CITRIX®

White Paper

Delivering the Secure Workspace of the Future

A state of the secure enterprise report by Stan Black, SVP, Chief Security and Information Officer, Citrix, and 2018 Cybersecurity Professional of the Year

Table of contents

I doubt Lennon and McCartney were contemplating the need for a more holistic security framework when they penned the lyrics "all together now." But those three words couldn't more aptly describe what Citrix is doing to solve today's complicated IT security environment. Historically, Citrix has delivered security-enabling technologies in the context of our functional solutions for virtualization, mobility management, networking, and business file sync and sharing (BFSS). Now, as the network perimeter is opened and extended to include SaaS apps, cloud services, BYO devices, and other innovations, our customers seek a more holistic security framework. We're delivering "all together now" so organizations are no longer stunted by an IT environment made up of disjointed legacy and emerging technologies. Citrix is unifying the management of users and capabilities across hybrid, multi-cloud and multi-device environments with a comprehensive suite of technologies.

Traditional security technologies focus on adding layers of defense or identifying threats, resulting in complexity and burdened user experience. As we see too often in the news, this disconnected approach didn't solve the security problem. Our goal is to provide an experience that's simple to use — intuitive — and secure. Not many companies hit that sweet spot. It's often security OR simplicity, but not both.

That's what we've changed at Citrix. We offer choice, simplicity and a great user experience. My job as chief security and information officer is to make sure you get all the applications and data you need, wherever you are, whatever device you're on and over any network or cloud you choose. And to make sure that wherever your data is, it's secure and accessible — always. My goal is to make sure all this is done behind the scenes, so you don't see those annoying error pop-ups like "device is out of policy" or "location invalid."

While we wouldn't call ourselves a security vendor in the traditional sense, we've always considered data protection and risk management central to our value proposition. That was true in the early days of virtualization and remote access, and it's even more true in today's era of hybrid infrastructures and the anywhere, any-device workforce.

By focusing on our core principles of experience, choice, and simplicity, we're able to securely deliver applications and data to more than 400,000 organizations and over 100 million users globally.

Again, this view aligns closely with the Citrix approach to security. Because we've always designed our products around centralized control over apps and data, security is built into the core of our solutions. Cybersecurity is front and center across almost every industry. By focusing on our core principles of experience, choice and simplicity we're able to securely deliver applications and data to the more than 400,000 organizations and over 100 million users globally of Citrix technology.

Our approach to security starts from within

Here at Citrix, we are Customer One. We use our own products to simplify, manage and secure what was once an incredibly complex IT environment. But not only that, we've made some organizational changes that allow us to streamline operations and develop creative solutions to security and IT challenges.

We unified our security and IT teams to work closely with key stakeholders to implement strategy and process for developing more secure products that reduce IT complexity and help facilitate policies that add visibility to find and stop threats faster. This structure also creates more opportunity to expand skill sets and drive career progression — which makes happier employees and a better place to work.

Our new Security Ninja program aims to unify IT, security, product development, and engineering to deliver secure products more efficiently. Through this program, team members can improve awareness and education on the practice of developing software, policies, and technology with a constant focus on security during the entire software development life cycle.

We are now evolving our solutions to deliver transparent control of data at rest, in motion, and in use, and extend validated protection throughout the data lifecycle. This will allow our customers to leverage the full IT and business benefits of the cloud—and a whole generation of digital innovation—without sacrificing security and control.

How we govern security at Citrix

As the Chief Security and Information Officer, I'm responsible for overall security governance at Citrix. We developed a Global Security Framework (GSF) to provide the overarching security and safety principles for our team to follow. Management from different functions across the company participate in the GSF governing body, which develops, sets, and reviews policies and standards for security at Citrix. We conduct regular reviews, evaluations and reports on the maturity and continuous growth of the program.

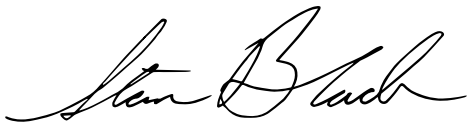
Security starts with people. Citrix personnel undergo legally permitted background checks prior to employment; employees in sensitive positions are also subject to periodic post-hire screenings. All employees are subject to confidentiality obligations and must comply with the Citrix Code of Conduct and Acceptable Use Policy. We maintain an innovative security awareness and training program, which includes live events, frequent communications, and role-based security engineering training.

Citrix's business continuity program covers people, processes and technology, and we make full use of our product line to ensure our customers don't have service interruptions when our office locations are affected by disasters. We test our recovery plans quarterly.

We use multiple mechanisms to enforce operational security policies and standards internally and across our services, including, as appropriate: layered network architecture, continuous monitoring and response, patch and vulnerability management, malware protection, strong authentication, role-based identity and access management, and regular access reviews. Our incident response program guides our team as they contain, analyze, remediate and communicate security and safety incidents impacting Citrix managed networks and/or systems.

