

Data Security, Regulatory Compliance, Disaster Recovery

CHALLENGES, IMPLICATIONS AND SOLUTIONS FOR IMPLEMENTING
INFORMATION SECURITY TODAY

Table of Contents

2	Executive Summary
3	Threat Prevention and the Network
3	Risk Management and the Business Initiative
5	Understanding the Implications for IT and Security Executives
7	Clearing the Hurdles: A Strategic Starting Point
8	On-Demand Access Holds the Key
9	A Foundational Approach to Security
11	Delivering Business Benefits with the Citrix Access Platform
12	Increase Data Security
19	Facilitate Regulatory Compliance
24	Speed Disaster Recovery

Executive Summary

Beyond the recent overarching focus of data security on defending the corporate network against threats from the Internet, and shaped by fundamental far-reaching changes in the business landscape, implementing information security today brings with it a new and broad set of challenges for the IT team and especially for key executives such as the CIO and Chief Security Officer.

Further extending these challenges is the instrumental, although not immediately apparent, role of information security in a wide spectrum of business initiatives and processes. Notably, information security is

- at the heart of an organization's ability to comply with the massive regulatory requirements now sweeping across countries and industries
- a vital component in an organization's ability to reduce the business impact of natural, accidental, and man-made disasters and other disruptive events

In this environment, implementing information security — whether as a data security initiative in itself or as a pivotal element in a successful business initiative — requires an understanding of the direct implications of today's challenges for IT teams and the executives who are accountable for security.

At Citrix, we believe that a strategic approach to implementing information security will yield the best results, with business benefits immediately and with flexibility for change over time.

This white paper examines:

- Threat Prevention and the Network
- Risk Management and the Business Initiative
- Understanding the Implications for IT and Security Executives
- Clearing the Hurdles: A Strategic Starting Point
- On-Demand Access Holds the Key
- A Foundational Approach to Security
- Delivering Business Benefits with the Citrix Access Platform
- Increase Data Security
- Facilitate Regulatory Compliance
- Speed Disaster Recovery

Threat Prevention and the Network

Beyond the recent overarching focus of data security on defending the corporate network against threats from the Internet, and shaped by fundamental far-reaching changes in the business landscape, implementing information security today brings with it a new and broad set of challenges for the IT team and especially for key executives such as the CIO and Chief Security Officer.

WHO'S ATTACKING?

Attacks on computer security infrastructure used to be little more than indiscriminate acts of vandalism by hackers who wanted to boast. Now, security intelligence experts have detected signs of organized crime and government espionage in attacks, and of hackers who are motivated more by financial gain than by personal or political fulfillment. In fact, according to the Computer Security Institute "2005 CSI/FBI Computer Crime and Security Survey", for 46% of companies, one out of every five security breaches originates from inside of the corporate walls.¹ The stakes are too high for companies to ignore security threats from within their own networks. They now need to step up security throughout their environments,² as those who have authorized access to internal resources often are far more dangerous than those who need to breach a perimeter firewall to get inside of the network.

WHERE'S THE PERIMETER?

At the same time, remote access and business partner connectivity mean the perimeter is disappearing, making it harder and harder to define, let alone defend. Now, corporate networks extend outside of the physical bounds of corporate facilities, blurring the line between internal and external networks and between "inside" and "outside" of the firewall. This requires a new way of thinking about data security and network security, and has triggered the formation of the Jericho Forum, a powerful and vocal security user group that includes organizations such as BP, Procter & Gamble, and the UK's Royal Mail. The group has introduced the concept of "de-perimeterization" and encourages organizations to look at securing the data rather than the infrastructure that supports the data.³ Along these lines, Gartner, Inc. predicts that by 2007, 40% of new enterprise security spending will be directed toward data security issues, not perimeter security.⁴

Risk Management and the Business Initiative

Further extending the challenges of implementing information security today is its instrumental, although not immediately apparent, role in a wide spectrum of business initiatives and processes. Notably, information security is at the heart of an organization's ability to comply with the massive regulatory requirements now sweeping across countries and industries, and it is a vital component in an organization's ability to reduce the business impact of natural, accidental, and man-made disasters and other disruptive events.

¹ "Securing the Network from the Inside Out", Forrester Research, Inc., 2005

² "Securing the Network from the Inside Out", Forrester Research, Inc., 2005

³ "The State of Security in SMBs and Enterprises", Forrester Research, Inc., 2005

⁴ "Organizations Must Employ Effective Data Security Strategies", Gartner, Inc., 2005

WHAT MUST BE DONE TO PROTECT CORPORATE INFORMATION?

Increased regulation worldwide, both by governments and within industries, has resulted in greater accountability for corporate officers when it comes to managing risk in their organization. The stringent audit requirements of the many and diverse regulations have increased the need for control, visibility, and accountability, directly linking information security to risk management and, in fact, driving its implementation.

In this environment, the CIO, CSO, Chief Information Security Officer, Chief Privacy Officer, and other key executives must demonstrate that they are protecting corporate information effectively — to regulatory authorities, to business partners, to their own boards of directors. This requires that measures be in place to protect internal resources, and, in turn, has created pressure to adopt a comprehensive approach to risk management. As a result, IT has become an enabler for enterprise risk management by leveraging technology to proactively monitor and manage regulatory compliance and other business risks.⁵ This, of course, is not a simple matter. Industry experts believe that implementation of security today depends on establishing strong security policies and procedures, not merely turning on auditing features or deploying encryption in a solution. End-to-end security implementation should be the goal for enterprises, according to these experts, combining database security with application-, network-, and infrastructure-level security.

HOW TO REDUCE THE IMPACT OF A DISASTER?

Sometimes called disaster recovery, and also referred to as business continuity, the ability to continue to do business — no matter what — has shifted from a safeguard in transaction-oriented industries, such as financial services, to an important concern for organizations in every industry. This stems from the dramatic increase in magnitude and number of potentially catastrophic events — man-made, natural, and accidental. Consider the span of terrorist activities, from Madrid and London to New York City and Bali... Of hurricanes, earthquakes, even an unprecedented tsunami... Of massive power losses, fires, and chemical spills... A severe incident, such as the September 11 disaster in the United States, would cause crippling damage to businesses, and some might never recover, according to Gartner, Inc.⁶

An organization's response to a disaster introduces diverse opportunity to reduce the impact on the business and to speed disaster recovery. For example, voice over IP and IP telephony can change call center recovery, and work-at-home programs can be used effectively for production and recovery. However, although technical and management techniques can help companies be more resilient after catastrophic events,⁷ disaster recovery plans must be individualized. Each organization must identify its own requirements, such as its recovery-time objective for how quickly information systems, services, and processes must be operational after an incident, including recovery of applications and data and end-user access to those applications. This, in turn, requires identifying and implementing an array of best practices for physical system backup and information security and IT systems, a natural convergence of physical and logical security that brings together many enterprise resources as a team.

⁵ "Securing the Network from the Inside Out", Forrester Research, Inc., 2005

⁶ "Management Alert: Effective Disaster Recovery Management Could Save Your Business", Gartner, Inc., 2003

⁷ "Use Good Business Continuity Management to Prepare for a Disaster", Gartner, Inc. 2005

Understanding the Implications for IT and Security Executives

In this environment, implementing information security — whether as a data security initiative in itself or as a pivotal element in a successful business initiative — becomes particularly important, as well as challenging. In fact, for most organizations, it is critical to sustaining competitive advantage and operating efficiently, requiring an understanding of the direct implications of today's challenges.

