CiTRIX®

Desktop virtualization and security: a global market research report

Research Note

The research presented in this paper was conducted by Vanson Bourne, an independent market research company, and commissioned by Citrix. A representative sample of 1,100 senior IT decision makers was polled from 11 countries across the globe during October 2011. Three-quarters of respondents were from organizations of more than 1,000 employees; the remainder were from organizations of 500 – 999 employees.

The 11 countries included in the research are: Australia, Brazil, Canada, China, France, Germany, India, Japan, the Netherlands, the United Kingdom and the United States.

www.citrix.com

Introduction

As desktop virtualization technology has matured and gained widespread implementation, organizations around the world increasingly recognize the broad spectrum of benefits it delivers and view it as a strategic investment that forms a fundamental part of their IT infrastructure. Beyond the impact on business flexibility, productivity and efficiency, desktop virtualization can also play an important role in risk management by transforming the way organizations approach information security and compliance.

Familiar advantages of desktop virtualization include the ability to enable a more flexible workplace, support for mobile workers and associated work styles, as well as providing IT with an effective way to manage the growing variety of computing devices in use across an organization. For many organizations, desktop virtualization contributes significant savings, from more-efficient desktop management to the reduction of office space and real estate costs. Security has now joined these benefits as a key factor in the decision to implement desktop virtualization. In fact, 92 percent of the organizations that will have desktop virtualization in place by the end of 2013 are adopting it in part to improve information security.

The security benefits of desktop virtualization are inherent in its architecture, which revolves around the centralization of desktops, applications and data for delivery to endpoint devices. This consolidation supports highly effective central management and granular, policy-based access control, and supports compliance requirements through the monitoring, logging and reporting of information access and usage. Flexible options for the delivery of desktops, applications and data to authorized workers, including the ability of these workers to use any type of endpoint device—PC, laptop, thin client, tablet or smartphone—enables the organization to protect its information while optimizing worker flexibility. Indeed, 95 percent of the senior IT decision makers implementing desktop virtualization consider it very effective for protecting information while enabling workers with fast and effective access to the information they require.

Citrix has long held the ideal that an effective information security strategy must ensure the security of an organization's data and application resources while allowing workers to access the resources they need, when and where they need them—a balance made possible only through desktop virtualization. Organizations in every part of the world increasingly share this view, and are making desktop virtualization a central part of their security strategy.

This research report is based on the insights and experiences of 1,100 senior IT decision makers from organizations of over 500 employees, across 11 countries in North America, South America, Europe and Asia. As one of the most comprehensive reports ever conducted into the security aspects of desktop virtualization, it reflects the growing consensus of those using technology to improve the performance of their organization.

Desktop virtualization moves to the forefront of information security

As today's virtual enterprises, distributed workforces and mobile work styles pose new information security challenges, desktop virtualization has emerged as a key strategy for maintaining control over information resources and the way they are accessed. This recognition comes in the context of a broad trend across organizations of all kinds to adopt desktop virtualization.

The vast majority of organizations surveyed (91 percent) have implemented desktop virtualization or plan to do so before the end of 2013. One-third (33 percent) of organizations have already deployed desktop virtualization to a significant level, with a further 58 percent planning to do so by the end of 2013.

