable and verified.

You can protect against data loss outside the corporate network by restricting data access and transfer to user devices. For example, employees travelling on business may lose their laptop (in a taxi for example), or have a device seized by border control, and you can restrict and protect the data on these devices.

You can implement privacy controls and configuration, to benefit both the organization and users.

The key areas, shown in the diagram, help you optimize your deployment and mitigate security risks and achieve your security and compliance strategy:

Identity and Access

Well-designed identity management and access control determines who can access resources, how they authenticate and, once authenticated, the resources available and the level of access granted. Identity and access are an important consideration for all types of accounts including users, administrators and service accounts.

Benefits of a sound identify and access strategy include secure and controlled access to resources from personal devices (for example, employees working remotely and employees bringing their own devices to the office) and non-employees (for example, contractors, partners, suppliers and students). Authentication within large scale deployments is simplified, with a common URL provided to log on and access the required and relevant resources.

Network Security

Appropriate network security is required to ensure network traffic is secured and encrypted throughout the deployment, from user devices through to servers hosting resources and data. The type and level of network security required may also need to meet specific standards. For example, you may need to ensure end-to-end TLS encryption and specific network Access Control Lists (ACLs).

For examples of end-to-end TLS and FIPS compliant XenDesktop and XenApp deployments (including NetScaler), see Citrix XenApp and XenDesktop 7.6 FIPS 140-2 Sample Deployments.

Application Security

Application provisioning, hosting and monitoring must be designed to ensure applications are available to appropriate users only and hosted across servers, as needed, to minimize security risks.

Contextual application security can be enabled using application policies to ensure that applications only have access to what is needed in a specific situation. You can host applications in appropriate silos and use third party tools to prevent cross application security breaches.

Data Security

Protecting data is paramount and a feature of Citrix XenApp and XenDesktop, where data is protected in the data center. Data security can be strengthened through the configuration of Citrix virtual channels, Windows policies and third party tools.

Data security policies ensure sensitive data is kept in the data center (and off user devices), restricting access to resources and sensitive data on a contextual per-application basis. For example, policies may only allow certain users and devices access to sensitive data and applications such as payroll data. You can enable and configure endpoint validation and control to ensure policy-verified access, residual data management, and restrict and define the level of access to user device drives and peripherals.

For examples of policy configuration to restrict access to user device drives and peripherals, see the relevant procedures in the Common Criteria Evaluated Configuration Guide for XenApp and XenDesktop 7.6, available from https://www.citrix.com/about/legal/security-compliance/common-criteria.html

Monitoring and Response

Monitoring is central to your security risk and ongoing assessment strategy. Monitoring allows you to determine application usage, compliance, optimization and security. Based on monitoring logs, events and alerts, you can proactively identify and respond to security risks.

Monitoring for security related issues, enables you to check the status of your deployment and identify irregular events or issues. You can respond as needed to address issues, refine configuration, and support users.

Security capabilities and recommendations in XenApp and XenDesktop deployments

Citrix products offer many security features that can be configured to suit your environment, requirements, risk assessment and compliance. You need to review your security requirements and configure the products and features appropriately.

Security should be a key consideration during the planning phase. Configuring, testing and refining your deployment in a staging environment, ahead of rolling out a production deployment, is highly recommended.

To ensure ongoing mitigation against security threats, continuous monitoring, auditing and assessment of your deployment is also essential.

Citrix recommends the following security design and implementation options to help address security challenges and threats.

Identity and access

To determine identity and access needs, consider and confirm the requirements for each type of account, defining the identity, authentication and access rights and privileges. Each account type presents different challenges and requires specific identity and access configuration.

Account type	Identity	Access
User	Authentication, as defined by administrator. The authentication required is tailored to your environment (for example, two-factor authentication may be required).	Based on their privileges, users are able to access appropriate published resources.
Administrator	Authentication to provide access to management tools and consoles.	Administrators have direct access to management tools and consoles, usually from within the network, with access to security sensitive resources and data. Administrators require elevated privileges.
Service Account	Autonomous service account used by specific program/process. Program-specific authentication.	Specific privileges to access programs, resources, and scripts.

