PCI DSS Success: Achieve Compliance and Increase Web Application Security

Protect web applications and cardholder information with solutions from Citrix

CITRIX®

Beginning in January of 2015, all entities that store, process, or transmit cardholder data (CHD) will be subject to version 3.0 of the Payment Card Industry Data Security Standard (PCI DSS). Although the changes introduced in this latest revision are relatively modest in scope, achieving and demonstrating compliance with its approximately three hundred individual requirements will still be a significant challenge, and investment, for most organizations.

This white paper examines the prevailing conditions driving evolution of the PCI DSS and the resulting challenges facing today's IT departments. It explains how Citrix® application delivery, virtualization and mobility solutions can help ease the PCI compliance burden while substantially improving the resiliency and security of an organization's business-critical web applications. By leveraging Citrix NetScaler®, XenDesktop®, XenMobile® and other related components, IT security and compliance teams can:

- Tightly control who has access to and maintain isolation of all corporate systems involving CHD – including for remote/mobile employees and external users.
- Reduce the total cost of PCI compliance by satisfying numerous individual requirements with a tightly integrated platform for delivering and protecting IT services.
- Reap the rewards of capabilities that go above and beyond the minimum requirements of the PCI DSS to not only provide superior protection against today's threats but also deliver a future-proof compliance solution capable of keeping up with the standard as it continues to evolve.

The net result is a solution set that enables businesses to streamline PCI compliance, both now and in the future, while also ensuring the availability, accessibility and security of business-critical applications and services.

The Threat: No Signs of Slowing Down

The original issues leading to the development and ensuing enforcement of the PCI DSS are alive and well today. If anything, in fact, the situation has gotten substantially worse in recent years. Just consider the following statistics:

- Between 2009 and 2013, global losses from payment card fraud increased 100%, from $7 billion to $14 billion[1].
- Between January 2008 and October 2014, the total number of records containing sensitive personal information involved in security breaches in the United States since 2005 increased nearly 330%, from 217 million to 930 million[2].
- According to the Verizon 2014 PCI Compliance Report, payment card data remains one of the easiest types of data to convert to cash – which is why 74 percent of attacks on retail, accommodation, and food services companies target this type of information[3].

1. http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3
2. http://www.privacyrights.org/data-breach
3. http://www.verizonenterprise.com/pcireport/2014/

- In a survey conducted by Software Advice, more than three-quarters of consumers indicated they would be less likely or completely unwilling to buy products from a company that allowed their personal data to be compromised[4].

High-profile breaches of major retailers, financial institutions and a wide variety of other businesses that process credit card data only serve to further demonstrate the need for better protection of sensitive customer information.

The Response: Evolution of the PCI DSS

To address mounting threats and account for the steady adoption of new technologies and delivery models, the PCI Security Standards Council has a plan in place to review prevailing conditions and issue updates to the PCI DSS approximately every three years. Consistent with this objective, version three of the standard, published in November of 2013, starts being enforced by auditors as of January 1, 2015.

This latest iteration of the PCI DSS retains and builds on the same framework of core requirements used from the beginning (see Table 1). In fact, the vast majority of changes in version 3 are relatively minor tweaks that only clarify existing sub-requirements.

PCI Data Security Standard – High Level Overview

Organizing Principles	Core Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personne

source: page 5 of https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

4. http://www.internetretailer.com/2014/07/17/consumer-confidence-shifts-physical-online-retailers

As for entirely new or significantly enhanced sub-requirements, version 3 introduces twenty of those. Notable examples include:

- New requirement 1.1.3, for a current diagram that shows cardholder data flows.
- New requirement 2.4, to maintain an inventory of system components in scope for PCI DSS to support development of configuration standards.
- New requirement 6.5.10, for coding practices to protect against broken authentication and session management.
- New requirement 8.5.1, for service providers with remote access to customer premises to use unique authentication credentials for each customer.
- New requirement 11.3.4, to perform penetration tests to verify that the segmentation methods used to isolate the cardholder data environment (CDE) from other networks are operational and effective.

