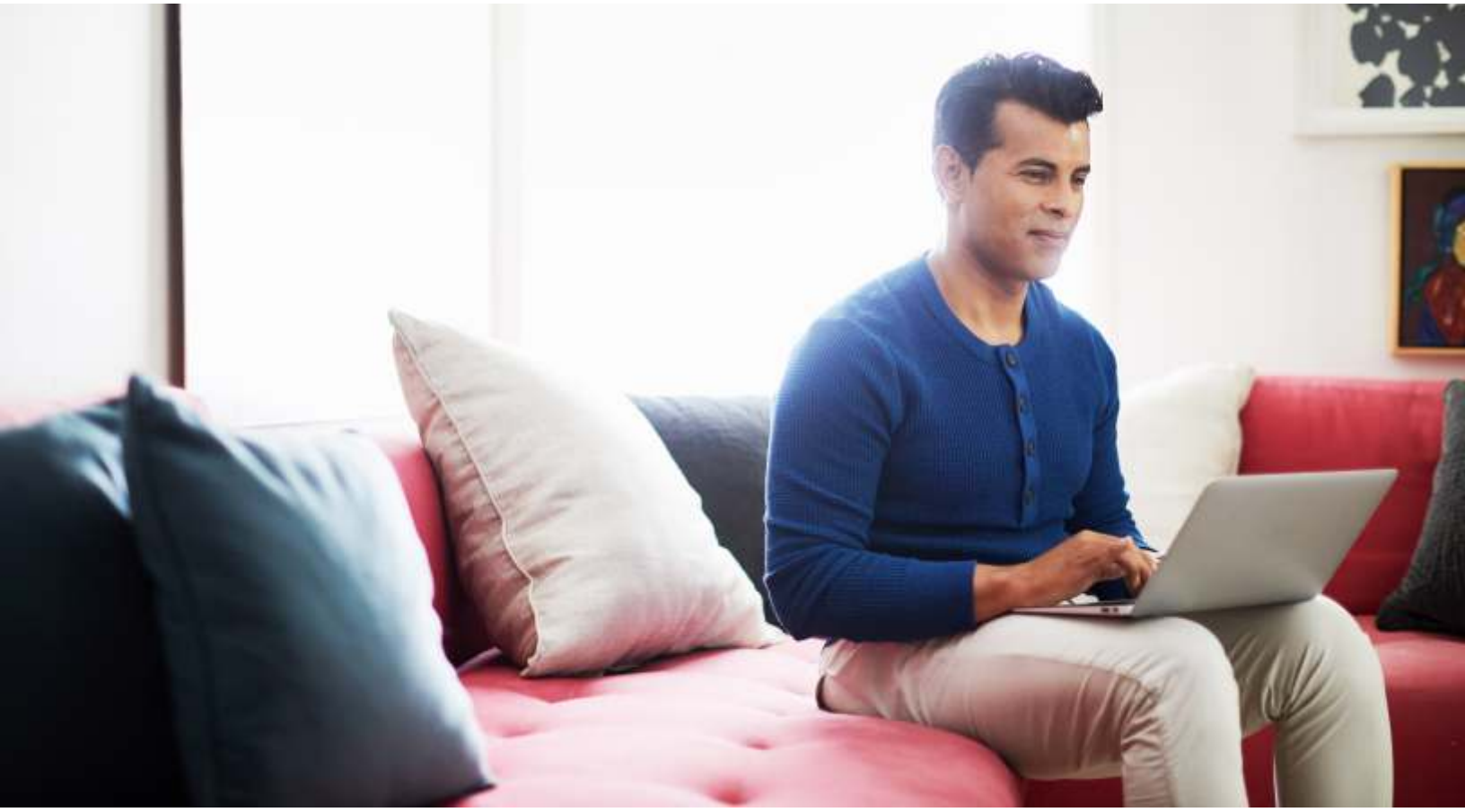

The Secure Digital Perimeter

Robust, flexible, and dynamic contextualized security for Citrix Workspace

Organizations are rethinking the ways that they secure their critical digital assets and infrastructure, driven by a move to cloud and Software as a Service (SaaS) applications and an increasingly mobile workforce. Traditional network security perimeters are no longer relevant, complicated by serious and escalating security challenges. Only a secure digital perimeter centered on verified context-aware identity can secure the modern digital workspace, while maintaining critical productivity for users and IT administrators alike.

