CITRIX®

Deliver a secure digital workspace with next-gen remote access solutions

Contents

Modern security for the digital workspace

Digital transformation is the rocket fuel that helps companies boost productivity, engage consumers, and empower their people. It has spurred companies to reimagine how work gets done by creating digital workspaces designed to foster agility, enhance service levels and accelerate time to success. No longer tethered to corporate desks and cubicles, employees work as virtual teams – communicating and collaborating anytime, anywhere, using the applications and devices they need.

Forty-three percent of employees spend at least some time working remotely[1]. A rise in employee mobility and applications moving to SaaS has businesses relying on their IT departments to ensure employees stay connected virtually anytime, and from any location. However, the new application infrastructure for SaaS, BYO, and the on-demand, work-from-anywhere environment is also posing new workflow challenges and security risks. In many cases, IT lacks end-to-end visibility and control, and struggles to deliver an optimal user experience for their employees and customers.

Back to contents

By 2021, 25% of corporate data traffic will bypass perimeter security, up from 10% today, and flow directly from mobile and portable devices to the cloud.[2]

As enterprises race to scale, IT teams find themselves purchasing disparate products for specific types of applications and device profiles. In addition, various business units subscribe to their own SaaS applications for collaboration or completing tasks. As a result, workers have to go to multiple gateways or access points to leverage different types of applications, creating a poor user experience. This lack of a cohesive strategy adds complexity to their IT infrastructure while potentially causing budget overruns. It also burdens already overworked IT teams to manage multiple solutions while addressing an increasing number of support issues. Ultimately, the use of multiple solutions and their associated complexity delays the implementation of critical access control policies.

There is a better way.

Next-generation access solutions from Citrix offer a broader set of use cases beyond traditional VPN technology. These solutions secure enterprise applications, underlying infrastructure and data within these applications. This provides consistent and granular security policies, simplified IT management, and a better user experience. Next-gen access solutions also deliver control and visibility across increasingly complex hybrid-cloud environments.

↑ Back to contents

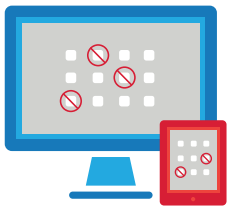
Security challenges for IT

Gartner predicts that by 2020, 90 percent of enterprises will implement business processes that depend on mobile devices.[3] Gartner also finds that Software-as-a-Service (SaaS) remains the largest segment of the cloud market, with revenue expected to grow 22.2 percent to reach $73.6 billion in 2018.[4] The global research firm expects SaaS to reach 45 percent of total application software spending by 2021.[4]

While the adoption of mobile and SaaS applications is designed to increase productivity and keep enterprises ahead of the innovation curve, it can also result in security challenges for IT, including:

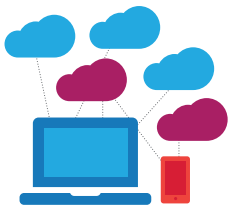
Security controls for SaaS

Traditional SSO vendors do not provide IT with controls to manage user actions in SaaS applications. As a result, a user can share information in SaaS applications with anyone they choose.



Shadow IT

Employees often adopt applications or cloud solutions for their own initiatives without IT's knowledge or approval – bypassing corporate security and compliance policies.



Cloud sprawl

Enterprises use services built on multiple cloud infrastructures and leverage numerous SaaS applications, expanding the environment to be secured.

Password neglect

IT teams preach the importance of establishing and enforcing strong password policies, However, according to a survey by LogMeIn, 62 percent of respondents reuse the same password for work and personal accounts.[5]

Global compliance

New and complex global compliance mandates such as the General Data Protection Regulation (GDPR) have IT teams scrambling to put the appropriate security infrastructure in place. More than half the respondents in a global study by Citrix and the Ponemon Institute voiced concerns about how their organizations will address the risks associated with the introduction of new international privacy and security regulations and cybersecurity mandates.[6]

Back to contents

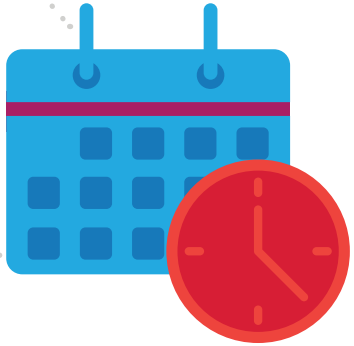
In order to secure an expanding network perimeter, many IT teams find themselves supporting a wide variety of specialty security solutions – each with their own management consoles and policies. It's no surprise that 83 percent of the Ponemon survey respondents said the complexity of business and IT operations leaves them vulnerable.[7]

The transition to digital business requires IT to rethink how they secure infrastructure, devices and data. A secure digital perimeter enables a modern, people-centric approach to reliability, performance and security for apps deployed in the data center, cloud, or delivered as SaaS. It allows IT to:

- Minimize and hide attack surfaces
- Gain full visibility across SaaS, hybrid, and multi-cloud environments
- Automate contextual actions and policies based on triggers
- Share threat intelligence across services to prevent malicious actions and behaviors

$7.35M
total organizational cost of a data breach in 2017, up from $7.05M in 2016[7]

68%
of breaches take months or longer to discover[8]



79%
of global networks have been compromised at least once by a successful cyberattack[9]

Back to contents

Leveraging remote access solutions to enhance security and improve user experiences

Today's digital workspaces require solutions that protect against familiar threats while anticipating new and emerging threats to sensitive business data and personal information – all without undermining productivity or impeding legitimate access. Next-generation secure remote access solutions help IT craft security strategies that consolidate resources, facilitate cost efficiencies, improve user experiences and assure the effectiveness of business compliance strategies. Here's what to look for when evaluating these solutions.