For reference purposes, a complete summary of all clarifications, enhanced requirements, and new requirements incorporated in version 3 of the PCI DSS can be obtained here: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

PCI Compliance Challenges

Taken individually, few, if any, of the new requirements or other changes introduced with version 3 of the PCI DSS qualify as being particularly onerous. This doesn't change the fact, however, that achieving, maintaining and demonstrating compliance with the PCI DSS in its entirety requires a significant investment of time, effort and financial resources by those organizations that are subject to it. Related challenges to also acknowledge include the fact that being compliant does not necessarily translate into being adequately protected from advanced cyber threats, and that web applications, in particular, require closer attention due to the relative degree of risk they present.

Compliance requires a significant investment

Achieving compliance with the PCI DSS means having and maintaining an answer for approximately three hundred requirements for each and every system component included in or connected to the organization's CDE.

To reduce their compliance burden, security and networking teams need to fully exploit network segmentation techniques and technologies that can effectively isolate their organization's CDE and shrink the amount of infrastructure designated as in-scope. Along with trimming the cost and complexity of PCI compliance, such an approach improves an organization's ability to contain the spread of threats and simplifies associated troubleshooting and forensic efforts.

For those components that remain in scope, a second strategy to reduce compliance cost and complexity is to focus on solutions that simultaneously address numerous requirements, ideally in a tightly integrated manner. Not only is the alternative of having many more solutions – each of which only covers a few requirements – often prohibitive from a cost perspective, it also leads to a highly fragmented security architecture and increased likelihood of "events of significance" slipping through the resulting gaps.

Compliance doesn't equal security

The PCI DSS itself indicates that it is only a "baseline" of requirements for protecting CHD. In other words, it represents a minimum standard of due care, rather than a comprehensive treatment of everything any given organization needs to do to sufficiently defend its CDE.

Compounding this situation is the nominal three-year period between updates to the PCI DSS. The delay this introduces pretty much guarantees that the specified requirements lag behind significant changes to the technology and threat landscapes, which are unfolding at a much quicker pace.

The net result is that security teams will typically need to go above and beyond the requirements of the PCI DSS, both to adequately defend against emerging threats and to more closely match their organization's actual tolerance for risk.

Web applications require more attention

As the front door to all sorts of lucrative information, including CHD, web applications lie squarely in the crosshairs of today's hackers. It also doesn't help matters that web applications and the technologies used to build them have proven to be notoriously vulnerable. Just consider the following statistics, all from 2013[5]:

- 77% of public websites scanned were found to contain vulnerabilities
- 1 in 8 websites was found to contain a critical vulnerability, making it relatively easy for hackers to gain access to sensitive data, alter the website's content, or compromise visitors' computers
- Approximately 67 percent of websites used to distribute malware were identified as legitimate, compromised websites

Another significant challenge is the increasing complexity of web properties and the diversity of components now requiring protection. These include:

- Cloud-hosted web apps/sites and content delivery networks
- SaaS and other cloud delivery options, such as platform as a service (PaaS) and infrastructure as a service (IaaS), where the enterprise owns and controls progressively less of the solution
- Mashups, where content is dynamically pulled together from numerous external sites
- Mobile solutions, where device-side micro apps communicate to sophisticated web-based back ends

Strictly speaking, the issue here is not a deficiency with the PCI DSS. Section 6.6 already acknowledges the need to protect public-facing web applications by requiring organizations either to assess them for vulnerabilities or front-end them with an automated solution for detecting and protecting web-based attacks, such as a web application firewall. Instead, the issue is one of organizations not pursuing these and other complementary measures as broadly or deeply as they actually need to be performed to sufficiently address the associated risks.

As a starting point for remedying this situation, security and compliance teams should consider the set of recommendations outlined in Appendix 1, "A Recipe for Web Application Protection and Compliance." To further address the challenges of PCI compliance, they should also consider the market-leading solutions from Citrix discussed in the following sections.

