



# PCI DSS success: Achieving compliance and increasing Web application availability

Protecting Web applications and cardholder information



# Table of contents

Introduction .....	1
The business challenge .....	2
PCI DSS – A coordinated response .....	3
Achieving compliance – The pressure is mounting.....	4
Six key recommendations.....	6
Citrix solutions for protecting Web applications.....	7
Addressing the PCI DSS requirements.....	9
Citrix advantages.....	11
Conclusion.....	11

# Introduction

Introduced in 2004 – but with roots dating back to 2001 as part of the Visa Cardholder Information Security Program – the Payment Card Industry Data Security Standard (PCI DSS) can hardly be described as new. What is relatively new, however, is the mounting pressure to achieve compliance with it, along with a shift in its status from “best practice” to “requirement” for guidelines applicable to Web-facing applications.

This paper elaborates on the changing nature of the PCI DSS landscape and its requirements. It then identifies applicable application networking compliance solutions from Citrix Systems, Inc., and provides recommendations to help ensure that organizations achieve PCI DSS compliance relative to their business-critical Web applications and accompanying information resources.

## The business challenge

During the past decade, organizations worldwide have become increasingly reliant on e-commerce, e-business, and the use of the Internet in general as business tools. The success of these online endeavors and strategies, however, is seemingly in a perpetual state of jeopardy. This is due in large part to ongoing issues and concerns stemming from the steady loss/theft of consumer data and subsequent occurrences of identity theft, credit card fraud, and so forth. For instance:

- \$3.6 billion is the estimated cost of e-commerce fraud for US merchants in 2007, an increase of 20% over 2006 (CyberSource Fraud Survey, 2007).
- As of January 2008, the reported number of records containing sensitive personal information involved in security breaches in the US since 2005 was approximately 217 million (Privacy Rights Clearinghouse).
- 78% of surveyed consumers indicated they would be unlikely to continue to shop at a store if they learned it had had a breach that may have compromised their credit account information (Javelin Strategy & Research, 2007).

To be clear, this is just a small sample of statistics that affect us all. And it does not help matters that recent years have been witness to a dramatic shift in hacker motivation. Rather than building reputations, the focus now is squarely on making money. This has sparked a substantial increase in hacker activity and greater focus on successfully evading commonly deployed countermeasures in order to obtain valuable information – such as credit account details. Not only are new threats being generated at a faster pace and greater volume than ever before, but they are also increasing in diversity and degree of elusiveness. In other words, the bad guys are not letting up. On the contrary, they continue to up the ante!

### Quick Takes

- Download and read the PCI standard from [www.PCISecurityStandards.org](http://www.PCISecurityStandards.org)
- Perform a PCI self-assessment
- Consider an AppFW for active protection of Web applications (satisfies PCI Section 6.6)

# PCI DSS – A coordinated response

To their credit, the major payment card brands, American Express, Discover, JCB, Visa and MasterCard, have long recognized the presence and implications of the situation discussed above. More significantly, they also recognized the need to do something about it. As a result of their collaborative efforts, the Payment Card Industry Data Security Standard (PCI DSS) was introduced late in 2004.

The goal of the standard is to establish a single approach to safeguarding sensitive cardholder data for all card brands. To this end it specifies 12 requirements logically organized according to six high-level control objectives, as shown in Table 1.

Table 1: Organization of the PCI Data Security Standard

	Requirements
Build and Maintain a Secure Network	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: Use and regularly update anti-virus software 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: Assign a unique ID to each person with computer access 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

Each of the 12 requirements is subsequently defined by several sub-requirements, yielding a total of more than 200 individual elements that specify the technologies, policies, and procedures necessary for protecting cardholder data. These can be viewed in their entirety by accessing the latest version of the standard at <https://www.pcisecuritystandards.org>

## Applicability

From an organizational perspective, the PCI DSS applies to any business that stores, processes, or transmits Primary Account Numbers (PANs). In practice, this means PCI applies to all merchants that accept card payments, as well as to the member financial institutions and service providers that process the associated transactions.

