okta

Putting the Spotlight on Zero Trust Architecture

Implementing a Zero Trust architecture is a must in today's distributed work environment. To get Zero Trust right, organizations should start with modernizing their identity and access management.

Traditional security architecture is network perimeter based: allowing trusted users to access resources on the network, and keeping untrusted users out. But as companies become more and more distributed and their workforces operate outside the corporate network, this approach no longer works and poses a significant security risk.

Instead, organizations should adopt a Zero Trust model that never trusts and always verifies users—regardless of their role, location, or device. Within a Zero Trust framework, each user, device, and application is verified and authenticated with contextually aware tools, ensuring that only the right people have access to the right resources.

Zero Trust from then to now

The term "Zero Trust" first emerged in 2009 in research conducted by Forrester's John Kindervag. Since then, Zero Trust has evolved, and there are now several frameworks now available to help guide companies as they build their modern Zero Trust architecture. While each framework is unique, they all have three basic principles in common:

- Ensuring secure access to internal resources
- Controlling and monitoring access regardless of where requests originate from
- Verifying and logging all traffic in the network

Let's take a closer look at the three leading frameworks:

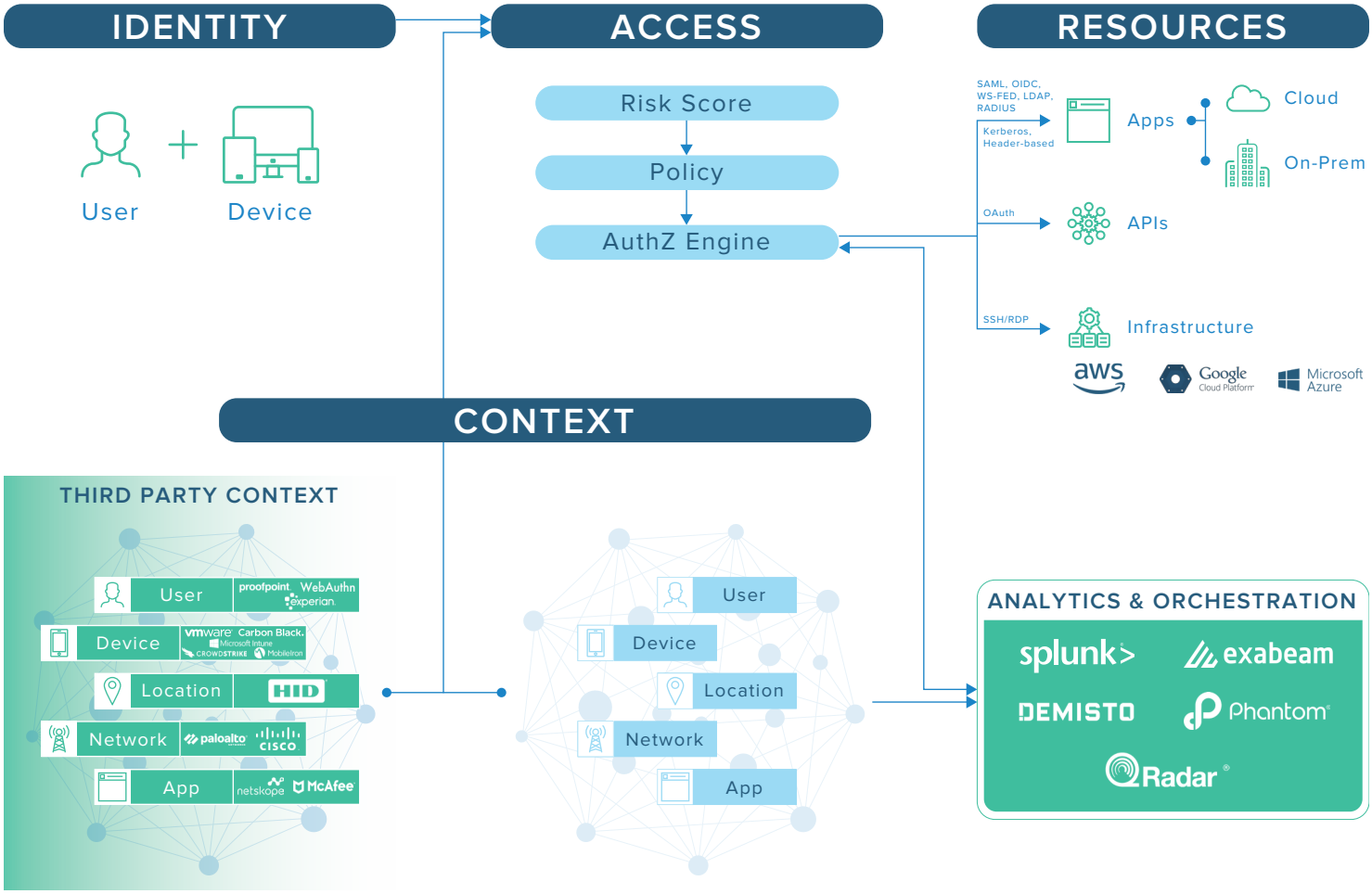
Framework	Forrester's Zero Trust Extended Ecosystem (ZTX)	Gartner's continuous adaptive risk and trust assessment (CARTA)	U.S. National Institute of Standards and Technology (NIST) SP 800-207
Origins	Released in 2018, it expands the focus on broadening modern security across technologies, including networks, devices, people, workloads, and more.	Introduced in 2017 and based on Gartner's Adaptive Security Architecture.	Following several drafts, NIST published the finalized framework in August 2020.
Principles	• Covers seven core pillars of Zero Trust (i.e., network, data, workforce, devices, workload, automation and orchestration, visibility and analytics). • Divides vendors into platform and best of breed vendors.	• Grounded in a "default deny" approach. • Continually assesses trust and risk, and applies this principle to all information security processes.	• Accounts for modern workforce practices and seeks to improve enterprise IT security postures. • Offers guidelines and uses cases to help organizations deploy Zero Trust architecture.

