citrix

Mitigating cybersecurity and compliance risks

A guide to selling security solutions

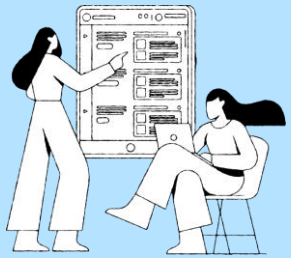
Security risks are growing globally

As organizations enabled remote work, IT teams loosened security controls beyond their typical standards to meet rapidly changing business requirements. Cyberattacks then increased exponentially. As a result, IT and security leaders now want to adopt zero trust security models to protect users, sessions, applications, devices, and infrastructures.

Hybrid work is increasing security and compliance risks

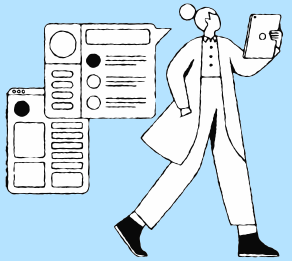
Risks

Compliance risks include out-of-state workers, BYOD devices, keyloggers, shadow IT and data, and more.



50%

Increase of cyberattacks in 2021.



70%

Of IT leaders say BYOD devices are the #1 source of cybersecurity risks.

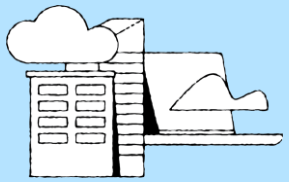
© 2022 Citrix

IT and security are overwhelmed by the pace of change

IT and security need help deploying zero trust network access models

26%

Of IT decision makers say hybrid cloud management is becoming more complex.



99%

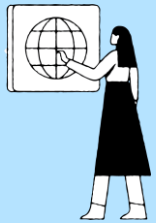
Of exploited vulnerabilities have been known to IT and security for at least a year.

93%

Of corporate networks can be penetrated by attackers.

#1

Business concern for 2022 is cybersecurity.



$265B

Ransomware will cost the world $265 billion by 2031.

79%

Of security decision makers are rethinking their long-term information security strategy.

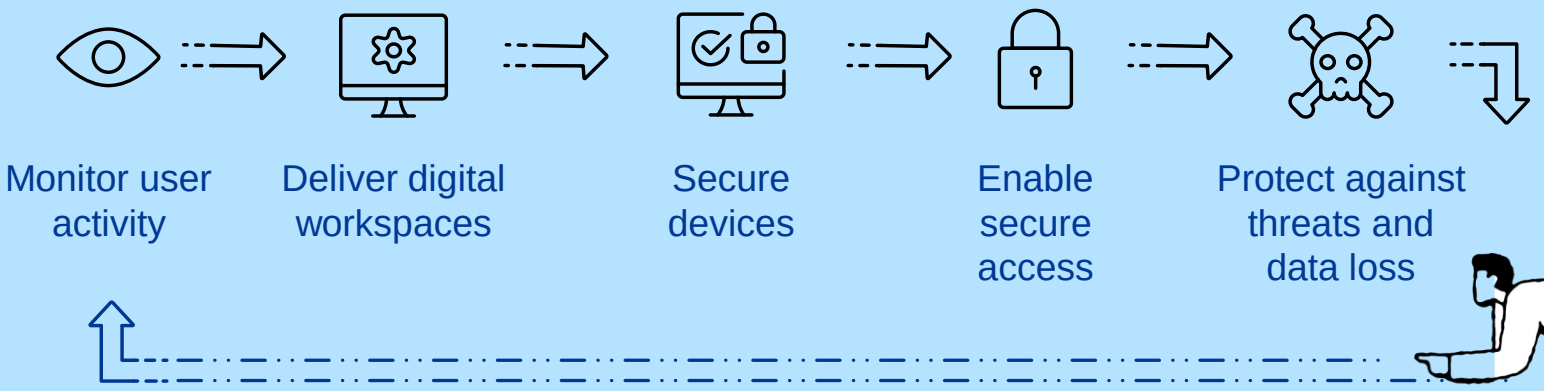
© 2022 Citrix

Organizations want to enable secure access and zero trust architectures

What is zero trust?