Identity and authentication

You need to determine how users must authenticate to access resources and review the required authentication policies.

When considering identity and authentication in a secure environment, multi-factor authentication is recommended. For example, a combination of user name, password, plus additional methods such as hardware or software-based token access. Multi-factor authentication is likely to be mandatory for remote access. Depending on your security requirements and policies, multi-factor authentication could be extended to within the corporate environment and network.

Smart card authentication is mandatory within certain environments. For example, in the US Department of Defense, smart card access is used to authenticate all users, local and remote. Smart card access is supported and can be configured in a XenApp and XenDesktop deployment. For more detail, see Smart Card Support.

StoreFront and, optionally, NetScaler are deployed and configured to manage access to published resources and data. For remote access, NetScaler is recommended. For internal access, StoreFront is often appropriate. However, the exact configuration depends on your security risks and needs.

To avoid security breaches, ensure appropriate password policies are in place. For example, the password policy may require passwords to comprise at least eight characters and include at least one upper case letter and one number or symbol. The password expiration period must also be defined. Other rules such as whether or not previous passwords can be reused may be defined. It is important to have a password policy in place and to ensure it is applied to all accounts (users, administrators and service accounts).

Access and privileges

Least privilege

For all account types (users, administrators and service accounts), you should grant the minimum privileges needed to allow completion of tasks. This is often referred to as the principle of least privilege.

Some organizations achieve this through granting elevated privileges to confirm everything works, then reset to minimum privileges and gradually increase privileges until the account has adequate privileges to perform the required tasks.

User privileges - publishing

For publishing purposes, use Active Directory groups and policies. Configure the required privileges for the relevant AD group and add the appropriate users to the group. Avoid publishing to all users (Domain Users), individual user accounts, anonymous (non-authenticated) users or shared accounts.

Administrator privileges

Accounts for administrators and support staff require elevated privileges. As with other account types, use groups (AD groups, for example) to provide access. The group must:

- Include the relevant users (administrators or support personnel)
- Be configured to allow access to the required consoles only
- Be based on role (access and privileges needed to complete tasks)
- Be configured to allow the level of logging required by governance and regulatory compliance

Regularly review reports to determine whether users can be removed from the group. This is particularly important with administrator accounts; roles and responsibilities are likely to change regularly and therefore group membership and management rights may need to be modified accordingly.

Ensure you have at least two users allocated to each group so there is no risk of only one person available to complete tasks (as that could result in a single point of failure).

Do not use default names and passwords for administrator accounts and, as with other accounts, ensure an appropriate password policy (and strong authentication) is in place.

Your deployment will include various administrator accounts, across various systems. For example, administrators for management of XenApp and XenDesktop, administrators to manage your data storage, administrators to manage your database infrastructure. Ensure you monitor and track all administrator accounts as they are all likely to have elevated privileges and data access.

Note that NetScaler, XenApp and XenDesktop (and other third party tools) include default delegated administrator roles. This may be a consideration when configuring AD groups for administrator purposes and roles. Consult the relevant product guides for more information on default roles.

Service account privileges

With elevated privileges and often poor password management (for example, password never expires), and in some cases access to multiple components, service accounts can be a target for security attacks.

Avoid using a single service account for multiple components or programs (avoid aggregated ‘super accounts’).