Citrix Solutions That Help with PCI Compliance

Used either individually or in conjunction with one another, each of the following Citrix solutions provides organizations with an extensive array of capabilities to help ensure the security, accessibility, and usability of their business-critical web applications. Equally important is how they help organizations achieve compliance with the PCI DSS.

5. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Citrix NetScaler

Citrix NetScaler is an all-in-one application delivery controller that enables organizations to address all of their web application security and optimization needs with a single, strategic platform. In addition to supporting NetScaler AppFirewall and NetScaler Gateway™ as tightly integrated software modules, NetScaler provides an extensive set of load balancing, application acceleration and infrastructure-layer security capabilities – including extensive protections for DDoS attacks. The result is a highly cost effective solution that thoroughly secures an organization's web applications at the same time that it substantially enhances their performance, accessibility, and availability. With NetScaler MobileStream, these same capabilities and benefits are extended to also ensure optimal performance and security for mobile networks and services.

NetScaler AppFirewall

NetScaler AppFirewall™ is the industry's highest performing, ICSA-certified and NSS Labs Recommended solution for protecting web and web services applications from all known and zero-day application-layer attacks[6]. Featuring a hybrid security model, NetScaler AppFirewall blocks all deviations from normal application behavior while efficiently scanning for thousands of automatically updated threat and vulnerability signatures. It analyzes all bi-directional traffic, including SSL-encrypted sessions, to protect against an extensive range of threats without any modification to the applications its defending.

In support of PCI security audits, NetScaler AppFirewall can generate a comprehensive report that not only details all security protections defined in the application firewall policy that pertain to PCI requirements, but also highlights those configuration settings that are "out-of-compliance." In addition, administrators can configure it to prevent the inadvertent leakage or theft of sensitive information, such as credit card numbers or custom-defined data objects, by either removing or masking content from application responses, so that sensitive information is not disclosed to anyone without a "need to know."

NetScaler Gateway

NetScaler Gateway is a secure application, desktop and data access solution that gives IT administrators granular application-level and device-level policy and action controls over access to corporate content, while allowing users to work from anywhere using SmartAccess and the XenMobile Micro VPN technologies. It provides a single point of control and tools to help IT administrators ensure compliance with regulations and protect corporate information with the highest levels of security, both within and outside the enterprise. At the same time, NetScaler Gateway empowers users with a single point of access—optimized for roles, applications, devices and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

Citrix XenDesktop

XenDesktop is a comprehensive desktop virtualization and VDI solution that delivers a complete Windows desktop and application experience as an on-demand cloud service. With XenDesktop, IT teams can quickly and securely deliver any type of virtual desktop or Windows, web and SaaS application to any PC, Mac, tablet, smartphone, laptop or thin client – all with a high-definition user experience.

In terms of PCI compliance, a major advantage of XenDesktop is that it introduces an operating model that effectively isolates client networks and devices from the datacenter and CDE,

6. http://www.citrix.com/content/dam/citrix/en_us/documents/oth/web-application-firewall-comparative-analysis.pdf

thereby allowing them to be designated as "out of scope." With XenDesktop, general-purpose, always-on and full-network layer connections can be replaced with tightly controlled and monitored access to individual applications and resources. Moreover, the nature of this "access" is such that while users retain all of the application functionality they are used to, the target resources – including all CHD and other sensitive data – never leave the CDE/datacenter.

Citrix XenMobile

XenMobile is a comprehensive solution for managing mobile devices, apps and data. With XenMobile, users have single-click access to all of their mobile, SaaS and Windows apps from a unified corporate app store, while IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. Users get the freedom to experience work and life their way, while IT gets the capabilities and control it needs to extend protection across the mobile environment and ensure compliance with applicable standards and regulations.