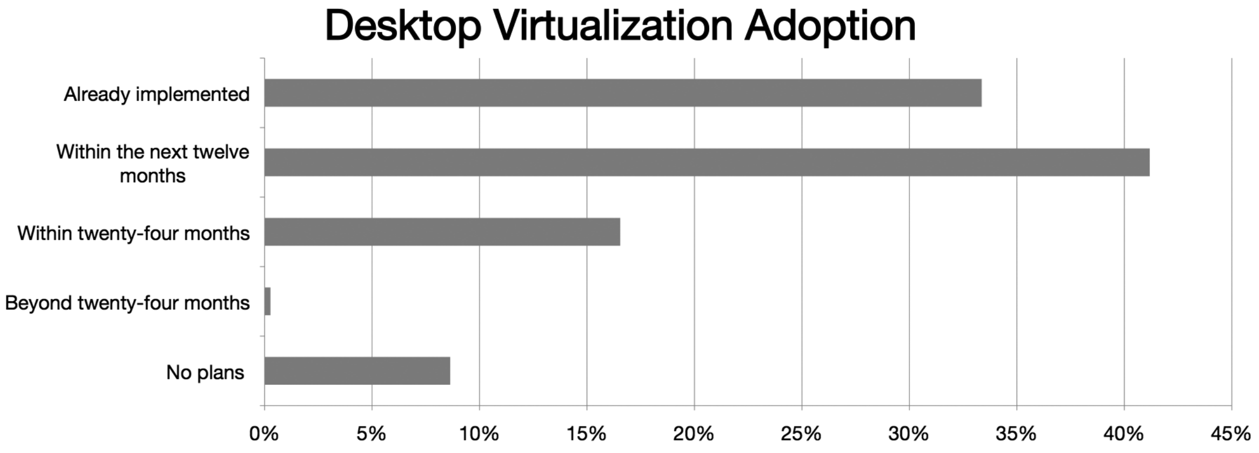

Figure 1 – Desktop Virtualization Adoption. Source: Citrix Global Security Index

Of the organizations planning to have desktop virtualization in place by the end of 2013, 92 percent are adopting it in part to improve information security. Indeed, three of the six principal benefits these senior IT decision makers attribute to desktop virtualization are security related.

The appreciation of the security-related benefits of desktop virtualization is not limited to those already planning to implement it. An overwhelming number (86 percent) of senior IT decision makers believe that desktop virtualization offers a strategic approach to improved information security, regardless of whether they intend to use desktop virtualization within their own organization.

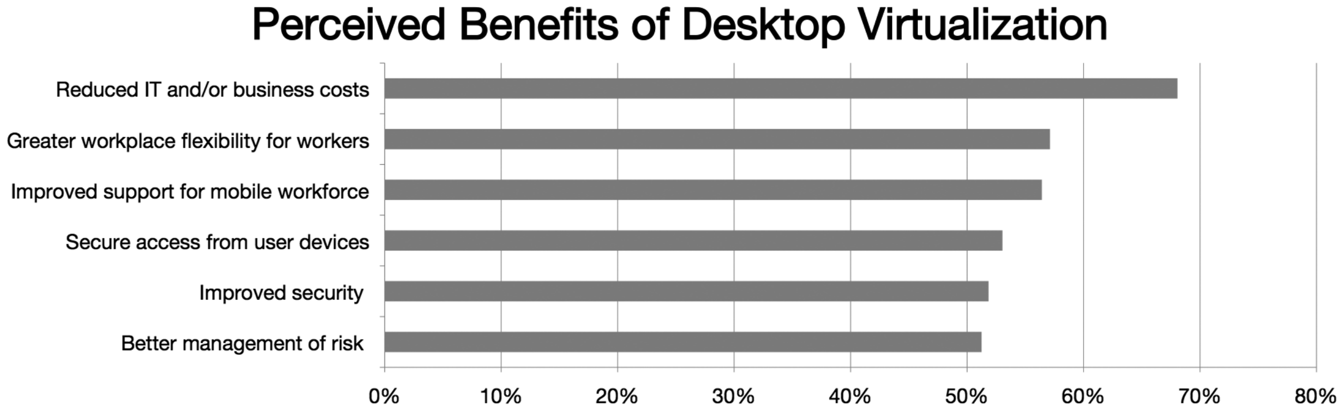

Figure 2 – Perceived Benefits of Desktop Virtualization. Source: Citrix Global Security Index

Resource centralization combines security with worker flexibility

The close relationship between effective desktop management and improved information security makes desktop virtualization central to two of the most pressing IT issues currently facing organizations.

Many organizations' IT departments have slipped behind the curve of trends such as the consumerization of IT, device proliferation, increased mobility and workforce flexibility. Data now sits everywhere, from enterprise networks, to public and private clouds, to a wide variety of endpoint computing devices, including worker-owned tablets, smartphones and computers. An increasingly dispersed and mobile workforce now extends across home offices, branches, project sites and customer settings, and in transit among these locations. More and more of these workers are likely to be outside of the traditional full-time employee model, including consultants, contractors, temporary workers and partners such as agencies and outsourcing vendors.

Desktop virtualization helps organizations support this distributed computing environment while maintaining control over IT resources by centralizing the management of desktops, applications and data, making them securely accessible from any endpoint device. This creates an inherently secure infrastructure layer that improves risk management efficiency and eliminates the need to "lock down" the computing environment through device standardization, overly restrictive user policies and cumbersome generic network and endpoint security measures. As a result, workers can work flexibly and securely from anywhere, on any device, in a user-friendly environment that enables improved productivity, superior customer service and greater business agility.

