okta + vmware

Getting Started with Zero Trust: Okta + VMware Workspace ONE (Whitepaper)

Never trust, always verify

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Executive Summary

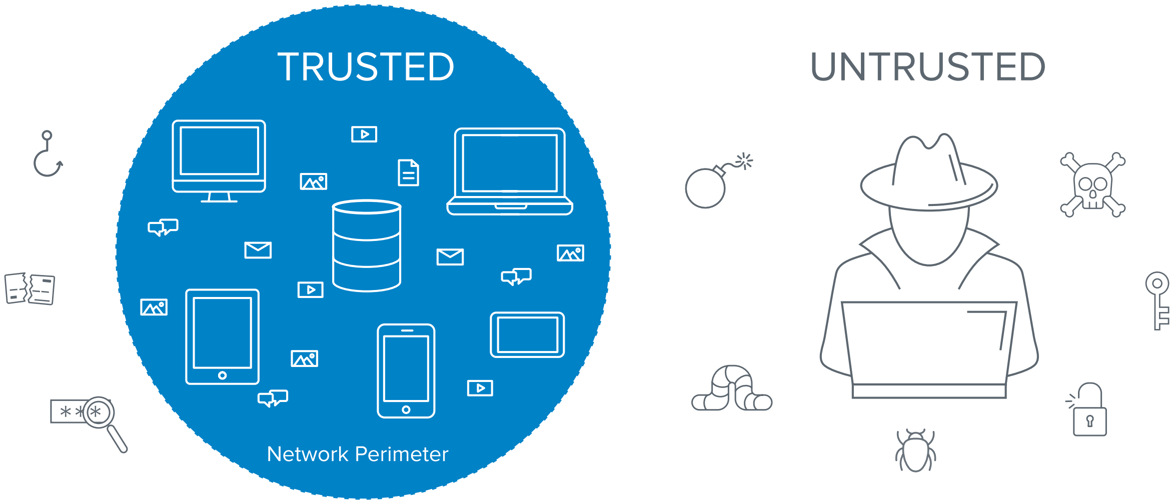
Zero Trust security throws away the idea that we should have a “trusted” internal network and an “untrusted” external network. The adoption of mobile and cloud means that we can no longer have a network perimeter-centric view of security; instead, we need to securely enable access for the various users (employees, partners, contractors, etc.) regardless of their location, device or network. There is no silver bullet when it comes to achieving a Zero Trust security architecture, but identity, access management and device management are the core technologies that organizations should start with on their Zero Trust journeys.

Here, we’ll explore the shifts in the security landscape that led to the creation of Zero Trust, what the Zero Trust Extended Ecosystem (ZTX) framework looks like today, and how organizations can utilize Okta and VMware Workspace ONE as the foundation for a successful Zero Trust program now, and in the future.

Challenge: When the Wall Protecting Your Data Vanishes

Traditional security architectures were built with two groups in mind: trusted individuals, able to access everything inside the organization, and untrusted individuals, kept on the outside. Security and IT teams invested in defensive systems that protected the barrier between them, focusing heavily on securing the network perimeter, often with firewalls. While they were successful in building a wall between potential threats and the safety of the corporate ecosystem, this full-trust model is problematic, because when that perimeter is breached, an attacker has relatively easy access to everything on a company’s privileged intranet—not to mention the havoc a rogue insider threat could wreak without even needing to breach the perimeter.

