CITRIX®

White Paper

Five Pillars of Security for Financial Services Organizations

How financial firms can better protect data, applications and networks

Financial services organizations are constantly deploying new technologies and applications that enhance productivity, mobility and customer service. They empower mobile workers to deliver consistent, high quality customer service across all channels and all locations. They also centralize and streamline IT to reduce costs, increase performance, and assure the highest levels of availability.

But at the same time, IT in financial services organizations must reduce security risks, ensure that sensitive customer data is protected, and battle continuously against fraud and identity theft, phishing attacks, distributed denial of service (DDoS) attacks, sophisticated malware and ransomware, and many other advanced attacks. IT also must ensure compliance with a wide range of industry standards and government regulations imposed by the Federal Financial Institutions Examination Council (FFIEC), the Financial Industry Regulatory Authority (FINRA), the Payment Card Industry Security Standards Council (PCI-DSS), the European Union, and countless other national governments and international organizations.

This white paper discusses how security and networking solutions from Citrix can help financial services organizations reduce business security risk and ensure compliance by strengthening five pillars of business security:

- Identity and access
- Network security
- Application security
- Data security
- Monitoring and response

1. Identity and Access

Financial services organizations are challenged to provide the right level of confidentiality, integrity and availability for apps and data without putting undue restrictions on how employees work or how customers access their data. That means using sophisticated authentication, authorization and access control techniques, while giving employees and customers simple, consistent authentication across all types of devices.

Authentication

Citrix solutions for financial services organizations support a wide range of multi-factor authentication methods for access requests. These include multi-factor methods such as tokens, smartcards, RADIUS, Kerberos, and biometrics, and two-step authentication methods such as codes sent by text and voice messages. Multi-factor authentication can be provided not only for traditional desktop and web applications, but also for SaaS apps such as Office 365, asset management and loan application apps, and legacy applications that do not natively support advanced authentication.

Citrix solutions also provide a consistent way to provide identity federation and single sign-on (SSO) through SAML (Security Assertion Markup Language) and a variety of single sign-on mechanisms.

These capabilities ensure that financial services employees get a consistent authentication and access experience as they move from the central office to branch offices, home offices, and client meetings. The same capabilities provide customers with simple but secure access to web apps from personal devices and self-service kiosks in branches.

Authorization

With Citrix solutions for financial services, IT can provide employees, contractors and business partners with appropriate levels of access to specific applications and resources. They can control access by using rules related to each person's identity, role, and group memberships. Authorization rules can even restrict access to specific network segments.

Access Control

To create the optimum balance between user-friendliness and risk, access to resources can be controlled by contextual factors such as the type of device making the access request, the employee's location, and whether or not the device is on a corporate network.

Citrix secure networking products can also reduce the risk of hackers penetrating the network through compromised endpoints. They do this by validating endpoints and blocking network access from devices that are not compliant with corporate policies or are missing defenses like anti-malware and encryption software.

2. Network Security

Financial services organizations have a critical obligation to ensure that data can travel securely from devices to the corporate network, and that the corporate network is protected from network-layer attacks.

Remote Access and Encryption

Citrix solutions for financial services centralize and simplify remote access. Administrators can customize portals for groups of employees and customers. These portals allow each user to access all authorized web, SaaS, mobile and virtualized applications at one URL. Administrators can manage these portals centrally, and use them to enforce authentication and remote access policies.

Citrix solutions can also ensure that remote network traffic for virtual desktops and applications is protected by SSL virtual private networks (SSL VPNs), and that traffic to and from native mobile apps is encrypted with micro-VPN tunnels.

Segmentation

Citrix secure networking products can segment networks into security zones and restrict access based on conditions such as the user's identity and the type and compliance level of the device making the access request. This segmentation enforces network access control, and limits the ability of attackers to move from one compromised device to other resources on the network. It also helps ensure compliance with FFIEC, PCI-DSS, and data privacy regulations that mandate strict controls over access to protected data.

Availability

Maintaining the availability of mission critical applications during an attack is another critical security objective. Citrix solutions for financial services include health monitoring, load balancing and rate limiting features that defend against malformed network traffic and DDoS attacks.

Security and Flexibility at Groupe Promutuel

Groupe Promutuel is made up of 26 independent entities operating through more than 140 offices across Quebec. Its workforce includes 1,650 internal users and 1,500 external insurance resellers.