Improved end-user experience

A next-gen remote access solution provides users with one access point and single sign-on (SSO) to business applications deployed in the data center, the cloud, or delivered as SaaS applications across a range of devices, including laptops, desktops, thin clients, tablets and smartphones. Users should be able to roam between the networks and across organizational boundaries without any disruption to their SSL VPN sessions and without having to manually start the VPN.

Back to contents

Contextual access control policies

With the constant threat of internal and external attacks, access management is top of mind. Look for multi-factor authentication, which asks users to provide additional credentials based on the user, their location, and the state of the device. An IT administrator should be able to create, manage, and enforce policies to access data securely in an application environment. These policies can be implemented for VDI, web, mobile, enterprise, and SaaS applications.

Enhanced security and control for SaaS applications

Next-gen solutions provide IT teams with tools to monitor and manage user behavior after they sign in to SaaS applications. Enhanced security policies allow IT to determine user actions such as copy, paste and download. They can also control whether users can take screenshots of data posted in SaaS applications. This prevents users from leaking company confidential data, either accidentally or on purpose, and allows an enterprise to move to SaaS and cloud-based applications with confidence.

Infrastructure consolidation

Next-gen solutions provide one URL and consolidate remote access infrastructure – helping to reduce IT costs and improve the ease of enforcing compliance and security policies. Consolidation also helps to reduce complexity, improve efficiency and lower the cost of ownership.

End-to-end visibility

A lack of visibility in the corporate infrastructure makes it difficult for IT teams to troubleshoot performance issues, leaving users frustrated and unproductive. Next-gen solutions provide deep visibility into all application traffic – ensuring application uptime and reducing help desk SLAs.

User protection

Controlling what users access on the Internet protects them from inadvertently clicking on malware links embedded in web sites. It also helps them adhere to compliance mandates such as the Child Internet Protection Act (CIPA) by preventing users from accessing objectionable content using company-owned devices or networks.

Only 48% of organizations have security policies in place to ensure that employees and third parties only have the appropriate access to sensitive business information.[10]

Back to contents

Cutting through complexity – 4 factors for modern security

IT leaders know that legacy security infrastructure may have served adequately in the days of corporate-owned, desktop-bound endpoints, when access to resources was limited to enterprise networks. But today's digital workforces require a modern approach to security that includes the following key elements.

Datacenter-to-cloud visibility and control, so IT teams can protect hybrid environments that span on-premises and public and private clouds.

Integrated security solutions, so organizations can defend themselves against a wide range of threats without having to create and maintain custom interfaces and connectors.

Centralized management, so a lean staff can deploy and maintain a consistent set of security policies across multiple security technologies, computing environments, and global regions.

Comprehensive security analytics, so IT can detect advanced, subtle, multi-vector security threats.

This combination not only simplifies management and reduces costs, but it also dramatically increases an organization's ability to deploy and modify applications with confidence.

Back to contents

Balance security risk with business priorities

Citrix's approach to securing the digital workplace gives you the flexibility to balance security risk with enabling ways of working that advance innovation and growth. Citrix solutions include contextual secure remote access, providing centralized management and distributed policy enforcement across every control point. Your teams can securely connect, collaborate and share information from any location, using any device they choose.

Back to contents

Address your top security challenges with Citrix solutions

Contextual and secure access
Provide employees and third parties with secure, contextual access to business apps and data regardless of device and location.

Mobility and device security
Manage mobile device and mobile app security to prevent threats and malware attacks without compromising productivity.

Secure collaboration and IP protection
Safeguard information from loss and theft, and IP from infringement and misappropriation.

Governance, risk and compliance
Address risk and global compliance standards and industry regulations.

Business continuity and app security
Address continuity of operations, applications and systems availability during business disruptions and cyberattacks.

With Citrix, you can protect apps, content, and networks, while proactively addressing threats in SaaS, hybrid and multi-cloud environments. You have the freedom to enable business priorities and user needs by adopting new innovations while remaining confident your data, apps, and network are secure.

Back to contents

CITRIX®

Learn more at Citrix.com/secure.

Sources

1. Galllup State of the American Workplace report, 2013
2. Gartner Security & Risk Management Summit 2017, Network Security Challenges for 2017 and Beyond, Peter Firstbrook, June 12-15 2017, National Harbor, MD
3. Gartner - How to Successfully Navigate the Hurdles of Global-Scale BYOB Implementations - Brian Taylor and Leif Olof-Wallin, January 29, 2018 https://www.gartner.com/doc/3849065/successfully-navigate-hurdles-globalscale-byod
4. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018 https://www.gartner.com/newsroom/id/3871416
5. Password Abuse Abounds, New Survey Shows - Jay Vijayan, DarkReading.com, May 1, 2018
6. The Need for a New IT Security Infrastructure: Global Study on Compliance Challenges and Security Effectiveness in the Workplace – Citrix and Ponemon Institute
7. Ponemon Institute's 2017 Cost of Data Breach Study
8. Verizon's 2018 Data Breach Investigations Report
9. 2017 Cyberthreat Defense Report, CyberEdge Group, LLC
10. The Need for a New IT Security Infrastructure – A Global Study from Citrix and Ponemon Institute

Back to contents