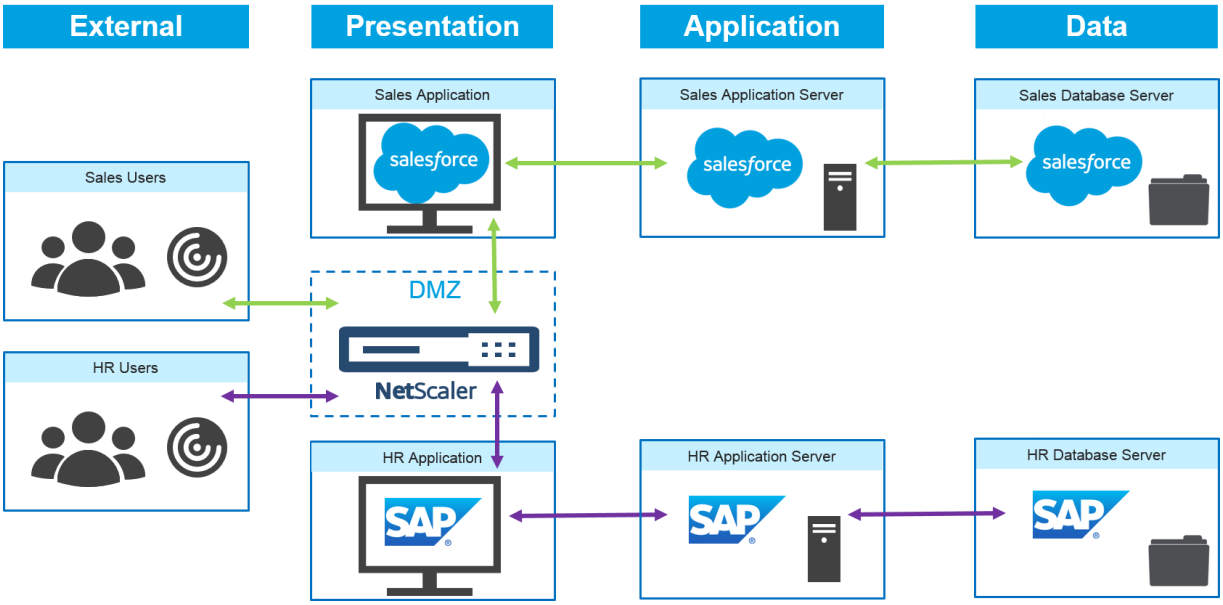
As with all accounts, ensure proper password policies are in place. Where a service account is a local computer account (rather than a domain account), it is necessary to manually update the password regularly.

Access Rights

You can configure SmartAccess, a feature of XenApp and XenDesktop, to help secure your deployment. SmartAccess allows you to control access to published applications and desktops based on NetScaler Gateway session policies. You configure pre-authentication and post-authentication conditions that must be validated to access published resources. These conditions can cover security related requirements such as checks for the correct version of virus protection software and domain membership. You can also configure conditions, based on XenApp or XenDesktop policies and/or NetScaler SmartControl, to control access to local devices and processes (for example, user device drive mapping, clipboard, and printer mapping). Additionally, specific privileges in XenApp, including clipboard usage, can also be configured on a per-application basis.

Network security

Citrix products provide many security features to help secure the network. Each network comprises layers (referred to as enclaves within government environments), as shown in this example:



In the example, users in the Sales group log on and access the Sales application (salesforce) and the salesforce data. Users in the Human Resources team access the HR application and data (provided by SAP). The diagram shows the location of components and resources within the network layers.

The network layers are described below:

Layer	
External	This includes devices and networks that are not controlled by the organization. This is of course the least trusted layer. In many cases, users and partners will access your network from here.
Presentation	This outermost layer managed by you (the external layer is not controlled by you), is the most likely to be attacked. It includes NetScaler, within a DMZ, and access to virtual applications and desktops.
Application	This layer contains your application servers and management consoles.
Data	The inner most layer and the most protected layer. It contains your data and intellectual property – hosted on your database and file server infrastructure

A well designed network, with secured and discrete layers, helps prevent security breaches. Each layer is protected and isolated; network traffic can move between adjacent layers only (traffic is unable to skip layers).

Firewalls are used to protect and control communication between the layers. Only essential ports are opened, restricting traffic to certain ports and protocols. Network traffic is encrypted, throughout the deployment and all layers. For an example of network encryption and firewall configuration, see the Representative deployment . In addition to firewall protection within the network, ensure appropriate firewalls are configured on user devices.

Data is kept secure and isolated. Management is conducted within the secure inner application layer to safeguard sensitive configuration and data.

Application security

Within a Citrix deployment, there are various techniques you can employ to protect the application layer. The biggest security threat is application jailbreaking (also known as application breakout), where potential malicious activity can occur after gaining access to the underlying network infrastructure.