Of the senior IT decision makers who will have desktop virtualization in place at the end of 2013, 95 percent believe it is very effective at protecting information while providing workers with unfettered access to the information they require.

More effective desktop management improves security

Effective desktop management enabled by desktop virtualization, including the ability to centrally maintain and update individual PCs, has important implications for information security. Industry analyst firm Gartner Inc. estimates that 90 percent of successful attacks occur against previously known vulnerabilities where a patch or secure configuration standard was already available[1].

By centralizing desktops, applications and data, desktop virtualization makes it possible for IT to deploy application and security updates and patches in a more timely and consistent manner, significantly reducing vulnerabilities and potential exploitations. The ability to instantly de-provision access to information resources for any worker, regardless of the location of their endpoint, is especially valuable as organizations rely on more third-party partners, vendors and workers, and delivers considerable protection against threats such as employee malfeasance.

Given this level of control, an overwhelming 97 percent of senior IT decision makers expect desktop virtualization to help their organization respond to new and emerging security threats, citing in part the ability to quickly and centrally update and patch applications on distributed PCs and other computing devices.

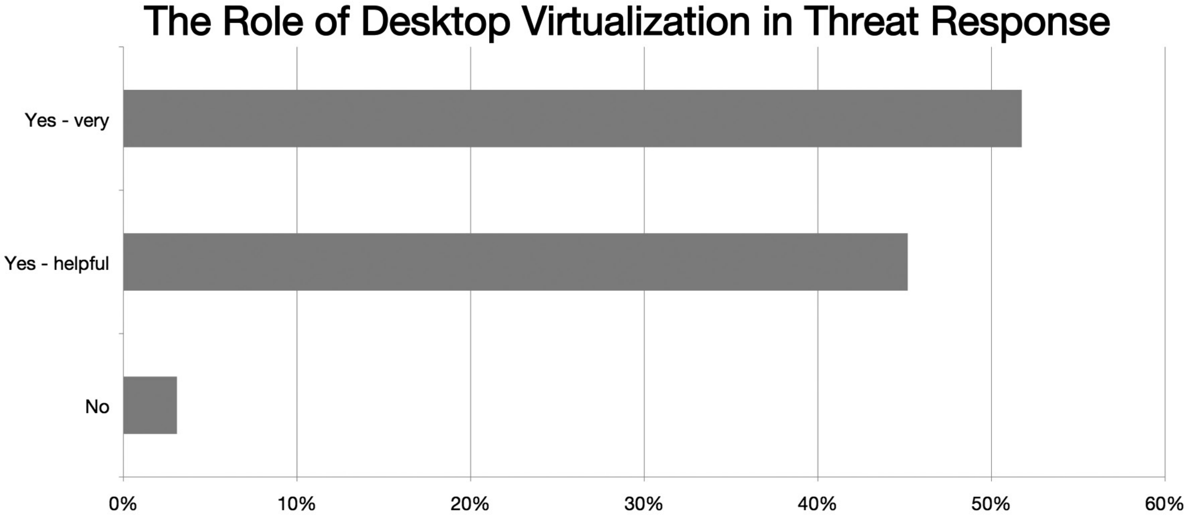

Figure 3 – The Role of Desktop Virtualization in Threat Response. Source: Citrix Global Security Index