IMPLICATIONS FOR DATA SECURITY

Although organizations tend to recognize the risks of external attacks and insider threats and the value of their data, with insiders involved in the majority of large, loss-bearing incidents,⁸ according to Gartner, many organizations still struggle with

- taking a comprehensive approach to data security
- understanding how to use and position products under various circumstances
- the role of data security in an overall security program

This is due to a number of factors: Data security products typically are not as mature as network security products, so security managers often must work with smaller point products. Data security includes solutions which aren't pure-security solutions. And data security can't stand on its own; it requires good network, application, and host security.

Another major obstacle facing organizations today is the problem of coordinating and managing multiple security technologies across the enterprise.⁹ As security technologies have become more complex, according to IDC, manageability of large networks that integrate a variety of point products has become significantly more difficult and more costly. This can be seen in the upgrades and reconfigurations now required to coordinate and manage technologies such as firewall, VPN, and intrusion detection, for example.

And finally, within this complex and still relatively undefined realm of security, the Chief Security Officer has a difficult role. These individuals are in charge of the logical security of the business, without necessarily having any real control over the operational or physical side of security. They recommend and set directions, but cannot always impose their views. And they have to deal with operational teams whose priorities are to work more effectively and more efficiently, often viewing security as yet another constraint to getting their job done.

IMPLICATIONS FOR REGULATORY COMPLIANCE

Many laws and regulations that have been adopted in the past decade impose information security requirements on companies and agencies. Some, such as the Health Insurance Portability and Accountability Act (HIPAA), California SB 1386, and the European Union Privacy Directive, relate to consumer privacy. Others, such as the Sarbanes-Oxley Act, focus on the sanctity of data and systems for trusted record keeping and reporting. Still others have yet to go into effect, such as the requirements and standards under Basel II which are to be implemented by 2007 and the Japan version of Sarbanes-Oxley which will not be in full operation until 2008.

⁸ "Organizations Must Employ Effective Data Security Strategies", Gartner, Inc., 2005

⁹ "Worldwide Security Software 2004-2008 Forecast and 2003 Vendor Shares", IDC, 2004

However, none of these regulations, according to Gartner, defines due care in security and no certification exists to ensure that a product or service will enable an organization to achieve compliance.¹⁰ Further, according to Forrester, although compliance requirements for many enterprises require them to take stronger measures than ever before to protect private data stored in databases, the regulations behind them typically do not offer strategies or best practices guidelines to meet the challenge.¹¹

As a result, many organizations are still struggling to understand the numerous regulations that potentially affect them and what that means from a business perspective.¹² Because today's organizations are increasingly information-intensive, technology is becoming a key part of strategic compliance initiatives, to ensure sustainability of compliance-related processes, mitigate risk, and manage ongoing costs.

In general, regulatory mandates seek to focus the enterprise on accountability and control, primarily through process discipline and corporate governance, and often are implemented in IT. Compliance requirements typically include

- use of authentication to assure the identity and authorization of users
- limitations on access to information
- privacy of personal information
- segregation of responsibilities between users and groups to limit abuses
- auditing, which is usually required to demonstrate compliance and brings with it the associated requirement for an appropriate level of reporting

The difficulties — and cost — of implementing compliance are exacerbated by the fact that many organizations have a highly distributed information infrastructure, with systems, devices, and data found throughout the enterprise.

These are not trivial considerations. Despite the fact that compliance timelines might be uncertain, some aspects of initiatives are already quite clear, such as the substantial penalties for non-compliance which often include personal liability for business executives. As well, incidents associated with loss of information security can lead to loss of customer confidence, brand damage, lost revenue, stock price impact, and class action lawsuits.¹³

IMPLICATIONS FOR DISASTER RECOVERY

After a major disaster, the priority of a company is to resume operations as quickly as possible. Production has to start up again, services to clients must be resumed, deliveries to customers have to be made, and suppliers have to be paid. Unless the business gets back on its feet quickly, it cannot survive a disaster, mainly because of its lack of cash flow. Accordingly, in order to facilitate business resumption, management teams that think ahead typically prepare a plan for disaster recovery or business continuity, reflecting a convergence of physical and logical security that brings together many enterprise resources as a team.

¹⁰ "Eight Steps Needed to Define Reasonable Security", Gartner, Inc., 2005

¹¹ "Trends 2006: DBMS Security", Forrester Research, Inc., 2005

¹² "Worldwide Outbound Content Compliance 2005 '2009 Forecast and Analysis: IT Security Turns Inside Out", IDC, 2005

¹³ "Eight Steps Needed to Define Reasonable Security", Gartner, Inc., 2005

Generally, such a plan has two main parts.

- The first part is economic and human and intended to ensure that key employees can be notified quickly to come and work in new premises. There, they should find their usual work environment, down to the same telephone numbers.
- The second part is technical and intended to give the employees precisely this work environment. This means new servers must start up from an emergency center, new workstations must become operational, and back-ups must be made available quickly. Above all, the security of the organization's valuable business information must be assured. It is imperative to maintain uninterrupted and secure access to all corporate resources, at all times.

Specifically, each organization must define its own response to a disaster, including the business processes, support for the community, and support for the employees' personal lives. In this endeavor, Gartner recommends classifying supported service levels and associated costs, as these factors drive tasks and spending in development and application architecture, systems architecture, and operations. Service-level definitions should include scheduled uptime, percentage availability in schedule uptime, and recovery-time and recovery-point objectives.¹⁴

Clearing the Hurdles: a Strategic Starting Point

Together, the new and broad challenges of today's business landscape and the consequent implications for IT teams and the executives who are accountable for security suggest that a strategic approach to implementing information security will yield the best results, both immediately and in the flexibility to meet new challenges over time. This requires:

- **a foundation** that is secure by design, not by chance, to help eliminate the traditional compromise between information security on the one hand and productivity and profitability on the other.
- **a platform** that delivers an integrated, end-to-end architecture, to close the security gaps inherent in a fragmented approach to information security and to reduce their related costs and inefficiencies.
- **a solution** that will help an organization to increase data security, facilitate regulatory compliance, or speed disaster recovery, both protecting and verifying the security of information, reducing the need for custom integration of individual products, accommodating legacy as well as future technologies — and everything in-between — and providing easy extensibility to meet any individual organization's information-security requirements and priorities over time.

¹⁴ "Effective Disaster Recovery Management Could Save Your Business", Gartner, Inc., 2003

“Working with independent agents means we have many users logging in from devices we don’t own, over connections we don’t control, and that raises security concerns. Citrix provides a number of security measures that help us protect corporate information. The products deliver secure, single sign-on and standards-based encryption of data over the network, and allow us to provide access based on user roles, so we can control who sees which information.”