The “Castle and Moat” Approach to Securing the Enterprise



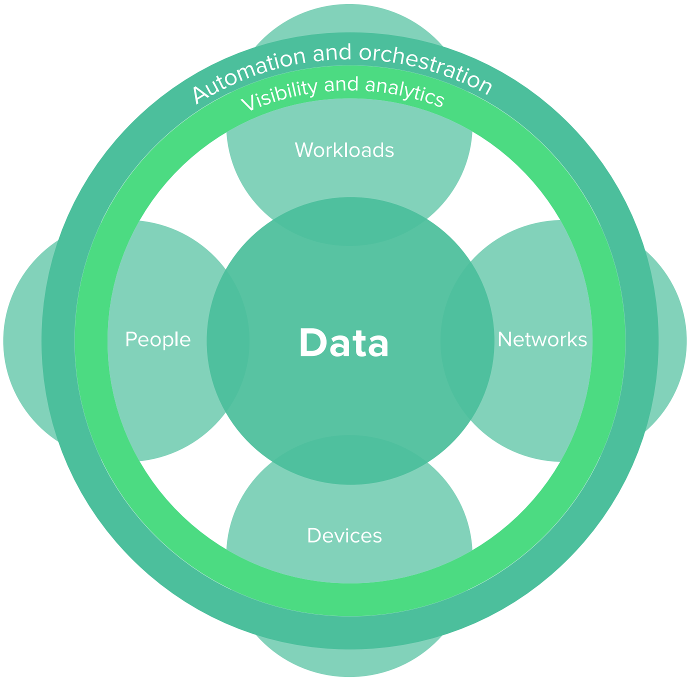
Add to that today's increased adoption of mobile and cloud technologies, where work is increasingly done outside the safety of a corporate network, and the network perimeter becomes increasingly difficult to enforce. In this world, there is no longer a wall around a business' sensitive assets: employees, contractors, partners and suppliers are all accessing data from beyond the traditional perimeter, representing potential threats.

And with more people, accessing more resources and data, from more devices and locations than ever before, the potential for one bad actor to cause damage across the entire ecosystem, if they break through, is massive. As a result, organizations can no longer assume trust across any part of the IT stack.

The Next Frontier: The Evolution of Zero Trust

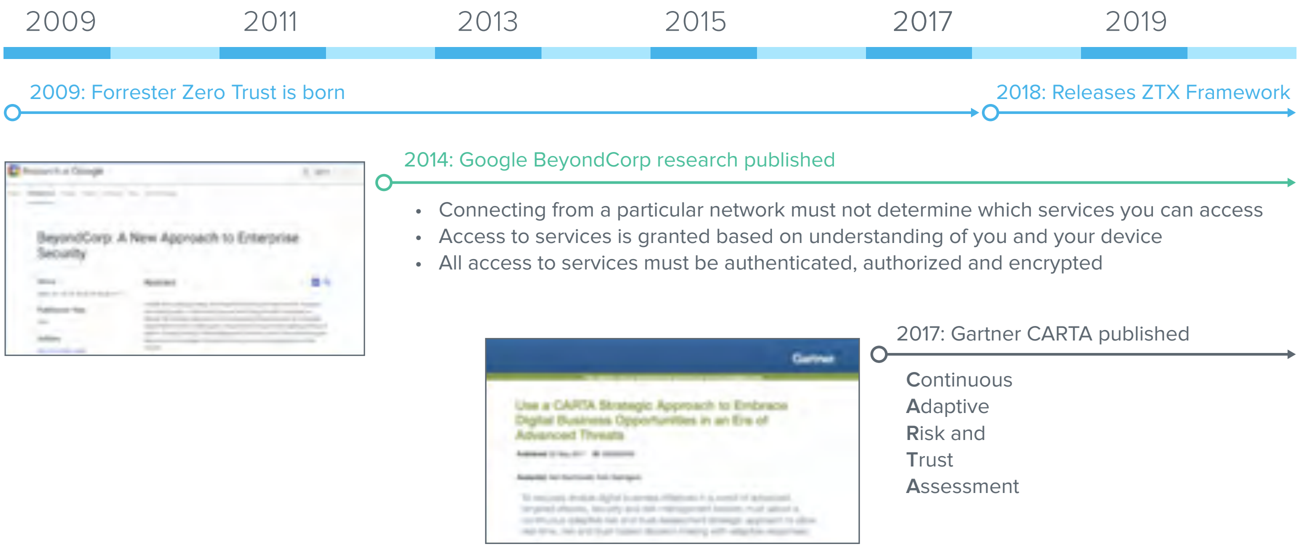
This shift in the security landscape is what led to the birth of Zero Trust. Zero Trust is a security framework, developed by Forrester Research analyst Jon Kindervag in 2009, that throws away the idea of a trusted internal network versus an untrusted external network; instead, he argued we should consider all network traffic untrusted.