Third party tools, such as Microsoft Windows AppLocker, help improve application security by restricting who can run applications and also the type of applications that can be run. Using AppLocker, you specify which users and groups have access to particular applications. You create rules for your organization, to allow or deny access to specific applications. AppLocker also allows you to restrict and prevent access to different types of files, including executable files and scripts.

You can configure separate and discrete application servers and files servers, within your XenApp and XenDesktop environment, to keep applications and data protected. For example, host payroll applications and data on separate dedicated servers and restrict access to the payroll applications (for example, only users in 'Human_Resources' group are able to access the payroll applications). With the applications and data managed on separate file servers and databases, they are protected should there be a jailbreak elsewhere in the deployment.

As with data security, publish applications to specific groups of users only. Avoid publishing to individual users, anonymous users or shared accounts. Also, if appropriate, you can enforce higher levels of credential access for more sensitive applications. For example, payroll applications may require a higher level of authentication such as multi-factor authentication.

Where a number of applications are hosted on the same server, you can isolate and restrict access to applications using NTFS (New Technology File System) permissions on the application folders. NTFS permissions can also be used to restrict access to management consoles and features such as session sharing (so authorized administrators only can access the management console and tools).

Your XenApp and XenDesktop provisioning scheme allows you to manage the base images, application hosting and silos. You manage these centrally on a per-image basis, simplifying rollout and updates.

Data security

Hosting data in the data center is a long standing security feature of Citrix XenApp and XenDesktop. To increase data security, consider the following:

Virtual channels: To determine the virtual channels needed and those that can be disabled, you must consider your user needs and use cases. This must be balanced with your security needs and compliance requirements. Where possible, restrict or prevent the use of virtual channels that allow data transfer to and from user devices, to ensure data is kept in the data center and protected. For example, client drive mapping and USB redirection allow transfer of data between the data center and user devices.

Where the requirements and needs differ for local and remote users, SmartAccess can be configured to manage the virtual channel settings. The virtual channels settings are applied based on whether or not the user is accessing the environment from within the corporate network or remotely.

Note that in some deployments, customer specific virtual channels may have been configured. If so, you should disable these customer specific virtual channels by default. If a particular application or use case deems a customer specific virtual channel absolutely necessary, you must determine whether the security risks are acceptable before enabling the virtual channel.

NetScaler Gateway: You can also configure NetScaler Gateway ICA proxy mode to further isolate sensitive data, ensuring data is available using published applications or desktops only (and not accessible directly, even for those within the network).

Access to restricted data: You may need to refine and increase the level of authentication required depending on resource access. For example, to access sensitive data, consider introducing increased levels of authentication. For example, in a health environment, smart card access may be required to access patient data.

Provisioning: Depending on the use case and provisioning scheme, XenApp and XenDesktop provisioning options provide the ability to contain security breaches. For example, if desktops are provisioned on a per-session basis in read-only mode, at the end of the session the desktop is discarded. Therefore, in the event of a security breach (for example, a malware breach), the threat is mitigated once the session is terminated.

Hosting applications and data

Ensure that data and applications are hosted appropriately and in relevant silos, as required. It should not be possible to run programs (for example, executables and scripts) on the data file server. It should also not be possible for users (or resources running on the user device) to access and modify files on the folders containing programs.

Monitoring and Response

Monitoring is essential for detecting and responding to risk, allowing you to determine deployment usage, optimization, security and compliance. You can monitor the deployment to detect and respond to suspicious behavior and attacks, detect abuse of privileged accounts, ensure products and components have the latest updates and security fixes applied, and check virus protection software is installed and up to date. You must have policies and processes in place to ensure regular review of monitoring reports. You must respond as needed to address issues, refine configuration, and support users.

Risk and compliance

Your organization's IT governance, risk management and compliance strategy is central to the design of your deployment. Monitoring and response is key to your risk and compliance strategy.

Risk

You need to confirm and review your risk strategy and confirm how to detect, deter, prevent and recover from risks. Data is likely to be central to your risk strategy. For example, how to safeguard sensitive data and intellectual property.