— Charlton Monsanto, Chief Information Officer, Prudential Fox & Roach REALTORS

On-Demand Access Holds the Key

As the global leader and most trusted name in on-demand access, Citrix since 1989 has been helping organizations to tie together information resources, access devices, and networks — securely and cost-effectively — and to leverage the power of access for the success of their business initiatives. In fact, Citrix was the first company to understand how organizations use access to run their business, and to deliver an access platform with access solutions based on the customer’s perspective. Citrix solutions help IT to both improve operating efficiencies and directly support their organization’s business goals and objectives.

Today, more than 180,000 organizations around the world use the Citrix Access Platform, including 100% of the *Fortune* 100 companies and 98% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and individuals. Many of these customers are using Citrix to help them increase data security, facilitate regulatory compliance, and speed disaster recovery, with lower operational costs, higher efficiency, and consequent opportunities for innovation.

For example:

- Prudential Fox & Roach REALTORS, the sixth-largest provider of real estate services in the U.S., uses Citrix to protect corporate data accessed by 3,700 geographically dispersed and mobile independent agents, while also cutting IT support costs by 20%.
- A leading business process outsourcing (BPO) company in India, part of LASON, Inc., USA, is using Citrix to ensure 100% security of customer data, while also increasing by 300% the productivity of online BPO jobs.
- Saint Anthony’s Health Center, a health care facility in the U.S. that offers state-of-the-art medicine administered with skill and care, is using Citrix to comply with requirements of the Health Insurance Portability and Accountability Act, while also saving \$700,000 on hardware replacement costs over 10 years and reducing IT administration costs.

-
- Mutual Service Corporation, a leading financial planning broker/dealer and investment firm and wholly owned subsidiary of Pacific Life, is using Citrix to meet the requirements of all government regulations for its industry, while also seizing an opportunity to dramatically change the way they do business.
 - Thomas H. Lee Partners, L.P., one of the oldest and most successful private equity firms in the U.S., brought Citrix into the organization for the highest level of information security over the network — considered pivotal to its competitive position — and got bulletproof security and IP telephony access as well.

A Foundational Approach to Security

As a company and through the Citrix Access Platform with its many product families, Citrix's foundational approach to security provides the right degree of protection for extending access anywhere, anytime — without compromising security. We call it secure by design, because it enables organizations of any size to treat security as an integral part of their architecture, not as an afterthought.

APPLICATION DELIVERY

Citrix is the only company that offers a service-oriented architectural approach for delivering all classes of applications with the highest security, lowest cost, and fastest performance: virtualization for client-server applications, optimization for Web applications, streaming for desktop applications. Enabling secure use of public networks, this combination offers unique opportunities for control of the endpoint environment, application execution, and information containment.

ACCESS SECURITY AND CONTROL

To deliver access security and control across IT and business initiatives, Citrix combines the power of two key security capabilities — SSL VPN and enterprise single sign-on. Both of these product families were the fastest growing in their respective industries at the end of 2005.

POLICY-BASED CONTROLS

Administrators can set end-to-end access policies that dictate what can be accessed from each specific access scenario. These access policies can take into account users, groups, device types, network locations, and end-point security.

ADVANCED AUTHENTICATION

In cooperation with partners, Citrix offers authentication to access resources with strong measures such as two-factor authentication, using tokens, smart cards and biometrics. Citrix is committed to ensuring that customers have the widest range of authentication options available, from leading authentication providers.

INDUSTRY PARTNERSHIPS

Citrix works closely with industry security leaders, to create certified tight integration with our products and services. Customers can be confident that Citrix has established the partnerships needed to tightly integrate secure-by-design capability with the security ecosystem, in areas such as authentication, identity management, and encryption.

INDUSTRY CERTIFICATION

Citrix is continually evaluating industry and government certification programs, and ensuring that products are submitted and certified where appropriate. These programs include FIPS 140-2, Common Criteria, and Section 508 accessibility.

INDUSTRY STANDARDS

Citrix is committed to both using and developing open, robust, secure standards for infrastructure security. We make use of established industry standards, such as Secure Sockets Layer (SSL) encryption, and are involved in the development of emerging standards, such as the Security Assertion Markup Language (SAML).

END-POINT SECURITY

In partnership with industry leaders ranging from Microsoft® to WholeSecurity, the Citrix Access Platform leverages new and innovative end-point compliance-enforcement solutions, centralizing the assurance that end-points are secure and compliant before access is delivered.

COMPREHENSIVE REPORTING AND AUDITING

A compliance audit could require reporting that encompasses the entire information lifecycle, including interaction with end-points as well as with the data center. Citrix's product families encompass both environments, able to provide comprehensive, auditable reporting that includes the user environment as well as the data center.

Although THLP does not currently have regulatory compliance issues, the firm expects that it will have to deal with regulations at some future date. "Right now, we feel secure with our Citrix implementation, which enables us to provide role-based access to information without opening up the network to vulnerability. When compliance issues arise, we are in a solid position to address them with this Citrix solution."

— Hoby Cook, Vice President of IT, Thomas H. Lee Partners, L.P.

Delivering Business Benefits with the Citrix Access Platform

The Citrix Access Platform provides a consistent, integrated, end-to-end infrastructure that can accommodate every access variable that's required to seamlessly and securely connect users, devices, and networks to company resources. It is the broadest portfolio of software solutions for secure, on-demand access to information, applications, and people that's offered by any company in the access-infrastructure industry today. All Citrix product families are built to work immediately and seamlessly with any IT infrastructure, no matter how distributed and diverse, and with each other. Collectively, Citrix's access products and services deliver business benefits that help organizations to implement information security today: increase data security, facilitate regulatory compliance, and speed disaster recovery.

Increase Data Security

Citrix makes it possible for organizations to take advantage of a range of options for delivering integrated data security with strong measures. As a result, it is easy to launch new applications and new services successfully, guaranteeing information system security without delaying projects, and to ensure that the integration of security tools into the legacy infrastructure does not cause any drop in existing levels of security or of productivity.

“Although it provides full network connectivity, the Citrix client hides the IP addresses of the remote network. This helps prevent worms, Trojan horses, and other threats from discovering a path to additional network resources.”

— Jon Prall, Vice President of Operations, Postini, Inc.

Here's what Citrix delivers:

MAKE SURE THE DATA STAY IN THE SAFEST PLACE

Among the greatest benefits that Citrix delivers is the ability to prevent data from leaving the data center, ever, with application virtualization. This is the best delivery method for client-server applications and Citrix set the industry standard with Citrix Presentation Server™, which protects information by

- Keeping applications, information, and servers in the data center, eliminating the need to install an application on the user device and minimizing loss of information and the risk of theft
- Controlling, and even eliminating when appropriate, the ability to print, copy, and save to the local device
- Avoiding the transmittal of text over the network, using instead vector graphic updates (partial screen updates), transmitting only screen pixels, keystrokes and mouse movements
- Mitigating the spread of viruses through unprotected client devices
- Building in policy-based controls that allow IT groups to easily restrict who gets access to what information and when, including limiting system administrators to “restricted / permitted” for a particular range of tasks and responsibilities

Similarly, the security of screen-sharing technology delivers comparable benefits for organizations using any of the diverse managed services of the Citrix Access Platform: Citrix® GoToMyPC® for remote access to PC desktops, Citrix® GoToMeeting™ for easy online meetings, and Citrix® GoToAssist™ for support staff of external contact centers and internal help desks to provide best-in-class support over the Internet.

