Best Practices for Enterprise Security

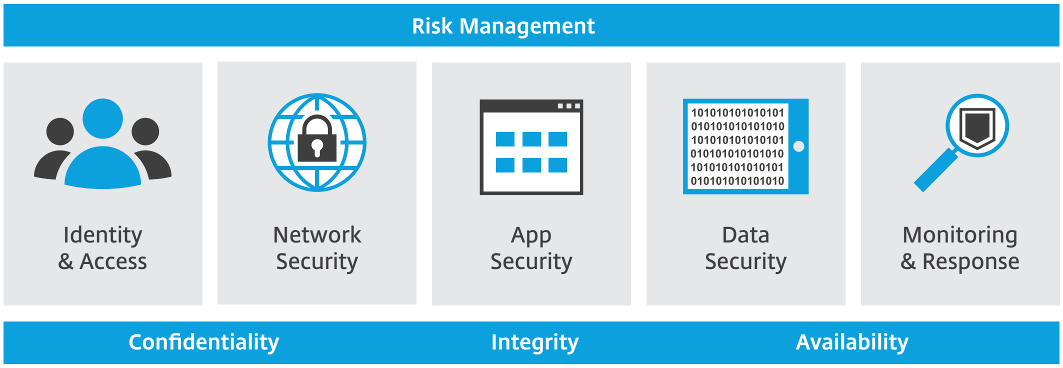
Enable secure productivity for the modern workforce

How Citrix helps organizations manage risk while empowering business mobility by controlling access to applications and data across any location, network and device.

IT and security leaders face the challenge of reducing business risk to acceptable levels while ensuring ease of use and productivity. People need to be able to work however best suits their purposes—any location, device or network—without being frustrated by an overly constrained or complex user experience. At the same time, it's essential to protect enterprise apps and data from being compromised by security threats, prevent loss and theft, and ensure full compliance with standards and regulations.

Citrix supports best practices for risk management across five key pillars of enterprise security: identity and access, network security, application security, data security, and monitoring and response. We enable customers to implement and manage these critical measures through a tightly integrated solution built on a foundation of confidentiality, integrity and availability. A mature application delivery model centralizes applications and data in the datacenter and provides contextual access control across any location, network and device. As a result, employees, contractors and partners have the flexibility to choose how they work, whether remote, mobile or in the office. End-to-end visibility of connections, traffic and user activity allows IT to address privacy, compliance and risk management priorities without compromising workforce productivity. Integration with third-party security vendors enables advanced levels of system management and identity, endpoint and network protection.

This white paper explores best practices to address key user productivity and security challenges, and how tightly integrated Citrix solutions allow customers to leverage the full benefits of business mobility while managing risk.



Secure productivity in the modern enterprise

The security challenge facing today's enterprises is growing rapidly across two dimensions, exacerbated by both escalating levels of risk, and the continued evolution and diversification of applications. At the same time, mobile productivity—a crucial capability for every enterprise —depends on a convenient, consistent and reliable experience for users wherever and however they work. This must extend across every type of app they use, over any network, on any device. Even as the requirements of the mobile workforce grow vastly more complex, IT must continue to strive for simplicity.

At Citrix, we believe that a great user experience goes hand in hand with security. Our solutions are built on security best practices designed to protect what matters—data, applications and usage—while allowing choice, freedom and a seamless experience for users in every scenario. These measures include:

Identity and access

- Two-factor **authentication** for all users
- Least-privilege **authorization**
- **Access control** based on user context

Network security

- Secure **remote access** for mobile and third-party users
- Network and host **segmentation** to shrink attack surfaces
- A multilayer approach to ensure **availability**

Application security

- **Centralization** and encrypted delivery of applications
- **Containerization** for mobile apps
- **Inspection** to protect web apps

Data security

- **Centralization** and hosted delivery of data
- **Secure file sharing** to reduce data loss
- **Containerization** for data in transit and at rest

Monitoring and response

- End-to-end **visibility** into application traffic
- **Auditing** and accounting of resource access
- Support for **compliance** with standards and regulations