CITRIX® Ready

With the prevalence of increasingly aggressive, costly, and frequent security breaches, organizations need to establish new levels of protection for their applications and data. At the same time, enhanced user productivity is essential. Users need to be able to authenticate quickly and easily — on any device, from anywhere— establishing their identity with a minimum of hassle and distraction. Rapidly changing application models, work patterns, and the use of personal mobile devices further complicates the challenge of implementing a modern and effective security perimeter. IT departments must have the ability to provide fine-granularity secure access for everyone — employees, partners, and customers—while supporting the full gamut of modern application delivery methods.

Citrix Workspace

Only Citrix offers the most complete and integrated workspace to enable people to securely access their apps, desktops, and data from anywhere. Rely on Windows app and desktop delivery from XenApp® and XenDesktop®, device security from XenMobile®, secure file sync and sharing with ShareFile®, and network security with NetScaler®. Only a Citrix Workspace offers you complete choice of device, cloud and network, streamlined for IT control and simple, secure access for users.

Citrix addresses these challenges with a secure digital perimeter, letting organizations deliver a unified and secure digital environment. By taking a people-centric approach to security, Citrix allows for personalized experiences and contextually aware security. In turn, IT can control and proactively manage security threats in today's distributed, hybrid multi-cloud, and multi-device environments. Citrix technology allows full aggregation of all apps and data — on-premises, in the cloud, or in multiple clouds — to deliver the right experience to the right user at the right time. Importantly, the Citrix Ready Identity and Access Management Program ensures that innovative and validated third-party security solutions work seamlessly with Citrix Workspace.

Grappling with growing complexity and risk in a highly-distributed workspace

It used to be straightforward to establish a security perimeter. Traditionally implemented at the network layer, firewalls and similar mechanisms kept intruders out. Virtual private networks (VPNs) provided access to a short list of privileged users. Usernames and passwords were considered sufficient to secure access to corporate assets and data. Those simple times are gone for good.

Multifaceted attacks are now inevitable in an increasingly challenging security environment. Professional hackers and cyberterrorists are behind constant phishing attacks along with targeted malware and ransomware, resulting in many high-profile security breaches. Traditional username/password mechanisms are a recognized vulnerability, generating increasing pressure to establish more robust ways of establishing and managing identity.

Complicating matters, the digital workspace has become vastly more complex and distributed, with centralized control over applications a thing of the past. Today apps are often purchased by individual business units and IT doesn't necessarily know what apps are being used by whom, or where they are located or served from. Each new application may also have its own credentialing mechanism. In an effort to cope, IT departments can't afford unbounded complexities and risks caused by myriad security point solutions and gateways. Neither can they be constrained by the innovations of a single security vendor.

Enterprise IT departments face increasing complexity as they seek to offer mobile users easy and secure access (Figure 1). Applications, devices, and authentication methods have all undergone significant change.

- Application proliferation. Only a few years ago, users could stay productive connecting to enterprise e-mail and a few centrally hosted applications over a single VPN. In contrast, modern enterprise users connect to scores of applications, ranging from legacy and on-premises apps to web, virtual, and SaaS applications and services (from one or multiple clouds).
- Device proliferation. Laptops, tablets, and smart phones are everywhere as a part of either bring your own device (BYOD) or corporate owned personally enabled (COPE) environments, or a combination. Users now access applications from anywhere on multiple devices hosting a variety of operating systems, security and compliance postures, and mixes of personal and enterprise applications and data.
- Authentication proliferation. Managing a patchwork of distinct authentication methods is increasingly complex. There are more authentication mechanisms to choose from than ever before (e.g., the Network Information System (NIS), Remote Authentication Dial-in User Service (RADIUS), formbased, Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), Diameter, and Kerberos). Organizations may deploy any or all of these in any number of combinations.