Citrix's patented technology tracks changes to the screen without installing a device driver and intelligent caching is used to only transmit changed screen images. These data security dimensions are delivered in concert with motion and mixed pixel compression that allows Citrix to achieve better screen compression rates — 5x better than Gif and 6x better than JPEG without JPEG artifacts. Being bandwidth adaptive allows Citrix to match the experience to the available session bandwidth, which equates to a better overall experience for end users, whether they are on broadband or running over a dial-up connection.

- GoToMyPC — the data never leave the office PC. All information is accessed remotely, eliminating the security risk of having the data themselves leave the premises on an employee's laptop, for example.
- GoToMeeting — the data are not posted on a hosting site. Screens are shared but the data are not passed from one attendee to another.
- GoToAssist — instead of requiring remote employees to send in their system when they need technical support, which represents yet another security risk, the repair takes place remotely.

KEEP SENSITIVE DATA CONFIDENTIAL WHEN SERVING MILLIONS OF CUSTOMERS ONLINE

Web applications provide direct access to some of the most sensitive and valuable data in any enterprise — including financial records, credit card numbers, and customer identity information. But delivering these applications securely is particularly challenging because Web vulnerabilities are generally easy to exploit, and attacks cannot be detected by traditional security products. Web applications require defenses against a wide range of application-layer threats, such as denial of service (DoS) and worm attacks. Citrix® NetScaler® application delivery systems, which include built-in SSL encryption, have been architected to forward valid client requests to servers and to block illegitimate requests. Plus, since Citrix NetScaler's single, unified device takes the place of a number of point solutions, overall network infrastructures are dramatically simplified, and overall operational costs are dramatically reduced.

- The Citrix NetScaler Application Switch has built-in defenses against DoS attacks. Content inspection capabilities enable the Application Switch to identify and block application-based attacks, including DoS and distributed denial of server attacks such as TCP SYN flood attacks, connection layer attacks, SSL flood attacks, and HTTP GET flood attacks.
- The Citrix NetScaler Application Firewall further improves security of Web applications and infrastructure by preventing the theft of sensitive information that might be exchanged via a Web portal, such as credit card numbers, financial data, and personal identity information. Such application-layer attacks, which target application vulnerabilities, account for nearly 75% of all attacks on the Internet today, according to Gartner. Some examples of this type of application-layer attack: cross-site scripting (XSS) attacks, SQL injection attacks, and parameter manipulation attacks.

TAKE A PASS ON THE PASSWORD PROBLEM

Citrix Password Manager™ provides centralized Enterprise Single Sign On (ESSO) for multiple resources, reducing user exposure to multiple passwords and logins and enhancing security while also reducing support costs. It can also enforce password policy requirements, such as strong passwords or password rotation. The value of Password Manager has been recognized by enterprise-class identity management vendors such as Hewlett-Packard, which has partnered with Citrix to make Password Manager the ESSO option for the HP OpenView Select Identity portfolio. Strong authentication is enhanced in the Citrix approach through cooperation with partners such as RSA Security and Secure Computing. These partners enable the integration of measures such as two-factor authentication using tokens, smartcards, and industry identity-linked encryption.

SIMPLIFY DMZ MANAGEMENT

Managing a DMZ is a permanent trade-off between security and user-friendliness. Traditionally, security officers have tried to control its perimeter whereas, for more simplicity, operational teams would almost prefer to have one big DMZ hosting all services or even no DMZ at all. Meeting these two requirements might sound like mission impossible and yet there is a solution.

- **One access point** — The Citrix Access Gateway™ is a universal SSL VPN appliance that provides a secure, always-on, single point-of-access to any information resource. It works through any firewall; supports all applications and protocols, including IP telephony; is fast, simple and cost-effective to deploy and maintain via its Web-deployed, auto-updating client; and ensures that devices meet company security standards with a worm-blocking client and integrated end-point scanning.
- **One door to the Internet** — The Access Gateway centralizes access control to all applications. The main gain is architectural: only one port needs to open to the Internet. The result: only one service is visible from the outside, no matter how many applications can be accessed. The Access Gateway provides a simplified firewall configuration, while at the same time reducing the exposure of the DMZ and of the applications that it hosts. In the same way, access to the company LAN from the DMZ can be restricted to traffic exclusively coming from the Access Gateway.

STRONG ENCRYPTION FOR APPLICATIONS

Citrix encrypts traffic end to end, regardless of the application requested, via an SSL/TLS tunnel from the client machine to the Access Gateway. Any application — Windows applications, Citrix Presentation Server-hosted applications, Web applications, company intranets, shared files — thus becomes immediately accessible via the Internet. All of this is achieved without having to modify the existing firewall configuration, as data streams use the same single port.

Citrix Presentation Server itself provides SSL/TLS encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser and the Web server. This Secure Gateway feature makes firewall traversal easier and provides heightened security via a single point of entry and secure access to an organization's server farms.

SPECIAL ENCRYPTION FOR MANAGED SERVICES

When anyone from an organization is in-session using any of Citrix's managed services, all end-to-end communications are protected using secure key establishment protocols and 128-bit AES encryption.

- Given the additional security issues that arise during collaborative exchanges, Citrix went even further for GoToMeeting. First, all endpoint-to-infrastructure links are encrypted with SSL. Then, a standard that was developed at the renowned Stanford University in California, called SRP, is used to do an authenticated group key agreement and establish a session encryption key shared only by the authorized meeting attendees. This is important because it provides extra assurance that a meeting is protected from eavesdropping and it means that at no time does unencrypted confidential customer information flow through the Citrix Online communications servers.

“An alternative solution to Citrix would have meant a huge investment in back-end hardware, cluster control, communication control, and more. As a part of our due diligence and sales presentation, we explain the cost-benefit analysis on higher productivity and lower per-transaction cost using the Citrix solution, which invariably is the winner with our potential customers.”

— Ranjit Pisharoty, Senior Vice President, Lason India

SECURITY FOR IP TELEPHONY SYSTEMS

Any organization that has an IP telephony system from Cisco, Nortel, Avaya, Mitel, Siemens, NEC, and Alcatel can increase data security with SSL encryption of the application traffic to and from its IP telephones. The Citrix Application Gateway™, an appliance which is used to deliver packaged, custom, and transformed HTML-based applications to the screens and speakers of IP phones, is so secure that its software code base is used by the Access Gateway, which is deployed in an organization's DMZ.

TAKING CONTROL OF WIFI

Wireless Fidelity networks are very practical, inexpensive and extremely simple to deploy. But despite their success and multiple benefits, these networks demand particular attention in terms of security. Whereas the Ethernet socket of a wired network is securely located within the business premises, a WiFi access point can be used by anyone, even from an organization's parking lot. Of course, good network architecture allows WiFi-related risks to be controlled, and effective protection methods exist, such as WPA, authentication via 802.1X, and the long awaited 801.1i. However, these solutions have only recently been standardized and their implementation or even their integration to the existing architecture can sometimes be cumbersome.