From a technological perspective, the PCI DSS applies to all system components connected to the cardholder data environment. These include network devices (e.g., routers, switches, security appliances, wireless access points), servers (e.g., Web, database, proxy, mail), and applications (e.g., internal, Internet) that either directly participate in the cardholder data environment or are not adequately isolated from it.

## Rationale

As stated earlier, one goal of the PCI DSS is to establish a uniform set of expectations across card brands regarding what is required to protect cardholder information. Beyond being an obligation to the payment system, however, compliance with the PCI DSS is intended to build a culture of security that benefits all parties, as illustrated in Table 2.

Table 2: Benefits of Complying with the PCI DSS

Everyone	<ul style="list-style-type: none"> <li>• Limited risk</li> <li>• More confidence in the payment industry</li> </ul>
Member	<ul style="list-style-type: none"> <li>• Protected reputation</li> </ul>
Merchant & Service Provider	<ul style="list-style-type: none"> <li>• Competitive edge gained</li> <li>• Increased revenue and improved bottom line</li> <li>• Positive image maintained</li> <li>• Customers are protected</li> </ul>
Industry	<ul style="list-style-type: none"> <li>• “Good security neighbors” encouraged</li> <li>• Information is safeguarded</li> </ul>
Consumer	<ul style="list-style-type: none"> <li>• Identity theft prevention</li> </ul>

## Achieving compliance – The pressure is mounting

Despite the potential benefits – not to mention the threat of being fined – most companies initially did not seem particularly concerned about complying with the PCI DSS. Indeed, compliance rates, even among merchants responsible for the highest volumes of card transactions, remained relatively low at the end of 2006.

The situation today is much different, however. Organizations are now finding themselves under considerable pressure to achieve compliance with the PCI DSS. This is because the card brands and the public at large have both been demanding action.

### Mounting public pressure

With 8-10 million identity fraud victims and nearly \$50 billion in associated losses per year in the US alone, it is no wonder that the public is starting to take action (source: Javelin Strategy and Research 2007 Identity and Fraud Survey). The earlier statistic indicating that 78% of consumers would shy away from a merchant that suffered a security breach is just one dramatic example. Another is the move by some state legislatures to effectively codify certain aspects of the PCI DSS. For example, Minnesota

passed a law that makes merchants responsible for the cost of blocking and reissuing credit cards in the event that they suffer a breach and are found to have been storing prohibited cardholder information.

## Formation of “The Council”

In September of 2006, six of the leading card brands established the PCI Security Standards Council and chartered it with responsibility for: (a) encouraging adoption of the standard; (b) maintaining the standard; and (c) certification of associated auditors (i.e., scanners and assessors). The significance of this move is that it amounts to a “mainstreaming” of the PCI DSS. As an open forum, the council includes a mechanism for affected organizations to participate and have a voice in the development and management of the standard. The point is that this democratization of the process effectively leaves participating organizations with less justification for not complying.

## Visa throws down the gauntlet

Perhaps even more significant was the launch by Visa USA in December 2006 of its PCI Compliance Acceleration Program (PCI CAP). This program established financial incentives, both positive and negative, to further encourage compliance with the PCI DSS. One-time payments and reduced interchange rates were provided to acquirers whose Level 1 and 2 merchants had validated compliance (and met a handful of other requirements) prior to August 31, 2007. More telling, however, were two other provisions of the program. First, the practice of only issuing fines in the event of a data compromise was changed. Recurring monthly fines are now being issued for acquirers of all Level 1 and 2 merchants that have not: (a) validated compliance; or (b) confirmed that they are not storing prohibited full-track data. The second provision of note is that the aforementioned incentives would only be available to acquirers that could demonstrate they had established a comprehensive plan for compliance of their Level 3 and 4 merchants. This is significant because, up to this point, most of these lower-level merchants have been operating with relative impunity. But now, the pressure is on for them, as well.