Groupe Promutuel's use of Citrix solutions to support its dispersed workforce began with the deployment of Citrix NetScaler® to accelerate and load-balance various web services. Next, the Group deployed Citrix XenDesktop® and Citrix XenApp® to centrally manage and deliver virtual desktops and streaming applications, first to its partner businesses, then to its own employees.

"It was very important for us to be able to normalize our work environment, including the desktops we provide to users, and to better control where our information is and who can access it," says Jamie Schofield, network architect at Groupe Promutuel. "Now we have everything in a centralized, controlled and secure environment. Citrix has changed the game in terms of what we're able to do." The Group is now using its Citrix environment as the foundation for a new business continuity and disaster recovery strategy.

3. Application Security

Applications are the source of much business risk. In addition, activities like configuring and patching are extremely time-consuming and error-prone. That's why financial services organizations seek security solutions that minimize risk and reduce the burden on IT administrators.

Centralized Administration of Apps

Citrix virtual application and virtual desktop solutions dramatically simplify the configuration and patching of apps, browsers, and operating systems. These tasks can be performed on a few master images in the data center, rather than on hundreds or thousands of remote systems. Centralization shortens the window of exposure to zero-day attacks, removes opportunities for errors and inconsistencies, and eliminates the risk of endpoint-based attacks such as memory and RAM scraping. Centralization also reduces the need to maintain local IT staff, cutting management and maintenance costs.

Containerization

Citrix solutions for financial services can work with mobile device management (MDM) solutions to "containerize" mobile apps so they run in highly secure, encrypted sandboxed areas in mobile devices. This allows IT to manage corporate data and apps without violating employee privacy regulations or norms. Business apps cannot be infected by malware downloaded by employees.

In addition, Citrix security solutions can identify which mobile devices have been jailbroken or rooted, and are therefore vulnerable to attacks (or have already been compromised). This information can be used to restrict or disable network access for mobile apps.

Inspection

By centralizing software and app management, and by providing effective monitoring tools, Citrix solutions make it easier to observe and detect zero-day attacks, logic flaws, and application-level DDoS attacks.

Citrix secure networking products help protect applications against dangerous web-based attacks, including SQL injection and XSS (cross-site scripting) attacks. They can also mitigate application-level DDoS attacks by detecting and throttling unusual spikes in traffic for specific applications.

4. Data Security

Today, customers expect to be able to access web and mobile apps from any device on any network available to them. Employees expect to access data from anywhere, synchronize files across multiple devices, and collaborate in ad hoc workgroups. These expectations make data security increasingly important, and increasingly challenging.

Centralization of Data

With Citrix virtual application and desktop solutions, data can be centralized in secure data centers, where it is protected by enterprise-grade security tools like next-generation firewalls and intrusion protection systems. Most data can be kept off endpoints, which are liable to be stolen, compromised or destroyed. "Data in motion" over the network can be encrypted to protect it from eavesdropping and man-in-the-middle attacks.

Containerization and Remote Wipe

When Citrix solutions for financial services containerize applications on mobile devices, they also protect the data used by those applications. All data inside the container is encrypted. Administrators can implement app-to-app data controls, for example preventing unmanaged apps from accessing data created by managed apps and allowing only approved apps to open email attachments.

When mobile devices are lost or stolen, both IT and the device owners can perform remote wipe on business data without endangering personal data or apps.

File Sharing

The Citrix file sharing solution allows employees to share documents securely with customers, for example when signatures are needed on consumer loan documents, or when collaborating with co-workers on insurance claims. IT can grant, monitor and revoke access to files, and create policies that prevent users from saving, copying, or printing files. When users share a link to a document, they can set an expiration date for files and folders, and can revoke access at any time. Every shared file is encrypted using a unique key, and keys are stored on different servers from the files themselves so files cannot be read unless both servers are compromised.

5. Monitoring and Response

Financial services organizations need visibility into user actions and security events, to respond to attacks and to demonstrate to auditors that security controls are in place.

Visibility

Citrix solutions for financial services organizations include monitoring tools that capture and analyze extensive data about user activities and network flows. IT can monitor user actions, including login attempts and requests to access systems and applications. Network monitoring tools help administrators identify anomalous traffic patterns, abnormal connection attempts, and other unusual behaviors. They also help forensics experts analyze and respond to attacks.

Auditing

The auditing and logging mechanisms in Citrix solutions give IT a detailed record of application usage, application-related events, and data access activities. The Citrix file sharing solution tracks and logs all user activities related to file sharing and file access. Other Citrix tools record

and analyze data related to indictors of attacks, such as unusual creation or use of privileged accounts, failed logins and access requests from unusual locations.