The Citrix solution allows a WiFi network to be implemented transparently. The security that will be applied to it will be exactly the same as that applied to any other connection. No matter where users access the network, including a non-secure WiFi base station, their session and data will travel through an encrypted tunnel which guarantees confidential exchanges. Moreover, this does not require any additional effort from the IT department or any change of habits for users who are familiar with the LAN access infrastructure. This is good news for administrators who, as a result, now only have to worry about user rights, and not their access methods.

BROWSER LOCK DOWN

Attacks perpetuated by malicious Internet sites and hackers against poorly informed Internet users often come down to the Internet browser of the victim being badly configured. From trapped ActiveX or JavaScript controls to cross-site scripting attacks to the common iFrame flaws or illegal downloads, the Web browser is often an open door to a system. And when the victim is a company employee, then the knock-on effect on the whole information system can be very serious. The most effective CSOs protect themselves against such abuses by making sure that operational teams deploy browsers in their most restrictive configuration and by requiring a particularly strict implementation of security patches. Unfortunately, in addition to the increased workload that this implies, users sometimes modify the configuration of their browser if it seems too restrictive for them or simply install the browser of their choice if a configuration is too difficult for them to modify.

- **Published browser** — With Citrix, the Web browser can be centrally hosted as a published application. This means there will be only one browser, installed and configured by the IT staff, which runs on Presentation Server.
- **One browser for all . . .** All clients access the same browser and use it exactly as if it were working only for them, on their PC. But in reality, the browser remains protected, out of their reach on the Presentation Server. Users cannot modify the configuration themselves. In addition to obvious security benefits, this also brings greater flexibility in terms of browser configuration: the IT staff changes the parameters only once, on the Presentation Server, for all modifications to become effective on all clients.

-
- **. . . and nobody else.** Plus, the business firewalls can be configured to authorize only outgoing Web traffic that comes from the Citrix server. As a result, any other browser that is installed on a PC will be unable to access the Internet.
 - **Taking control of confidentiality** — When the nature of the business demands greater confidentiality for data accessed via the browser, Citrix provides another great benefit: the cache which usually stores visited Web pages and cookies on the client is located on the application server and therefore it is beyond the reach of any malicious hacker who might attempt to take control of the client.

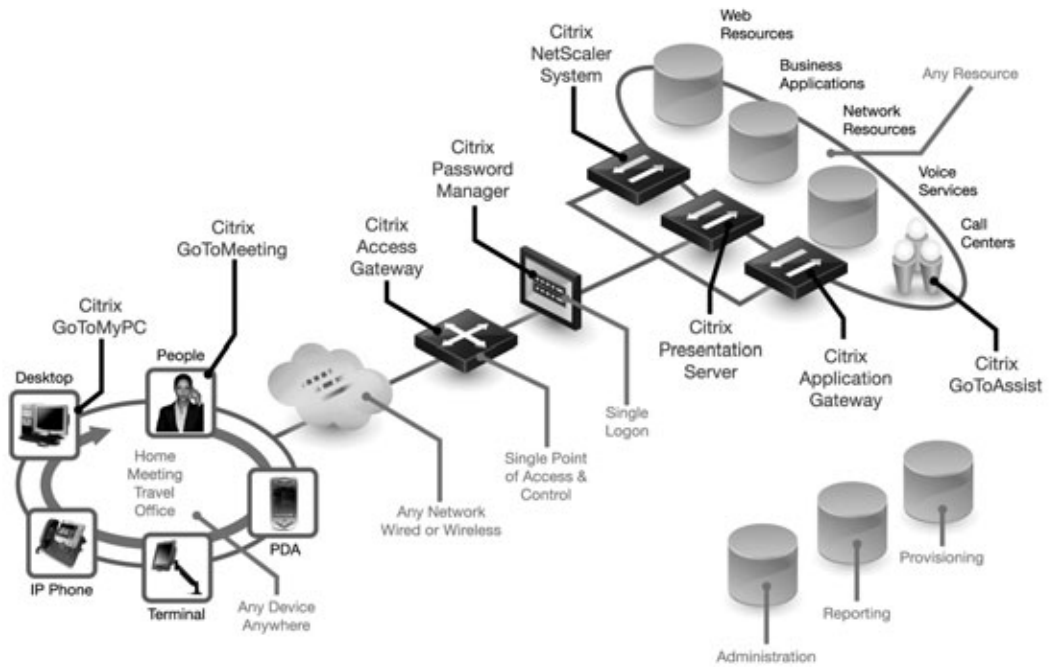
EASY PATCH MANAGEMENT

Managing patches is a difficult art to master. Patch programs must be tested before they are deployed; some are incompatible with the systems in use, while others need servers to be restarted, which of course requires a specific schedule for each system. Multiply this by a few hundred servers and a few thousand clients, including mobile devices that cannot easily be repatriated, and the task quickly turns into a big nightmare.

- **Centralized applications** — Citrix allows the majority of business applications to be hosted on servers, which means the operating system can be shared among all business applications. As a result, the same Citrix Presentation Server can run the ERP solution, the office suite, the intranet and even the Web browsers. And all of these applications are located on centralized servers managed directly by the IT department. Instead of updating each of these applications individually, with the same patch distributed to each client and server, each patch only has to be installed once, on a single server which replicates the updates to all Citrix Presentation Servers.
- **Centralized updates** — Not only can the operating system be updated easily, but also updating applications is greatly simplified, particularly in situations in which client software does not natively support automatic or remote updates. Presentation Server addresses this particular issue by allowing all clients, wherever they might be located, to benefit from the latest updated software every time they log on.

At A Glance

Citrix Product Family	Data Security
Citrix Access Essentials™	
Citrix Access Gateway™	•
Advanced Access Control option	•
Citrix Application Gateway™	•
Citrix® Voice Office option	
Citrix® GoToAssist™	
Citrix® GoToMeeting™	•
Citrix® GoToMyPC® Corporate	•
Citrix® NetScaler® Application Accelerator	
Citrix® NetScaler® Application Switch	•
Citrix® NetScaler® Application Firewall	•
Citrix Password Manager™	•
Citrix Presentation Server™	•



Citrix for Data Security

Facilitate Regulatory Compliance

Citrix combines benefits that deliver a very high degree of control which can be leveraged throughout an organization, from the data center to the endpoint, whatever the endpoint might be and wherever it might be found. This level of control corresponds to significant compliance requirements for internal IT controls and business processes. As a result, organizations can balance information security with business productivity and cost-efficiency, optimizing controls with extremely high granularity but also great flexibility. This includes an exceptional capability to limit critically sensitive information solely to the right people, in the right context, at the right time, facilitating compliance with the mandates of regulations throughout the world and its industries.

“Our Citrix solution has given us a world-class access infrastructure for our representatives and their clients. It has also helped us meet all government regulations, such as the Patriot Act and the Anti-Money Laundering Act.”

— **Christopher Grant McDaniel, Senior Vice President and Chief Information Officer,
Mutual Service Corporation**

Here's what Citrix delivers:

APPLICATION CONTROL, REPORTING, LOGGING, AND MONITORING TO REDUCE COMPLIANCE COSTS

Citrix assists organizations to meet internal standards and comply with government and industry regulations by making it easy and cost-effective to centralize and consolidate applications, delivering the power to observe, monitor, and measure resources with robust business reporting, delegated administration, a common management infrastructure, and integration with third-party network and systems-management tools. For example, much of regulatory compliance involves reporting, logging, monitoring, and alerting. Citrix Presentation Server provides this functionality with a unified management console and reporting center. Visibility into the health and status of a Citrix Presentation Server farm is provided to third-party network-management tools so that administrators can monitor the wider computing environment from their preferred tool.