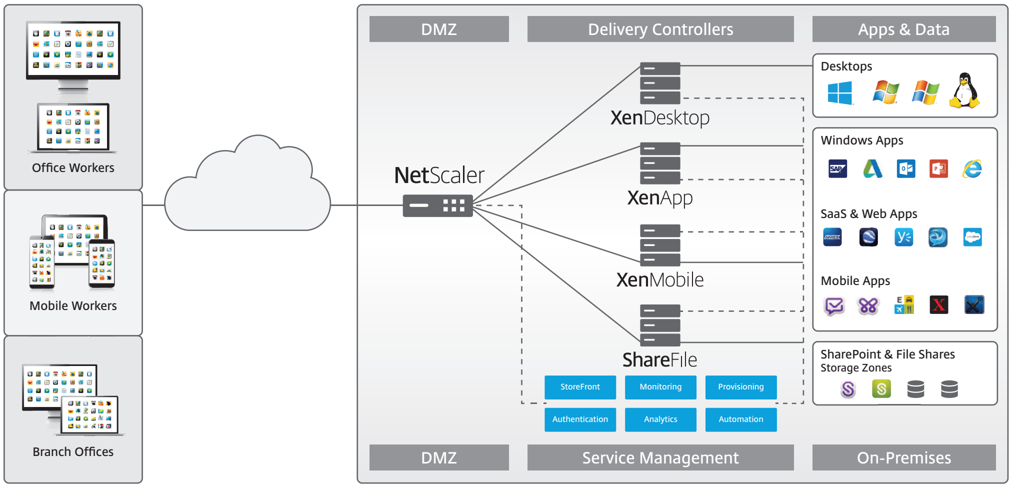
Explored in depth in the following sections, these best practices define our approach to security across all of our products. Customers experience their benefits every day in solutions including:

- **Citrix NetScaler** to contextualize and control connectivity with end-to-end system and user visibility

- **Citrix XenApp** and **XenDesktop** to manage apps and desktops centrally inside the data center
- **Citrix XenMobile** to secure mobile applications and devices with a great user experience
- **Citrix ShareFile** to provide controlled and audited data access, storage and sharing both on-premises and in the cloud

In this way, we help organizations meet security requirements and meeting business objectives without impeding productivity.

Citrix Architecture



Identity and access

Preventing unauthorized access to applications, data and the network is a fundamental security requirement. Users at all levels, from line-of-business workers to administrators and executives, are frequently targeted by phishing attacks. A damaging breach is always just an authentic-looking email or mistyped URL away. As attackers focus on stealing credentials, even strong, routinely changed passwords are no longer enough to prevent the compromise of security measures such as database encryption. A single stolen username/password combination can be enough to unlock multiple sites and services—a careless action on a personal social media account can put an organization's flagship product or service at risk. Managing user access calls for a balanced approach that's both convenient for users and more secure than a simple username and password combination.

Authentication: Require two-factor authentication for all users

Given the vulnerability of passwords to compromise, two-factor authentication to applications and desktops is essential for effective security. The principle is to require two different forms of authentication—one, something the user knows; the second, something he or she uses, such as a physical token. This poses a significant barrier to user impersonation even if the primary password has been compromised. As part of this up-leveling, authentication should also be added to legacy applications that do not natively support it, a capability provided by NetScaler and XenApp.

To encourage the use of strong passwords while reducing user confusion and frustration, IT can apply measures allowing a more seamless login experience, including:

- **Federation of identity** – The use of third-party cloud services can require users to manage an additional set of credentials. By securely sharing authentication and authorization data between parties over public networks, federation of identity eliminates the need for a separate login. In effect, the organization binds access to services such as Microsoft Office 365 to their user directory. IT If an individual leaves the organization, IT can centrally remove access to all third-party services as easily as in-house resources. Both NetScaler and ShareFile support SAML, the standard that commonly handles federation.
- **Single sign-on** – In both federated and non-federated environments, single sign-on (SSO) can reduce user frustration by eliminating the need to enter the same credentials multiple times into multiple systems. NetScaler supports common SSO mechanisms including form-based, 401-based and Kerberos Constrained Delegation, and can also maintain authentication session cookies to provide SSO across all the web applications accessed via a website, dashboard or portal such as Microsoft SharePoint.

Authorization: Implement least-privilege authorization using contextual access control

Authenticated users should be authorized for access to only the applications, desktops and data essential to complete their work—the principle of least privilege—with rights reduced once no longer required. Along similar lines:

- To reduce the risks associated with malware, administrators should not log into workstations as administrators unless the task requires the privileged account, instead using standard user credentials for routine actions such as checking email and browsing the web.
- Applications and services should be configured to launch with the fewest possible privileges, and service accounts should be created with the minimum required permissions.
- Administrative duties should be separated to restrict the power held by one person and prevent a single rogue admin from being able to both commit and conceal an attack.