Key features and capabilities IT teams can leverage to help achieve PCI DSS compliance include the following:

- Tight integration with NetScaler Gateway melds "need to know" with "secure enough to know" by delivering the ability to tightly control which users have access to which resources, under which specific operating conditions and from which devices.
- The Micro VPN features replaces full network-layer connections with secure, per-application tunnels, thereby reducing the potential for users (or hackers) to "hop around" and gain access to other, unauthorized systems and resources.
- For Worx-enabled mobile apps, a dedicated, encrypted workspace provides protection for all sensitive data regardless of who owns the client device.

Meeting and Exceeding Multiple PCI Requirements

Together, the Citrix solutions introduced in the previous section provide a tightly integrated platform that enables enterprise security and compliance teams to meet and, in many cases, exceed numerous PCI DSS requirements.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The Citrix platform can be used to deny all traffic from untrusted networks and hosts (requirement 1.2) by restricting connections to:

- Approved protocols and methods.
- Sessions originating from trusted networks and devices.
- Authenticated users with right levels of authorization for the resources being accessed.
- Precisely the individual resources needed, as opposed to entire segments/networks.

It can also be used to facilitate implementation of a DMZ (requirement 1.3) by providing highly secure, fully locked-down intermediary devices for brokering, controlling and monitoring traffic from/to the Internet.

Requirement 2: Protect stored cardholder data

Logging capabilities can be configured to omit card verification codes, personal identification numbers (PINs) and primary account numbers (PANs) from transaction and activity logs (requirements 3.2.2, 3.2.3, and 3.4). In addition, NetScaler AppFirewall can mask or block PANs (requirement 3.3) and otherwise prevent leakage of CHD, regardless of programmer oversight, logic flaws or targeted attacks.

FIPS 140-2, Level 2 compliant versions of NetScaler, NetScaler AppFirewall and NetScaler Gateway provide secure storage for the keys and certificates used for encryption of cardholder data and all application-specific and network-layer connections/tunnels (requirement 3.5.2).

Requirement 3: Encrypt transmission of cardholder data across open, public networks

Each of the Citrix solutions can be used to SSL-enable applications that were not designed to use secure communications protocols (requirement 4.1). In addition, the NetScaler AppFirewall can inspect the contents of all SSL/TLS encrypted sessions, ensuring session validity and blocking attacks – a capability that is not generally available in traditional network firewall and intrusion prevention products.

Requirement 4: Protect all systems against malware and regularly update anti-virus software or programs.

Integral device inspection capabilities can deny access and alert administrators when client anti-malware solutions are out-of-date, disabled, or otherwise misconfigured (requirements 5.2 and 5.3). Going above and beyond the letter of the PCI DSS requirements, the Citrix platform also provides an additional layer of malware protection for all devices and systems by delivering a robust set of network-based defenses for both known and unknown threats.

Requirement 5: Develop and maintain secure systems and applications

As discussed previously, NetScaler AppFirewall provides unparalleled protection against threats and vulnerabilities targeting modern web applications and services, in all of their diverse and complex forms.

Requirements 6/7: Restrict access to cardholder data by business need to know / Identify and authenticate access to system components

The Citrix solutions support all of the associated sub-requirements. Robust policy development and enforcement capabilities enable granular control over who has access and to which specific information resources. Support is provided for multiple user authentication mechanisms, including the use of two-factor methods for remote access scenarios, and all passwords are encrypted during transmission.

Conclusion

Citrix application delivery, desktop virtualization, and mobility management solutions substantially reduce the burden of achieving, maintaining and demonstrating compliance with the Payment Card Industry Data Security Standard, while simultaneously improving the security, accessibility, and performance of an organization's web applications and mobile services. By taking advantage of Citrix NetScaler, NetScaler AppFirewall, NetScaler Gateway, Citrix XenDesktop and Citrix XenMobile IT security and compliance teams can:

- Tightly control who has access to and maintain isolation of all corporate systems involving cardholder data – including for remote/mobile employees and external users.
- Reduce the total cost of PCI compliance by satisfying numerous individual requirements with a tightly integrated platform for delivering and protecting IT services.
- Reap the rewards of capabilities that go above and beyond the minimum requirements to not only provide superior protection against today's threats but also deliver a future-proof PCI compliance solution capable of keeping up with the standard as it continues to evolve.