INFORMATION CONTAINMENT

One of the distinctive innovations in the Citrix Access Gateway and its Advanced Access Control option is the power to intelligently automate security and compliance measures based on the access context, providing a high degree of control over sensitive information. Citrix SmartAccess™ technology senses the context of the endpoint and delivers policy-compliant access accordingly. SmartAccess determines who is requesting access, where they are, when access is requested, and how it is requested. If compliant, then and only then will Smart Access enable access to resources according to policy.

GRANULAR SECURITY ZONES

Compliance might require the segregation of resources among specific users and groups. At the level of application delivery, Presentation Server and the Access Gateway both enable applications to be isolated in their execution environment between specific users, roles, and user groups. This centralizes isolation of controls on application management and ownership, even when the same application is available to different user or ownership groups on the same server environment. Finely grained Citrix access management also includes features that support content redirection, to ensure that proper and secured centralized applications are used rather than those local to the endpoint. This restricts access to specific resources as administratively defined.

MORE COMPREHENSIVE AUDITS

The best security tools are useless without a clear view of how the information system is used: who uses it, how, under what conditions. But this view is often just a dream for IT and security teams because a multitude of security solutions, all keeping their own logs, prevent their having a session-oriented view of the information system — unless they go searching for the information left by each user in the firewall log, in the authentication system log, and in the logs of each application used. That is, of course, if all of these applications support such a functionality. And yet, access to this kind of information is not only very useful when investigating a security incident, it can also be essential for ensuring regulatory compliance when an organization is required to keep detailed logs on the use of its information system.

- **Automated reporting** — As part of Citrix Presentation Server, the Resource Manager provides the administrator with the tools for monitoring and analyzing the use of the information system. From a single console, an administrator can find out who connected from where and what applications were used for how long. This logging applies to all clients, no matter where they come from and regardless of their authentication method, without the need for the organization to deploy a third-party logging tool. The administrator can also find out how much server memory and CPU resources are used individually.

CENTRALIZED AUTHENTICATION

Inadequate password management is known to be the cause behind the majority of security incidents. Three high-risk practices are particularly common: passwords themselves are too weak, such as too short or chosen from a dictionary; passwords are stored in a non-secure place, such as written on piece of paper by the keyboard, which is a classic; and, finally, passwords are not changed frequently enough. These bad practices combined with an ever increasing number of passwords for each user to remember — often 10 or more per user — lead to a single conclusion: organizations can no longer afford to ignore password management. Unfortunately, implementing an adequate solution is not as simple as it might seem, mainly due to of the lack of authentication standardization. Indeed, too many applications still use their own authentication database without offering the possibility of integrating it into a directory, or even a public key management infrastructure.

-
- **Integrated ESSO** — Citrix Password Manager, as an Enterprise Single Sign On (ESSO) solution, is designed to take care of all authentication requests that are required by Windows, Web, and host-based applications. The integration of a new application within a company's infrastructure does not affect its operating mode in any way, including authentication. It keeps its own proprietary user database and its own in-house authentication method.
 - **Technology working for the user** — By entering passwords on behalf of the user, Password Manager simplifies password management and reinforces security at critical points. It enables passwords to be entered only once — at first launch. After that, Password Manager will submit them automatically on the user's behalf each time an application requires them. Those encrypted log-ins are stored both locally and remotely, in the company directory where they are just simple objects attached to the profile of each user, or on a network share. Because users no longer have to deal with passwords, these can be as long and complex as is necessary for security. The administrator can define their length, the minimum amount of figures, letters or special characters, and so forth. And, of course, they can be changed as often as desired, completely transparently from a user perspective.
 - **Simplified integration** — Password Manager easily integrates with the Windows and Novell OS because it does not require the GINA authentication library to be replaced. Instead, it makes the most of the Microsoft chaining capabilities, which allow its own library to be used after the main authentication has taken place.

"The Citrix solution supports our key Health Insurance Portability and Accountability Act goal — giving people access to only the information they need. Recently a HIPAA security risk assessment was conducted and the consulting firm found no security holes or problems with our Citrix system. That was great news."

— **Tim Kruse, Supervisor of IT Development, Saint Anthony's Health Center**

INTEGRATING STRONG AUTHENTICATION TO THE LEGACY

IT and Security teams are only too familiar with the problem of strong authentication: the organization obviously can't do without it, but even when the solution is deployed, everything remains to be done. For example, it must be ensured that every new module added to the information system can integrate into it, which is not always as easy as it seems. As another example, an application imposed today by the operational teams might not recognize the two-factor authentication solution chosen by security architects the year before. In such a situation, a software relay needs to be installed in order to translate authentication requests — until the next such incident occurs.

- **It all starts from the legacy** — With Citrix, there is no ripping and replacing of the existing infrastructure. The authentication procedures implemented use the standard Microsoft and Novell GINA libraries, as well as UNIX authentication procedures. Furthermore, the Citrix architecture does not have its own user base. Instead it uses the existing one, such as the company directory, for instance. Therefore, log-in procedures do not need to be modified.
- **Smart cards and secure tokens** — What is more, existing authentication procedures by smart cards or tokens, such as RSA SecureID, Secure Computing SafeWord or Vasco, can easily integrate with the Citrix architecture. As a result, these methods can be used to authorize Citrix sessions for remote access to business applications, data, and so forth.
- **Smart card authentication on Windows 9x** — Although the Windows 9x operating systems do not natively support smart card authentication, Windows 9x-based clients can recognize smart cards when opening a session on a Citrix server. The process is completely transparent and is made possible only by Presentation Server's native smart card support; however, the card cannot be used to control local log-ins. This allows strong authentication to be provided on existing software, thereby extending its lifecycle. As well, through Password Manager, the Citrix solution can integrate with most two-factor authentication solutions that are currently available, including token, biometric, and proximity security systems.