Compliance

Citrix solutions for financial services can help IT centralize and monitor applications and data, ensure the encryption of data in motion and data at rest, containerize and wipe data on mobile devices, restrict the sharing and copying of data, and segregate protected data in restricted spaces that can be closely monitored. These features make it easier for organizations to comply with regulations and standards like PCI-DSS, Consumer Financial Protection Bureau (CFPB) and Federal Information Processing Standards (FIPS) 140-2, and to cope with mandates from FFIEC, FINRA, the European Union, and other standard bodies and government agencies.

Secure Access and Mobile Device Management at Standard Bank

Standard Bank, Africa's largest bank, has 1,300 branches across 20 countries.

Gerdien Hay, Head of End-User Computing, explains, "We saw XenMobile® as the solution to managing the growing BYOD reality within the bank." Consequently, Standard Bank selected Citrix XenMobile Enterprise Edition and file sync and sharing with Citrix ShareFile®. The 10,000 XenMobile licenses provide secure access for mobile users to email and the bank's web applications, while also integrating with Standard Bank's existing XenDesktop/XenApp infrastructure to provide virtualized applications and desktops on mobile devices.

By combining MDM and MAM, XenMobile has not only secured the bank's business information used by remote workers across Africa, it has also provided a much improved user experience. Bank staff can securely access email, intranet sites and a range of centrally managed line-of-business applications on any device (bank-owned or personal), even on substandard connections – improving their productivity. At the same time, should a device ever be lost or stolen, access to sensitive resources can be withdrawn instantly.

Conclusion

Financial services organizations face numerous challenges in their quest to reduce business security risk and ensure compliance with regulations and standards. Citrix offers solutions that help them strengthen the five pillars of business security:

- Supporting advanced identity and access management with multi-factor authentication, identity and group-based authorization, context-based access control, and other features that strike the right balance between risk and simple access.

- Maintaining network security with centrally managed employee and customer portals for controlled access, advanced encryption, network segmentation, and features like rate limiting and load balancing that ensure high availability.

- Providing application security through features like centralized administration of apps, containerization of mobile apps, and protection against application-level attacks.

- Strengthening data security by centralizing protected information behind firewalls, creating secure containers for data on mobile devices, and promoting secure file sharing.

- Enhancing monitoring and response by providing detailed information on user activities and network flows, and extensive data and tools for auditing and compliance.

By strengthening the five pillars of business security, Citrix solutions help IT enhance customer service and empower financial services employees, without putting sensitive customer data at risk or impacting compliance.

For more information about Citrix solutions for financial services, visit citrix.com/financialservices.

Additional resources:

Secure app and data delivery for a mobile financial services workforce

Meeting financial services security and compliance requirements

Best practices for enterprise security

Appendix

Citrix Solutions for Financial Services Organizations

XenApp® and XenDesktop® for Secure App and Desktop Virtualization

Citrix XenApp® and Citrix XenDesktop® are application and desktop virtualization solutions. Windows, web, SaaS and Linux apps and desktops execute on central servers, but can be accessed securely from anywhere, on any device—including laptops, tablets, Chromebooks, desktop computers, thin clients and terminals.

XenMobile® for Secure Enterprise Mobility Management

Citrix XenMobile® is a comprehensive enterprise mobility management solution that manages and protects mobile devices, apps and data. It unifies the delivery of mobile, Web, SaaS and Windows applications to employees on all types of mobile devices, enforces device security policies for application and data access, and delivers MDM, MAM, and MCM capabilities.

ShareFile® for Secure Data Sync and Sharing

Citrix ShareFile® is an enterprise file sync and share (EFSS) solution that enables users to access, sync, and securely share files from any device. It allows IT to control where data resides in corporate datacenters or in the cloud, and provides centralized management, robust reporting, and DLP integration.

NetScaler® and NetScaler SD-WAN™ for Secure App Delivery

Citrix NetScaler® and Citrix NetScaler SD-WAN™ are networking products that help enterprises optimize, secure and control the delivery of enterprise apps and cloud services. NetScaler is an application delivery controller that provides load balancing, WAN optimization, and security services. NetScaler SD-WAN (formerly CloudBridge) is a software-defined WAN solution that combines multiple network paths into a single virtual WAN, for better performance, reliability and security.

CITRIX®

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