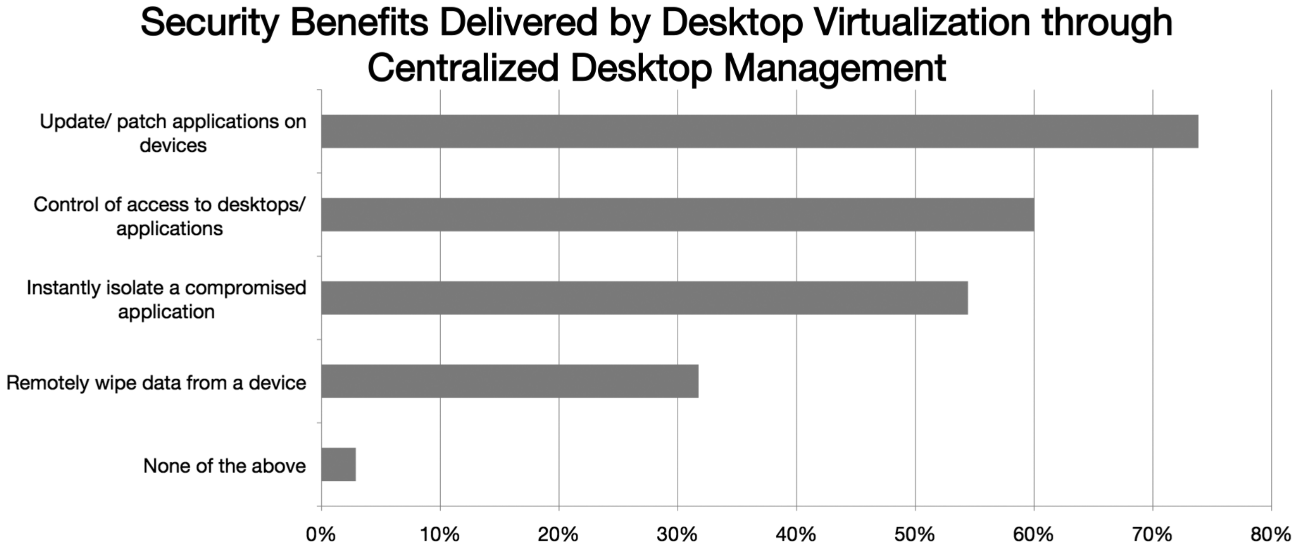

Figure 4 – Security Benefits Delivered by Desktop Virtualization through Centralized Desktop Management. Source: Citrix Global Security Index

[1] Gartner, "Managing the Next Generation of Client Computing," Terrence Cosgrove, February 2011

Desktop virtualization protects information resources and ensures compliance

The security benefits of desktop virtualization extend beyond a secured desktop environment to encompass infrastructure-level capabilities, as well as a way to facilitate and improve compliance. By creating a secure layer of IT infrastructure that extends from the datacenter to user endpoints of all types, desktop virtualization provides a comprehensive security solution to protect against and counter a broad range of threats such as the theft of intellectual property, data loss or tampering, the exposure of client or customer data and the violation of client confidentiality. In this way, desktop virtualization helps organizations prevent breaches that can incur serious liability risks, damage brand reputation and lead to significant financial loss.

This diverse range of security benefits is reflected in the views of senior IT managers. Two-thirds (66 percent) of those implementing desktop virtualization say that the secure delivery of applications and data was an important factor in their decision to do so. Regardless of whether they intend to implement now, the majority of senior IT decision makers felt that desktop virtualization both addresses compliance requirements and protects against a wide range of security threats. Many also cited access management and activity monitoring, logging and reporting, as well as the ability to support a wide range of user devices.

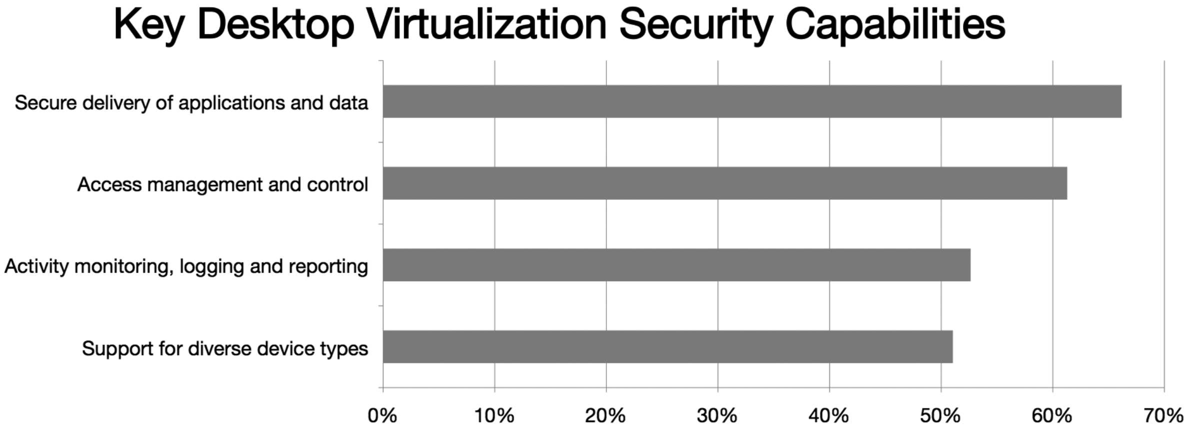

Figure 5 – Key Desktop Virtualization Security Capabilities. Source: Citrix Global Security Index

By centralizing resources in the datacenter, desktop virtualization enables IT to manage and secure applications and data simply and effectively in a single location rather than across thousands of different locations throughout the organization and beyond. As a result, senior IT decision makers regard desktop virtualization as very effective in protecting against malicious threats, such as custom malware and targeted hacking, data loss and intellectual property protection, the exposure of private data, theft of confidential information and wrongful tampering with enterprise data.