## Applications take center stage

Another aspect of the mounting pressure to achieve compliance has to do with two major changes pertaining to the treatment of applications. The first takes the form of Visa’s payment application security mandates, which became effective January 1, 2008. These mandates effectively ban the use of payment applications known to retain prohibited data and also require that all payment applications adhere to Visa’s Payment Application Best Practices (PABP). The expectation is that the mandates will be formally incorporated as requirements of the PCI DSS at the time of its next revision.

The second change involves requirement 6.6 of the PCI DSS. This “requirement” indicates that all Web-facing applications should be protected either by installation of an application-layer firewall or by reviewing all custom application code for vulnerabilities – and then fixing those vulnerabilities. Many casual readers of requirement 6.6 see code review as a passive event, which is not the case, as the uncovered vulnerabilities have to be remediated. The main issue with this requirement is that organizations that have not already done so will soon need to take action because as of June 30, 2008, section 6.6 will become an actual requirement, as opposed to just a best practice guideline.

## Six key recommendations

For most organizations that handle credit card data, achieving compliance with the PCI DSS is no longer an option; rather, it is a necessity. Consequently, it is also a necessity to provide adequate protection for Web applications that enable access to or otherwise process sensitive cardholder information. Citrix provides the following recommendations to help organizations achieve compliance for their Web application environments. PCI DSS.

### 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 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 using an application layer firewall because of its numerous TCO advantages: providing continuous protection against 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 that 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 and appropriate security practices – and not just for cardholder data, but for all other types of data and computing resources as well. By way of example, Web application firewalls: (a) can be used to address numerous PCI DSS requirements; (b) can be used to protect more than just cardholder data; and (c) at least in the case of the offerings, can be deployed in the form of a full-featured application delivery system that yields substantial performance and availability benefits as well. Meeting compliance mandates using solutions that meet multiple strategic imperatives (e.g., application availability, application acceleration) helps avoid the “point product sprawl” that frequently occurs when single function products are used to tactically achieve compliance.

### 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 not suffer a loss/theft of cardholder data, at any time, period. As a result, the usage logs for Web applications should be audited on a routine basis to help detect any abnormal or unauthorized activities. 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, all Web applications should periodically be re-assessed to ensure that they are still handling sensitive information properly. In this regard, a Web application firewall could be used to alert an administrator of any changes in application behavior that may result in violations, to mitigate the deficient condition until such time that the application is fixed, and to proactively protect the application and Web server. 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 for executing a swift response and minimizing 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.

## Citrix solutions for protecting Web applications

Providing adequate protection for business-critical Web applications is an issue for all organizations. Those that have not yet achieved compliance with the PCI DSS are clearly under pressure to do so. On the other hand, those that are currently compliant may still need to address the soon-to-be requirement 6.6. Furthermore, shoring up the protection of their Web applications even makes sense for those organizations that are not subject to the PCI DSS.

Not only are Web applications exceedingly vulnerable, but they are also widely recognized as the primary vehicle for e-commerce and customer portals and, therefore, act as a “front door” to all sorts of lucrative data. The net result is that Web applications are now a favorite target of hackers everywhere. Just consider the following handful of statistics that dramatically demonstrate the extent of the situation:

- 61% of the 2,461 vulnerabilities documented in the first half of 2007 were attributed to Web applications, and 79% were designated as “easy to exploit” (source: Symantec Internet Security Threat Report, Volume XII, Sep 2007);
- 73% of Web sites are susceptible to cross-site scripting attacks (source: WhiteHat Web site Security Statistics Report, Oct 2007); and
- Gartner estimates that 75% of all attacks are now aimed at Web applications (source: see page 2 of “A Practical Guide to Web Application Security”).

Citrix is ready to help! Citrix offers three solutions in particular that are well-suited to helping organizations protect their business-critical Web applications.