The only truly secure digital perimeter is one that is based on identity itself, allowing for simplified management and a choice of best-of-breed identity and access management solutions.

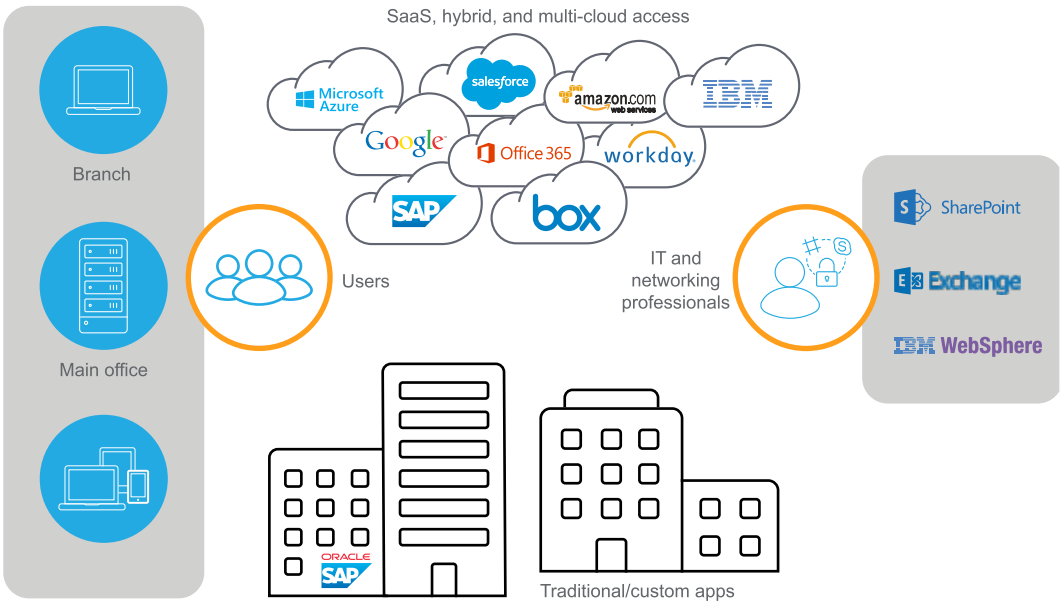

Figure 1. IT departments face significant challenges securing a diverse and distributed workplace.

As a result of these trends, users often have to remember multiple logins and bookmark multiple websites and portals to stay productive. IT departments find themselves managing multiple remote access points, specialized gateways, and identity and access control solutions for different devices and applications. The need to vet all those different remote devices, users, and authentication mechanisms for security policy compliance is daunting. The complexity not only consumes IT resources, but opens new security vulnerabilities, thanks to:

- Bad user password habits. Users respond as best they can, but the unavoidable complexity often results in password reuse across applications, weak passwords, and passwords stored in e-mail or text files — or on paper.

- Inefficient IT processes. Unresponsive IT processes can allow users to improperly retain access to sensitive applications and information after they leave an organization or switch devices.
- Security inconsistencies. Vulnerabilities and uneven services can result from managing access by multiple device types, services, vendors, access control mechanisms, and support services with different features, architectures, quirks, and terminology.

Securing the modern digital workspace

Properly securing complex modern environments requires new ways of thinking about security, access, and authentication. Specifically, it requires moving from a traditional attack-centric model to one that is people-centric, and centered on identity itself. To bring about this transformation, organizations must:

- Move from defending against attacks from unknown entities toward a zero-trust model that allows access only to known users based on policy.
- Move from worrying about where to apply policies to applying policies on the digital workspace itself.
- Move from forcing users to where security exists to securely following the user wherever they happen to be.
- Move from a zone-based approach (trusted demilitarized zone, intranet) to context-based user interactions with apps, data, and networking.
- Move from a model that abstracts doors and locks to a system of detectors.