- **Detect**: Monitoring can help detect security risks. For example, you can use NetScaler Security Insight feature to help identify and highlight security risks, parse NetScaler logs to automatically detect context-sensitive reporting and highlight compliance issues.
- **Deter**: Monitoring user behavior (and letting your users know they are being monitoring) not only helps detect issues but may also deter user activity that may result in security issues.
- **Prevent**: Techniques such as segmentation of users, applications and data, plus policy-based access to applications and data, can help prevent risk. Data security also ensures protection of data loss outside our organization (for example, restricting the data stored on remote devices). Training users may also help prevent issues.
- **Recover**: Virtualization of applications and desktops provides inherent features to assist with recovery and response to issues. For example, with shared and read-only desktop images, security breaches are contained and discard on termination of sessions. If you identify a security risk or breach, you may also need to reconfigure your deployment, and revisit your procedures and processes, to prevent further issues.

Compliance

You need to consider your compliance requirements. For example, do you need to comply with market specific compliance requirements? You may need to consider and meet the requirements for the Payment Card Industry Data Security Standard, for example, if working with payment systems and data.

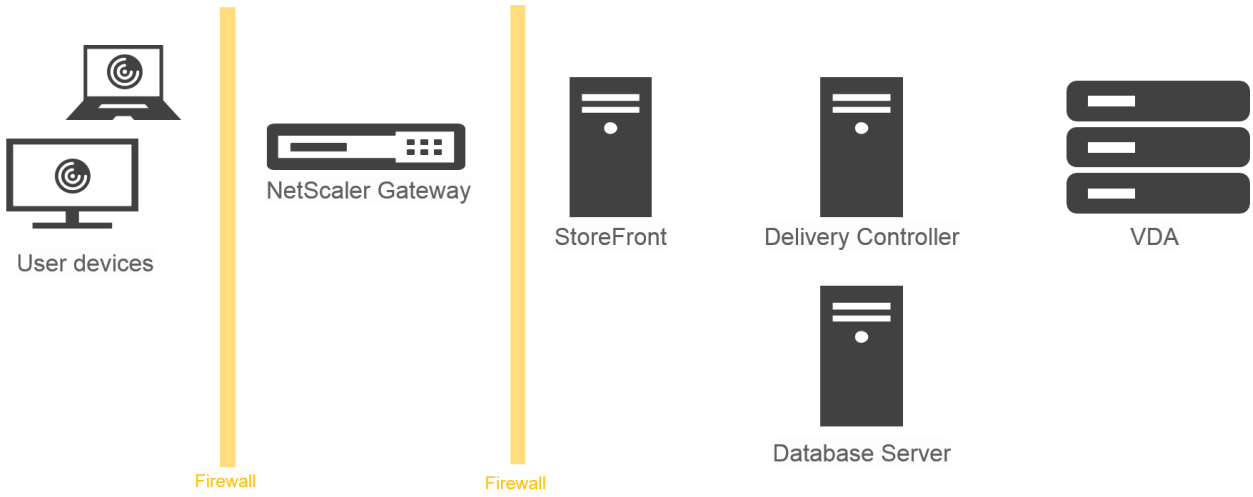
Appropriate encryption, segmentation of users and access to resources, and managing the location of data, helps provide compliance that is more consistent, enforceable and verified.

Representative deployment

The deployment below is an example of a Citrix deployment designed to meet the guidelines detailed in this document.

The deployment includes Citrix Receiver, NetScaler Gateway, StoreFront, XenApp and XenDesktop (Delivery Controller and VDA). For simplicity, only one Delivery Controller and VDA are shown.

The deployment is based on the XenApp and XenDesktop 7.6 Long Term Service Release. However, the deployment includes the addition of StoreFront 3.5, as this allows encryption of network traffic using TLS 1.2. NetScaler Gateway MPX 11.0 (with the 2.2 level Cavium firmware applied) is included in the deployment s it also supports TLS 1.2.



Users log on and authenticate using NetScaler Gateway. NetScaler Gateway is deployed and secured in the DMZ. Two factor authentication is configured.

