Defend Web Properties from Modern Threats with Citrix NetScaler

CITRIX®

Defending your organization's web properties has never been more challenging. In the past, IT security teams had just a handful of enterprise web apps to defend. Now they must protect the web backends of many mobile apps, SaaS apps and other cloud-delivered solutions.

At the same time, the number and diversity of threats are increasing. For example, modern defenses must account for far more than just the most prominent part of the threat landscape, advanced malware. Other targeted threats that require diligence include web-specific application-layer attacks, denial and distributed denial of service (DoS/DDoS) attacks and security-induced usability issues.

This white paper examines the challenges of defending modern web properties from modern threats. It explains how the Citrix® NetScaler® application delivery controller (ADC) complements advanced malware protection and other high-profile security products to provide an ideal solution for defending against new threats and protecting more targets. The benefits of utilizing NetScaler in this capacity include:

- Reduced security risk by thwarting not only advanced malware but also DoS and targeted application-layer attacks.
- Reduced business risk as security automation, enhanced usability and improved performance increase customer utilization and retention rates.
- Increased business agility from IT's ability to fully embrace transformative mobile, web and cloud solutions without fear of compromise or other types of infrastructure-related failures.

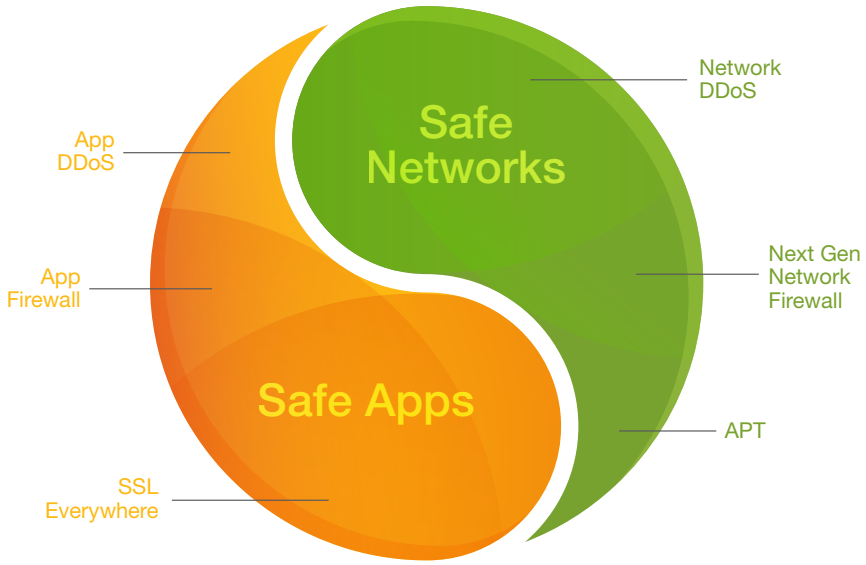

Figure 1: A complete solution for defending web properties

"What about APTs?"
Although vendors of advanced malware protection often lump them together, advanced persistent threats (APTs) and advanced malware are by no means the same thing. In reality, APTs are more about the threat actor—who is well-organized, well-funded and persistent—than the specific class of threat mechanism being employed. In fact, APTs typically employ multiple attack methods and techniques over their duration, including not only advanced malware but also app-layer and DoS elements, for example, to gain access to data and then create a diversion as that data is being exfiltrated.

Modern web properties: not just your typical web apps

In the beginning, web properties involved little more than a browser—typically Internet Explorer—interacting with a corporate website. Fast forward to the present, however, and it is an understatement to say that web solutions have wildly evolved. Now, enterprise web properties entail diverse components, including:

- Numerous browsers interacting with numerous web app components and sites.
- Cloud-hosted web apps/sites and content delivery networks.
- SaaS and other cloud delivery options, such as platform as a service (PaaS) and infrastructure as a service (IaaS), where the enterprise owns and controls progressively less of the solution.
- Mashups, where content is dynamically pulled together from numerous external sites.
- Powerful APIs for enabling supply chain integration and greater automation.
- Mobile solutions where device-side micro apps communicate to sophisticated web-based backends.

