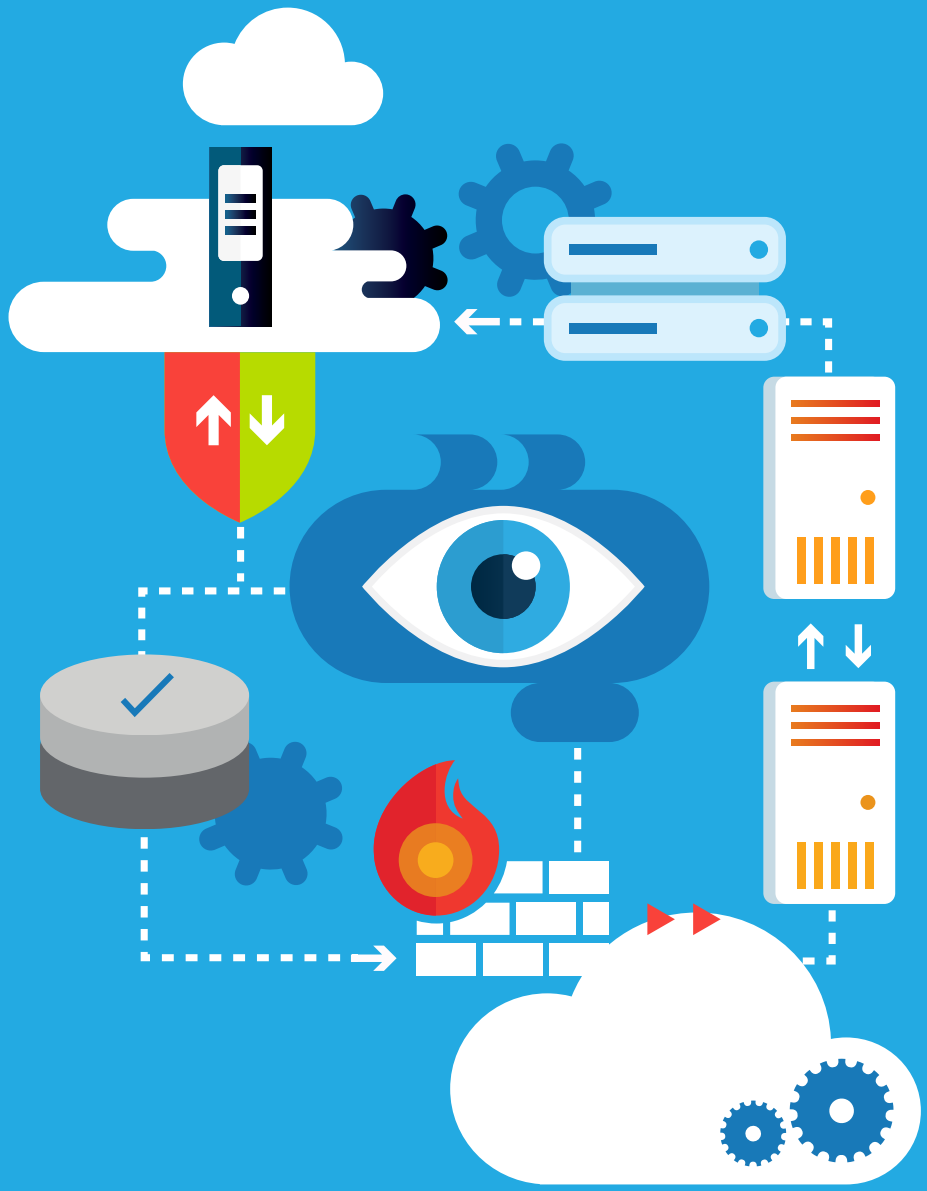
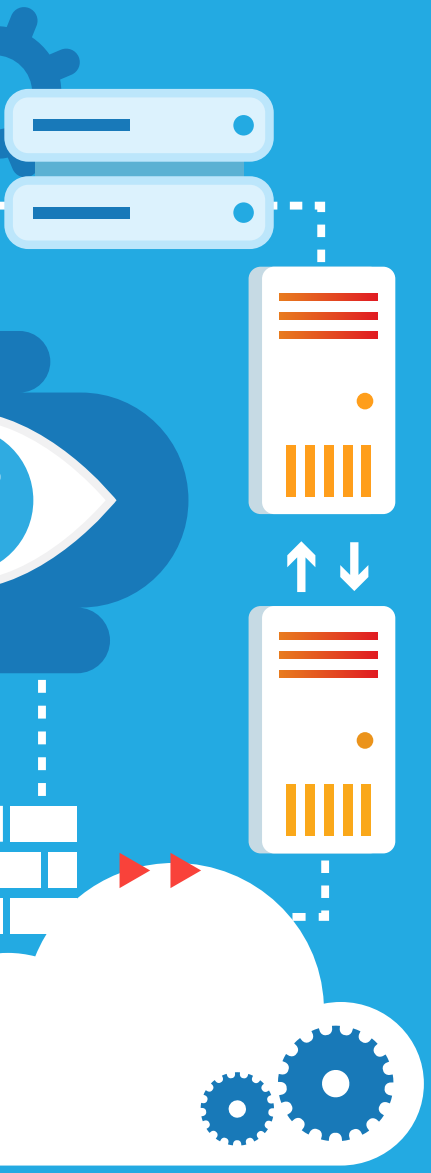
CITRIX®