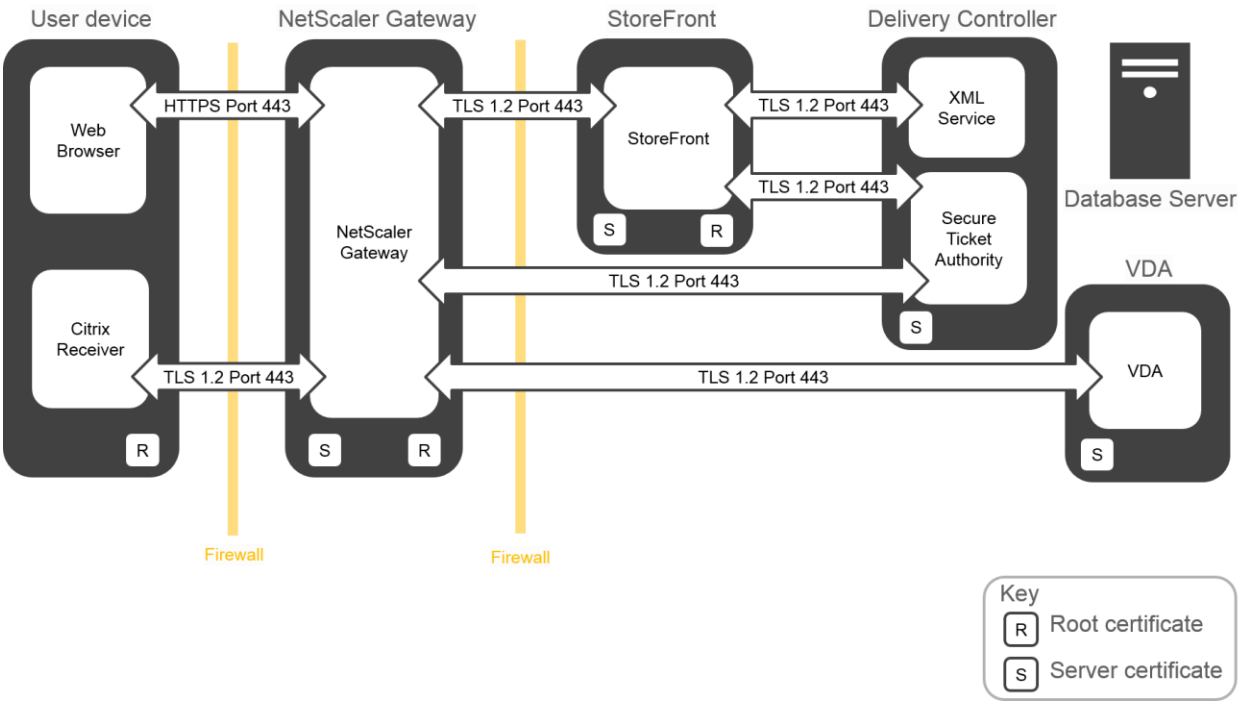
Based on the user credentials, users are provided with the relevant resources and applications.

Applications and data are located on appropriate servers (not shown on the diagram), with separate servers used for security sensitive applications and data.

The deployment includes monitoring utilities to check usage, risks and security issues. Procedures are in place to review and respond to security risks.

How the components interact

This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



NetScaler Gateway is deployed in the DMZ to provide secure remote access to XenApp and XenDesktop environments.

Traffic between the web browser on the user device and NetScaler Gateway is secured using HTTPS. All other traffic is secured using TLS 1.2.

NetScaler Gateway terminates the TLS/HTTPS connections from the user device (browser and Citrix Receiver). Traffic from NetScaler Gateway through StoreFront, Delivery Controller, and the VDA is secured using TLS 1.2 .

Network traffic is encrypted end-to-end, using TLS 1.2. As noted, StoreFront 3.5 is required (TLS 1.2 support was introduced with StoreFront 3.5).

Security Standards

This section provides details regarding security standards that may be relevant top your deployment. Some standards may be mandatory depending on your use case and environment.

Common Criteria

Common Criteria certification is an internationally recognized standard for evaluating the security of IT products and systems. Common Criteria certification provides assurance that products were thoroughly and independently tested and validated against a set of requirements established by the worldwide International Standards Organization to ensure IT security.

For customers, especially US Federal and international government agencies, Common Criteria certification is an important requirement when procuring IT products and systems. Common Criteria certification is also applicable to private sector industries such as healthcare and financial.