Authorization levels are typically tied to user identity through group membership, but this approach can lack the granularity required for every use case. Task-oriented or location-based authorization can be more effective, especially for remote access use cases such as teleworkers, offshoring and third-party access. Integrating with role-based access mechanisms such as Microsoft Active Directory, NetScaler allows predefined access policies to be tailored at both group and user level.

Access Control: Manage access by validating endpoints

As organizations leverage the productivity and employee satisfaction benefits of practices such as telework and flexwork, they also face the need for more granular access control. Security policies may require allowing different levels of access depending on whether a given user is working inside or outside the corporate network, as well as making distinctions between corporate and third-party workers. Diversifying endpoints and the rise of BYOD hade made device-based access management far more complex. Some organizations allow any laptop, computer, phone or tablet to access the network, sometimes without requiring any form of malware, antivirus or application restriction.

Citrix best practices call for providing the appropriate level of access to applications and data based on the combined attributes of the user, device, location, resource and action. Before granting access, NetScaler interrogates the endpoint to ensure it is healthy and compliant in terms of domain membership, antivirus and malware protection. This analysis enables the SmartAccess policy engine to trigger adaptive session policies based on the "Five W's of Access": who, what, when, where and why. Administrators have complete flexibility to define varying access scenarios and corresponding rules based on their organization's security policies, while users are free to work from any device. For devices out of compliance, users can be quarantined and granted limited access to remediation sites and resources.

Network security

The growing role of mobility in the modern enterprise makes remote access a core IT function—and a prime vector for attackers seeking entry into the organization's network. The consequences of a breach can be devastating. The compromise of a business partner's network can lead directly to an attack on the organization itself, offering attackers a weak link to exploit as a network gateway. Once inside, the attacker will seek privilege escalation and then move laterally to core components such as domain controllers. In one highly publicized breach, attackers were able to communicate from networked store devices such as point-of-sale registers directly to the core network. At this point, a backdoor or Remote Access Trojan (RAT) typically has little difficulty connecting to a Command and Control (C2) server using an outbound call to an external system.

Freely available network stressors and DDoS tools can be configured and controlled in botnets with command and control, as with Low Orbit Ion Cannon (LOIC). More advanced tools include nation state-backed "Internet Cannons" that weaponize valid internet user traffic by rewriting HTTP requests to flood targeted websites.

Remote Access: Require secure access for employees and third parties

Remote access capabilities allow users outside the corporate network to access apps, desktops and data. Allowing, controlling and securing this access is the role of NetScaler Unified Gateway, which:

- **Extends remote access** and SSO to all enterprise and cloud apps
- **Consolidates infrastructure** to reduce the proliferation of access methods
- **Intercepts incoming traffic** as a full reverse-proxy gateway before it is sent to the applications on the backend
- **Provides a single URL** to consolidate a wide range of existing solutions by incorporating the capabilities needed to support all types of access scenarios, including mobile

One such scenario is a full SSL VPN providing a direct network-level connection to the datacenter. For the majority of users who do not require a full VPN, NetScaler provides an ICA Proxy to XenApp, connecting hosted applications and desktops to Citrix Receiver. As with SSL VPN, all data transmitted between the client and datacenter is encrypted. This is the recommended configuration for high-security environments including PCI DSS. One URL gives end users one simple location for remote access to web, SaaS and Citrix applications from any device, with the ability to do two-factor authentication, SSO and Federation.

NetScaler simplifies and centralizes access control and visibility by providing a single point of configuration and enforcement. SmartControl acts as an ICA firewall to centralize access control logic to manage contextual authorization based on parameters such as client device OS and patch levels, and whether anti-virus is installed, running and up to date. Features can also be blocked based on client and server IP and port as well as user and group membership. Virtual channels access such as cut-and-paste, mapping, client drive mapping or printing can be enabled per application to provide the right level of access.

Segmentation: Implement network security zones

Segmentation extends the rule of least privilege to the network and hosts by defining security zones that minimize unwanted access to sensitive applications and data. Firewalls and gateways restrict traffic to their respective zones, reducing lateral movement and attack surface to contain the blast radius of a breach.