Build a strategic approach to network and app security

How to secure your entire digital ecosystem.





Content

Sophisticated application attacks like WannaCry and NotPetya garnered a lot of attention in the news — and with good reason. They're evolving, persistant, and rapidly increasing in frequency.

But app attacks aren't the only threats that should be on your radar. Threats of every kind can be pervasive. From the network to applications, attacks continue to hit organizations at every layer of the infrastructure. Historically, the solution has been to tack on another point product, but this approach leaves gaps in security. Only a comprehensive, end-to-end solution can fully protect your data — regardless of where it lives.

The balancing act between security and usability

Users want choice when it comes to their apps and devices, and the flexibility to work anywhere, anytime. But that creates a lot of undo complexity, security risk, and systems sprawl for IT to manage. With the right solution, organizations don't have to give one priority over the other — they can have both.

Regardless of where data resides, your organization can give employees the tools they want, while ensuring IT has the visibility and control to actively monitor your entire ecosystem from a unified console.

← Pg. 3 | Pg. 5 →

Back to contents

Threats morph to outsmart security

Attacks are constantly evolving to outsmart security.
They're now pervasive at every level of your IT infrastructure.
Here's a snapshot of how attacks are changing.

Common types of network attacks:
Historically, networks have been the target of most attacks. The best forms of defense included firewalls, patching, and education, which were never great options, but as long as the data was tucked behind a firewall, organizations could typically maintain control. That is, until threats advanced up the stack chain and outside of the data center.

Network attacks

- Brute force
- Worm attacks
- DNS
- Port scans
- Other

Common types of web and app attacks:
As data began spreading outside of the data center and across clouds, web, devices, and apps, it's become harder to secure. Sophisticated attacks started following data up the stack layers and outside of the firewall — to the cloud, web, and app layers.

Web and app attacks

- Browse
- URL Interpretation attacks
- SQL Injection attacks
- Impersonation attacks
- Buffer overflow attacks
- DDoS (distributed denial of service)

← Pg. 4 | Pg. 6 →

Back to contents

Traditional methods no longer work

In an attempt to outpace emerging threats, a lot of organizations have tacked on individual point solutions to address individual security needs. One for endpoint protection, another for apps, and yet another for the network. These disparate systems don't work because they:

- **Add complexity.** As data moved from the data center to cloud, and even endpoint devices beyond the firewall, IT teams were left with different systems for managing and securing them all.

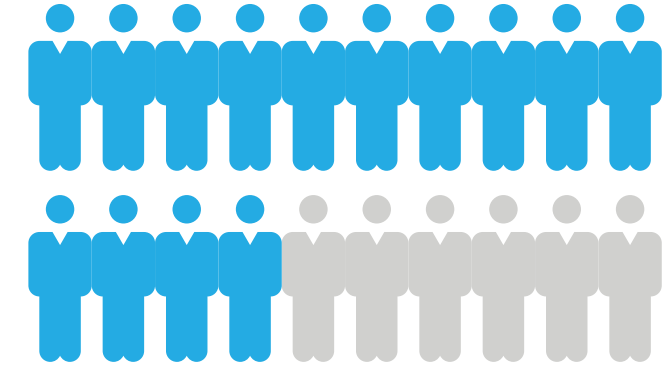
- **Leave holes.** Different systems weren't designed for end-to-end coverage, and leaving gaps where malware can slip through.