Citrix XenApp and XenDesktop 7.6 and NetScaler 10.5 were evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and meet the Common Criteria, conformant requirements of Evaluation Assurance Level EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures. NetScaler 10.5 also meets Protection Profile for Network Devices v1.1.

FIPS 140-2 with XenApp and XenDesktop

FIPS 140-2 is a U.S. federal government standard that details a benchmark for implementing cryptographic software.

The security community at large values products that follow the guidelines detailed in FIPS 140-2 and the use of FIPS 140-2-validated cryptographic modules.

To facilitate implementing secure application server access and to meet the FIPS requirements, Citrix products can use cryptographic modules that are FIPS 140-2-validated for implementations of secure TLS/SSL connections.

The FIPS-enabled NetScaler Gateway MPX-FIPS appliance (NetScaler Gateway 10.x) is fully compatible, allowing full TLS configuration in deployments that include NetScaler Gateway. NetScaler Gateway MPX-FIPS appliances are FIPS 140-2 Level 2 compliant.

To facilitate implementing secure application server access and to meet the FIPS requirements, Citrix products can use cryptographic modules that are FIPS 140-2-validated for implementations of secure TLS connections. When configured for FIP 140-2, Citrix XenApp and XenDesktop, StoreFront and Receiver, use cryptographic modules provided by the Microsoft Windows operating system. NetScaler uses the FIPS 140-2-validated Cavium cryptographic module.

The representative deployment in this guide is configured with TLS connections enabled with FIPS 140-2-validated cryptographic modules.

TSL/SSL

Transport Layer Security (TLS) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity and optional client authentication for a TCP/IP connection.

In Citrix deployments, you can configure TLS secure communications between user devices and XenApp and XenDesktop servers, ensuring data and traffic is encrypted throughout the deployment.

Secure Socket Layer (SSL) is the previous standard, superseded by TLS. You can configure both TLS and SSL within a Citrix deployment. The server certificates in your deployment support both TLS and SSL.

Citrix products – support for TLS 1.2

This table shows Citrix products and components that support and can be configured for TLS 1.2 (the latest recommended release of TLS).

Product	TLS 1.2 support
NetScaler – version 11.0	Yes *
NetScaler – version 11.1	Yes
StoreFront – version 3.5	Yes
Windows Virtual Desktop Agent – version 7.6	Yes
Linux Virtual Desktop Agent	No
Receiver for Windows	Yes
Receiver for Linux – ARM – version 13.2	Yes
Receiver for Linux – x86 – version 13.2	Yes
Receiver for Mac	Yes
Receiver for iOS	Yes
Receiver for Android – version 3.7	Yes
Receiver for Chrome	Yes
Receiver for HTML5	Yes
Receiver for Windows 10 Mobile	No

* NetScaler 11.0 requires the 2.2 level Cavium firmware.

IP Security

IP Security (IPsec) is a set of standard extensions to the Internet Protocol (IP) that provides authenticated and encrypted communications with data integrity and replay protection. IPsec is a network-layer protocol set, so higher level protocols such as Citrix ICA can use it without modification.

Current and recent versions of XenApp and XenDesktop support end-to-end TLS encryption, so there is no reliance on IPsec. However, for earlier versions of XenApp and XenDesktop, IPsec was required for full encryption of network traffic within a virtual private network (VPN) environment.

IPsec is described in Internet RFC 2401. All current versions of Microsoft Windows have built-in support for IPsec.

Smart cards

You can use smart cards with XenApp and XenDesktop, to provide secure access to published resources and data. Using smart cards simplifies the authentication process while enhancing logon security. XenApp and XenDesktop support smart card authentication to published applications, including “smart card enabled” applications such as Microsoft Outlook.

In a business network, smart cards are an effective implementation of public-key technology and can be used to:

- Authenticate users to networks and computers
- Secure channel communications over a network
- Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published using XenApp and XenDesktop. In addition, smart card functionality within these published applications is also supported. For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the user device to log on to a server running XenApp or XenDesktop. After users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix supports the use of Personal Computer Smart Card (PC/SC) based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card. In addition, you can use two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

Smart Card Support

Citrix continues testing various smart cards to address smart card usage and compatibility issues with XenApp and XenDesktop. XenApp and XenDesktop fully support the Common Access Card (CAC) and Personal Identity Verification (PIV) cards, with the appropriate versions of Citrix Receiver.

