Addressing Today's Endpoint Security Challenges

Protect apps and data across every endpoint to complete your enterprise security posture.

Mobile and endpoint security is a complex equation with all too many variables and unknowns, from the devices and networks people may be using at any given time to the myriad combinations of OS, apps, configurations and patches on each endpoint. To maintain security wherever people work, IT needs a way to simplify the steps to produce desired security outcomes. The key is to focus on protecting the apps and data that power mobile productivity, using context-aware policies to allow the appropriate levels of access and usage for each particular device and situation.

Citrix helps companies maintain the security of their apps and data even if an endpoint is lost, stolen, destroyed or compromised. Our unique security solution creates a software defined perimeter that combines secure access to apps and data with contextual control, visibility and behavior analytics across devices, networks and clouds. By extending control beyond the traditional datacenter to mediate user interactions with apps and data, IT can proactively secure, detect and mitigate risk with intelligence applied to each unique scenario.

This paper discusses the elements of a complete strategy for mobile and endpoint security, including multilayered protection for apps, data, devices and networks.

Securing the Mobile Workforce

Endpoint security has become a major issue for enterprise IT as business mobility, bring-your-own device (BYOD) and a multi-party workforce render traditional perimeter-based protection ineffective. Mobile devices containing sensitive business data can all too easily be lost or stolen, but users—including both employees and third-party team members—are often resistant to letting IT control or manage the personal devices they use for work. As work takes users beyond the enterprise network to connect over public WiFi, consumer broadband and other unknown access points, IT can no longer rely on its own secure perimeter for comprehensive protection.

In trying to secure and ensure policy compliance, up-to-date protection and patch levels across a dizzying matrix of device types, OS and configurations, IT can easily spiral into complexity that undermines both the efficiency and the effectiveness of these efforts. It's also easy to lose sight of the real goal: not ultimately to protect the device itself, a replaceable commodity, but to ensure that mobile usage doesn't put business apps and data at risk. IT needs granular control over access and usage of apps and data based on the specific context in which the user is working—location, device and network—to maintain security without impeding productivity. By focusing on this goal, IT can achieve more effective protection, more simply.

Citrix helps companies address the endpoint security challenges of an increasingly complex mobile world. Contextual access to resources based on user, device, location or network helps IT protect sensitive data from being lost or stolen wherever and however people work. Unified management applies security policies with fine-tuned precision wherever, whenever and by whomever access to critical apps and data is needed. By making it possible to leverage contextual protection of centralized apps and data, Citrix makes it simpler to safeguard information, manage risk and achieve compliance in any location, over any network, on any device.

Citrix secure workspace solutions let IT weave this situational approach to security through every element of their mobile infrastructure, including access, apps, devices, data and networks.

Contextual Access

As a foundational layer of protection, Citrix enables a holistic approach to security by using contextual awareness to allow just the right balance of security and flexibility for any situation. IT can control access to resources based on user, device, location or network to protect sensitive data from being lost or stolen while at rest, in use, and in motion on devices, servers or the cloud.

Citrix SmartAccess and SmartControl features let IT define context-aware policies to authorize access to specific apps and their data based on the user's identity, role, location, device type and status of device compliance. To define such policies, IT can consider questions such as:

- Do we have some applications that are too sensitive to use outside the office or require heavily controlled physical locations?
- What data must be accessible but never exposed on the device for international travelers? Are there country-specific policies that need to be applied?
- Which users are working with the enterprise's most sensitive data on mobile endpoints? In addition to employees, consider non-employee contractors in human resources, legal and M&A, as well as engineers and auditors.
- What type of usage is appropriate in specific scenarios, such as on managed vs. unmanaged devices, over secure vs. unsecured networks, or accessing public vs. sensitive data of various levels of classification?
- How do I know that the situation is appropriately secure? As a user? As an administrator? Policy must continuously be tuned to reflect new use cases and work situations.
- How do we evaluate all contextual information (device, location, time, data sensitivity, identity) to assess the risk and apply the right level of control? For example: If operating on an unmanaged device in a risky location, limit access to public data only.
- As data proceeds through its lifecycle, such as transitioning from confidential work-in-progress to a public document, how can security controls be applied dynamically to reflect changing tolerance for risk?

Application Security

Citrix enables IT to control access to apps, including where, on what device and over what type of network people can use a given app and its data. Users must first authenticate their identity; for additional security, admins can also activate multi-factor authentication or require a PIN for specific apps. For a more seamless user experience, IT can deploy single sign-on across apps of all types.

Mobile App Security

Citrix can also control the way mobile apps interact with data and with each other. Citrix XenMobile provides mobile application management (MAM) capabilities to enable centralized management, security and control for mobile apps, including restricting the ability to cut and paste across apps. Open-in management—the ability to control which apps can be used to open a particular piece of content—lets IT 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.