Segmentation measures supported by NetScaler include:

- **Authentication and proxy** of client connections in the DMZ to block malformed packets and malicious requests at this point
- **Optimization, multiplexing and rate limiting** of connections to backend servers to protect their resources
- **A software-defined architecture** that uses virtualization to enable the hardware platform to be securely carved up into separate and unique instances, each with separate SLAs and assigned memory, SSL, CPU and virtual NICs that are either shared or dedicated

NetScaler itself is architected with segmentation as a key design principle.

- **Traffic domains** segment traffic for different applications and tenants into fully isolated network environments on a single appliance.
- **Admin partitions** segment individual NetScaler appliances into separate resources with dedicated administration and separate login UI, views, configuration files and logging—for example, using application-specific partitions for the Citrix, networking and Microsoft applications teams.

Availability: Use intelligent load balancing and multilayer denial of service protection.

Availability is challenged daily by both hardware and software failures as well as DDoS attacks that disrupt services through the exhaustion of bandwidth, compute and memory resources.

Load balancing, a core NetScaler function, distributes incoming client requests across multiple servers hosting web applications and content. This prevents any one server from becoming a single point of failure and, together with utilization optimization methods such as Least Connection or SNMP-based metrics, improves overall application availability and responsiveness. Global Server Load Balancing (GSLB) provides an additional layer of protection, failover and optimization for organizations with multiple sites and geographically distributed services. As part of its multilayer approach to availability, NetScaler also provides:

- **DDoS protection** – NetScaler checks client connection and request parameters to prevent flood attacks such as SYN, UDP, ICMP, Smurf and Fraggle, waiting to proxy the connection until a valid application request has been submitted.
- **SSL/TLS offloading** – By proxying, validating and, if needed, rate-limiting connections, NetScaler protects web services against attacks such as HeartBleed, Shellshock and Poodle that target SSL/TLS vulnerabilities.
- **Surge protection and priority queuing** – NetScaler mitigates against traffic spikes and surges that can overload backend servers by caching and prioritizing connections, and then delivering them as the server load is reduced so that none are dropped. NetScaler also provides DNS protection for DNS servers and supports DNSSEC to protect against forged and corrupted host records spreading to new targets.

Application security

Applications of all types are popular targets for exploitation. Even when security researchers find a vulnerability before hackers do, it can take months for an organization's systems to be patched or updated. Even then, many successful breaches have exploited vulnerabilities for which patches have been available for years, notwithstanding mature application delivery models with established processes for finding, testing and fixing vulnerable software on a timely basis.

On mobile devices, natively installed apps face risks such as insecure data storage, insecure data transmission and sensitive data leakage. As smartphones and tablets quickly become a business standard, the line between personal and business apps has become blurred, exposing sensitive and confidential data to the risk of sharing via cloud storage, on social networks, between apps or peer-to-peer.

Web applications are vulnerable due to poor security configuration, incomplete patch management of the underlying operating system, vulnerabilities in the coding language, or unpatched and zero-day vulnerabilities in third party dependencies. Legacy or unsupported applications risk attacks that tamper with fields, overflow buffers or perform command injection and remote code execution. Application-layer attacks are well above the controls provided by network firewalls and IDS/IPS, which don't understand logic attacks.

Centralization: Virtualize applications and require encrypted delivery

Application virtualization protects sensitive data by centralizing apps in the datacenter and allowing only a pixelated representation of the application to reach the endpoint—no actual data transfer occurs. Virtualization also allows the classification of applications based on their security requirements; sensitive apps can be siloed onto dedicated servers within a separate network segment with different sensitivity classifications and restrictions, and multiple isolated versions of web browsers can be published to address diverse security and legacy requirements of web apps. IT gains a single point of visibility and control to define and enforce access policies on a group or user level.

Decentralized security configuration and patch management for locally installed applications is inefficient and often inconsistent. With centralization, OS patches, service packs, hotfixes, and application and configuration updates are performed on a single master image, accelerating testing and rollout. Endpoint-based attacks such as memory or RAM scraping no longer present a risk.

Functionality and communication between the Citrix Receiver client and XenApp servers take place over virtual channels for graphics, disks, COM ports, LPT ports, printers, audio, video and smart cards, with XenApp policies controlling the ability to save, copy, print or otherwise move data. For organizations that require the additional layer of protection, SmartControl on NetScaler enables filtering at the network level. Encryption is integrated into every component of the communication flow, including multi-layer ICA and SSL/TLS.