For more information on Citrix NetScaler and other solutions from Citrix, please visit www.citrix.com.

Appendix 1: A Recipe for Web Application Protection and Compliance

The following recommendations outline an approach organizations can use to improve the security of their web application environments and cost effectively ensure compliance with applicable PCI DSS requirements.

Recommendation #1 – Establish and minimize the scope of the problem

Inventory all web applications and associated data stores. Eliminate all instances of capturing/storing prohibited information. Re-assess the need to handle and/or store all other cardholder information. If it is not needed, then it should not be processed/stored. Follow the other recommendations below to ensure that all remaining cardholder data is efficiently and effectively protected at all times.

Recommendation #2 – Approach PCI DSS compliance sensibly

Although requirement 6.6 of the PCI DSS presents a choice between conducting code reviews and installing an application layer firewall, organizations need to understand that the best approach is to implement both of these measures. That said, if a choice must be made – perhaps due to financial constraints – then organizations should favor the approach of using an application layer firewall because of the numerous advantages it yields, including delivering protection that is continuous, that accounts for both known and unknown attacks, and that accommodates multiple applications simultaneously.

Recommendation #3 – Approach PCI DSS compliance strategically

To the extent possible, ensure that actions taken to fulfill a specific requirement can actually be leveraged to support multiple requirements, or at least help address other needs the enterprise has – including compliance with other regulations. Overall, this strategy should not be difficult to pursue, especially since the requirements of the PCI DSS are fundamentally sound security practices that can be applied to all types of data and computing resources. For example, web application firewalls: (a) can be used to address numerous PCI DSS requirements, (b) can be used to protect more than just CHD, and (c) at least in the case of the Citrix offering, can be deployed in the form of a full-featured application delivery controller that also provides substantial performance and availability benefits.

Recommendation # 4 – Approach PCI DSS compliance as an ongoing/continuous effort

On one hand, compliance must be re-validated annually. On the other hand, an even more important concern is that the organization does not suffer a loss/theft of cardholder data, at any time, period. As a result, security operations personnel should routinely audit the usage logs for web applications to help detect any abnormal or unauthorized activities that might be occurring. Furthermore, organizations need to account for the fact that web applications are rarely static; they are always being modified to incorporate new

functionality. As a result, the security team will need to periodically re-assess all web applications to ensure they are still handling sensitive information properly. In this regard, a web application firewall could be used (a) to alert an administrator of any changes in application behavior that may result in violations, and (b) to mitigate the deficient condition until such time that the application is fixed. Finally, it is also unlikely that the applicable requirements will remain static. Organizations, therefore, must monitor the activities of the PCI Security Standards Council and be prepared to address any new requirements that emerge. Once again, a robust web application firewall could be a boon in such a situation based on its potential to support compliance without having to modify all of the affected applications.

Recommendation #5 – Approach compliance realistically

Despite all of an organization's best efforts, the potential for a security incident involving cardholder data will always remain. Stakeholders must manage expectations accordingly and be prepared for such a situation. Having the appropriate people, processes, and technology in place in advance is critical to being able to execute a swift response and minimize the impact – including any fallout from governing regulatory bodies.

Recommendation # 6 – Be sure to secure the back end

Web applications rarely operate alone. They may be the primary interface for handling data, but they almost always rely on databases as well. Thus, organizations ultimately need to implement appropriate security measures for these crucial back-end components too, including: access control, data encryption, and logging/auditing for all data access and configuration activities.

Appendix 2: PCI Security Requirements Supported by Citrix Solutions

Citrix application networking, virtualization, and mobility solutions support many of the approximately three hundred requirements specified in the PCI DSS, as summarized in the following table.