## Citrix NetScaler

Citrix® NetScaler® is a full-featured application delivery system. It offers organizations a strategic alternative in the form of a single platform that addresses Web optimization and security needs. In addition to supporting integrated Application Firewall and Access Gateway as licensable software modules, NetScaler also provides a comprehensive set of content switching, load balancing, and application acceleration capabilities. The result is a highly cost-effective solution that secures an organization's Web applications at the same time that it substantially enhances their performance and availability. Moreover, section 6 compliance requirements are achieved using a solution that has long-term strategic value and use.

Used individually, or in conjunction with one another, each of these solutions provides organizations with an extensive array of capabilities to help ensure the security and usability of their business-critical Web applications. Equally important in this context, though, is that the solutions also help organizations achieve compliance with the PCI DSS.

## Citrix Application Firewall

Citrix Application Firewall™ is a high-performance security appliance that blocks attacks against Web applications and infrastructure. Application Firewall enforces a positive security model that permits only correct application behavior, without relying on attack signatures. It also analyzes all bi-directional traffic, including SSL-encrypted communications, protecting against Web application vulnerabilities without any modification to applications. Furthermore, available business object protection modules help secure sensitive objects, such as credit card numbers, as well as custom-defined data objects. Citrix Application Firewall is available as a standalone appliance (that can be upgraded in the field to a full featured NetScaler solution), or as an integrated feature of Citrix NetScaler.

## Citrix Access Gateway

Citrix Access Gateway™ is a family of SSL VPN appliances that provides secure access to an organization's applications and data. The use of encrypted tunnels for all sessions is combined with the enforcement of granular policies that control access based on both user identity and client machine trust level to ensure the highest levels of confidentiality and integrity. Access Gateway can also determine whether direct or virtualized access is warranted and automatically invoke the appropriate connectivity method for the end-user.

# Addressing the PCI DSS requirements

PCI DSS differs from most regulatory compliance mandates in that it specifically states recommended or required technical actions. Of the 12 requirements, section 6.6 is the most explicit stating:

- (a) "having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security"; or
- (b) "installing an application layer firewall in front of [the] Web-facing applications".

In this case, the ideal/recommended approach would be for organizations to pursue both measures. For code reviews, however, it is important to recognize that the results are only valid until the application is modified, or until a new attack vector is developed that is beyond the scope of current code review techniques. Moreover, if a code review is performed and a vulnerability is identified, that vulnerability must then be mitigated. In this regard, a solution such as Citrix Application Firewall has some distinct advantages that make it a more efficient and effective approach. For instance, it provides continuous active protection against attacks, dynamically adjusts to code changes, and can support multiple Web applications simultaneously. And, if vulnerabilities are discovered, the Citrix Application Firewall can mitigate them immediately, freeing the organization from having to immediately having to undergo the time and expense of changing the application.

Another important benefit is that the Citrix solutions have broad applicability. In other words, they not only enable organizations to address requirement 6.6, but also help with fulfillment of many of the other PCI DSS requirements as they pertain to Web applications.