A secure digital perimeter for Citrix Workspace

Security perimeters are traditionally deployed along trust boundaries to protect the user as well as the organization and its critical information. Now trust boundaries are all over the organization. They extend to users as they work remotely—on remote devices, in different locations, using the full gamut of application types. As environments have evolved, providing a software-defined secure digital perimeter around identity makes real sense.

Figure 2, shows how a secure digital perimeter provides a flexible and integrated way to deliver and manage the applications, desktops, and data devices that users need. By defining a people-centric and identity-centric approach to security, organizations reap the benefits of hybrid and multi-cloud environments, while simultaneously simplifying management. Contextualized access and performance offers a unified and productive experience for users, while unified endpoint management along with application and content control provides a simplified and secure environment for IT and networking staffs.

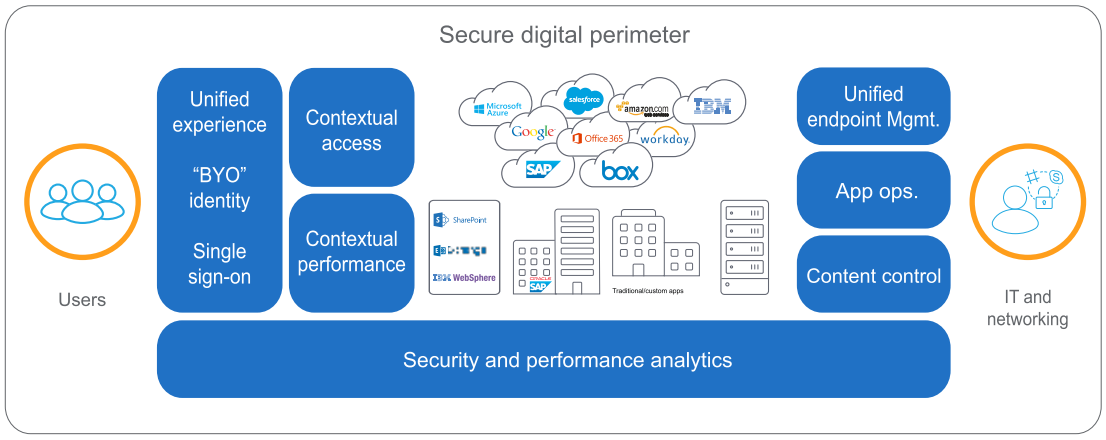

Figure 2. A secure digital perimeter for Citrix Workspace benefits both users and IT administrators.

Federated access and single sign on (SSO)

Many organizations choose single sign-on (SSO) infrastructure to simplify the process and improve productivity for their users. With Citrix Gateway, Citrix provides SSO while allowing IT departments to take control and proactively manage security threats. The approach effectively combines an onpremises enterprise directory (e.g., Active Directory) with federation, multifactor authentication, and centralized access control. Administrators can fully aggregate all apps and data across all applications—both on-premises and in the cloud—to deliver the right experience to the right user at the right time.

Citrix Gateway (Figure 3) provides users with a single URL and login to access all their enterprise applications and services, potentially including all of Citrix Workspace (XenDesktop, XenApp, StoreFront, and ShareFile). Through the Citrix Ready Identity and Access Management Program, a wide variety of third party multifactor authentication mechanisms can be used as an Identity Provider (IdP) — supporting everything from existing hardware and software tokens to adaptive multifactor authentication and biometrics. This approach provides IT with a singular identity, access control, and management infrastructure, closing the inevitable security and management gaps inherent with juggling multiple gateway solutions. Even with extensive use of diverse devices and cloud and multi-cloud services, authentication against enterprise directory services can remain on-premises where it can remain secure and be closely controlled.

The Citrix Ready® Program

The Citrix Ready Program showcases verified products that are trusted to enhance Citrix solutions for mobility, virtualization, networking and cloud platforms. The Citrix Ready designation is awarded to third-party partners that have successfully met test criteria set by Citrix, and gives customers added confidence in the compatibility of the joint solution offering.