- **Don't talk to each other.** Siloed point solutions can't spot anomalies or alterations and therefore can't proactively prevent threats from breaching your network.

- **Can't identify unknown attacks:** A big problem for many disparate security systems are the threats they can't see. Also known as zero-day attacks, they can go unnoticed for extended periods of time, allowing hackers access sensitive data for however long it takes them to be discovered.

- **Don't prevent internal threats.** Most security solutions are geared at keeping the bad guys out, but they aren't designed to stop leaks from the inside. Point solutions aren't designed to recognize and halt unusual behavior. As a result, they're unable to prevent sensitive information from moving outside the network.

- **Can't segment access based on user needs:** Managing user behavior across endpoints (especially those on BYOD devices) is much harder with individual point solutions and puts additional burdens on already overloaded IT teams.



of executives say the chief culprit for cybersecurity risk is the proliferation of BYO devices and applications that employees are bringing into the workplace.[1]

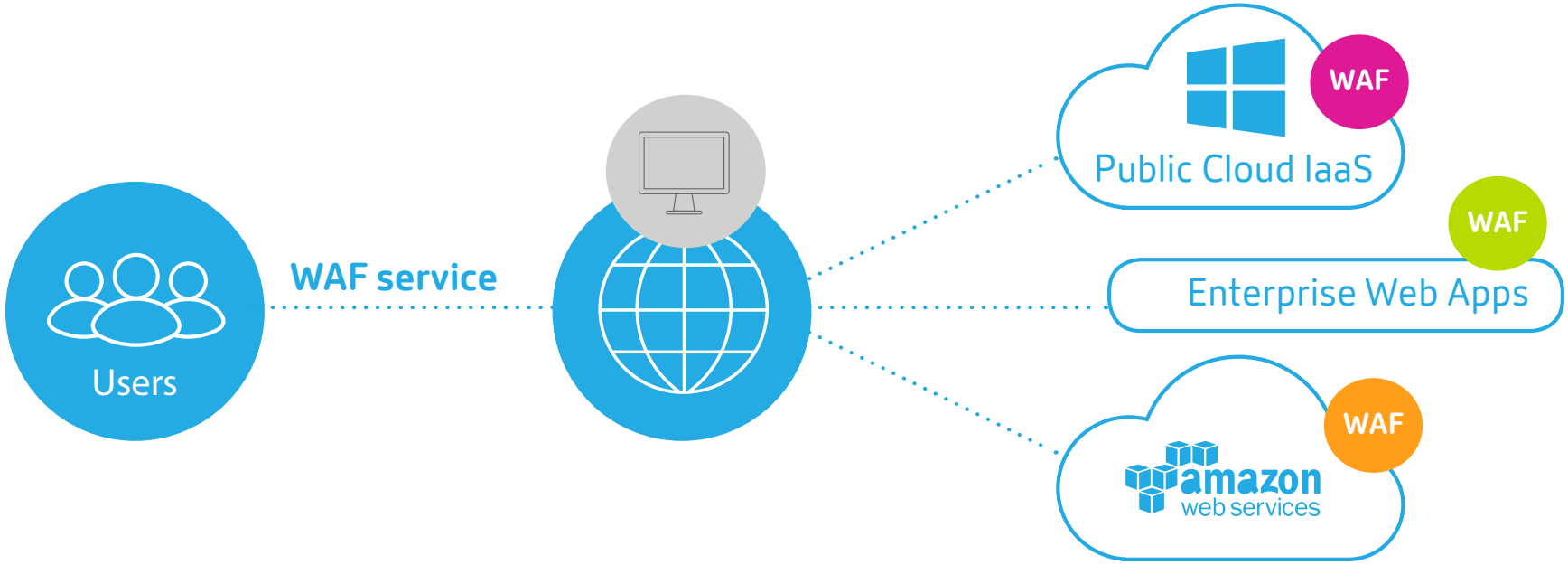
← Pg. 5 | Pg. 7 →

Back to contents

Why a new security approach is paramount

With a proliferation of cloud services today, there's a good chance your organization will face new kinds of threats. And you need a platform that can secure your data anywhere — regardless of whether it's at the network, web, or app layer.

