



One-Minute Webinar: Zero Trust in Practice

Too busy to watch the [Zero Trust in Practice](#) webinar? Don't worry—we've got you covered.

There's a lot of hype around Zero Trust security, but it's proving to be more than just theory

Trust used to be a binary decision determined by the network, but as organizations move to mobile and cloud based services, the perimeter as we knew it has essentially dissolved. We can no longer assume trust based on the network, and trust is no longer a binary decision.

Those who know the concepts around the [Zero Trust model](#) are now seeking the real-world, positive security outcomes promised by it. Regardless of where you are in the journey to Zero Trust security, you're probably asking yourself, how can I tie these concepts and architectures into my own organization?

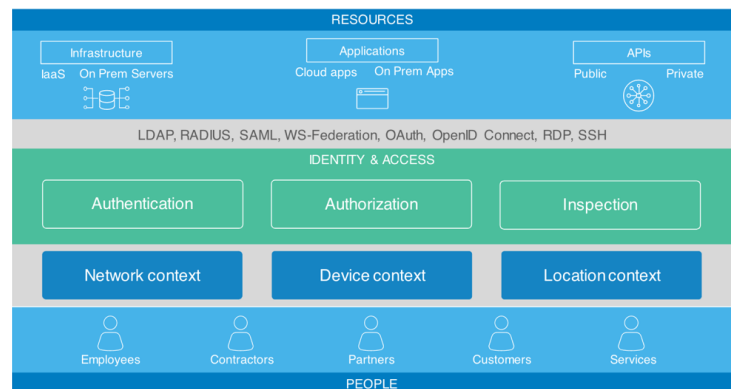
Why start with identity?

A unified identity layer sets the foundation for building smarter access controls, building policies over time, and allowing your systems to get smarter and smarter. Access is given based on trust, and trust is determined by context.

Align trust to context

Step 1: Map your resources and the identity of your users. Are they in a high-risk user group? What's the resource they're trying to access? Is it a low risk tool or high-risk infrastructure?

Step 2: Look at the context of the authentication event. What is the network, device, and location context? New IP? Logging in from a corporate IP zone? New or managed device? New city, state or even blacklisted geo-location?



Step 3: Combine steps 1 and 2 to create a contextual response: do you prompt for a 2nd factor, allow/deny access or raise a security alert?

Step 4: Go beyond discrete access policies based on context, and evaluate the overall risk associated with the login, assessed on a continuous basis.

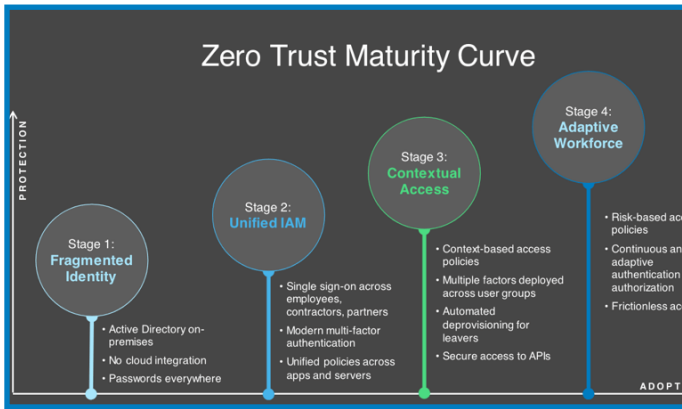
If implemented correctly, you'll achieve what Zero Trust promises: The right people have the right level of access to the right resources in the right context, assessed continuously. The goal, of course, is to achieve this with the least amount of friction possible. Security should be an enabler, not a blocker forcing users to hop around to different networks or enter different passwords.

Pain points

With Zero Trust, we're addressing some key IT and security pain points: multiple user stores with no source of truth, password sprawl across company resources, manual PKI and key management, and no way to enforce the least privileged access. With a lack of visibility into user behavior, only network traffic was visible, so sometimes breaches were discovered weeks, months, or even years later.

Steps to get to Zero Trust

Whether Zero Trust is a broad-based organizational initiative or a bottoms up project, this maturity curve, which many of our customers have followed, can guide you in your Zero Trust journey.



The takeaways

There's no silver bullet for Zero Trust, but the journey starts with Identity: Identity lays the groundwork, drives security, and drives experiences. With a solid identity layer, users earn trust based on a context that is continuously assessed.

Okta is your modern Zero Trust platform and jumping off point. Industry analyst firm Forrester Research recently included Okta in their evaluation of the Zero Trust market, [The Forrester Wave™: Zero Trust eXtended \(ZTX\) Ecosystem Providers, Q4 2018](#), and had this to say:

“Okta is skilled at securing end users and their ability to access the network, which is a key factor for all Zero Trust strategies and organizations. The company has spent significant time and resources to enable easy security for end users and enterprises, and thanks to its exceptional growth and expansion, it has a strong install base that are ‘in love’ with the solution.”

Want to dive deeper? [View the full webinar here.](#)

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device.

Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

www.okta.com