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, including personal apps. In this way, IT can segregate and protect this data through container-based security measures including encrypted storage and usage, app-to-app data control and data wipe policies.

Secure mobile apps designed for business included with XenMobile let IT avoid the risks associated with consumer-grade native apps. XenMobile includes apps for email, web access, note-taking, workflow automation and time management, file sync and sharing, mobile editing and remote desktop access.

These can be installed natively on mobile devices, sandboxed in a secure container that admins can remotely manage, control, lock and selectively wipe without touching any personal data or apps on the device.

Application Virtualization

For Windows applications accessed on mobile endpoints, including both laptops and other types of devices, app virtualization powered by Citrix XenApp and XenDesktop lets IT deliver enterprise apps on-demand while data stays 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, compromised or destroyed endpoints.

Single-Purpose Browsers

To improve security for browser-based apps, IT can publish and maintain individual browser versions for each. By configuring the browser specifically to support the unique security needs of each application and use case, extraneous settings, unnecessary active content and other undesired capabilities can be disabled. The virtualized browser also keeps sensitive data off the endpoint. All web usage, including hyperlinks in emails and social media apps, can be redirected to open in the sandboxed one-time-use virtual browser, isolated from key resources, greatly limiting the potential impact of malware.

Data Security

The core of the Citrix approach to endpoint security is to use app virtualization and remote access via XenApp and XenDesktop to keep data centralized and off devices as much as possible. To prevent exfiltration of remotely accessed data, IT can also configure policies for virtual channels to deny printing, file transfers, microphone usage and the clipboard when not required.

For data that does need to be on the endpoint, such as for mobile apps, XenMobile enables containerization and encryption as described in the previous section, as well as remote wipe, selective wipe and kill pill capabilities for lost or stolen devices. Selective sync and drive mapping tools reduce the attack surface by minimizing the data footprint on the endpoint.

Secure File Sync and Sharing

Data access has historically allowed data distribution — but it doesn't have to. Data governance with Citrix ShareFile allows easy access and sharing on any device, from any location, while maintaining strict protection. Users can access and collaborate around centrally hosted versions of documents rather than downloading or forwarding the file itself, thus reducing the data footprint on the endpoint and its associated risk.

For data shared using ShareFile, information rights management (IRM) can package security controls with the data to bring security closer to the data. This helps address data collaboration use cases where data need to leave the corporate network in a controlled manner. IT gains visibility and control over file sharing with the ability to grant, monitor and revoke access. 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. Data security and IRM features follow the file so that authentication and data lifecycle management continue to be enforced even after it leaves the ShareFile system. Both users and admins can perform remote wipe on ShareFile data and passwords stored on mobile devices in the event of loss or theft.

On-premises and cloud-based data loss prevention (DLP) capabilities give IT visibility and control over sensitive data. ShareFile integrates with popular DLP systems and cloud security solutions to restrict document sharing based on the file's DLP classification.

Advanced document workflows including forms, feedback, approvals and signatures track data access, usage and collaboration for files, including sensitive change management data, approvals and logs. Able to access the workflow as the authoritative source for a document and its associated activity, users have no reason to download and save separate copies of documents and approvals on their endpoints.

Why Use MAM if I Already Use MDM?

Mobile application management (MAM) and mobile device management (MDM) are complementary technologies that can each have a valuable role to play in endpoint security.

- **MAM** can be used to protect, control and manage business data and resources separately from personal content. These app-specific measures make MAM especially suitable for BYOD; IT can protect business data without the need for device-level management. MAM is also useful in cases where the user does not set a device passcode, which can leave data unencrypted. By providing an additional layer of app-level encryption, MAM protects data even if the device itself is uncompromised.
- **MDM** enables device-level policies to configure, secure and support mobile users. IT can enable device-wide encryption, enforce restrictions for VPN and WiFi, track a device's location, and automatically lock or wipe a lost or stolen device. MDM is most appropriate for corporate-owned devices that do not contain personal data.

Device Security

While the Citrix approach to endpoint security focuses largely on apps and data, device-level measures play a valuable role as well. SmartAccess acts as a firewall to manage contextual authorization based on parameters such as client device OS and patch levels, whether a device has been jailbroken, and whether anti-virus is installed, running and up to date. IT can also enforce password standards, encryption, and allowed WiFi and VPN connections. Once a device has been checked for compliance, SmartControl applies the contextual security policies defined by IT to control access to apps and data based on user, device, location and network.

Mobile Device Management

For situations where platform, root of trust and TPM (Trusted Platform Module) ownership are required, XenMobile provides mobile device management (MDM) for fully managed devices. Admins can configure policies, actions and security functions to protect devices and the data they contain at a system level, such as placing restrictions on what users can download from app stores, performing full or selective wipe, or tracking geolocation data.