An end-to-end approach, that includes a fully integrated web application firewall (WAF), lets you manage threats across all clouds, networks, devices, and users. It also ensures a consistent user and IT experience in every environment.



← Pg. 6 | Pg. 8 →

Back to contents

74%

of enterprises agree — a new IT security framework is needed to improve security posture and reduce risk.[1]

← Pg. 7 | Pg. 9 →

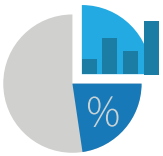
Back to contents

An ideal security approach is holistic

A unified, contextual, and secure method delivers available and reliable systems while ensuring data remains confidential and protected through:

360-degree visibility

You need a complete view of traffic and transactions traversing your ecosystem so you can spot threats or unusual activity, such as a sign on credential used at an atypical time from an unlikely location.



Provide actionable insights from analytics

Advanced telemetry allows you to collect data from any source (device logs, server logs, application logs and counters, emails, third party SIEM products, etc.). You can then track, analyze, and spot anomalies throughout your networks, clouds, apps, web traffic, and users, proactively alerting IT to potential issues before they infect your systems.

Simplified access

Whether BYOD, a dedicated desktop, or a shared device, single sign-on (SSO) simplifies the access process for users while minimizing the burden IT resolving employee password problems or expired access privileges.

Ability to manage, renew, set, and enforce policy

Ensure your organization can control access levels so that only approved individuals are privy to sensitive data.

Push updates and patch at the global level

Patching and updating the myriad devices used is nearly impossible. Managing systems from a centralized location means teams are able to roll out patches and updates in minutes instead of hours.

Protect against targeted application layer attacks

Apply a set of rules to protect servers web application firewall (WAF) to help protect against common attacks such as cross-site scripting (XSS) and SQL injections.

Deliver end-to-end encryption

Manage traffic and certificates to provide data center resiliency and protect across hybrid and multi-cloud environments.

← Pg. 8 | Pg. 10 →

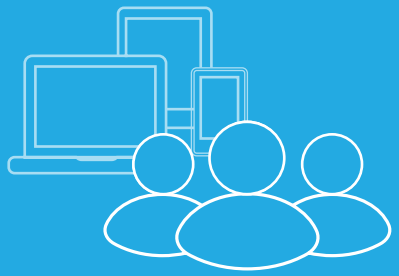
Back to contents

Complete security with a secure digital workspace

Unify

IT can configure, monitor, and manage your entire IT infrastructure through a single pane of glass to deliver a unified user experience.

Secure



A people-centric security approach puts the user at the center of your security framework, synthesizing everything known about the user and their behavior to provide contextual access, security controls, and predictive analytics for full visibility across the network and user ecosystem.