Containerization: Manage mobile apps to prevent data loss

Citrix best practices for mobile app security are based on containerization, a form of segmentation at the device level. Users can use a single device with both personal and business apps, with business apps and data managed by IT. The security of the hardware, operating system and individual apps is extended by container-based security measures including encrypted storage and usage, app-to-app data control and data wipe policies.

Building on the containerization approach, XenMobile enables organizations to centralize management, security and control for apps as well as data and settings.

- **Micro-VPN** – XenMobile and NetScaler provide dedicated micro-VPN tunnels for native mobile apps; encrypted SSL/TLS sessions between the app and NetScaler are protected from other device and micro-VPN communications to ensure that resources on the internal network are not exposed to traffic from personal apps infected with malware.
- **Device validation** – Because containerization alone can't ensure security for a device that has been jailbroken or rooted to allow the installation of pirated or non-validated apps—a common vector for malware designed to acquire super admin status—XenMobile validates device status and blocks jailbroken devices prior to device enrollment.
- **Managed native apps** – Citrix mobile business productivity apps including WorxMail and WorxWeb for secure and managed email and Web browsing install natively to mobile devices, sandboxed in a secure container that IT can remotely manage, control, lock and selectively wipe without touching personal data or apps on the device.

Inspection: Protect web applications against attacks

Web apps are rich targets for hackers, offering a highly vulnerable attack surface with direct connectivity to databases containing sensitive customer and company information. Such threats are often devised specifically for the target, making identification by network-layer security devices such as intrusion protection systems and network firewalls impossible. This leaves web apps exposed to application-layer attacks using known and zero-day exploits. NetScaler AppFirewall closes this gap by delivering centralized, application-layer security for web apps and services.

Logic attacks based on injections flaws exploit an application's failure to filter user input, such as when SQL injection is used to pass arbitrary commands through an app to be executed by the database. Cross Site Scripting (XSS) uses the web app as a weapon to attack other users, again via a failure to validate input. Having become part of the application, the payload is returned to the victim's browser, where it is treated as code and executed to perform session hijacking or attempt credential theft through phishing.

AppFirewall stores custom injection patterns to protect against injection attacks of all types.

- Administrators can use field format protection to restrict user parameters with regular expressions; form fields are checked for consistency to validate that they have not been modified.
- To prevent SQL injection, AppFirewall inspects requests for a combination of SQL key words and characters.
- For dynamic and context-sensitive protection against XSS attacks, AppFirewall looks for input that resembles an HTML tag and checks against allowed HTML attributes and tags to detect XSS scripts and attacks.

Because web apps are often the target of DDoS attacks, protection must extend beyond the network and session layers. NetScaler uses application-level DDoS protection to block or throttle attack traffic that appears valid at the network layer.

- HTTP DDoS protection challenges client requests to ensure that they are coming from a valid browser; requests from scripts and bots typically cannot answer the challenge correctly and are thus denied.
- When a POST request is received, it is first checked for a valid cookie. If it does not have one, NetScaler sends a JavaScript to the client asking it to resend the information with a new cookie, which becomes invalid after four minutes. Every response to the client is sent with the new cookie. During an attack, all cookies sent beforehand become invalid and an error page with a cookie is sent. New connections as well as connections that cannot provide valid cookie data are put into a low-priority queue.

AppFirewall enforces both positive and negative security models to ensure correct application behavior. The positive security model understands good application behavior and treats all other traffic as malicious—the only proven approach delivering zero-day protection against unpublished exploits. Administrators can create managed exceptions and relaxations when an application's intended and legal behavior might otherwise cause a violation of the default security policy.

Using a negative security model, AppFirewall also performs scanning against known attacks using thousands of automatically updated signatures. The advanced web application protection profile adds session-aware protections to protect dynamic elements such as cookies, form fields and session-specific URLs. Attacks that target the trust between the client and server are stopped. Such protection is imperative for any application that processes user-specific content, such as an e-commerce site.

Data security

Data of all kinds, including legal documents, contracts, R&D data, marketing and sales info, entertainment media or any other form of intellectual property, is a vital organizational asset that must be protected. Thousands of known breaches in recent years have resulted in millions of compromised customer and patient records, many with personally identifiable information (PII), including credit card numbers, Social Security numbers, dates of birth, driver's license, addresses, health records, student records, government and veteran records with fingerprints and security clearance data.