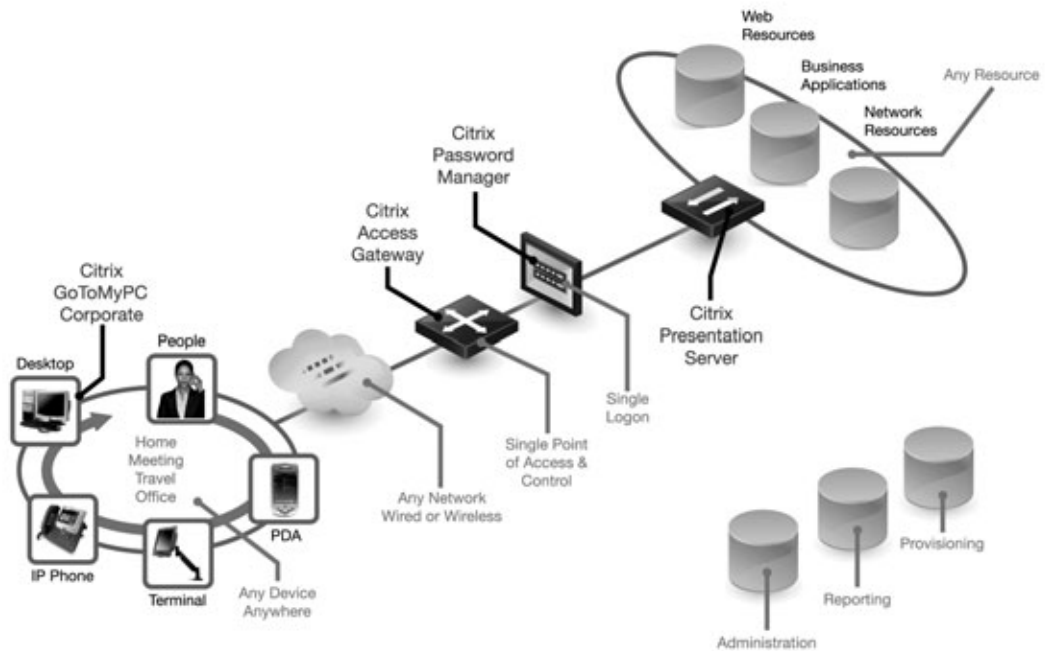
REMOTE ACCESS TO PCs IN COMPLIANCE WITH HIPAA AND GRAMM-LEACH-BLILEY

The Health Insurance Portability and Accountability Act (HIPAA) calls for privacy and security standards that protect the confidentiality and integrity of patient health information. Every business that is part of the U.S. healthcare industry needs to comply with the federal standards regulating patient information. In addition to protecting worker health insurance coverage, HIPAA sets forth standards for protecting the integrity, confidentiality, and availability of electronic health information. Citrix GoToMyPC Corporate is a HIPAA-compliant remote-access solution that can help an organization or an office to meet these guidelines.

The Gramm-Leach-Bliley Act of 1999 establishes standards for financial institutions relating to administrative, technical, and physical safeguards regarding customer records and information. The GoToMyPC Corporate managed service applies to these provisions: Section II: Standards for Safeguarding Customer Information, Sections A and B, and Section III: Development and Implementation of Customer Information Security Program, Section C. The security architecture of managed services offered by Citrix includes policy definition and enforcement mechanisms consistent with the best-practice guidance given for user management and remote access with the Act.

At A Glance

Citrix Product Family	Regulatory Compliance
Citrix Access Essentials™	
Citrix Access Gateway™	•
Advanced Access Control option	•
Citrix Application Gateway™	
Citrix® Voice Office option	
Citrix® GoToAssist™	
Citrix® GoToMeeting™	
Citrix® GoToMyPC® Corporate	•
Citrix® NetScaler® Application Accelerator	
Citrix® NetScaler® Application Switch	
Citrix® NetScaler® Application Firewall	
Citrix Password Manager™	•
Citrix Presentation Server™	•



Citrix for Regulatory Compliance

Speed Disaster Recovery

Citrix enables displaced workers to serve customers and access the company information and people that they need, from anywhere, securely. This vital component of a complete disaster recovery solution reduces the impact of natural, accidental, and man-made business interruptions by enabling organizations to recover the comprehensive information infrastructure, from the data center to the endpoint user environment, quickly, securely, and with minimal business impact, and to create a virtual workplace that preserves employees' sense of corporate community and their ability to conduct business as usual.

"I chose to evacuate my family to North Carolina just prior to the storm (Hurricane Frances, when state officials ordered the largest evacuation in Florida's history). Through the powerful combination of Citrix capabilities and high-speed wireless connectivity, I was able to maintain continuous access to email and other critical applications both during the trip and once I reached the destination."

— **Dave Lauer, Chief Information Officer, City of Jacksonville, Florida**

Here's what Citrix delivers:

QUICKLY RE-ROUTE EMPLOYEES TO BACKUP SYSTEMS

Citrix Presentation Server™ provides secure, Web-based access to essential business resources to allow users to work from anywhere using any device, over any network connection. Presentation Server simplifies disaster recovery, assuring access to corporate resources by automatically and seamlessly connecting users to the best and/or nearest server group that is available. With Presentation Server, an administrator has the ability to configure zone preference through the use of a policy rule. This policy rule allows the administrator to direct user connections to particular zones in the server farm and to configure failover in the event that a zone is not available. If this policy is configured, the user connection is directed to the server with the highest zone preference and the smallest load.

MAKE ANY PC ANYWHERE AN OPERATIONAL WORKSTATION

Citrix differentiates applications, their format, and their users, and does not require that these factors be in the same geographical location. This special feature greatly facilitates staff relocation, as any PC can immediately become an operational workstation because a simple Internet browser, or the installation of the Citrix client software, is all that is required, essentially creating a common universal client device.

WHEN THE OFFICE IS OKAY, BUT THE EMPLOYEES CAN'T GET THERE

From train strikes to mud slides and health hazards such as bird flu, an organization's ability to conduct business as usual can be impacted when its people can't get to the office, even though the facility is fine. Citrix GoToMyPC allows employees to access their usual work environment, if their office PCs are up and running. In fact, many Citrix employees in California used this capability after a mud slide in 2005 that closed key roads — they were online and had access to everything they needed to work from home.

REDEPLOY WORKSTATIONS AND CAPTURE EMPLOYEES' USUAL WORK ENVIRONMENT

By remotely connecting via a browser or a Citrix client, users regain exactly the same work environment — including their files, their business applications, their office suite, and their interfaces — wherever they are: at home or in temporary business premises. All of this is made possible by a simple Web browser or by a unique software client which does not take more than a few megabytes of disk space — and which is available as a free download from the Citrix Web site.

PRESERVE USERS' STORED CREDENTIALS AND THEIR EASY, SECURE ACCESS TO APPLICATIONS

Citrix Password Manager deployments can be designed and implemented to take advantage of redundant, or disaster recovery, sites, providing continued single sign-on access to applications and preserving users' stored credentials in a secure fashion. Password Manager stores its administrative settings and each user's credentials in Active Directory. If there is an Active Directory domain controller or restored backup in a disaster recovery site, then — via replication — all of the users' settings and credentials would be preserved. With Password Manager as part of an organization's overall disaster-recovery strategy, users do not lose their credentials when there is a disaster and they will continue to have a single-sign-on experience when they access applications on a presentation server in the disaster-recovery site. As well, if the users have Password Manager installed locally and are unable to connect to a datacenter, they will still be able to achieve single-sign-on to their accessible applications because Password Manager has the ability to work in offline mode.

RE-ESTABLISH THE CORPORATE COMMUNITY, ONLINE

Fostering employees' sense of corporate community is challenging when everyone is scattered, working at home, perhaps, or in temporary facilities. As well, returning to business as usual means meetings as usual, training as usual, collaboration as usual. Citrix® GoToMeeting™, as a managed service, enables organizations to bring everyone together, to instantly and easily meet online, regardless of their geographic dispersion.

REMOTE TECHNICAL SUPPORT THAT REMAINS WORLD CLASS

Any time that employees are not working on site, technical assistance from the support staff of external contact centers or internal help desks is critical to their productivity. When there are disasters and other business disruptions, this becomes even more important. During these events, Citrix® GoToAssist™ enables organizations to continue providing best-in-class support over the Internet; as a managed service, it maintains the infrastructure that supports the service.