In this initial framework, Kindervag focused on revamping the network perimeter and recommended organizations inspect all network traffic in real time, which requires a network segmentation gateway. Specifically, the three principles that made up his Zero Trust include: 1) all resources must be accessed in a secure manner, regardless of location; 2) access control is on a need-to-know basis and is strictly enforced; and 3) organizations must inspect and log all traffic to verify users are doing the right thing.



Since 2009, the rise of cloud and mobile has served as a catalyst for evolving Kindervag's original Zero Trust model. Gartner's 2017 CARTA framework[1] echoed Kindervag's Zero Trust framework with an added focus on not just authenticating and authorizing access at the front gate, but continuously throughout the user's experience through an adaptive, risk-based assessment to identify potential threats. Google's BeyondCorp research was published in 2014[2] and today serves as the marquee example of Zero Trust done right at massive scale.

Forrester's evolution of the Zero Trust framework—the Zero Trust Extended Ecosystem (ZTX), led by analyst Chase Cunningham—also emphasized this shift beyond network segmentation, expanding to data security, workload security, workforce security, device security, visibility and analytics, automation and orchestration. Cunningham's evolution extends Zero Trust beyond 'Next Generation Firewalls' to also include 'Next Generation Access,' making command and control over who has access to the network and data key to success.



2009: Forrester Zero Trust is born

2018: Releases ZTX Framework

BeyondCorp: A New Approach to Enterprise Security

2014: Google BeyondCorp research published

- Connecting from a particular network must not determine which services you can access
- Access to services is granted based on understanding of you and your device
- All access to services must be authenticated, authorized and encrypted

Gartner

Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats

2017: Gartner CARTA published

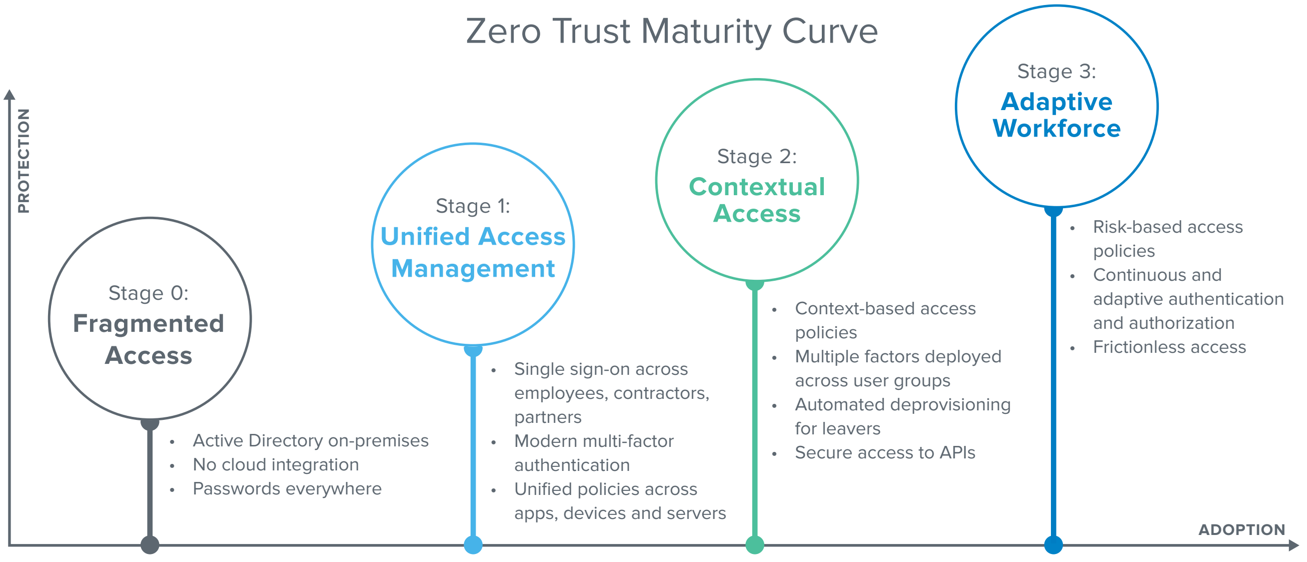
Continuous
Adaptive
Risk and
Trust
Assessment