Not every breach results from hacking, malware and other attacks. Other causes include unintended disclosure, hacking and malware, payment card fraud, insider fraud, loss of documents, loss of media, and loss of both mobile and stationary devices. The popularity of consumer-grade cloud storage among users is especially problematic, moving data off the trusted network to servers not under the organization's control.

Centralization: Centralize, monitor and control data egress

In a virtualized environment, data resides in the datacenter. Applications execute on the server with only mouse clicks and keystrokes sent to the user device—not data—mitigating against loss and leakage caused by lost, stolen or destroyed endpoints. Organizations can further protect against bulk data loss by preventing the transfer of files and databases to workstations.

To prevent data from being saved on removable media such as USB drives, emailed among users, printed out or otherwise exposed to loss or theft, IT can centrally administer policies controlling users' ability to save, copy, print or otherwise move data. Device policies to further enhance data security include the ability to:

- **Segment client-side data from applications** by blocking virtual channels such as client drive mapping, print, and copy/paste.
- **Define folder redirection** to map the user's My Documents folder to a central file store in the datacenter.
- **Restrict where files are saved** to protect against loss, theft or destruction of the endpoint.

Containerization: Encrypt data both in transit and at rest

When mobile apps are run natively, date is stored locally, increasing the risk of data leakage and loss. XenMobile addresses insecure mobile data storage with containerization and encryption.

- With containerization, or app-level segmentation, the data for each app resides inside the container in which it is executed and cannot be accessed by apps residing elsewhere.

- IT can encrypt data within a secure and isolated container on the endpoint, mitigating against data loss.

The implementation of BYOD makes it essential to separate personal and business apps and their associated data, especially given the widespread sharing of data among mobile apps, such as by built-in system applications like Contacts. XenMobile secures iOS data using open-in management, which allows IT to control data flow and access between managed and unmanaged apps. For example, administrators can block users from using an unmanaged app to open data created in a managed app, or vice versa. Email attachments can be opened only in apps approved by the company, and links to web sites are forced to open in a secure browser.

XenMobile leverages industry-standard encryption for application data either at compile time or via wrapping technology. All application data is stored in a secure container that encrypts both files and embedded SQL technology on the devices. Data held in local database files is encrypted using AES-256.

Secure sharing: Enable secure file sharing to reduce data loss

As users seek to collaborate efficiently, they find the path of least resistance to share data among themselves and with third parties, including shadow IT solutions that are out of the visibility, approval or control of IT. This leads to data sprawl and non-secure file sharing via USB drives, the Internet and personal cloud services that often lack either basic or advanced controls against data leakage. Employees may turn to FTP, which lacks secure authentication—credentials are transmitted in cleartext—or unencrypted email, even sending files accidentally to unauthorized individuals inside and outside the organization.

Citrix addresses the secure file sharing challenge with security built in at every level of ShareFile:

- **Authentication** – Multiple two-factor and two-step authentication methods include forms and token-based authentication as well as SMS, voice and backup codes. ShareFile also supports single sign-on authentication mechanisms including SAML, requiring users to authenticate against the enterprise identity provider first.
- **Authorization** – IT gains visibility and control over file sharing with the ability to grant, monitor and revoke access. For added data protection, users themselves can expire file links after the message has been sent, and set a date for the deletion of a folder and its contents. Both users and IT can perform remote wipe on ShareFile data and passwords stored on mobile devices in the event of loss or theft.
- **Auditing** – ShareFile tracks and logs all user activity, including both data access and data sharing, to support compliance requirements and provide visibility into data usage. To aid compliance and address requirements for on-premises data storage, ShareFile allows organizations to use the ShareFile control plane for file management and storage in the datacenter.

- **Encryption** – Each file is encrypted using a unique key before it is copied to its permanent location, and decrypted prior to download to a user browser; encryption keys are not stored on the same server as the files themselves to ensure that physical access to a storage server does not allow access to the files residing there. ShareFile also offers encrypted emails using Microsoft Outlook to protect sensitive information contained both in the body and the attachments, and supports compliance for HIPAA, HITECH and CFPB.

Monitoring and response

Even in the best-secured environment, preventing a breach by advanced and persistent threat actors is nearly impossible. This makes security monitoring and detection absolutely critical. Organizations must gain higher visibility into the network and apps using log collection, analysis and escalation; filter noise from salient information; detect abnormal connection attempts; and identify indicators of attack and compromise that can be used to aid incident response.