As a result, defending web properties is no longer simply a matter of protecting enterprise web apps. The scope of resources needing protection has expanded considerably, most notably to include mobile and cloud solutions.

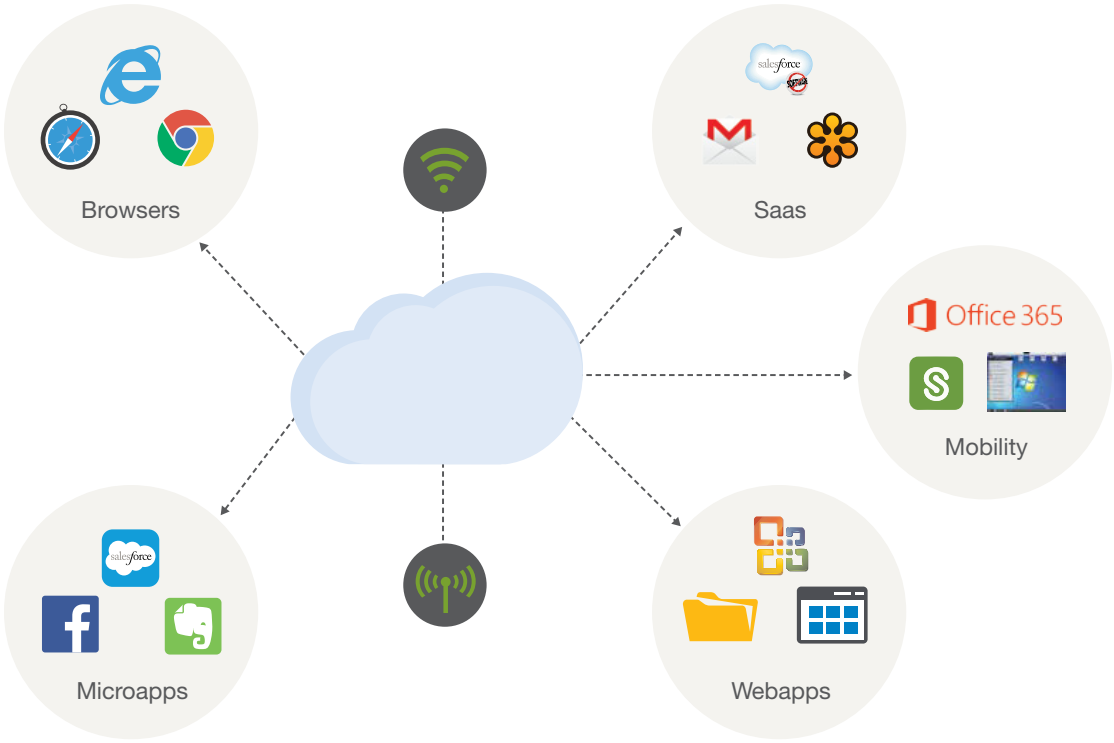

Figure 2: Complex world of web properties

Modern threats: Sophisticated malware is only the tip of the iceberg

Advanced malware is commanding a lot of attention these days, and rightly so. Commonly deployed signature-based defenses are no match for the new generation of malware that is designed specifically to evade them—for example, by targeting previously undisclosed vulnerabilities, leveraging compromised credentials or using polymorphism and other techniques to rapidly change the malicious code's footprint or capabilities.

The result is a clear and present need for today's organizations to invest in advanced malware protection solutions that are not dependent on signature-based mechanisms limited to only detecting previously identified threats—also referred to as known threats. However, advanced malware is only one class of threats that pose significant risk to an organization's web properties. In particular, DoS attacks, web-specific app-layer attacks and usability issues also require threat mitigation.

