citrix

White Paper

# Zero Trust & Citrix

Zero Trust application access.

Zero Trust is a security framework that assumes every access attempt, even from a trusted user or device, is a potential threat. It strengthens security posture by reducing reliance on perimeter-based defense. Zero Trust assumes no inherent trust of users, and focuses on securing access to resources and data based on continuous verification and contextual factors.

Citrix has delivered zero trust access to virtual applications and desktops for over two decades. This zero trust security model is now extended to Web and SaaS app access. This ensures a common infrastructure and consistent set of policies where workflows and ecosystem integrations are applied to both virtual and web/SaaS applications.

This paper provides details on Zero Trust principles and how Citrix's Zero Trust Application Access enables secure access to all enterprise applications: virtual, native, and Web/SaaS.

## Zero Trust principles

The fundamental principle of Zero Trust security can be summarized as "never trust, always verify." Zero Trust operates on the premise that all access requests should be treated as potential threats, regardless of their origin. It recognizes the inherent risks associated with trust and eliminates the concept of a secure perimeter, hence earning the moniker "perimeterless security." By adopting a Zero Trust framework, organizations minimize the possibility of data loss resulting from insider and external threats, as it mitigates the unrestricted lateral movement across the network that implicit trust permits.

Zero Trust is based on 3 primary principles to enhance protection and reduce risk in today's evolving threat landscape.

These principles are:

### 1. Never trust, always verify.

By minimizing trust assumptions, Zero Trust eliminates a default assumption of trust within a network. This improves the chances of recognizing threats that originate from external and internal resources, including compromised devices or malicious insiders. Regardless of origin, every access request is scrutinized and verified under a Zero Trust model.

### 2. Least privileged access must be dynamic.

The implementation of strict access controls and continuous validation must occur throughout a user session. This approach reduces the attack surface, prevents lateral movement, and limits the potential impact of security breaches by ensuring only authorized users and devices can access critical information. Adopting contextual and adaptive access considers factors such as user identity, device health, location, and behavior when granting access. This adaptive control allows organizations to dynamically adjust privileges based on the current risk profile, ensuring that access decisions align with the evolving security landscape.

### 3. Continuous monitoring.

Granular visibility and the continuous monitoring of network traffic, user activities, and device behavior gives security teams heightened visibility in their environments. This empowers security teams to detect and respond to potential threats by promptly identifying anomalous behavior or malicious activities within the network.

### 4. Proactive prevention.

A heightened level of security and resilience is created by operating under the assumption that every access request could cause a breach or compromise of security. Every surface such as user, access request, device, and network component is treated like a breach and scrutinized to ensure data is protected and therefore restricted in the event of an activity that triggers a risk indicator.

## Citrix Zero Trust application access

Due to changing nature of threats and the limitations of a traditional perimeter-based security model, the National Institute of Standards and Technology (NIST) has released the NIST SP 800-207 that provides an abstract definition of what a Zero Trust Architecture (ZTA) is and suggested deployment models.

