okta

Zero Trust with Okta: A Modern Approach to Secure Access from Anywhere

How Okta enables a Zero Trust solution for our customers

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

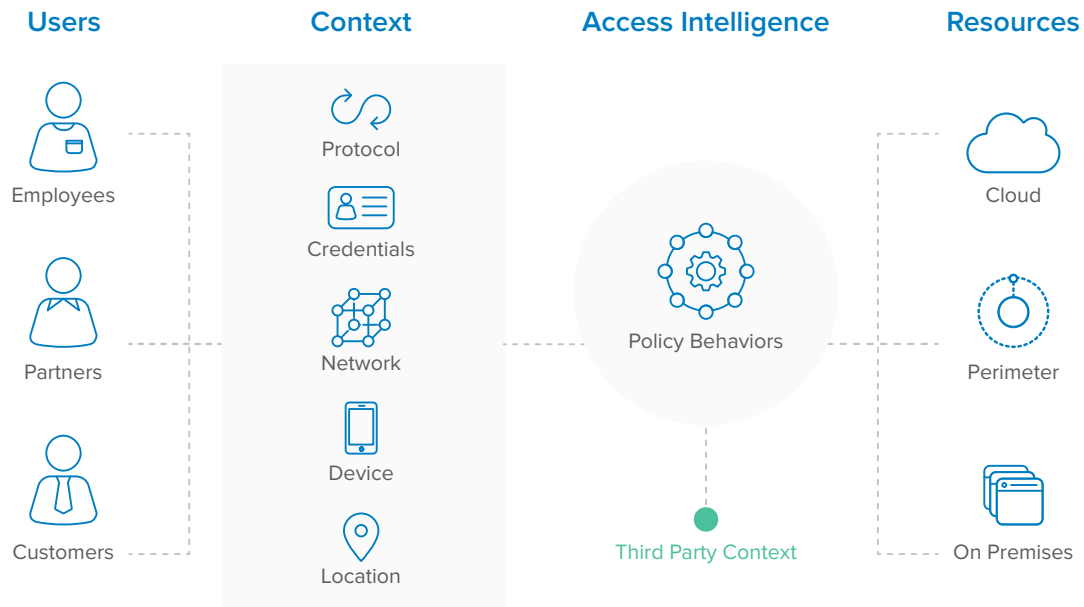
info@okta.com
1-888-722-7871

Zero Trust with Okta: A Modern Approach to Secure Access from Anywhere

People Are the New Perimeter

In the era of managing cloud identities across your enterprise and extended enterprise, users have redefined what it means to secure the corporate perimeter. For most enterprises, the conventional security approach was to be fully dependent on on-premises infrastructure to create an obvious layer of security across corporate resources. In recent years, we have seen a proliferation of devices in the enterprise; people no longer work just from their office—anywhere there is an internet connection is a potential workspace. This introduces a problem for IT, however, as it is now more difficult to control the devices and networks people work from. Traditional security solutions are only effective if IT own both the device, and the network. However, the traditional perimeter based approach has now faded, and while we used to rely on servers, VPNs, firewalls to enforce security, not only is the perimeter based approach no longer secure enough, it is also too restrictive for users who need to be productive from anywhere, at any time--and on devices which may or may not be controlled by IT.

This is where identity as a centralized control point is critical. As businesses evolve and recognize the value of embracing cloud technologies alongside BYOD, it is critical to redefine the perimeter and focus on a user centric approach, where all users are considered “internet” users. We can no longer derive trust solely based on devices and networks. Security for the extended enterprise needs to take into consideration not just employees, but also partners, contractors and customers who want consumer like digital experiences to stay productive. A simple, one size solution may seem easy, but when we have users accessing applications across a wide range of clients, operating systems and browsers, organizations need a solution that ensures broad application coverage, best of breed interoperability, a great user experience, and low complexity.



Security for Everyone and Everything

We have seen a few commonly accepted approaches to modern enterprise security, the most prominent of which are the Zero Trust Model introduced by Forrester, and BeyondCorp, introduced by Google.