AN INTERCHANGEABLE APPLICATION INFRASTRUCTURE

In order to benefit from such a quick recovery, the company's application and Presentation Servers need to be operational at all times. As a preventive measure, they might be located at a remote site. However, even if they were affected by the disaster, the modularity of the Citrix architecture makes a timely resumption possible. If the company has put in place a backup Citrix Presentation Server farm and the application servers, users can be automatically redirected towards a new entity in failover mode and continue to work as if nothing had happened. Plus, the simplification of backups and the centralization of applications allow the information system to be rebuilt much more quickly and, above all, much more easily.

SIMPLIFY BACK-UPS

The difficulty in backing up business data is not so much of a technical nature, but rather of an organizational nature. Companies must identify all of the information that needs to be backed up, no matter where it is located, and the information very often is scattered across hundreds of servers and thousands of clients. Plus, the backup plan must be constantly updated in order to include new applications. By centralizing business applications on a limited number of servers and by removing the need for information-rich clients, Citrix allows organization to avoid storing sensitive data on client devices.

- **Storing data centrally** — With Citrix, data from client applications and users' personal folders are stored centrally — not on each desktop. This information is published by file servers at the heart of the information system where RAID-based storage technology can be deployed and backup solutions implemented.
- **Anti-theft protection** — Centralization also allows intellectual property to be more tightly protected. The loss or theft of client devices no longer involves the risk of data being stolen. Devices do not, in fact, contain any data, but simply the standard Citrix client or even a simple standard browser to connect to the access center via the Citrix Access Gateway.
- **Tightened control for sensitive documents** — Finally, to ensure that users do not keep copies of the documents on which they work, the Citrix solution can forbid remote users from saving them locally or from printing them.

LEVERAGE IP TELEPHONY FOR FAST ACTION

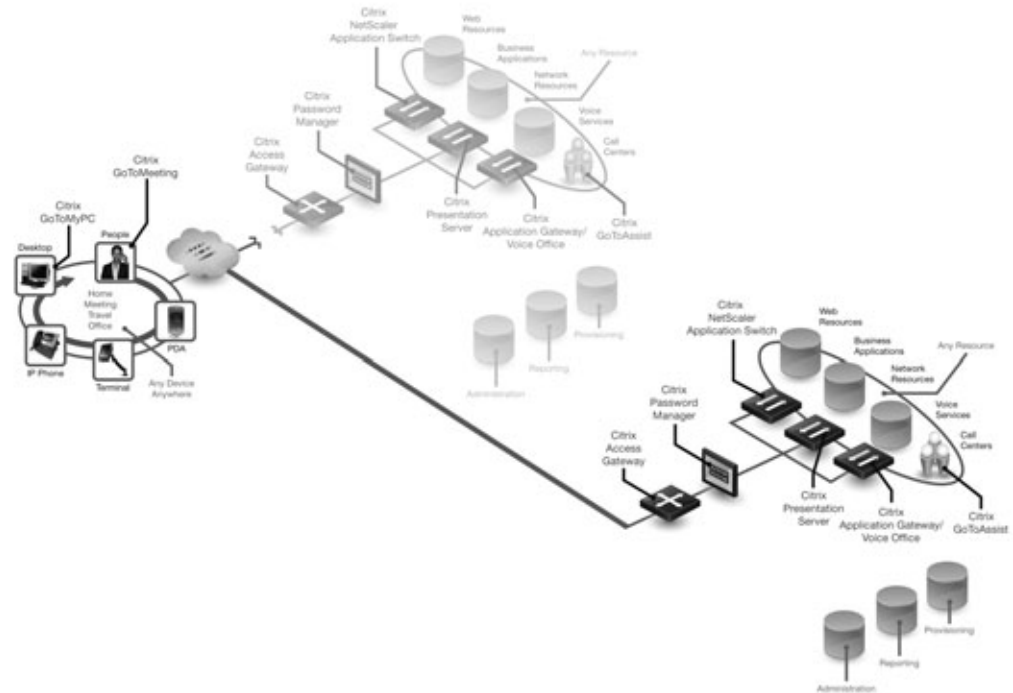
Because it is easier and faster to get an IP network up and running than it is the regular telephone system, due to the ability to put in a portable IP telephony system just about anywhere, organizations can leverage their IP telephony systems for disaster recovery in several ways. For example, call centers could be up and running faster, and use the Citrix Application Gateway™ to deliver high-performance, converged voice and data applications to the screens and speakers of the IP telephones, securely and simply. As well, the Citrix® Voice Office suite of packaged, converged IP telephony applications for organizations with Cisco and Nortel IP telephones can be used for both emergency and non-emergency functions. Delivered by the Application Gateway, Citrix® Zone Paging can replace an overhead paging system that has been destroyed or rendered useless because the facility is inaccessible. Using Zone Paging, the IP phones essentially replace overhead speakers for delivering audio messages. Citrix® Broadcast Server can transform IP phones into information kiosks, delivering priority messages such as emergency, IT, and weather alerts to the screens of the IP phones.

KEEP SERVICING ONLINE CLIENT REQUESTS BY THE MILLIONS

On any given day, organizations throughout the world are servicing the client requests of many, many millions of Internet users. Some of these organizations themselves operate on a vast scale, with multi-site application environments, increasing by orders of magnitude the impact of a disaster or other event that affects application availability. The Global Server Load Balancing (GSLB) feature option for the Citrix NetScaler Application Switch maintains application availability when there is a data center outage, transparently redirecting user traffic to the closest surviving data centers, based on either geographic or network proximity. In addition, proximity-based GSLB dynamically detects changes in global network performance and site reachability, further protecting against application outage scenarios.

At A Glance

Citrix Product Family	Disaster Recovery
Citrix Access Essentials™	
Citrix Access Gateway™	•
Advanced Access Control option	•
Citrix Application Gateway™	•
Citrix® Voice Office option	•
Citrix® GoToAssist™	•
Citrix® GoToMeeting™	•
Citrix® GoToMyPC® Corporate	•
Citrix® NetScaler® Application Accelerator	
Citrix® NetScaler® Application Switch	•
Citrix® NetScaler® Application Firewall	
Citrix Password Manager™	•
Citrix Presentation Server™	•



Citrix for Disaster Recovery

Citrix Worldwide

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com

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.



Best Access Experience. Anytime. Anywhere.

About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and most trusted name in on-demand access. More than 180,000 organizations around the world rely on Citrix to provide the best possible access experience to any application for any user. Citrix customers include 100% of the *Fortune* 100 companies and 98% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and individuals. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Citrix annual revenues in 2005 were \$909 million. Learn more at www.citrix.com.

©2006 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler®, GoToMyPC®, Citrix Presentation Server™, Citrix Password Manager™, Citrix Access Gateway™, Citrix Access Essentials™, Citrix Access Suite™, Citrix SmoothRoaming™, Citrix Subscription Advantage™, GoToMeeting™ and GoToAssist™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. UNIX® is a registered trademark of The Open Group in the U.S. and other countries. Windows® is a registered trademark of Microsoft Corporation in the U.S. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

30691/0506/2500