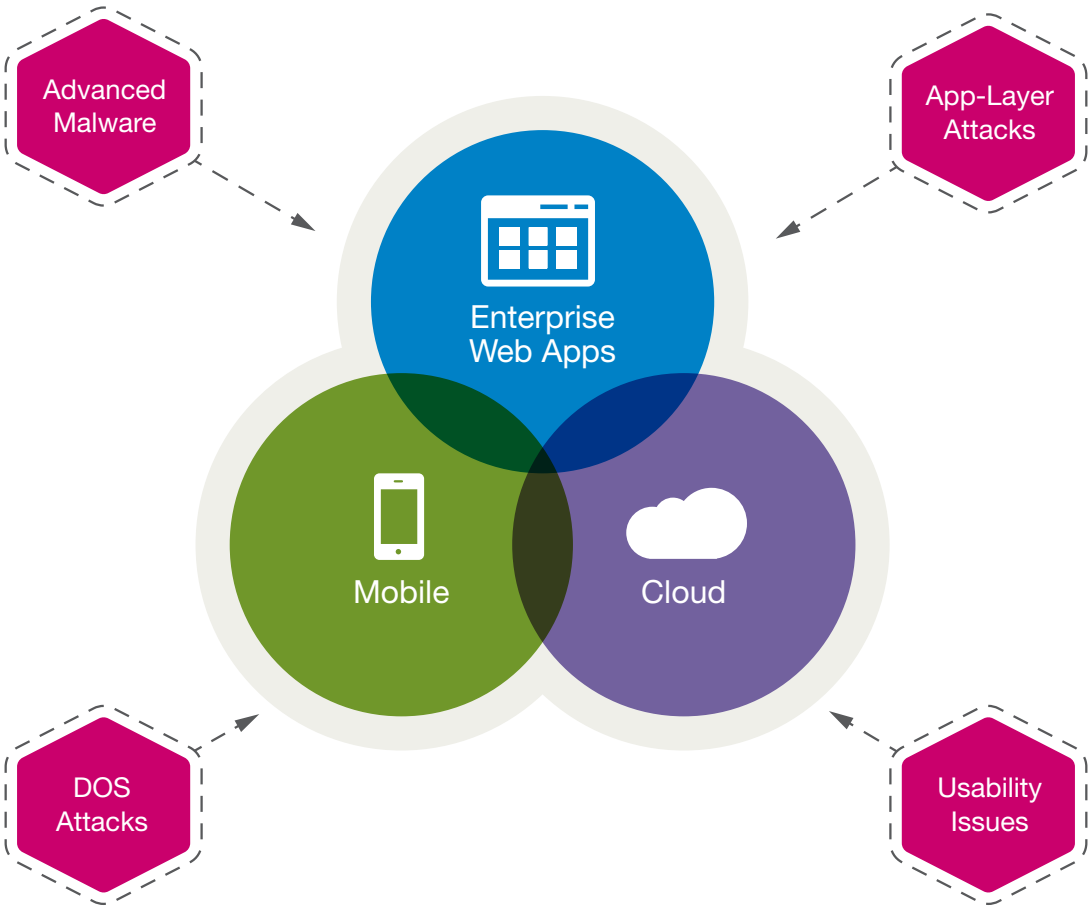

Figure 3: Modern threats landscape

DoS attacks – Over the past couple of years there has been a marked resurgence of DoS attacks, along with significant changes in the nature of the threat itself. No longer are only the largest Internet properties coming under fire. Thanks to the widespread availability of inexpensive toolkits and botnets—for DoS creation and execution, respectively—now every business, regardless of size or industry affiliation, is at risk. Detecting these attacks is also much harder than in the past, as

stealthy, low-bandwidth, application-layer variants focused on exhausting backend resources have now joined the ever-familiar, high-volume attacks intended to flood your Internet pipes or knock over frontend network devices such routers, firewalls or basic ADCs.

Web-specific, app-layer attacks – The threat in this case is not new, but continues to be significant. Faced with a plethora of commonly deployed defenses operating at the network layer, hackers have logically chosen to focus their efforts at the higher layers of the computing stack to achieve more-favorable results. The outcome is a substantial percentage of attacks targeting weaknesses discovered in both widely distributed web technologies and components—such as the HTTP protocol itself, Java or popular web servers and apps—and an organization's own custom web apps. Common threats that fall into this category include cross-site scripting, cross-site request forgery, SQL injection and buffer overflow attacks, just to name a few.