There are many different types of smart card and smart card vendors. Within the US Government, both of these cards are used extensively:

- The Common Access Card (CAC) is used by employees and other personnel in the US Department of Defense (DoD). The CAC includes a photograph of the user, plus their name and associated details. The CAC is used to gain physical access to DoD buildings and areas and is also used to log on to the IT systems on the NIPR network. The CAC uses a proprietary on-card applet and requires proprietary middleware. Note that a Personal Identify Verification (PIV) authentication applet and certificate can be installed on modern CAC cards post-issuance using the User Maintenance Portal for CAC users, for users that also require access to PIV-protected systems (see below).

- The Personal Identify Verification (PIV) card is similar to a CAC, used by employees and contractors working in US Federal agencies. It includes a photograph and user details and is used to gain physical access to federal buildings and used to log on to IT systems. However, unlike CAC, PIV developed as a result of the Homeland Security Presidential Directive 12 (HSPD-12), does not necessarily require proprietary middleware and is supported by default on Microsoft Windows 7 or later. For further information, see http://csrc.nist.gov/groups/SNS/piv/

The Citrix Ready Marketplace includes details of verified smart card and smart card hardware products. See www.citrix.com/ready. Contact your smart card vendor or Citrix representative for further information regarding supported versions of smart card hardware and software.

Citrix tests smart cards using certificates from common certificate authorities such as those supported by Microsoft. If you have any concerns regarding your certificate authority and compatibility with XenApp and XenDesktop, contact your local Citrix representative.

For guidance regarding smart card configuration in US Government environments, see http://support.citrix.com/article/CTX200939.

Finding more information

The following documents and resources provide supplementary and additional information regarding securing Citrix deployments. The resources include links to specific product documentation plus security related technical articles and whitepapers.

Compliance and standards

Common Criteria

- XenApp 7.6 and XenDesktop 7.6 and NetScaler 10.5 – Common Criteria Information: https://www.citrix.com/about/legal/security-compliance/common-criteria.html

FIPS

- Citrix XenApp and XenDesktop 7.6 FIPS 140-2 Sample Deployments: https://www.citrix.com/content/dam/citrix/en_us/documents/about/citrix-xenapp-and-xendesktop-76-fips-140-2-sample-deployments.pdf

Healthcare

- Citrix XenApp and XenDesktop 7.6 Healthcare Design Guide: http://docs.citrix.com/content/dam/docs/en-us/solutions/industries/downloads/healthcare-design-guide.pdf

Smart cards

- Smart Card - Support Updates: http://support.citrix.com/article/CTX132230

Finance

- Payment Card Industry and Citrix XenApp and XenDesktop Deployment Scenarios: https://www.citrix.com/content/dam/citrix/en_us/documents/support/payment-card-industry-and-citrix-xenapp-and-xendesktop-deployment-scenarios.pdf

Best Practices

Best Practices for Enterprise Security

- https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

Citrix Ready Marketplace

- The Citrix Ready Marketplace includes an extensive list of verified products, trusted solutions, and enterprise-enabled apps. See www.citrix.com/ready

Products

XenApp and XenDesktop

- XenApp and XenDesktop 7.6 product documentation: https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6.html
- System Hardening Guidance for XenApp and XenDesktop whitepaper: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf

NetScaler

- NetScaler Gateway 10.5 product documentation: https://docs.citrix.com/en-us/netscaler-gateway/10-5.html
- NetScaler Gateway 11.0 product documentation: https://docs.citrix.com/en-us/netscaler-gateway/11.html

StoreFront

- StoreFront 3.0 product documentation: http://docs.citrix.com/en-us/storefront/3.html
- StoreFront 3.5 product documentation: http://docs.citrix.com/en-us/storefront/3-5.html

Receiver

- Receiver 4.4 product documentation: http://docs.citrix.com/en-us/receiver/windows/4-4.html

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.