Contextual

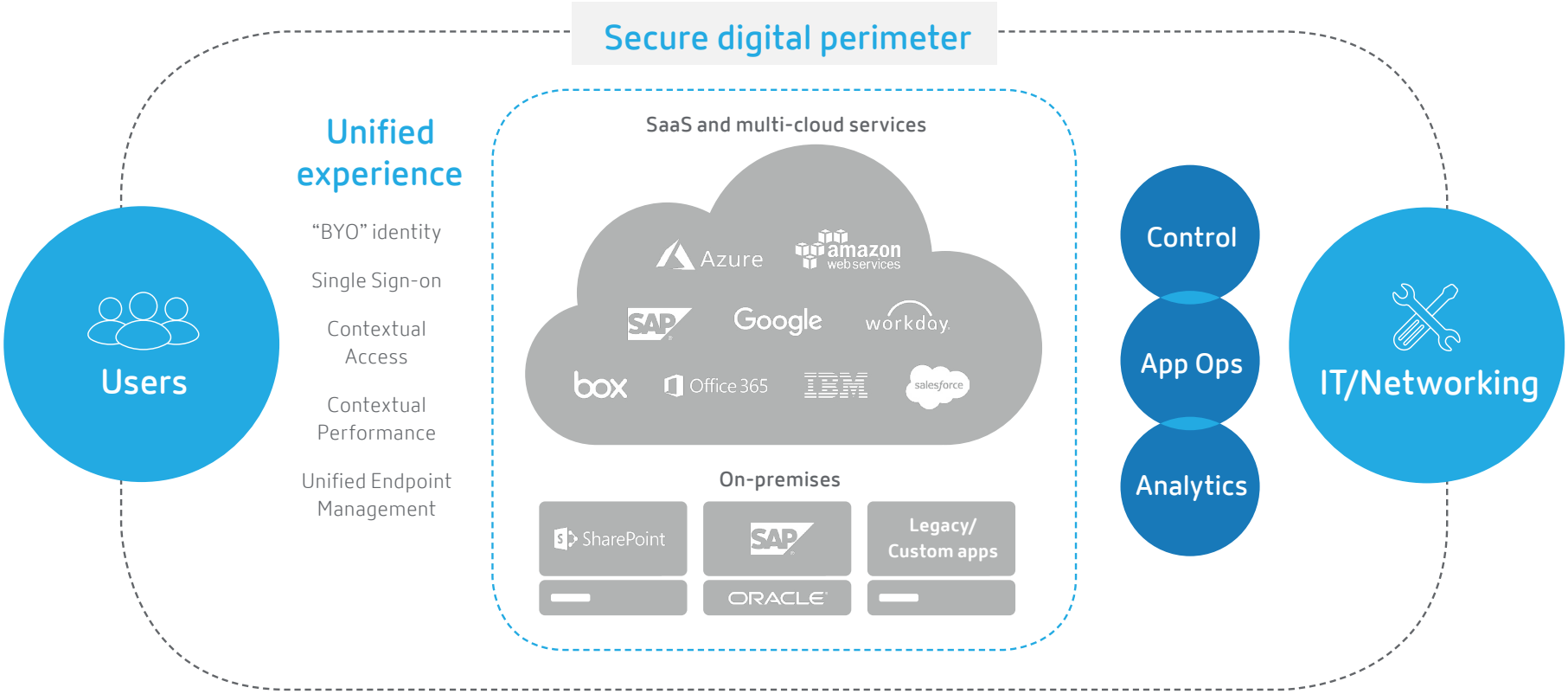
Digital workspaces use machine learning to adapt to each worker's patterns and exceptions so they can get work one securely remain productive from wherever they are.

← Pg. 9 | Pg. 11 →

Back to contents

Deliver the right experience to the right user at the right time

Managing an ever-increasing complexity of network, and number of applications running across any number of clouds is unwieldy and increases your security risks. Citrix Workspace enables IT to take control and proactively manage security threats in today's distributed, hybrid multi-cloud, multi-device environments. Instead of managing multiple point products that don't integrate and as a result may have gaps in providing end-to-end security, Citrix is the only vendor that allows for a comprehensive approach to application and network security at multiple levels. It ties in the security offering with Citrix Analytics to provide you with a single dashboard to monitor, manage and remediate the security risks.



← Pg. 10 | Pg. 12 →

Back to contents

Additional business benefits of our security approach

Secure collaboration with intellectual IP protection:
Built from the ground up for enterprise-class security, Citrix enables business users to exchange and collaborate on documents easily, securely, and professionally while ensuring industry standard AES 256 encryption of all meta-data and content.

Governance, risk, and compliance (GRC):
By enveloping the scope of GRC within the framework of the Citrix security approach, and supporting it through our comprehensive analytics capabilities, we're able to deliver a much more synchronized approach meet all your security and compliance needs.

← Pg. 11 | Pg. 13 →

Back to contents

Our management was aiming for a flexible and efficient way of working, but we had to make sure it was reliable. With Citrix Workspace, we know we have optimal security, which is vital when handling the sort of sensitive financial information that Stater does.

— Frank Veldink, ICT Infrastructure Architect at Stater

CITRIX®

Discover how an integrated, intelligent approach to security can help you deliver the access, control, and security you need at **citrix.com/secure**.

Sources:
*"The Need for a New IT Security Architecture," Ponemon Institute, sponsored by Citrix, 2017

Back to contents