XenApp provides tools to support end-to-end monitoring of its infrastructure, including comprehensive infrastructure monitoring, performance monitoring, event monitoring, services monitoring and availability monitoring. IT can quickly identify user experience degradation and accelerate root cause analysis. Smart policies, rigorous enforcement, and deep monitoring and reporting enable effective security without impeding user access.

Visibility: Implement monitoring to address degraded availability and performance

Visibility challenges grow as the number and complexity of applications and deployments increase across lines of business, as well as the tools and techniques used for monitoring. NetScaler simplifies monitoring by providing a central point through which all application information travels. While the primary purpose of this design is to allow load balancing and SSL offload for scalability and availability, it also ideally positions NetScaler to parse both web and ICA traffic for any type of application using any type of encryption. Performance data for this traffic is then sent to NetScaler Insight Center, which uses AppFlow to define and extract visibility information.

Security Insight helps admins focus on the most relevant monitoring data quickly and efficiently with automated tools that apply built-in expertise to:

- Identify configuration patterns and highlights inconsistencies that may weaken your security posture
- Parse your mountain of NetScaler logs looking for issues that may be dangerous—going beyond anomaly detection for true context-sensitive reporting
- Highlight any issues with PCI compliance to make the audit process that much easier to work through

For user experience monitoring, HDX Insight provides end-to-end visibility into ICA connections proxied through the NetScaler to help IT addresses performance issues such as slow applications or desktops. As a triage tool, NetScaler helps IT determine if the issue exists at the client, server, application or network side, and provides a breakdown of bandwidth consumption within the ICA channel, SmartControl and Geo Maps information.

Web Insight provides visibility for services that run over the web or HTTP/S layer by collecting and providing analytical reports on the AppFlow records for this traffic. A central dashboard provides application visibility information across all dimensions, from end clients to backend application servers. The ability to correlate visibility facts to user pain points aids troubleshooting exercises.

Auditing: Integrate logging and alerting to detect attacks and breaches faster

Regular auditing and accounting of user access, configuration changes and account management logs aid threat detection by capturing early indicators of attack and compromise. These can include unusual and large volume of outbound traffic, unusual account activity—especially for privileged accounts—and failed and successful logins from unusual locations. This data also helps IT clean up inactive accounts as best practices recommend. As successful intruders often clean up logs to delay detection of their breach, log files should be stored externally to the system.

NetScaler auditing provides logs for a number of real-time and historical actions including:

- Authentication failures and successes
- Authorization failures and success
- Current, timed out and all AAA sessions for all application traffic going through NetScaler

Centralized access control allows admins to consolidate management for all the applications within the same domain and appliance rather than using separate controls for each.

In addition to simplifying and accelerating troubleshooting, the ability to track and report on changes made to the configuration of a XenApp server farm, by whom and what time, ensures accountability and aids security—especially in environments where multiple administrators make modifications. Configuration logs also capture an audit trail for change management, configuration tracking and reporting of administration activity. Administrators can record active XenApp virtual application and server hosted desktop sessions based on user, application or server, and then archive recordings for forensic analysis or reference when needed.

Compliance: Reduce the scope of audits by designing focused architectures

Strict adherence to high encryption standards has long been a requirement for government agencies, and FIPS compliance is quickly becoming a topic of interest in commercial spaces as well as banks, credit card processors and healthcare organizations seek to secure traffic inside their datacenter.

XenApp and XenDesktop provide native FIPS 140-2 compliance of the HDX protocol to provide the highest level of data access security in virtual environments. All user connections to virtualized apps and desktops are encrypted using NIST-mandated FIPS 140-2-validated modules. NetScaler integration provides FIPS 140-2 Level 2 compliance for an even higher level of information assurance with a hardened appliance. Data centralization, hosted delivery and remote display restrict PCI data to a small, protected space that can be audited more completely and efficiently than an entire internal network.

XenApp, XenDesktop and NetScaler also constitute the only end-to-end app and desktop delivery solution available that meets Common Criteria certification, an ISO standard for software security function that evaluates authentication, access control, administration and secure communication.

Conclusion

The modern enterprise workforce calls for deep, comprehensive security to keep data safe no matter how people work—any location, any device, any access method. Built on a foundation of confidentiality, integrity and availability, Citrix best practices for security encompass identity and access, network security, application security, data security, and monitoring and response to ensure both protection and productivity in every user scenario. To learn more about ensuring security through tightly integrated Citrix solutions, please visit URL.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

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.