Usability threats – Degraded usability is often overlooked or discounted on the basis that it is technically more of a performance problem than a true security threat. However they are classified, though, usability issues introduced by security solutions are still a very real threat, at least as far as the business is concerned. Poor performance resulting from compute-intensive inspection routines, SSL overload, convoluted logon processes and inconsistent access capabilities can lead users to pursue insecure workarounds and prompt customer dissatisfaction and, ultimately, defection. In addition, compensating for these conditions may require organizations to purchase considerably more or higher-capacity hardware than originally planned. IT security teams, therefore, need to be mindful that security solutions themselves can become a threat if not architected to avoid or otherwise compensate for these types of usability problems.

The bottom line is that defending modern web properties requires accounting for all of these classes of threats, not just advanced malware. The risks incurred by failing to do so include greater potential for data loss or exposure, customer defection, higher total cost of ownership (TCO) and non-compliance liabilities.

Modern defenses: The role of NetScaler

NetScaler, the best ADC for building enterprise cloud networks, is also the ideal solution for defending modern web properties. Already a strategic component in thousands of enterprise datacenters and cloud provider networks, NetScaler delivers extensive web defense capabilities that perfectly complement advanced malware protection solutions, such as those available from FireEye and Palo Alto Networks. With NetScaler, enterprises obtain everything they need to ensure the availability, security, usability and agility of their web properties while successfully thwarting DoS and app-layer attacks intended to disrupt the business and exfiltrate valuable data. Moreover, all of these essential capabilities are available as a tightly integrated solution on a single, highly scalable platform. As a result, enterprises no longer need to invest in and incur the added complexity of operating multiple, standalone security products.

Keeping the lights on

Web properties that are not accessible due to outages are next to worthless, and can even cause damage to a company's reputation. Therefore, NetScaler defenses for web properties start with an extensive set of capabilities for protecting against threats that can disrupt operations and render key services unavailable.

- **High availability (HA) for critical components** – In the event that a web server or other key component of a web property fails for any reason, core load balancing algorithms dynamically route affected traffic to alternate instances configured as part of a pool managed by NetScaler. In this way, NetScaler provides continuous availability during scheduled maintenance and unanticipated failures, as well as attack-induced outages.
- **Health monitoring for proactive failure management** – NetScaler health checks monitor the status of key components and engage core load balancing features to proactively avoid trouble spots. Unlike many competing solutions that merely confirm that a network connection is available and the underlying server is online, NetScaler provides extended content verification checks to further establish that key system-level services and individual software routines are also in proper working order.
- **GSLB for disaster recovery** – A robust global server load balancing (GSLB) feature set provides seamless disaster recovery for modern web properties. If an entire site becomes unavailable for any reason, affected traffic is automatically directed to an alternate datacenter. A consistently positive user experience can also be ensured by taking advantage of intelligent monitors and policies to regularly route sessions to the optimal site based on administrator-selected priorities such as proximity, resource utilization levels or overall performance.
- **Multi-layer protection for DoS attacks** – With NetScaler, organizations obtain a powerful, first line of defense against all types of DoS threats. Coverage is provided not only for volumetric attacks intent on consuming all of your Internet bandwidth, but also for more insidious ones looking to exhaust device state tables, abuse infrastructure or application layer services (e.g., DNS, SSL and HTTP), or somehow misuse application-specific features in a way that substantially degrades performance (for example, by repeatedly issuing requests that lead to complex calculations, backend queries or search operations).

Increasing difficulty of detection

	Sample Attacks	NetScaler Mitigation Features
Application	GET and malicious POST floods; slowloris, slow POST, and other low- bandwidth variants	Application protocol validation, surge protection, priority queuing, HTTP flood protection, HTTP low-bandwidth attack protection
Connection and Session	Connection floods, SSL floods, DNS floods (udp, query, nxdomain)	Full-proxy architecture, high- performance design, intelligent memory handling, extensive DNS protections
Network	Syn, UDP, ICMP, PUSH and ACK floods; LAND, smurf, and teardrop attacks	Embedded defenses, default-deny security model, protocol validatio, rate limiting

Figure 4: "Citrix NetScaler – A Powerful Defense Against Denial-of-Service Attacks"

Surge control for unintended overload events – Major spikes in utilization for a web property can have the same impact as a DoS attack. NetScaler addresses this situation with surge protection, a capability that gracefully handles intermittent traffic surges by basing the rate at which new connections are presented to backend servers on the servers' capacity for handling them. Significantly, no valid connections are dropped with this mechanism. Instead NetScaler caches and delivers connections in the order in which they were received, but only when the backend servers are ready to handle them.