Forrester also published new Zero Trust research that further emphasizes the importance of access in late 2018. The report, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018, included a number of vendors, including both Okta and VMware. Key criteria for this analysis included all seven of the ZTX ecosystem pillars: network security, data security, workload security, workforce security, device security, visibility and analytics, automation and orchestration, as well as manageability and usability and API usage.[3]

[1] Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, Inc., May 22, 2017
[2] BeyondCorp: A New Approach to Enterprise Security, Google, 2014
[3] The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., January 19, 2018

The Foundation for Zero Trust: Okta + VMware

Put simply, the core of Zero Trust is to "never trust, always verify," ensuring the right people have the right level of access, to the right resources, in the right context, that is assessed continuously—and all without adding friction for the user. That Zero Trust nirvana doesn't happen overnight, and as organizations implement Zero Trust architectures, we've seen several stages of infrastructure maturity:


Zero Trust Maturity Curve
PROTECTION
ADOPTION
Stage 0: Fragmented Access
Active Directory on-premises
No cloud integration
Passwords everywhere
Stage 1: Unified Access Management
Single sign-on across employees, contractors, partners
Modern multi-factor authentication
Unified policies across apps, devices and servers
Stage 2: Contextual Access
Context-based access policies
Multiple factors deployed across user groups
Automated deprovisioning for leavers
Secure access to APIs
Stage 3: Adaptive Workforce
Risk-based access policies
Continuous and adaptive authentication and authorization
Frictionless access

Stage 0: **Fragmented Access Management**

Many organizations begin their Zero Trust journeys with a variety of on-premises and cloud applications that are not integrated together or with on-premises directories such as Active Directory. As a result, IT is forced to manage disparate identities across a number of systems as well as the many applications and services used without IT awareness. For the user, this also means numerous (and, most likely, insecure) passwords. Without visibility and ownership over these fragmented identities, IT and security teams are left with potentially large windows for attackers to exploit access into individual systems.

Stage 1: **Unified Access Management**

The first step to resolving the security gaps left open by fragmentation is consolidating under one access management system. This Stage 1 consolidation, via single sign-on (SSO), is critical to managing access and shouldn't be limited to solely customers but instead any user that needs access to a service, including the full extended enterprise of employees, contractors and partners. Layering a second factor of authentication to that centralized identity access point further helps to mitigate attacks targeting credentials. Additionally, unifying access policies across devices, applications as well as servers, a critical part of IT infrastructure, is key to bringing IAM together into one secure, manageable place for IT across on-premises and cloud.