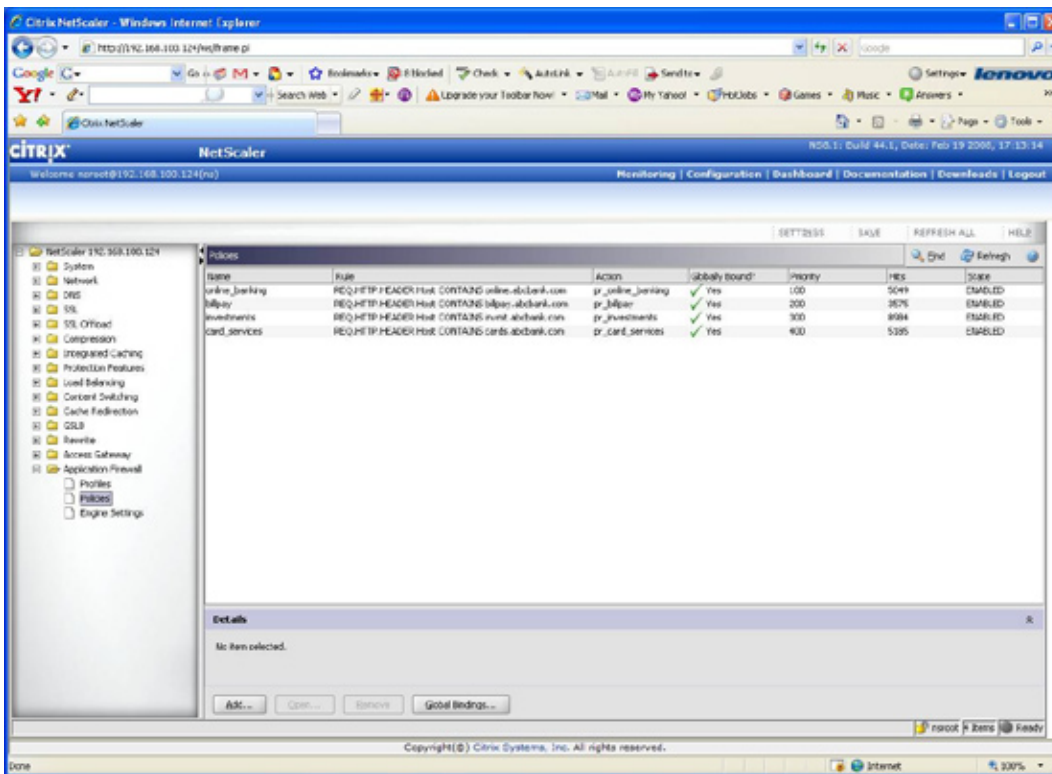


Figure 1: NetScaler Application Firewall PCI DSS protections.

1.2 – Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.

The PCI DSS mandates that organizations build and maintain a secure network by using core Web protocols and VPN technologies to deliver and secure cardholder data across networks. Citrix Application Firewall, Citrix Access Gateway, and Citrix NetScaler restrict access to applications and data by allowing: (a) only the use of approved protocols and methods; (b) only connections from trusted networks; and (c) only access to users who are authenticated and authorized. A further measure of assurance is also derived from the fact that Citrix Application Firewall has obtained ICASA Labs Web Application Firewall Certification.

3.3 – Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Citrix Application Firewall is easily configured to mask or block Primary Account Numbers and otherwise prevent the leakage of sensitive cardholder data, regardless of programmer oversight, logic flaws, or targeted attacks.

3.5 – Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

The protection of encryption keys is paramount to maintaining the confidentiality of encrypted cardholder data. If an encryption key can be uncovered, all previous, current, and future transactions that use the key can be decrypted and disclosed as clear text. Cryptographic protection standards such as FIPS 140-2 have proven to be a best practice for financial organizations that require strong key protection, and will be a consideration in PCI DSS compliance. Citrix Application Firewall, Citrix Access Gateway, and Citrix NetScaler appliances securely maintain the certificates and encryption keys used for SSL/TLS and are all available in FIPS 140-2-compliant versions.

4.1 – Use strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Each of the Citrix solutions can be used to SSL-enable applications that were not designed to use secure communications protocols. Furthermore, Citrix Application Firewall can inspect the contents of SSL/TLS encrypted sessions, ensuring session validity and blocking attacks – a capability that is not generally available in conventional network firewall and intrusion prevention products.

5.2 – Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

When using technologies that provide direct access to applications it is imperative that the client machine be free from malware. Before access is allowed, the SmartAccess component of Citrix Access Gateway automatically checks that minimum defined security requirements have been met, contextually allowing application usage by clients that have been determined through policy to be trustable.

7 & 8 – Restrict access to cardholder data by business need-to-know. Assign a unique ID to each person with computer access.