The first step on the road to Zero Trust is identity

Regardless of the framework you choose to adopt, the first step in implementing Zero Trust is deploying modern identity and access management (IAM). As the perimeter continues to dissipate, individual users should be a core focus for any Zero Trust architecture. This is why you need a robust and flexible identity management platform that effectively authenticates users and controls access.

While IAM sits at the foundation of your Zero Trust architecture, you'll also need a network of security tools that work together to enable Zero Trust maturity. The best approach for your organization will be one that seamlessly integrates with your technology, providing the same level of protection across on-prem and cloud-based applications, APIs, and infrastructure.

At Okta, our Zero Trust architecture starts with user and device identity on the Okta Identity Cloud. We have internal tools and third-party integrations to review the context of each login, and also analyze the risk profile of each access request before granting the right level of access to the appropriate resources. Behind the scenes, there are also several analytics and orchestration tools, SIEMs, and SOARs that are responsible for ongoing analytics, response, and remediation.



How to get started with Zero Trust architecture

Getting started with Zero Trust might feel like a complex endeavor, but it doesn't have to be. The first step is to implement some of the features of modern IAM.

"**Start with identity and device security**: We consistently find that enterprises have the earliest and rapidest success if they focus on improving identity management and device security. These two core components of the Zero Trust eXtended (ZTX) ecosystem drive rapid risk reduction and build confidence with executives that the organization can realize security benefits from its Zero Trust program quickly."

A Practical Guide To A Zero Trust Implementation
Chase Cunningham, Forrester Research, 15 January 2020

With this in mind, here are some of the tactical IAM projects you can focus on on your way to Zero Trust maturity:

- Deploy single sign-on across employees, contractors, and partners
- Adopt modern MFA and use multiple factors across user groups
- Unify policies across apps and servers
- Develop context-based access policies
- Automate deprovisioning for departing users
- Incorporate secure access to APIs
- Employ risk-based policies
- Incorporate continuous and adaptive authentication and authorization
- Allow for frictionless (and secure) access

To learn more about how Okta can support you as you embark on your Zero Trust journey, read our Getting Started with Zero Trust whitepaper. You can also take our free Zero Trust Assessment for your personalized roadmap to Zero Trust maturity.