Thwarting advanced threats

Overcoming availability-oriented threats is only a starting point—albeit a critically important one. With NetScaler, organizations also benefit from a solution capable not only of directly thwarting targeted application-layer attacks, but also of working alongside leading third-party products to counteract the latest generation of sophisticated malware.

Protocol defenses for broad-spectrum, application-layer protection – Enforcing RFC compliance and best practices for HTTP use is a highly effective method used by NetScaler to eliminate an entire class of attacks based on malformed requests and illegal HTTP protocol behavior. Custom checks can also be added to the security policy by taking advantage of integrated content filtering, custom response actions and bi-directional HTTP rewrite capabilities. The result is broad-spectrum protection against reconnaissance (e.g., by removing information from server responses that could be used to perpetrate an attack), HTTP-based malware (e.g., Nimda, Code Red), and other application-layer threats.

NetScaler AppFirewall for targeted application-layer threats – Traditional network firewalls lack the visibility and control required to protect against the more than 70 percent of Internet attacks that target application-layer vulnerabilities. In comparison, NetScaler AppFirewall™ is an ICSA-certified security solution that analyzes all bi-directional traffic, including SSL-encrypted communications, to counteract both known and unknown application-layer threats without requiring any modifications to an organization's web properties. Key capabilities include:

- **Attack protection** – A combination of positive and negative security models provides the most comprehensive protection against all modes of attack. To defeat new, unpublished exploits, a positive-model policy engine understands permissible user-app interactions and automatically blocks all traffic falling outside this scope. A negative model engine simultaneously employs attack signatures to guard against and report on known threats to applications.
- **Data theft protection** – Safe Object data checks protect against unexpected leaks of sensitive business information—such as intellectual property or credit card numbers—whether the associated event is due to an actual attack, misuse by an authorized user or a flaw in a web application's design. A combination of administrator-defined regular expressions and custom plug-ins tell NetScaler App Firewall the format of this information, while associated rules specify the appropriate action to take, such as masking the protected field or blocking the entire response from the application.
- **Compliance protection** – NetScaler AppFirewall enables enterprises to achieve compliance with the Payment Card Industry Data Security Standard (PCI-DSS), which explicitly encourages the use of web app firewalls for public- facing applications that handle credit card information. NetScaler produces detailed reports to document all protections defined in the firewall policy that pertain to PCI-DSS or other applicable governance and compliance mandates.

Figure 5: NetScaler protects against leakage of sensitive data, regardless of the type of threat responsible for causing the leak. (source: NetScaler for datacenter security wp)

Citrix Ready partner solutions for stopping advanced malware – While NetScaler does not provide direct detection of all forms of advanced malware, its extensive set of security features nonetheless offers a considerable measure of protection against this ever-growing class of threats. In particular, NetScaler can diminish the impact of malware, for example, by stopping any blended components utilizing common web attack techniques, any components that cause or rely on abnormal application behavior and attempts by malware to exfiltrate sensitive business data. The corresponding network and app-layer event data generated by NetScaler can also be used, typically in conjunction with other event streams, to initially reveal and subsequently help pinpoint the presence of malware. In addition, solutions from Citrix Ready partners explicitly designed to address advanced malware provide threat-specific protection to high-profile enterprises.

Ensuring usability

The need to avoid outages for modern web properties is a given. Less obvious, but arguably more impactful due to their increased likelihood, are usability issues such as poor performance and convoluted or inconsistent processes for gaining access to web properties. Unlike most security solutions, which tend to exacerbate these problems, NetScaler actively works to overcome them through a combination of intelligent design decisions and numerous features specifically focused on accelerating application performance.

High performance assurance – NetScaler features that help enterprises overcome security-, network- and application-induced performance obstacles include:

- Embedded TCP optimizations such as advanced buffering, window scaling and congestion control techniques increase system capacity, lower packet loss rates and improve response times by more efficiently utilizing available bandwidth and server resources.
- In-memory caching of both static and dynamic content (NetScaler AppCache™), combined with aggressive data compression routines (NetScaler AppCompress™) reduce network and server congestion while significantly accelerating application response times.
- By incorporating dedicated SSL acceleration hardware and support for large encryption keys (2048-bit and larger), NetScaler delivers essential encryption capabilities that avoid the need to make tradeoffs between stronger security and a high-performance user experience.