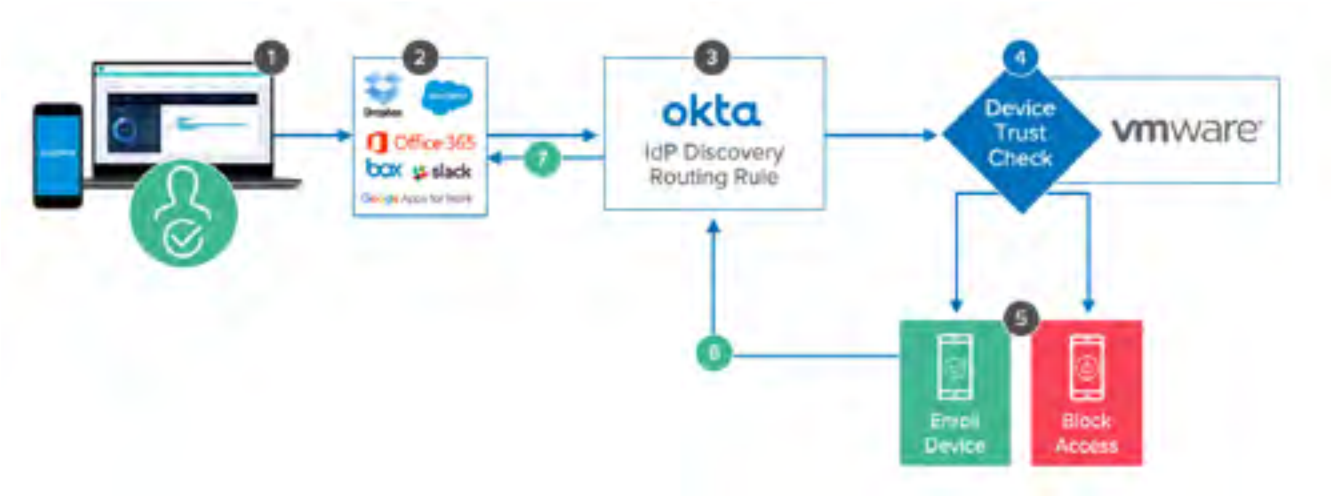
Thousands of organizations use Okta SSO to unify their user identities. Often paired with Okta Universal Directory, a cloud-based directory service that can serve as a single source of truth for IT organizations, it serves as an integration point to multiple ADs and other on-premises directory services, Okta SSO makes managing and securing the extended enterprise simpler for IT and eliminates the password proliferation that plagues users. Combined with VMware Workspace ONE mobile SSO, end users get seamless authentication to their mobile applications across their mobile devices. VMware Workspace ONE mobile SSO means end users do not get prompted for their credentials and instead get immediate access to their applications, enabling consumer simplicity while maintaining enterprise security. VMware Workspace ONE Unified Endpoint Management further helps IT manage credentials on any device, including Windows 10, macOS, iOS, Android and more. And with Okta Advanced Server Access, IT can extend the access control to the server layer, bringing secure access management to the full breadth of endpoint, on-premises and cloud resources IT needs to manage.

Stage 2: **Contextual Access Management**

Once IT has unified access management with unified endpoint management, the next stage in Zero Trust security is layering in context-based access policies. This means gathering rich signals about the user's context (i.e. Who are they? Are they in a risky user group?), application context (i.e., which application the user is trying to access), device context, location and network, and applying access policies based on that information. For example, a policy could be set to allow seamless access to managed devices from the corporate network, but unmanaged devices logging in from new locations would be prompted for MFA. Organizations can also employ multiple factors across user groups to step up authentication based on an understanding of those authentication attempts. Examples might include low risk users without smartphones using one-time passcodes, or high value targets would be required to use hard tokens using a cryptographic handshake to securely authenticate to a service. Furthermore, if a user leaves or changes roles within an organization, automated provisioning ensures the user has access only to the tools s/he needs to do their work (or, in the case of a departure, automatically revokes all access, mitigating the risk of orphaned accounts or latent access after a departure). Finally, these rich access controls should be extended to all technologies used by the workforce, including secure access to APIs that are the building blocks of modern applications but can expose sensitive data to the web.

Many organizations today are already using Okta's contextual access management feature set with Okta Adaptive MFA, as well as VMware Workspace ONE for device management, compliance, configuration, and health across all devices. By processing a variety of contextual insights about a user, location, network, application, and also with contextual insights about a device from Workspace ONE, the Okta policy framework can serve up a contextual response. This response is based on an organization's risk tolerance, which acts as the first line of defense in keeping an organization secure.

For example, if a user attempts to authenticate from their usual corporate laptop on the corporate network, an organization could set a policy that only requires that user to successfully enter a password. But, if the user attempts to authenticate from the corporate laptop in a foreign country or on a public wifi network, the policies could require both a password and a second factor. If a device's security posture is found to be at high-risk due to zero-day malware, Workspace ONE policies can help quarantine the device by reducing or removing application access. This kind of contextual access benefits both the user and IT/security, only prompting for a second factor during risky authentication attempts, not every time.