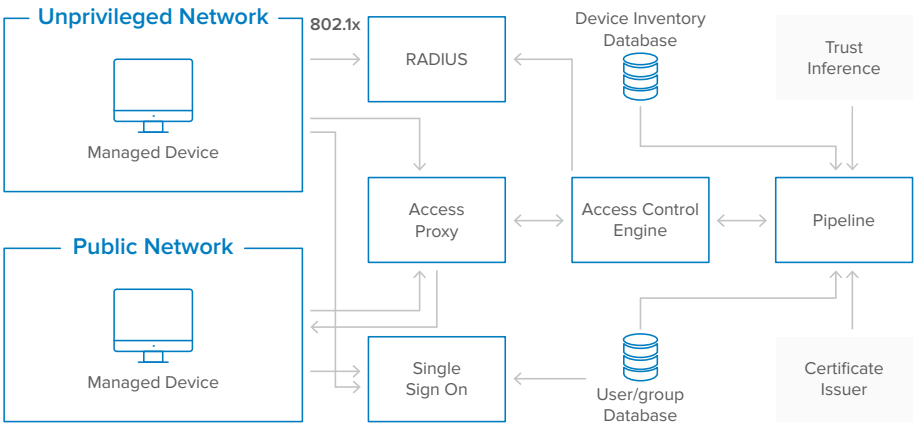
Forrester's Zero Trust Model was developed in 2009 as a response to targeted attacks initiated by malicious insiders—in these scenarios, the perimeter based model is ineffective. As the underlying theme of the Zero Trust Model is "trust no one", Forrester's approach to secure the modern enterprise is to throw out the idea of having a trusted internal network vs an untrusted external network—essentially, these should be considered equally insecure[1]. Forrester recognized that the increased use of mobile technology is a driving force for an updated information technology security model. The Zero Trust Model encompasses three core concepts[2]:

- Ensure all resources are accessed securely regardless of location
- Adopt a least privilege strategy and strictly enforce access control
- Inspect and log all traffic

To summarize these three core concepts, customers should:

1. Assume that all traffic is a threat unless it has been verified and authorized
2. Allow minimal permissions for both end users and admins to access corporate resources
3. Invest in network analysis tools and logging to follow a "verify and never trust" methodology

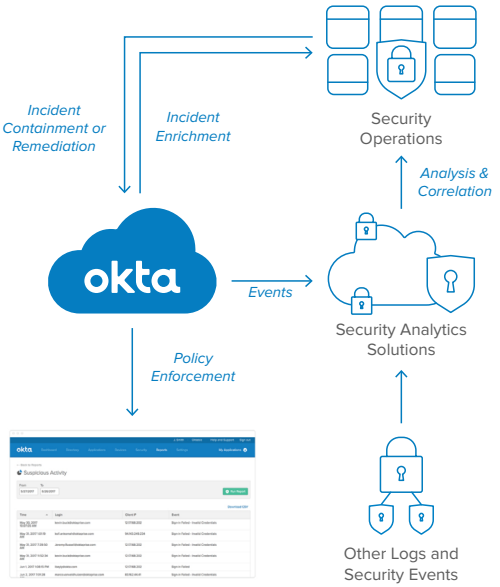
Google has recognized the need for an updated approach to enterprise security with their BeyondCorp implementation—a realistic and practical security model which shifts access control from the standard network perimeter to individual devices and users[3]. The BeyondCorp architecture consists of Data Sources, Access Intelligence, Gateways and Resources—each of these components are associated with various controls that help to dynamically determine an access tier for a user and their associated devices. BeyondCorp uses the concept of trust levels that are organized into different tiers, and each resource (such as an application or service) is associated with a minimum trust tier required for access.



BeyondCorp components and access flow (as designed by Google)

The Zero Trust model and BeyondCorp methodologies apply across all organizations - you will notice that neither methodology calls out specific technologies or vendors, but rather highlight the importance of a secure, flexible, and scalable information security approach to protect corporate resources and data.