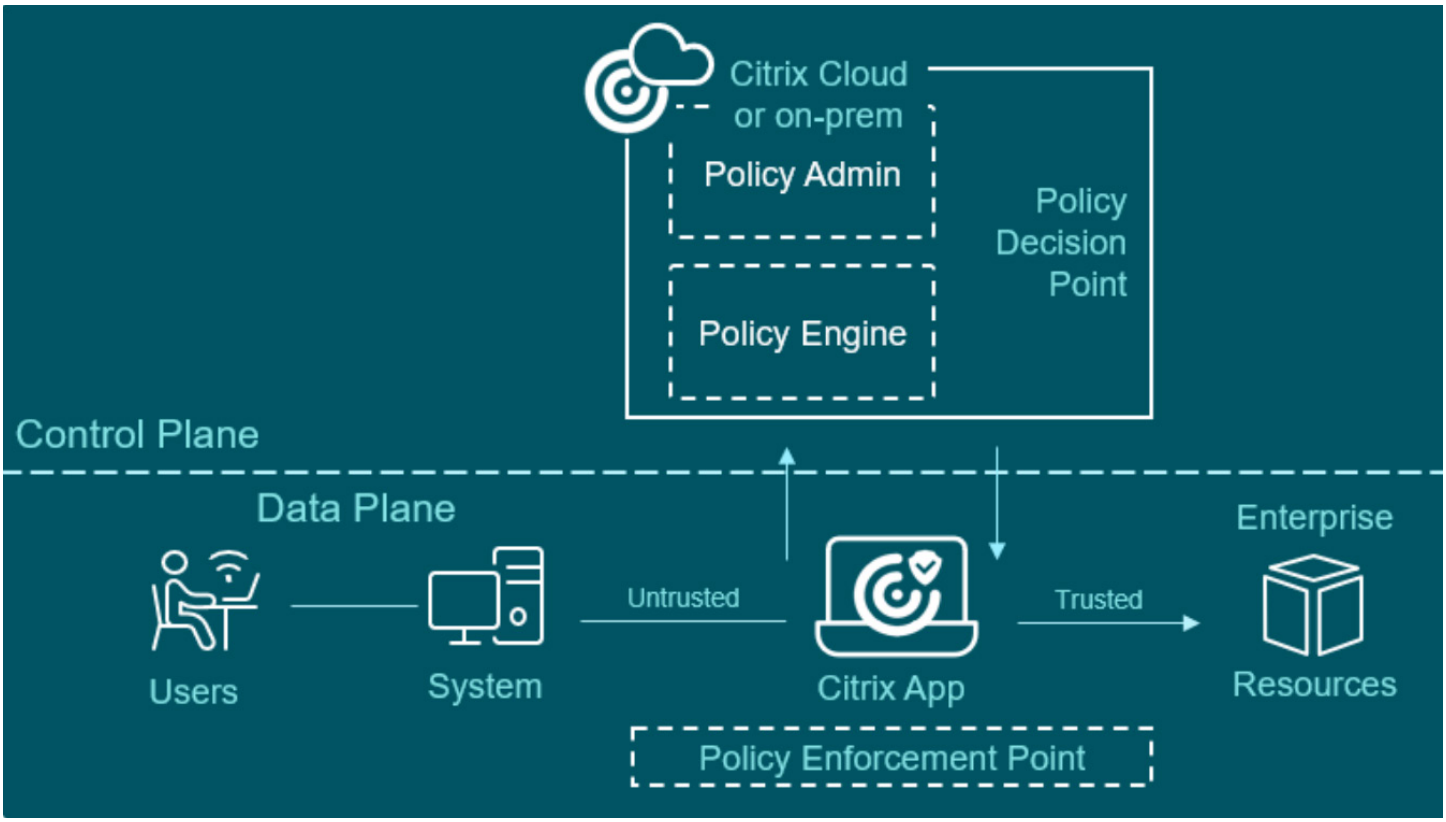
Integrating Citrix Zero Trust Architecture in accordance with the NIST SP 800-207 empowers your organization to forge a resilient and adaptive security framework, aligning seamlessly with industry-leading standards. This strategic alliance fortifies your defenses against threats, safeguarding critical assets and data with utmost effectiveness.

The Citrix app acts as an enforcement mechanism for verifying the authenticity, authorization, and contextual attributes of users, devices, and applications attempting to access resources within the protected environment.

The Citrix app acts as a gateway between users and enterprise resources. When a user requests access to a resource, Citrix app acts as a Policy Enforcement Point (PEP) and evaluates the requests against security policies defined by the Policy Decision Point (PDP).

Based on the evaluation of these attributes, Citrix adjusts access privileges based on real-time context and facilitates continuous monitoring of user behavior to detect anomalous activities.

This forms a crucial part of the Zero Trust Architecture by ensuring only authorized users access specific enterprise resources – whether they are virtual, non-virtual, or SaaS based. Zero Trust Architecture can also be applied to cloud, hybrid and on premises deployments.