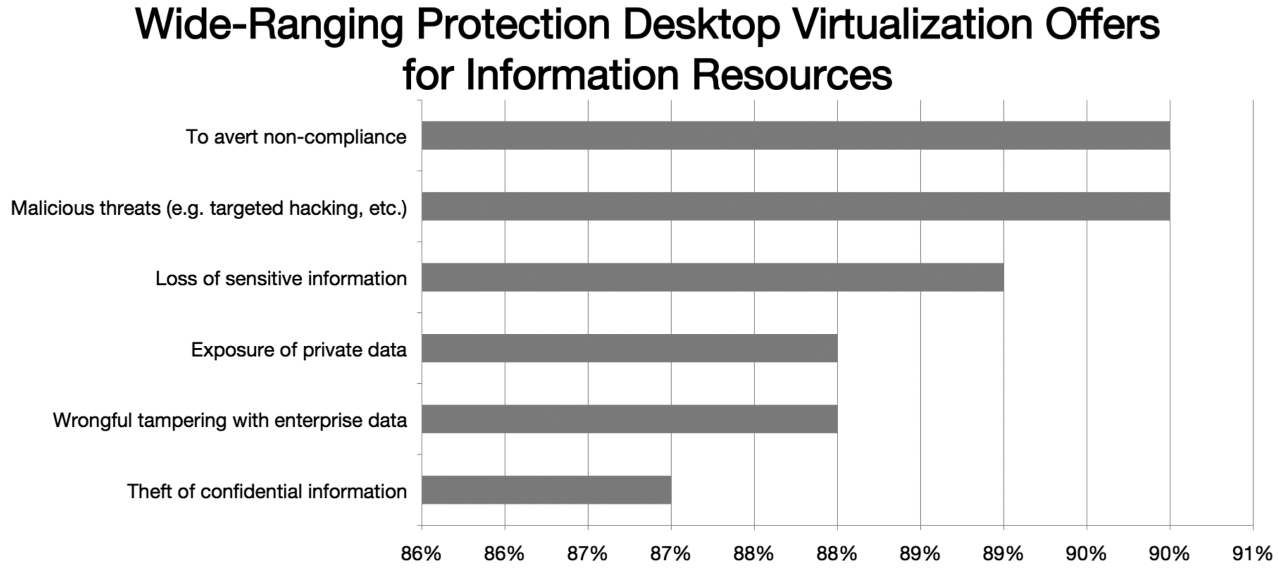

Figure 6 – Wide-Ranging Protection Desktop Virtualization Offers for Information Resources.
Source: Citrix Global Security Index

Instead of worrying about data being saved on removable media such as USB drives, e-mailed among users, printed out or otherwise exposed to loss or theft, IT can set policies to control the ability to save, copy, print or otherwise move data through a central point of administration. For business cases that require offline or locally installed resources, desktop virtualization can also support the encryption, isolation and control of data on the endpoint.

Centralized, granular policy control helps IT take a proactive approach to compliance with increasingly strict national and international regulations, industry standards and internal policies to which organizations must adhere. The combination of resource centralization, strict access control and full activity monitoring, logging, reporting and auditing helps the organization develop and support a strategy to meet not only regulatory requirements but also its own industry, needs and risk profile. Of all senior IT leaders surveyed, 90 percent considered desktop virtualization very effective for ensuring compliance.

The centralization of information assets in the datacenter helps improve information privacy. The IT department can control who has access to what data and applications (determined by granular access policies), and control end-to-end encryption. IT can engage the compliance features of this model, leveraging monitoring, logging and reporting to track access to information and further safeguard data.

Desktop virtualization is complemented by other security technologies

Desktop virtualization delivers a secure layer of IT infrastructure that organizations see as a critical component of their overall information security strategy and a foundation for new measures to address emerging security needs. The 91 percent of organizations across the globe that will have desktop virtualization implemented by the end of 2013 plan to complement it with cloud-based security services, as well as additional data loss prevention, identity management and authentication measures. There will, of course, also be a continuing need for dedicated threat management systems such as antivirus, anti-malware, firewall and intrusion detection.