Our products are only as secure as our development processes. Citrix's Secure Development Lifecycle includes standards and change control procedures designed to address security requirements of information systems, code review and testing, and security around the use of test data. A specialized security engineering team manages and monitors this process. They're also responsible for design review, threat modeling, manual code review and spot checks, and penetration testing. We use a software-based system for managing open source reviews and approvals, and periodically scan and audit our products for open source compliance.

I invite you to learn more about how we reduced operational security costs over 30 percent year-over-year, while improving our end users' experience.



Stan Black
Chief Security and Information Officer, Citrix

Citrix Security Controls — Summary

Following is a summary of the physical, logical and administrative controls Citrix uses across services as of the date of publication. This summary may be updated from time to time; the current version will be posted at:

https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html

Security Focus	Control(s)
Security Program Management	**Security Ownership** Citrix has appointed one or more security officers responsible for coordinating and monitoring the security controls for the services. **Security Roles and Responsibilities** Citrix personnel with access to customer content are subject to confidentiality obligations. **Service Security Policies** Citrix maintains a comprehensive Global Security Framework (GSF), which provides the overarching security and safety principles established and approved by Citrix executive management. Policies provide security requirements in a clear and concise manner. Standards define the process or methodology of meeting policy requirements. The GSF security program undergoes regular reviews and evaluations. Citrix maintains a summary of the GSF program and will provide it to customers upon request. **Product Risk Management** Citrix performs assessments of key areas of risk associated with the services including, by way of example only and as applicable, privacy risk assessments, open source reviews and export control analysis.
Asset Management	**Asset Inventory** Citrix maintains an inventory of Citrix-managed equipment used to perform the services ("Assets"). Identified system owners are responsible for maintaining and updating the inventory as needed. **Asset and Data Handling** Citrix identifies and classifies customer content to ensure access is appropriately restricted. Citrix imposes restrictions on printing customer content and disposing of printed materials that contain customer content. Citrix personnel must obtain authorization prior to storing customer content on portable devices, remotely accessing customer content, or processing customer content outside facilities managed by Citrix or its service providers.
Customer Security Obligations	The customer is responsible for managing security not expressly included as part of the services. This includes, but is not limited to: • Limiting Citrix's customer content access to only to what is needed for customer to receive the services. • Protecting its network and service components against interference, including monitoring and securing its networks and computing equipment. • Downloading customer content where needed, both during the term of services and upon termination. • Citrix either encrypts data in transit by default or offers customers means to encrypt data in transit. Further detail is provided in the product documentation for the services. Customer is responsible for ensuring that data is appropriately secured in transit.

Security Focus	Control(s)
Access Management	**Access Policy** Citrix maintains a record of security privileges of individuals having access to customer content and follows the principle of least-privilege. **Access Authorization** Citrix maintains and updates a record of personnel authorized to access Citrix systems that contain customer content. New access to systems is reviewed and approved by management prior to being granted. Citrix performs regular reviews of user accounts and assigned permissions for key systems. Citrix identifies those personnel who may grant, alter, or cancel authorized access to data and resources. Citrix ensures that where more than one individual has access to systems containing customer content, the individuals have separate identifiers/log-ins. **Least-Privilege** Citrix restricts access to customer content to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** Citrix requires that users secure computers and data while unattended. Citrix requires that passwords remain unintelligible throughout their lifecycle. **Authentication** Citrix uses industry-standard practices to identify and authenticate users accessing information systems. Where authentication mechanisms are based on passwords, Citrix follows industry-standard practices for password handling and management, including: • Passwords are renewed regularly, as dictated by system requirements and Citrix standards • Passwords must meet length and complexity requirements, including a minimum length of 8 characters • Personnel are prohibited from sharing passwords • De-activated or expired identifiers are not granted to other individuals Citrix maintains procedures to deactivate passwords that have been corrupted or inadvertently disclosed. Citrix monitors repeated attempts to gain access to the services using an invalid password. Citrix uses practices designed to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored.
Loss Prevention	**Malicious Software** Citrix uses anti-virus software and other controls to avoid malicious software gaining unauthorized access to customer content, including malicious software originating from public networks. **Media Disposal** Citrix disposes of media when no longer required based on classification and using secure deletion processes.