PCI DSS Requirement	Supported Sub-Requirements	Description of Capabilities
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.2, 1.2.1, 1.3, 1.3.1, 1.3.8	Features such as SmartAccess, Micro VPN and centralized authentication and authorization capabilities enable administrators to fully implement a least privileges access control model for all networks involving cardholder data (i.e., deny all users, devices, applications, and data except for that which is necessary). Availability of security-hardened appliances facilitates creation of DMZs to act as buffer zones between the Internet and internal CDE networks and systems.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.2, 2.2.3, 2.3	The NetScaler/NetScaler AppFirewall PCI Compliance Report indicates whether the default password has been changed for the system's root account and flags use/availability of insecure management protocols or interfaces. In addition, all solution components require user authentication and implement strong encryption for all non-console and remote administration sessions, whether the component is accessed directly or via the applicable central management system (e.g., Command Center).

Requirement 3: Protect stored cardholder data	3.2, 3.2.2, 3.2.3, 3.3, 3.4, 3.5, 3.5.2	NetScaler AppFirewall enables masking/blocking of Primary Account Numbers (PANs), and a confidential logging feature can be utilized to keep all PANs and other sensitive authentication data (SAD) from being logged. FIPS 140-2, Level 2 compliant hardware appliances, provides secure storage of private keys used for encrypting cardholder data and related communication sessions.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	4.1, 4.2	Secure remote access is enabled by a full-featured SSLVPN capability. In addition, the Micro VPN feature enables secure tunnels to be established in an even tighter, per-user, per-application manner.
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	5.2, 5.3	Integral device inspection capabilities can deny access and alert administrators when client anti-malware solutions are out-of-date, disabled, or otherwise misconfigured.
Requirement 6: Develop and maintain secure systems and applications	6.6	NetScaler AppFirewall, available either as a standalone solution or an integrated module of the NetScaler application delivery controller, is an ICSA-certified solution that provides fully automated protection of public-facing web applications and web services from both known and unknown threats.
Requirement 7: Restrict access to cardholder data by business need to know	7.2, 7.2.1, 7.2.2, 7.2.3	Granular, policy-based control over users, applications, devices and data enables organizations to implement definitive least privileges access control that truly limits access to cardholder data based on business need to know, with "deny all" for everything else. Tight integration with Active Directory and other identity stores, plus support for role based access control, enables enforcement of privileges assigned to individuals based on job classification and function.
Requirement 8: Identify and authenticate access to system components	8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.3, 8.5, 8.6	Native capabilities and tight integration with Active Directory and other identity stores support a wide range of authentication policies, including: use of unique user IDs, immediate revocation for terminated users, culling of inactive accounts, lockout after a specified number of failed login attempts, lockout duration, idle session timeouts, and password reset and minimum strength requirements. Support is also provided for several forms of multi-factor authentication, including tokens and smartcards.
Requirement 9: Restrict physical access to cardholder data	n/a	n/a
Requirement 10: Track and monitor all access to network resources and cardholder data	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.6, 10.6.1, 10.6.2, 10.6.3	Extensive logs/audit trails are maintained for all device configurations, system changes, alerts, access sessions and detected/prevented threats. Daily and periodic review of log data is supported with both native, customizable reporting capabilities and the ability to write log data to a syslog server for archival and analysis by third-party management solutions (including popular security event and information management systems).
Requirement 11: Regularly test security systems and processes	11.4	NetScaler delivers multi-layer protection against distributed and non-distributed denial of service attacks designed to take down an enterprise's external-facing services, or mask other threats/attacks intent on finding and ex-filtrating sensitive data. In addition, NetScaler AppFirewall uses an automatically updated database of signatures to scan for and block a wide range of known threats and vulnerability-based exploits.
Requirement 12: Maintain a security policy that addresses information security for all personnel	n/a	n/a

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

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 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.