At Okta, we are making the Zero Trust Model a reality for our customers with our new contextual access management feature set—Okta device trust. Along with the Zero Trust Model, device trust also follows the data sources and resources components of BeyondCorp to provide an identity and device centric approach to your organization's overall security strategy. We have also introduced a growing ecosystem of integrations with leading security analytics vendors that enables both visibility and response. And, we have been working on enhancements to our Adaptive MFA behavioral detection policies to allow you to track anomalous user login activity to Okta. Device trust and our ecosystem of security integrations can be implemented alongside Okta's powerful and trusted SSO and Adaptive MFA policies to provide a full security solution for your users. Okta's implementation of the Zero Trust Model today is just the first step of our larger contextual access management vision to provide streamlined and secure access to your corporate resources. As our contextual access management feature set progresses, our solution will further encompass the network security focus of Zero Trust with the device centric approach of BeyondCorp.



Respond to account compromise with Okta

Today's challenge in visibility and response encompasses the following:

- Disappearing perimeters introduces new difficulties in responding to risk - how do you best administer access control to devices, services and people?
- Pinpointing the root cause of compromise is difficult
- Having disparate security systems working together to provide true security visibility is a significant barrier to reducing risk

Okta's policy engine enforces strong authentication to your applications, helping to reduce risk of breach. Our security analytics partner technologies call our API or consume our systems log to offer additional insight in managing the security of your Okta org. When combined with our security analytics partners, Okta contributes valuable data on users, applications, and devices - giving you a holistic view of security across your enterprise. Read more on our security analytics integrations here.

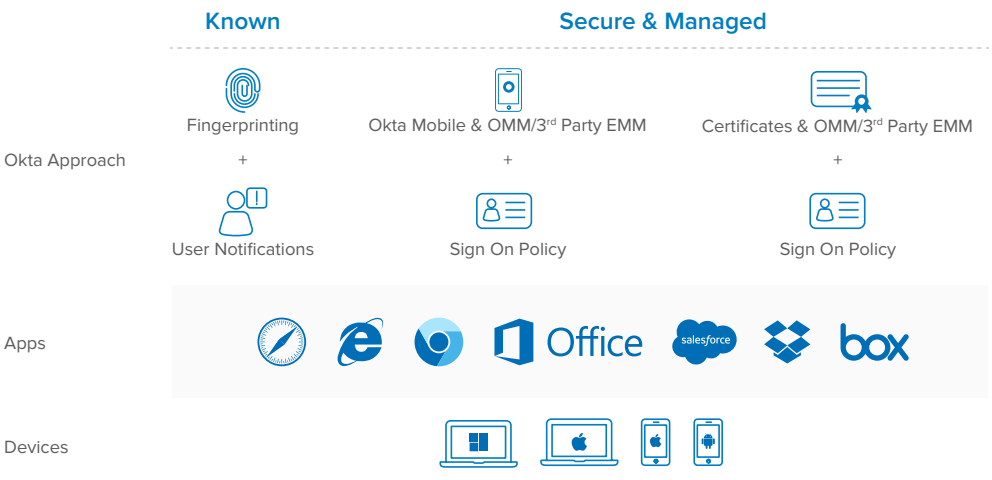
Okta's Approach to Secure the Modern Perimeter

The strongest context signals come from the devices your people are using to access corporate resources. Okta's concept of the Zero Trust Model consists of processing a variety of contextual insights about a user—including their credential, device, location, network and the application or browser a resource is accessed from. The Okta policy framework is a condition and actions engine that acts as the first line of defense in keeping your organization secure, and based on the conditions you have defined, the policy engine will respond with actions such as allow, deny, prompt for MFA and more. Our upcoming behavioral detection policies enhance the Okta policy framework to track unusual activity such as anomalous location, anomalous IP, and anomalous devices.