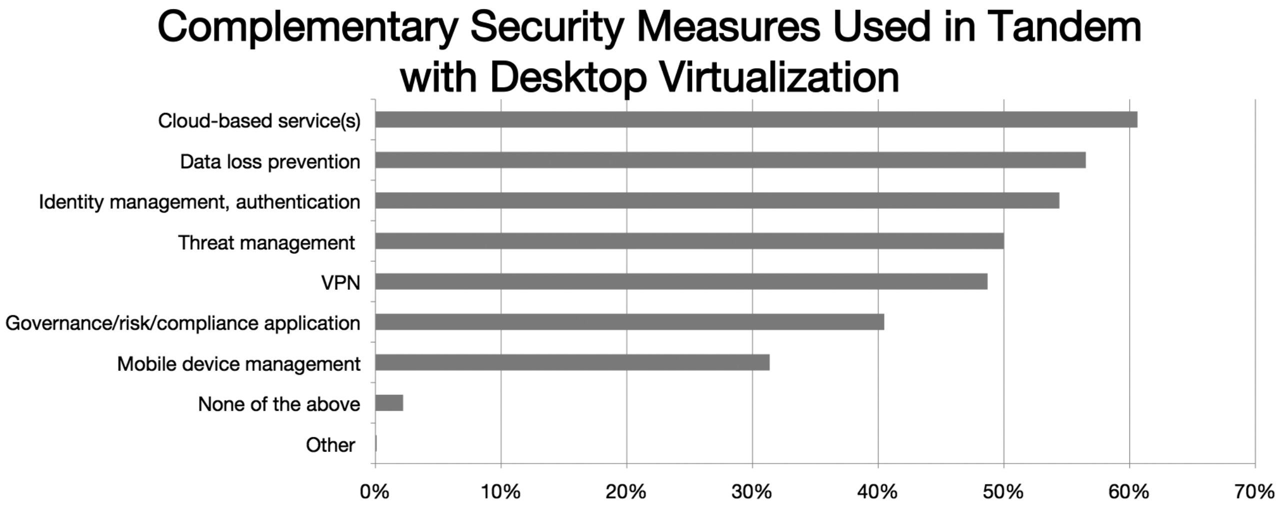

Figure 7 – Complementary Security Measures Used in Tandem with Desktop Virtualization.
Source: Citrix Global Security Index

Desktop virtualization creates secure infrastructures

The research discussed in this report makes it clear that for organizations of over 500 employees, the minimum size included in this survey, desktop virtualization is now at the heart of the modern information security strategy.

The inherent weaknesses of legacy security strategies for today's more-complex computing environment make it difficult, if not impossible, to regain control over desktops, applications and data through these approaches. A common reaction is to lock down access and force everyone to work within the enterprise LAN on standard, enterprise-owned devices. However, with the need for greater business agility, workplace flexibility, cross-enterprise collaboration and consumerization of IT, such draconian security measures place unacceptable constraints on business productivity. They are also often counterproductive, compelling workers to seek ways of circumventing the rules to get their jobs done, which creates significant additional risk.

Desktop virtualization enables organizations to transform their approach to information security and compliance. By centralizing data, applications and access control, desktop virtualization delivers an unprecedented level of information security management, even across the complex IT environments typical of large organizations. At the same time, it empowers both workers and their organizations to leverage benefits of the consumerization of IT and to take advantage of workplace flexibility by shifting work to preferred times and locations.

As organizations seek to address critical information security and compliance priorities, desktop virtualization offers both comprehensive capabilities for improving control over enterprise data and applications and well-established best practices for realizing the full benefits that inherently secure technology makes possible.

Additional resources

White papers

Five Customers Use Desktop Virtualization for Security

Top 10 Reasons to Strengthen Information Security with Desktop Virtualization

Desktop Virtualization: Empowering Information Security

Refactoring Sensitive Data Access: Benefits of Desktop Virtualization Security

Websites

www.citrix.com/secure.

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

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 6301-10, 63rd Floor
One Island East
18 Westland Road
Island East, Hong Kong, China
T +852 2100 5000

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

www.citrix.com

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2010 was $1.87 billion.