Stage 3: **Adaptive Workforce**

The final stage of Zero Trust implementation extends organizations' focus on authenticating and authorizing access. This means authentication no longer occurs just at the front gate, but continuously throughout the user's experience through an adaptive, risk-based assessment to identify potential threats. This looks like adding an intelligent, risk-based engine to the contextual responses from Stage 2, going beyond the discrete policies set in the prior stage to now allow IT to set risk tolerance and allow the risk scoring based on those contextual signals to determine the riskiness of a particular authentication event, and prompt for a second factor based on that insight. That trust is also no longer absolute: this adaptive authentication would be continuously monitored for a change in one of those signals, re-prompting for authentication and authorization verification should an aspect of that user's context change. Finally, while security is increased through these intelligent, risk-based access controls, the experience for the end user would ultimately be simplified—allowing for frictionless access and, in cases where IT has set a policy to allow for it, passwordless authentication.

Okta allows administrators to use policies to transform the end user authentication experience, and includes completely removing the password from the authentication flow. Replacing passwords with an alternate factor (such as Okta Verify or a YubiKey) as the primary factor for authentication, IT administrators have choices. They can set risk-based authentication policies that require step-up authentication based on risk tolerance around the varied signal inputs. If confidence is high that the user is who they say they are, that user is only prompt for that first, non-password factor.

VMware Workspace ONE mobile SSO further enhances the user experience on mobile devices and ensures device security. Workspace ONE Intelligence provides IT with insights and automation to enhance user experience and increase security across users and devices. Using these insights, organizations can manage application access based on data that's aggregated and correlated from different data sources, such as devices, apps, identity and location. Automation capabilities in Workspace ONE Intelligence helps IT improve their day-to-day operations by leveraging integrations with third party solutions, such as a service desk, removing time-consuming manual tasks. Service desk tickets can automatically be opened, and actions can automatically be executed based on the insights gathered by Workspace ONE Intelligence.

And while intelligently controlling access to corporate resources is the foundation of behavioral monitoring, pinpointing the root cause of a compromise is difficult—especially when the problem is an issue of who, not what. The Workspace ONE platform further extends an organization's security footprint by ingesting threat intelligence from third party security solutions through the Workspace ONE Trust Network, giving IT even greater insights and automations through Workspace ONE Intelligence. With security analytics and Security Information and Events Management (SIEM) integrations, Okta enables organizations to take advantage of Okta's rich identity context and user activity and enforce remediation actions against compromised accounts. Okta also integrates with Cloud Access Security Brokers (CASBs) to provide organizations with detailed visibility and alerting for continuous checks on risky events during the authenticated sessions. Alongside Okta's SIEM partners, Okta can provide valuable authentication data to better detect anomalies, allowing CASB services to issue a response back to Okta, which can then revoke access at the identity layer.

End User Experience

In order for users to continue to adopt technologies to be productive across all stages of the Zero Trust maturity curve, Zero Trust security has to embrace end user experience. Unifying access through Okta SSO gives end users a single access point to get into all of their workplace services, without needing to maintain multiple sets of credentials. Contextual access also allows security and IT to simplify the authentication experience for the end user, with multiple factor options—including passwordless experiences—to simplify the end user experience without compromising security. The Workspace ONE Intelligent Hub gives end users a single point of entry to securely access any application from any device. Within the Workspace ONE Intelligent Hub, Workspace ONE mobile flows enables users to interact with application data without opening the actual application. For example, a user can interact with a CRM application, like Salesforce, directly from the Workspace ONE Intelligent Hub without launching the CRM application.

Wrap up

Most organizations today are at ground zero of the Zero Trust maturity curve, but as they continue to adopt the never trust, always verify approach to their IT security, Okta and VMware continue to support additional features that enable stronger, simpler access management. These capabilities, such as in-app feature access, risky behavior analysis that leads to actionable insights, and integrations with solutions like ServiceNow to quickly address potential threats will further help IT evolve with the Zero Trust maturity curve. To learn more about Zero Trust with Okta and VMware Workspace ONE, visit okta.com and workspaceone.com.

About Okta

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

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them 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.

Learn more at www.okta.com

About VMware

VMware software powers the world's complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Headquartered in Palo Alto, California, this year VMware celebrates twenty years of breakthrough innovation benefiting business and society.

For more information, please visit https://www.vmware.com/company.html.

okta

+

vmware®