Intelligently controlling an access decision 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.' With the security analytics integration, Okta has enabled organizations to use their existing monitoring tools to consume the Okta events and logs APIs—you can collect Okta data in your security analytics or SIEM system to assess anomalous activities against Okta accounts. Okta's rogue accounts report compares assignments in Okta to accounts that exist in a specified app and lists the discrepancies. This allows you to find accounts that were created directly in the application without going through Okta, and correct them to ensure all access to the app is managed through Okta. And, Okta already integrates with CASBs like Netskope and Skyhigh Networks to provide you with detailed visibility and alerting for corporate resource access.

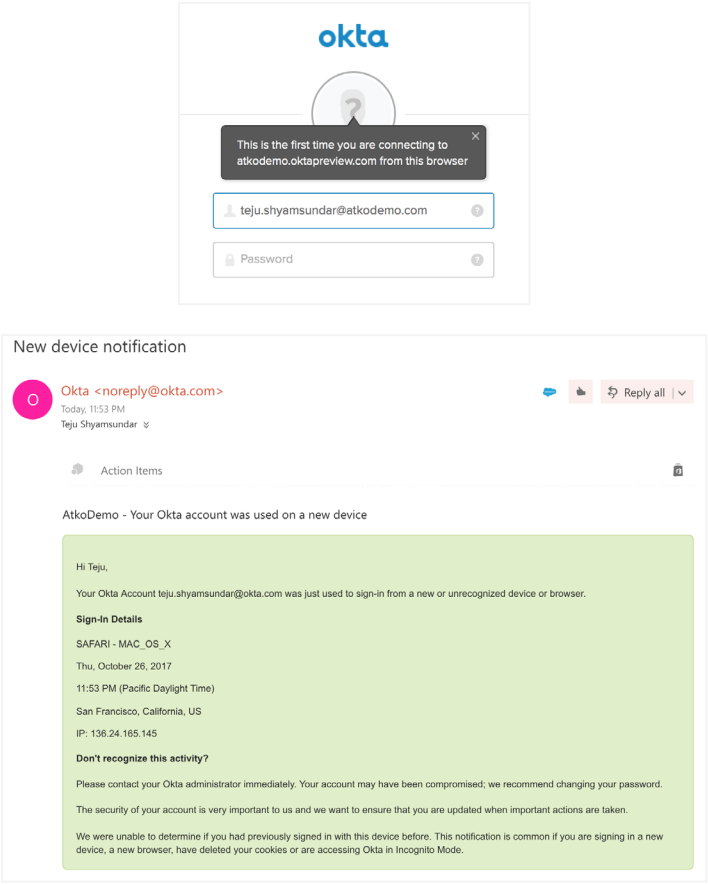
Secure Access from Any Device, Anywhere

Okta plays a critical role to ensure that your users are only able to access applications and resources from devices that you can trust. The process of proving a user's identity and the security posture of their associated device has different levels. We first need to recognize if access is initiated from the correct user, then assess that it is a known device. Then, we need to assess if the platform and client that the user is attempting to access from follows your organization's security policy. Okta's Adaptive MFA policy settings are the first step in making a user specific access decision. Once Okta has verified that the correct user has in fact initiated application access, we can move on to the device specific checks. Okta's device trust solution offers two different methods to evaluate what a trusted device means to an organization.



Device Trust—The Specifics

Certificates are a very common method organizations use to identify a known device, and Okta is now able to issue device certificates from an Okta Certificate Authority. Okta has separated the management of Okta Certification Authority issued certificates from the deployment of the certificate, so that organizations can use Okta alongside a 3rd party device management solution to establish and manage device trust. And, while certificates are a very strong trust signal, there are technical limitations that arise from using certificates to assess a trusted device. Okta has identified scenarios in which the certificate based approach needs to be modified to successfully assess trust across all native mobile applications. To address these technical challenges, Okta is also providing an application based model for device trust to cover more applications and more platforms via an enhancement to our Okta Mobile application. The application based approach will ensure that Okta Mobile integrates with 3rd party mobile device management solutions that organizations are already using to manage their mobile devices. Once Okta has identified that the device is managed, the last step is to assess if the client that the user is accessing a resource from—web browser vs native application, should be allowed. In a scenario where the device is not managed, but Okta has evaluated that the user should have access after securing the device, the user is prompted to complete an enrollment flow that will ultimately allow access to their corporate resource. And, if a user is accessing Okta protected applications on a new device, within seconds they receive an email with detail on where access is initiated from.