Security Focus	Control(s)
Physical and Environmental Security (Access Control, Availability Control)	**Physical Access to Citrix Facilities** Citrix limits facilities access to authorized individuals. ID badges are required for employees, contractors and guests and must be visible at all times when in the facility. Citrix monitors facility entry points using various methods including security guards, intrusion detection and CCTV cameras. **Protection from Disruptions** Citrix uses systems to protect against loss of data due to power supply failure or line interference, including global and redundant service infrastructure that is set up with disaster recovery sites; evaluating data centers and Internet service providers (ISPs) to optimize performance regarding bandwidth, latency and disaster recovery isolation; situating data centers in secure facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy; and uptime agreements from key suppliers. **Hosted Data Centers** When Citrix uses third-party co-located data centers for provision of the services, Citrix requires that the service provider meets or exceeds the physical and environmental security requirements of Citrix-managed facilities. Minimum security requirements include, but are not limited to: • Physical access restrictions and safeguards (authentication, logs, monitoring, etc.) • Adequate separation of environments • Fire suppression, detection, and prevention mechanisms • Climate control systems (temperature, humidity, etc.) **Cloud Computing** When Citrix uses XaaS [Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)] for provision of the services, Citrix contracts with XaaS providers that provide a materially similar level of physical access control to its hosted data centers.
Application and Development Security	**System Development & Maintenance** Citrix maintains a Secure by Design process, which includes standards and change control procedures designed to address security requirements of information systems, code review & testing, and security around the use of test data. This process is managed and monitored by a specialized security engineering team, which is also responsible for design review, threat modeling, manual code review & spot checks, and penetration testing. **Open Source Management** Citrix uses a software-based system for managing open source reviews and approvals. In addition, Citrix conducts periodic scans and audits of its software products to confirm open source compliance. **Change Management** Citrix maintains change control procedures that address security requirements of information systems, testing, acceptance of testing, and security around the use of test data. Software and configuration changes are managed and tracked using standard ticketing systems.

Security Focus	Control(s)
Secure Operations	**Network Design** Citrix implements mechanisms designed to enforce access management policies and standards across the services, including network controls over access to customer content. These include, as appropriate: configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic; and separating web and application servers from the corresponding database servers in a tiered structure that restricts traffic between the tiers.
Incident Management	**Incident Response** Citrix maintains an incident response program designed to contain, analyze, remediate and communicate security and safety incidents impacting Citrix managed networks and/or systems or customer content. **Incident Notification** If Citrix determines that customer content within its control has been subject to a security incident, the customer will be notified within the time period required by applicable law. **Incident Recording** Citrix maintains a record of known security incidents with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, and the procedure for recovering data and services as applicable.
Vendor Management	**Onboarding** Citrix performs security assessments of service providers that will have access to customer content and/or to components of the services that process customer content. Citrix requires service providers connected with the services to comply with the level of security which are applicable to the services they provide. Service providers that may access customer content subject to European Union law are required to self-certify to EU-U.S. and EU-Swiss Privacy Shield programs or to execute Standard Contractual Clauses. **Ongoing Maintenance** Service providers are assessed periodically, based upon the sensitivity and risk associated with their services. **Off-boarding** Upon termination of a supplier relationship, the service provider is required to return all customer content in its possession or to certify that all customer content has been securely destroyed.
Business Continuity and Disaster Recovery	**Business Continuity** Citrix maintains emergency and contingency plans for the facilities in which Citrix information systems that process customer content are located. **Disaster Recovery** Citrix's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer content in its original or last-replicated state.

Additional Controls for Cloud Services

Security Focus	Control(s)
Data Protection (Availability Control, Transmission Control, Data Deletion)	**Failover Procedures** Citrix implements mechanisms designed to address loss of availability of customer content, including storing copies of customer content in a different place from where the primary computer equipment processing the customer content is located. **Data Beyond Boundaries** Citrix encrypts or enables the customer to encrypt customer content that is transmitted over public networks that are part of a Service. **Retention** Citrix may retain customer content following the service period and archiving for customer access where required for legal purposes. Citrix will comply with the requirements until such customer content has been permanently deleted. Citrix is under no obligation to retain customer content following termination of the service. **Return** Subject to availability and the applicable services description, the customer has thirty (30) days to download customer content after expiration. **Data Deletion** Citrix will securely delete customer content when no longer needed for a legitimate purpose.
Secure Operations	**Event Logging** In certain services, Citrix collects logs. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant activity. Logs are used (i) for providing, securing, managing, measuring and improving the services and associated analytics, (ii) as directed or instructed by the customer and its users, and/or (iii) for compliance with Citrix policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the services and related components. The customer may not block or interfere with this monitoring. Citrix may supplement logs with information collected from third parties for the purposes specified above. Logs may be used only in aggregate form for purposes that not specified in the agreement or terms.
Business Continuity and Disaster Recovery	**Back-ups** Except where otherwise noted in the respective services description, services are maintained in high availability, active-active clusters spanning multiple physical sites. Systems not maintained in an active-active configuration are backed up according to the specific service's Service Level Goals.

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

©2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).