Manage risk by protecting apps, data and usage

Trusted to address risk management priorities by controlling application and data access across any location, network and device

Although billons of dollars are spent on security solutions, information remains vulnerable as new threat and attack vectors are emerging everyday and the volume of incidents is on the rise. The tools and processes implemented in the past are often too general in scope and do not adequately defend the organization today. Citrix helps organizations address risk management priorities by protecting sensitive information as business mobility and transformation imperatives—including mobile and distributed workforces, BYO, global operations, and third party consultants, outsourcing vendors, and partnerships—become the norm. Across every industry, including the most highly regulated sectors, customers rely on Citrix to assure privacy, protect sensitive information and enable compliance of apps and data without compromising workforce flexibility and productivity.

Information security requires a new approach

While IT continues to control the corporate network perimeter and manage many business applications, the perimeter of where work is done is evolving and expanding. Devices are now both corporate and personally owned, many users select cloud-based applications, employees no longer do all their work within a corporate facility and traditional office hours are a thing of the past. Together the multiplication of devices, apps and locations increases the security burden, and a new approach must be sought. This approach must enable workforce mobility where remote, flexwork, and telework are common, and consultants, contractors, partners and other third parties are part of the core team—but not generically part of the core network. Contextual access and controlled connectivity that mediates usage of corporate apps and data from various locations is a critical requirement. Organizations must be able to support yet separate personal apps, business apps and data on both managed and unmanaged devices (taking into account BYO as well as company-issued devices) without sacrificing security or introducing increased risk.

Additionally, organizations must ensure sensitive business data, personal information and IP are protected with strict enforcement of policies and complete visibility, reporting and auditing to achieve compliance. Ensuring continuity of operations by providing secure, high-performance access from anywhere, at any time, even during planned and unplanned disruptions is paramount.

Best practices to control apps and data

Here are some important best practices to control apps and data:

- **Focus on balancing security needs with user experience demands.** Rather than manage only the device, successful organizations take a holistic view of security where the focus is on balancing the user experience and productivity with security across devices, apps, data, networks and identity.
- **Enable flexible options for data storage, access and management.** With the convenience and cost benefit of a globally dispersed workforce, storing business information anywhere—from mobile storage to cloud apps—requires increased IT control on where information should reside and with whom it can be shared. Many organizations are looking for a flexible mix of centralized control across datacenter servers, cloud storage and endpoint containerization.
- **Offer rich policy engine for contextual controls.** Instead of giving users an all-access pass to the network, all of the time, enforce contextual security, which combines insights from personas and roles, where people are located at a given time, what type of device is being used and who owns it, as well as what type of information they are trying to access—allowing IT to set policies that manage contextual access to information including confidential and restricted data for all business scenarios.
- **Enable efficient compliance management and reporting.** Globally, organizations face more than 300 security and privacy-related standards, regulations and laws, with more than 3,500 specific controls. Security solutions should provide complete and automated monitoring, logging and reporting of data, user and network level activity to help respond to audits quickly, efficiently—and successfully.
- **Reduce the attack surface while lowering IT costs.** With an overall goal of reducing the attack surface, organizations can lower operational costs and reduce spend on individual security technologies, particularly for devices, by focusing on app and data security and usage. Organizations should deliver secure apps with encryption for data in use, data at rest, and data in motion.

A new mindset for specifically protecting information is the first step. The next is focusing on solutions that enable your organization to protect its most sensitive apps, data and usage.

Citrix security protects apps, data and usage

While people expect instant and convenient access to their data and apps on any device they use, along with the rich experience they're used to, businesses need to be able to assess and manage risk to sensitive information. With Citrix, organizations can provide the right level of confidentiality, integrity and availability for data without placing undue restrictions on the ways people choose to work. Citrix offers trusted solutions to address risk with powerful and flexible options to control identity and access, network security, app security, data security, monitoring and response across all scenarios. The core security pillars of the Citrix offering include:

Identity and access

- Authentication – Control and secure access to all apps including SaaS apps (e.g. Office 365) by providing two-factor authentication and federation
- Authorization – Provide appropriate levels of access specific to applications and resources based on group membership, location, and task
- Access Control – Perform endpoint analysis and enable contextual access control where access to resources is granted or restricted based on dynamic parameters such as the user's endpoint and other situational aspects

Network security

- Remote Access – Provide encrypted delivery of virtual applications and desktops to employees and third parties (contractors, vendors, partners) wherever they may be working
- Segmentation – Enforce network access control and dynamically segment networks and services to limit lateral movement throughout the network while assuring compliance and security
- Availability – Provide service optimization and load balancing with intelligent health monitoring to maintain the highest level of service uptime and performance

App security

- Centralization – Application and operating system patch management and configuration management are centralized to avoid inefficiency, inconsistency and security gaps
- Containerization – Provide a suite of securely containerized business productivity apps that have micro VPN access to organizational resources even from employee-owned smartphones and tablets
- Inspection – Provide protection against zero-day, logic flaws, and denial of service attacks against critical business services

Data security

- Centralization – Prevent data from residing on the endpoints by keeping data in the data center to mitigate against data loss and leakage due to lost, stolen, compromised or destroyed endpoints
- Containerization – Address insecure mobile data storage with containerization to separate personal and business apps along with their associated data to enforce segmentation at the app level and data encryption
- File Sharing – Enable file sharing within and outside the organization that has security built-in at every level from authentication, authorization, and auditing to DLP, encryption and expiry

Monitoring & response

- Visibility – Visibility into user level activity enables IT to triage performance degradation and quickly identify the source, whether on the endpoint, network, or server side
- Auditing – Multiple levels of monitoring and detailed logging exist to detect misconfigurations, attacks and usage patterns
- Compliance – Secure traffic from the endpoint to inside the data center using Common Criteria validated configurations and FIPS 140-2 capabilities across Citrix HDX protocols and Citrix NetScaler to comply with regulations and requirements and reduce the scope of audits

Citrix delivers across security pillars with a complete portfolio including XenApp and XenDesktop to manage apps and desktops centrally inside the data center, XenMobile to secure mobile applications and devices with a great user experience, ShareFile to provide controlled and audited data access, storage and sharing both on-prem and in the cloud, and NetScaler to contextualize and control connectivity with end-to-end system and user visibility. Citrix solutions also integrate with third-party security products for advanced levels of system management and identity, endpoint and network protection.

Citrix is proven and trusted to protect the most sensitive information

As organizations focus on introducing new technologies to enable business and personal mobility, dynamically assessing and managing risk is crucial. And, these risks must be managed while delivering all apps (Windows, web, SaaS and mobile), building agile data centers and leveraging cloud services. Citrix is trusted to protect our customers' most sensitive information, giving powerful options to control application and data access across any location, network and device. At the same time, employees, contractors and partners have the flexibility to choose how they work. Simple and secure access to their virtual workspace with all the resources they need whether remote, mobile or in the office allows them to best perform their job. Moreover end-to-end visibility of connections, traffic and user activity allows IT to address privacy, compliance and risk management priorities without compromising workforce productivity and workplace transformation initiatives.

No other vendor offers the breadth of app, data and networking security proven to protect and secure the world's most important apps—the apps businesses run on. Best-of-breed technologies for security and integration across app, data and usage makes Citrix the clear choice for protection of sensitive information, privacy and compliance without compromising workforce flexibility and productivity.

Learn more about Citrix security at www.citrix.com/secure.

CITRIX®

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.