The Citrix solutions are fully capable of supporting all of the associated sub-requirements. Robust policy development and enforcement capabilities enable granular control over who has access to specific information resources. Multiple user authentication mechanisms are supported, including the use of two-factor methods for remote access scenarios, and all passwords are encrypted during transmission. Sessionization presents a compensating control that provides session enforcement.

## Citrix advantages

The market for Web application protection solutions is still in its formative stages and not particularly crowded – at least not yet. Still, there are enough products out there that organizations will be faced with a choice. Consideration should be given, therefore, to the many advantages of selecting Citrix and its corresponding solutions:

- Citrix has a proven track record. Citrix is a highly successful and stable provider of enterprise-class application delivery solutions. Citrix Application Firewall is the market share leader in its segment, while Citrix NetScaler, with more than 7,000 deployments worldwide, is designated as a Leader in Gartner Group Inc.'s Application Delivery Magic Quadrant (30 April 2007).
- Citrix is a participating organization of the PCI Security Standards Council. This enables Citrix not only to contribute to future development of the PCI DSS, but also to remain on top of impending changes so that it can proactively incorporate appropriate features in its solutions. One example of such a feature is the NetScaler PCI DSS Report that enables administrators to view a report of technical configuration details mapped to PCI DSS as depicted in Figure 1 .
- Citrix gives enterprises choices. To begin with, selecting Citrix means that organizations have multiple options when it comes to implementing their Web application firewalls. Citrix Application Firewall can be deployed
  - As a separate, standalone solution
  - As a standalone device working in close coordination with other Citrix application delivery products, or
  - As an embedded component of the self-contained application delivery workhorse, NetScaler.

In addition, Citrix has a broad portfolio of other essential solutions, ranging from a comprehensive set of virtualization solutions – including the longstanding centerpiece of the portfolio, Citrix XenApp™ – to a rich suite of remote access and collaboration offerings in the form of the Go-To line of hosted services. In this way, organizations can achieve greater economies of scale and simultaneously reduce the burden of having to engage an unwieldy number of solution providers to meet their needs.

## Conclusion

Organizations that embrace these key recommendations can efficiently and effectively enhance the security of their Web application environment while helping to ensure its compliance with the PCI DSS. Furthermore, organizations that select Citrix as their technology partner in this endeavor can be confident with this choice because of Citrix Systems' proven track record and ongoing commitment to provide market-leading solutions that address the requirements of the PCI DSS, both now and in the future.

## Notice

The information in this publication is subject to change without notice. THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THE USE CASES IN THIS PAPER ARE PROVIDED ONLY AS POTENTIAL EXAMPLES AND YOUR ACTUAL COSTS AND RESULTS MAY VARY.

## Citrix Worldwide

### Worldwide headquarters

Citrix Systems, Inc.  
851 West Cypress Creek Road  
Fort Lauderdale, FL 33309  
USA  
T +1 800 393 1888  
T +1 954 267 3000

### Regional headquarters

#### Americas

Citrix Silicon Valley  
4988 Great America Parkway  
Santa Clara, CA 95054  
USA  
T +1 408 790 8000

#### Europe

Citrix Systems International GmbH  
Rheinweg 9  
8200 Schaffhausen  
Switzerland  
T +41 52 635 7700

#### Asia Pacific

Citrix Systems Hong Kong Ltd.  
Suite 3201, 32nd Floor  
One International Finance Centre  
1 Harbour View Street  
Central  
Hong Kong  
T +852 2100 5000

#### Citrix Online division

6500 Hollister Avenue  
Goleta, CA 93117  
USA  
T +1 805 690 6400

[www.citrix.com](http://www.citrix.com)

## About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 200,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the *Fortune* 100 companies and 99% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2007 was \$1.4 billion.

©2008 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler®, Citrix XenApp™, Citrix Access Gateway™ and Citrix Application Firewall™ are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

36342/0208/PDF



[www.citrix.com](http://www.citrix.com)