- Priority queuing provides a QoS mechanism for prioritizing incoming requests based on the relative importance of the associated applications.
- By incorporating a SPDY gateway, NetScaler enables use of this increasingly popular protocol that optimizes how HTTP requests and responses are sent over the network without having to modify server-side applications.
- NetScaler ActionAnalytics feature enables fully automated monitoring and response to degraded performance conditions, while NetScaler Insight Center™ provides administrators with in-depth visibility to help identify and remedy emerging issues before they become full-blown problems.

Seamless access – NetScaler features that help mitigate the threat of poor usability by enhancing the user experience in other, non-performance-related ways include support for:

- **Single sign-on (SSO)** – Users need only sign in once, as NetScaler transparently logs them in to all resources within a given domain.
- **Centralized authentication and authorization** – The same extensive set of access control services can be leveraged across all of an organization's web properties, and for all of a user's devices. This capability not only simplifies administration of mobile users and web property, but also ensures a consistent user experience.

Delivering affordability and agility

Another way that a security solution can effectively be a threat—at least from the perspective of business management—is by costing too much or failing to align with key business objectives. Citrix, however, has purposely developed and packaged NetScaler to mitigate these challenges, too.

Unmatched consolidation – NetScaler is the only application delivery solution that combines load balancing, GSLB, SSL VPN connectivity and more on an integrated, highly scalable platform. Competing solutions force organizations to purchase, implement and integrate multiple, separate products and devices to obtain a similar set of capabilities for thoroughly defending and delivering web properties. With NetScaler SDX™, IT departments also gain the ability to consolidate their ADC infrastructure by implementing up to 80 isolated NetScaler instances on a single platform.

Alignment with cloud migration – The ongoing move to enterprise cloud networks is facilitated by the availability of cloud-ready NetScaler VPX™ virtual appliances. A full-featured, software-only version of the NetScaler App Delivery Controller™, this solution provides the flexibility to implement NetScaler threat defense and performance optimization capabilities on demand, anywhere within either the enterprise or a third-party cloud datacenter. NetScaler VPX enables organizations to securely run their web applications and services in whatever location is best for them.

Support for user mobility – When it comes to supporting enterprise mobility initiatives, NetScaler does not stop at defending and optimizing associated web properties. It also provides the same services for related management infrastructure, in particular Citrix XenMobile®. A comprehensive solution for managing mobile devices, apps and data, XenMobile gives users the freedom to experience work and life their way. While IT gains full control and the ability to protect the entire

mobile environment, users gain single-click access to all of their mobile, web, SaaS and Windows apps from a unified corporate app store. Combining NetScaler with XenMobile delivers:

- High availability for key components of the enterprise mobility infrastructure.
- Additional layers of protection for mobile devices, apps and data.
- The ability to scale mobile operations without disrupting employees or requiring forklift upgrades.

Conclusion

Defending your organization's web properties entails far more than protecting a handful of enterprise web applications from the scourge of advanced malware. Defenses must also be mounted for web backends supporting native mobile apps, SaaS solutions and other cloud-delivered services. Moreover, these defenses must provide coverage for other, equally troublesome classes of threats, including application layer attacks, DoS attacks and security induced usability issues.

Citrix NetScaler is an ideal complement to today's high-profile, advanced malware solutions. The NetScaler ADC:

- Reduces security risk by mitigating other top classes of threats to web properties, including DoS and app-layer attacks.
- Reduces business risk by enhancing web property usability and performance to increase user attraction and retention.
- Lowers total cost of ownership by providing extensive opportunities for infrastructure consolidation and optimization of resource utilization.
- Increases business and IT agility by providing organizations the security and other critical capabilities they need to confidently pursue initiatives in user mobility, IT consumerization and enterprise cloud networks.

To find out more about how NetScaler can help your organization defend its business-critical web properties, visit www.citrix.com/netscaler.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.