Network Security

Citrix NetScaler helps IT maintain comprehensive control over apps and data while simplifying access for users. Admins can enable single sign-on to desktop, web and SaaS applications for a streamlined access to apps across any datacenter or cloud. A single point of administration ensures consistent policy enforcement across every device people use.

Mobile Networking

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. Even if the device is comprised, the data being transmitted from the app remains protected.

Analytics and Insights

To maintain security, compliance and threat protection in a world of mobile endpoints, Citrix provides visibility, analytics and insights across the network, and access to apps and data. End-to-end monitoring of infrastructure, performance, events, services and availability allows IT to filter noise from salient information, detect abnormal connection attempts, and identify indicators of attack and compromise that can be used to aid incident response. Citrix Management and Analytics Service leverages analytics and data telemetry from all Citrix products to enable profiling and detection of security incidents.

Regular auditing and accounting of user access, configuration changes and account management logs aid compliance and threat detection by capturing early indicators of attack and compromise. 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. The ability to track and report on changes made to the configuration of a XenApp server farm, for example, 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.

Complementary Technologies

As part of a comprehensive, multilayered strategy, Citrix enables integration with leading security solutions to enable a broad range of complementary measures.

Client Hardening

As a complementary security technology for the endpoint, organizations can leverage partner solutions to harden the Citrix Receiver client on laptops and mobile devices. Integrated with NetScaler Gateway, these solutions make it possible to protect the browser, logon process and Citrix session from keylogging, screen-scrapping and other malicious attacks while enforcing and deploying a consistent installed Citrix Receiver version.

Cloud Access Security Broker (CASB)

Integration with leading CASB solutions enables XenMobile and ShareFile customers to control the cloud services users are able to access, including cloud-based storage and file sharing services. By introducing a security enforcement layer between users and cloud service providers, IT can prevent the unauthorized and unmanaged use of consumer-grade cloud services that can put data at risk and violate organizational and industry security standards. IT can define policies based on service category and risk, and can either block services entirely or apply selective measures such as block, alert, bypass, encrypt, quarantine, and coach for policy enforcement.

Data Loss Prevention (DLP)

Integrated easily with both traditional on-premises DLP solutions and SaaS DLP solutions, ShareFile works with an organization's existing DLP infrastructure to detect when sensitive content is added and allows IT to restrict access and sharing based on the results of the DLP scan. The ability to control and restrict sharing based on the actual content of files is especially valuable in highly regulated industries, making it possible to enforce strict security and compliance regulations and requirements.

Compliance Management

Integrations with advanced monitoring tools give IT full visibility into the infrastructure to detect and respond more quickly to threats, misconfigurations and performance issues that can compromise compliance. Organizations can define compliance objectives for both industry regulations and internal corporate standards to manage risk more effectively; reduce the scope of security and compliance audits; and address issues quickly to avoid user interruption.

Identity and Access Management (IAM)

Because passwords are so vulnerable, requiring people to use at least two forms of authentication—like a password and token—to access apps and desktops is essential for effective security. Integration with multifactor authentication solutions makes it significantly harder for an attacker to impersonate a user, even if the primary password has been exposed.

Malware and Ransomware Protection

Citrix malware protection is complemented with partner malware integrations to enable visibility and protection across both physical and virtual environments, as well as cloud services. Advanced measures such as anomaly detection, static and dynamic threat detection, and machine learning help IT guard against both known and unknown threats.

Mobile Threat Detection

Third-party mobile threat detection solutions work in tandem with XenMobile to scan mobile devices for jailbroken or rooted status, blacklisted or low-reputation apps, and other potential threats, then initiate automated measures for out-of-compliance devices before they are allowed into the enterprise environment. The compliance status reported to XenMobile is also available to XenApp and XenDesktop to determine whether to allow virtual apps and desktops to launch on the device for an additional dimension of protection.

Conclusion

Citrix helps customers manage data protection as business mobility, BYOD and the multi-party workforce transform endpoint security requirements. Centralized control and contextual awareness make it simpler to safeguard information and manage risk on any device people use, over any network, wherever they work. Complementary technologies for app, data, device and network security provide the right level of protection in any scenario without impeding productivity or degrading user experience and through services from Citrix Consulting, customers can assess and harden their Citrix environment to thwart attacks and increase protection across infrastructure. By creating a software-defined perimeter, IT can extend control beyond the datacenter to proactively secure, detect and mitigate risk according to the specific context of each user session and activity.

For years, customers across every industry, including the most highly regulated sectors, have relied on Citrix for secure app and data delivery to any device, over any network, and from any cloud. Today, as the pace of transformation accelerates for both markets and businesses, we empower organizations to combine agility and productivity with security.

To learn more, contact your Citrix rep or partner for a personalized mobile security plan, or visit www.citrix.com/secure.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States