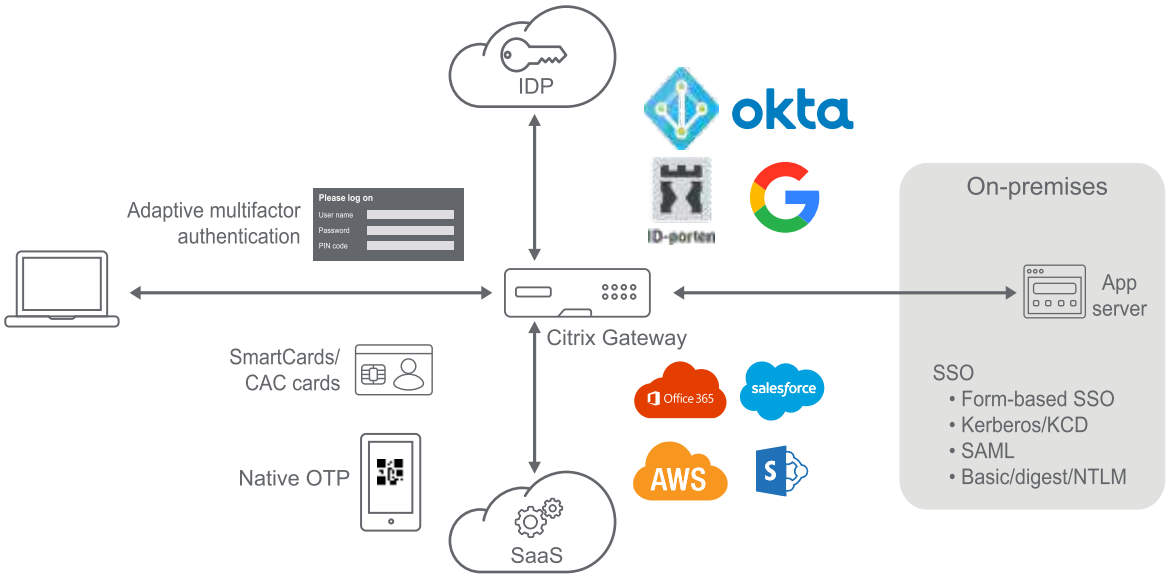

Figure 3. Citrix Gateway is at the center of a flexible secure digital perimeter.

Citrix Ready Identity and Access Management Program

With the complex security challenges facing organizations today, no single vendor can satisfy every essential enterprise security need. The resulting proliferation of point solutions in the security space is testament to the rapid innovation occurring in the marketplace. Instead, organizations need to be able to take advantage of the latest thinking and the newest and most robust security products, without creating a patchwork of disparate security gateways that introduce their own security risks through complexity.

The Citrix Ready Identity and Access Management Program features Citrix Ready verified identity and access management products that integrate tightly with Citrix technologies. Citrix actively seeks

partnerships that provide solutions that meet the needs of mutual clients, extending functionality and mutually enhancing product offerings. A wide range of solutions can be deployed in the cloud, on-premises, or in hybrid environments to provide basic and advanced capabilities for Citrix environments.

Citrix security solutions help organizations proactively protect information, manage risk, and achieve compliance. Integrated with partner's Identity and Access Management products, these unique joint solutions offer a secure digital workspace and secure digital perimeter by combining secure access to apps and data with contextual control, visibility and behaviour analytics across devices, networks and clouds. Together, these enable customers secure access, mobile security, data and IP protection, compliance, and business continuity.

For more information on the partners participating in the Citrix Ready Identity and Access Management Program, visit:

citrixready.citrix.com/program/identity-and-access-management-program/resources.html

Conclusion

Applications and work environments are evolving, and so are enterprise security threats. Organizations need to be able to move beyond simple passwords toward single sign-on environments with a choice of effective multi-factor authentication mechanisms and solutions. With a secure software-defined digital perimeter, Citrix Workspace provides an ideal platform to proactively manage security threats in modern distributed multi-device hybrid multi-cloud environments. The Citrix Ready Identity and Access Management Program adds considerable depth by providing diverse security solutions with the assurance that vendors have worked closely to verify solutions with Citrix, reducing risk and saving organizations valuable integration time.

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix Ready
Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.