## Citrix has a strong heritage in embracing the principles of Zero Trust.

### Key components of a Citrix Zero Trust strategy

Citrix plays a significant role in implementing and aligning with a zero-trust approach by collecting a rich set of signals from each access scenario, analyzing the risks, and automatically taking action. Citrix provides various capabilities and technologies that enhance identity-centric security and access control, including the following::

Identity and Access Management (IAM): Citrix offers robust IAM capabilities including federating authentication with 3rd party on-prem and cloud identity providers. This enables organizations to authenticate and authorize users based on their identities before granting access to resources. By implementing and supporting strong authentication mechanisms, and multi-factor authentication (MFA), Citrix helps enforce identity-centric security in a zero-trust environment.

Contextual and Adaptive Access Control: Citrix provides granular control over resource access based on contextual factors such as user identity, device posture, network, geolocation, and behavior. Citrix also integrates with 3rd party detection response and unified endpoint management solutions for device posture. By incorporating these contextual attributes into access control policies, organizations can enforce a zero-trust approach by dynamically granting or denying access to resources based on real-time risk assessments.

Virtual, Web, and SaaS application access: Citrix Virtual Apps and Desktops, along with Citrix Secure Private Access, provide secure access to virtual Windows, Linux, and Web or SaaS applications. A common infrastructure and framework is used across these applications to provide administrators with a consistent view across all enterprise applications.

Security Analytics: Citrix solutions incorporate security analytics capabilities to monitor user and entity behavior, detect anomalies, and identify potential security threats. By leveraging these insights, organizations can proactively respond to security incidents and enforce zero-trust principles to minimize the impact of potential breaches.

Overall, Citrix solutions align with Zero Trust principles by providing robust identity and access management, contextual and adaptive access control, and security analytics for all enterprise applications. These capabilities help organizations implement a Zero Trust security model that focuses on the continuous verification of identities and dynamic access controls, enhancing security posture and mitigating risks.

Citrix has a strong heritage in embracing the principles of Zero Trust, and we remain committed to evolving as new security threats arise.

## Citrix Zero Trust maturity model

The Citrix  Zero Trust maturity model enables organizations to assess their current state and plan to strengthen their security defenses, moving away from a reactive approach and towards a proactive, data-centric, and context-aware secure access strategy.

At a foundational level, organizations embark on the initial steps of a Zero Trust transformation by establishing a basic, centralized policy control over distributed PC apps and desktops via virtualization in order to control access. Citrix provides feature sets that ensure enterprise resources are kept secure while providing a positive work experience for users.

At an advanced level, Zero Trust solutions become more mature by incorporating an understanding of the scenario to control not only access, but also actions. Telemetry about the device, the security status of the device, the network, etc., are factored in, and additional protections against malware and risky actions like screen captures are applied. Also in this stage,

the organization will extend this framework beyond virtualization to include Web and SaaS protections, which provides additional coverage, especially when hosted off-premises or externally accessible.

At an optimal Level, organizations begin a proactive and dynamic approach towards security where the controls over access and actions become adaptive. Contextual app protection applies security controls dynamically, based on information about the user, location, or risk factors. Automation and orchestration play a pivotal role in streamlining security operations, while advanced monitoring prevents potential threats. Access controls become highly dynamic, adapting to ever-changing user context in real time, thus ensuring a highly resilient and agile security posture.


Citrix Pathway to Zero Trust Maturity

The Citrix platform offers a range of solutions and capabilities that align well with the implementation of a Zero Trust Architecture, including:

- Modern App and Desktop virtualization (VDI and DaaS)
- Web and SaaS application security overlays
- Legacy or Multi-tier app access
- Contextual Access and Continuous Monitoring for multifactor identity brokering
- Adaptive Authentication, Device Posture, and Security Analytics

Additional application security is also available from Cloud Software Group through NetScaler Application Delivery Controllers, Web App Firewall, and API Protection.

To learn more about Citrix solutions and how you can extend zero-trust to all your application types, please reach out to your Citrix partner or sales representative.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States