Zero trust is a security model that trusts no one by default. All users and access attempts must be continually verified by mechanisms such as multi-factor authentication.

The zero trust continuous lifecycle



Why organizations need it

No single solution can provide the security organizations need. Instead, they need an end-to-end strategy and platform that provides visibility, management tools, and controls.

Embedded controls enable organizations to enforce policy compliance for sensitive data and related business processes.

© 2022 Citrix

Key use cases across all industries

Enable zero trust network access

Gain a more secure access solution than third-party VPNs

Simplify and scale secure access across the hybrid workforce

Continually verify user identities, sessions, devices, and more

Manage access across both corporate and BYOD devices

Use analytics to improve security policies

Provide contextual access

Improve IT's ability to identify phishing and malware attacks

Adapt to the latest security risks and threats

Securely manage digital workflows to protect sensitive data

Allow or restrict functionalities based on user authentication or device posture

Ensure secure BYOD

Effectively manage non-sanctioned corporate devices

Restrict or permit access to users based on their roles

Increase security by layering multi-factor authentication or single sign-on for BYOD devices

Transition more seamlessly to the cloud and SaaS apps

Key use cases across all industries

Secure remote workers and other users

Monitor, analyze, and address both known and unknown threats

Implement a secure Desktop as a Service solution across multiple devices

Maintain readiness and combat ever-changing threat actors, strategies, and tactics

Consolidate and manage solutions that secure devices

Increase application and API security

Secure a multi-cloud infrastructure more easily

Simplify global server load balancing

Improve application security performance and scale results

Automate management processes and analyze results

Mitigate threats

Transition to a permanent secure work from home/hybrid work strategy

Protect remote workers from web and SaaS access attacks

Ensure secure access to cloud apps

Protect business apps from zero-day risks

Customer Success Stories

Synopsys

Industry: Software

Location: U.S.

Citrix Secure Private Access helped protect Synopsys' smart chip IP, while reducing cybersecurity risks. Citrix put app protection policies in place and mandated multi-factor authentication for external entry points.

"A Citrix zero trust architecture helps prevent malware, data exfiltration, or VPN breaches and attacks. Citrix Secure Workspace Access, user identity verification, and secure workspaces are the mechanisms that help alleviate these risks."

- Sriram Sitaraman, CIO

Rohde & Schwarz

Industry: Electronics

Location: Germany

Citrix Web and API Protection provides holistic protection against attacks.

"Another central component for us is the integrated web app firewall from Citrix. This protects our customer portal's web applications from application-level attacks such as DDoS attacks, cross-site scripting,, Security Architect. and SQL injection."

- Stephan Zimmermann

City of Corona

Industry: Government

Location: California, USA

The City of Corona gained end-to-end monitoring of its infrastructure with Citrix Analytics for Security.

"The easiest part of all was setting up Citrix Analytics. It was just click, click, connect. We loved the simplicity of it."

- Kyle Edgeworth, Deputy CIO

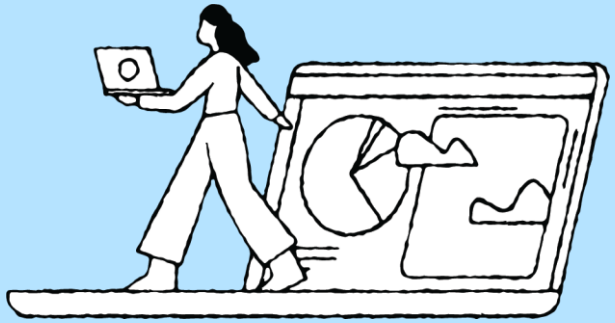
Win with security solutions from Citrix

Citrix allows users to securely access any app, any cloud, anywhere. Enable customers to securely grow their business, improving visibility into—and management over—their distributed network infrastructure.

Citrix helps customers provide secure remote access without third-party VPN solutions, protect data and secure user sessions, and equip IT and security teams with visibility and analytics.

Citrix Secure Private Access:
Secure access to IT-sanctioned apps with adaptive authentication and zero trust access.

Citrix Web App and API Protection:
Keep apps and APIs secure with application security as a cloud service.



Citrix Analytics for Security:
Proactively detect and prevent insider threats with user behavior analytics.

© 2022 Citrix