Okta's policy framework plays a critical piece in all three steps—user identification, device & platform security assessment and client access assessment.

For many enterprises, secure mobile access is a key component when evaluating an overall contextual access management strategy. The Okta device trust solution will cover more scenarios and device platforms as the product evolves.

Today, the reality is that many organizations will need to remain in a hybrid environment for a significant period as they begin their cloud transformation. Okta can easily work alongside your existing infrastructure – we can work with directories such as Active Directory, asset management tools like LANDESK or System Center Configuration Manager, and mobile device management tools like Airwatch and MobileIron. You can use your existing asset management tools for policy enforcement settings like disk encryption, patch levels or application versions, or enforcing a PIN code and deploying managed applications to mobile devices, but then use Okta to verify that the device is managed and trusted.

Okta's Role in Evaluating a Device's Security Posture

Okta's device trust service is built to integrate with the technology you already have.

The approach we take to verifying that a device is trusted is optimized for the most commonly used platforms, and we allow customers to leverage existing device management tools. When it comes to desktop, you can continue to use your device management systems like System Center Configuration Manager, IBM BigFix, or LANDESK. And for mobile, we know customers use solutions like Airwatch and MobileIron for device management, and you can continue to use those solutions alongside device trust.

All you will need to do in Okta is determine which applications need to be associated with a device trust policy. Your device trust policy, along with Okta's other context aware policies, will work cohesively to ensure secure access across all device platforms and clients.

Zero Trust with Okta—Looking Ahead

Today, Okta has a robust policy driven approach that incorporates signal data from devices, credential, networks, IP reputation, and sessions. But, we are not stopping there. We will continue to evolve Okta's policy engine intelligence to become much more behavioral in nature. Malicious access attempts can't always be anticipated, and writing a rule for every access combination you want to prevent isn't realistic - but we have you covered here. You will be able to rely on Okta to detect anomalous behavior and make the right decision.

As Okta continues to evolve our Zero Trust and BeyondCorp solutions, you'll start to see security enhancements across the full Okta offering. We have added TouchID support on iOS and fingerprint support on Android for the Okta Mobile application. In the upcoming months, you will see major updates to our Adaptive MFA offering via the behavioral detection engine that will address common concerns such as anomalous logins, risky locations and networks, and common password detection.

The shift to a cloud first environment can be a difficult one, but fortunately, Okta has developed our contextual access management solution to allow for a phased deployment – and optimized for hybrid environments. As you begin to shift your organization's perimeter away from the traditional on-premises approach, Okta's method of deployment will help you to answer the common questions:

- Which applications are the most important to my business?
- Who will receive contextual access management policies first?
- How does an end user remediate a non-compliant device?
- What does your ideal solution encompass? Remember, Okta can help you to deploy secure solutions like:
    - Adaptive MFA factors and policies for your Okta managed applications
    - MFA for on-premises resources
    - Application sign-on policy
    - Device trust
    - Security analytics integrations

Okta's vision is to deliver an end to end contextual access management solution that encompasses monitoring, remediation, and device management across all platforms and applications. We have already taken the first steps to support this vision in an integrated manner that works alongside your existing directory, security and device management tools to preserve your choice of vendors. Okta has proven our ability to integrate with thousands of applications across our Okta Integration Network, and we are developing a contextual access management solution with the same approach—enabling your organization to evaluate and adopt various technologies to ensure that you are covered.

[1] No More Chewy Centers: The Zero Trust Model of Information Security—
https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682
[2] BeyondCorp A New Approach to Security—
https://cloud.google.com/beyondcorp/
[3] Developing a Framework to Improve Critical Infrastricutre Cybersecurity—
https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf
[4] Security Analytics Partner Integration Guide—
https://www.okta.com/sites/default files/Okta_Security-Analytics_Partner-Integration-Guide.pdf

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 enterprises. 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


okta