Whitepaper

Getting Started with Zero Trust Access Management

Trust Begins with Secure Identity Okta Inc.

Contents

Executive Summary

There is no denying that the perimeter has shifted with the adoption of mobile and cloud and we can no longer rely solely on a network perimeter-centric view of security. This transformation has accelerated more recently to a fully distributed and hybrid working environment requiring a new model for security. Zero Trust is a security strategy that challenges the notion that there is a "trusted" internal network and an "untrusted" external network, trust can no longer be implied. Organizations need to be able to establish trust relationships in order to securely enable access for various people (employees, partners, contractors, supply-chain, etc.) regardless of their location, device, or network. There is a new modern perimeter that needs to be protected, and that perimeter begins with Secure Identity.

There is no silver bullet solution when it comes to achieving a zero trust security architecture: this is not something that happens overnight, or is in fact ever actually 'complete'. Adopting a zero trust security strategy provides the ability for organizations to transform and innovate, adopt new technologies and practices, optimize productivity and reduce their risk surface. This paper explores why identity and access management (IAM) solutions offer the core technology 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 a zero trust strategy looks like today, and how organizations can utilize Okta as the foundation for a successful zero trust program now, and into the future.

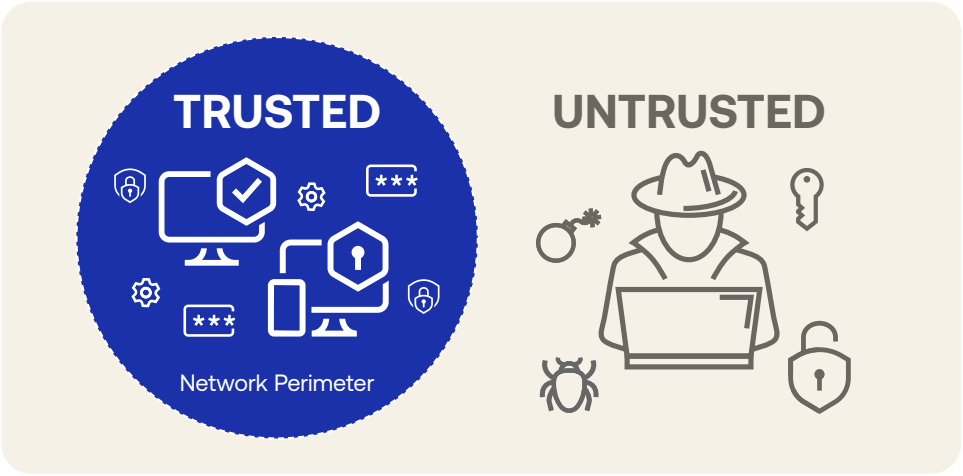
Challenge: When the Wall Protecting Your Data Vanishes

Zero Trust is not a novel concept or idea. The industry has been discussing the reality of the shifting perimeter for nearly two decades, with origins back to the Jericho forum. It has really only been within the last 5-10 years that we have finally reached a point where organizations are prioritizing security strategy and technology has seen enough innovation to support the implementation of these new strategies.

This was brought into sharp focus in 2020. The worldwide pandemic forced many organizations to shift operations to support remote work overnight, effectively dismantling traditional security models, accelerating the adoption of cloud technologies, and forcing the shift to support remote work outside the safety of a corporate network. As the world emerged from the pandemic, many organizations made the decision to continue to support a dynamic work model, meaning they must maintain flexibility while securing fully distributed workforces and hybrid working models. The modern

workforce—comprised of employees, contractors, partners, and suppliers—are all accessing more resources and data (stored in the cloud and on-premises), from more devices and locations than ever before.

This isn't to say that traditional security architectures (castle and moat) suddenly become irrelevant, they still serve a purpose. Security and IT teams who have invested in defensive systems focused heavily on securing the network perimeter, using firewalls and VPNs to enforce access policies, are faced with new challenges in securing a more hybrid work model. This requires innovative thinking and agnostic solutions that can augment and compliment existing infrastructures while supporting digital transformation and modernization initiatives.



As the infrastructure has evolved, the risk surface has expanded with an increasing number of access points and these are being exploited at an alarming rate. Reported incidents of cyberattacks have exponentially increased. While methods of attack have elevated in sophistication, they still primarily target identity. Credential abuse and highly targeted phishing attacks remain the leading cause of breaches today. Gaps in identity protection introduce risks like account takeover, supply-chain, and ransomware attacks. As a result, organizations should no longer automatically assume trust across any part of the IT stack. Regardless of industry or geography, secure trusted users have become more important than ever—and identity is the modern perimeter.

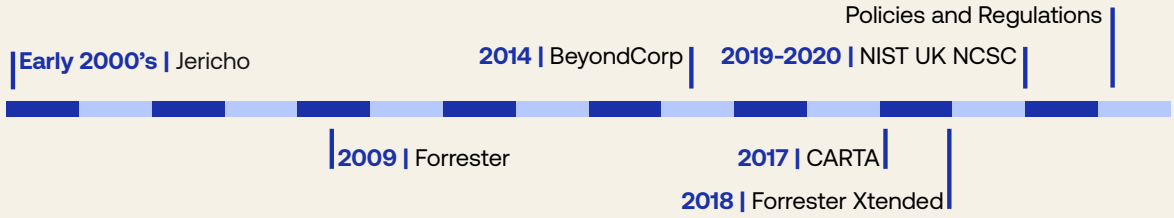
The Next Frontier: The Evolution of Zero Trust

To understand where we are, it's helpful to understand where we came from and how this has evolved. The notion of the shifting perimeter has its origin story as far back as 2004, when the Jericho Forum was founded with the mission to define the problem and solution for deperimeterization. In 2009, John Kindervag introduced the term "Zero Trust" during his tenure with Forrester—at the time, this was based on the idea that all network traffic should not be trusted and that any request to access any resource must be done securely. This original concept of Zero Trust based on a network-centric design focused on leveraging micro-segmentation to enforce more granular rules and limit lateral movement by attackers. As the concept of Zero Trust continued to evolve, a more identity-centric approach started to gain prominence.

Google's BeyondCorp research was published in 2014, and this model shifts access controls from the perimeter to individual devices and users. In 2017, Gartner published the Continuous Adaptive Risk and Trust Assessment (CARTA framework) which faintly 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. Forrester has even updated their framework and in 2019 published the Zero Trust Extended Ecosystem (ZTX) Forrester's team calls out capabilities such as single sign-on (SSO) as a critical feature, and notes that multi-factor authentication (MFA) "reduces access threats exponentially."

Frameworks provide a solid foundation for understanding how technologies can support new security models but there has been a lack of direction or guidance around how organizations can realize and adopt Zero Trust. In 2019, NIST released its first draft of Special Publication 800-2073. This publication combines elements of the above Zero Trust frameworks and discusses the components NIST sees as making up a zero trust architecture.

Over the past two decades the industry, analysts and practitioners, have collectively evolved the understanding of a zero trust security strategic approach to match advances in technology and the way we work. In all cases, the approach has become increasingly more risk-based and identity-centric—this is where Okta can support organizations. Okta is able to help address the business challenges being faced and accelerate adoption of a zero trust security approach by providing the foundation for secure identity and context-aware access protecting the modern perimeter.

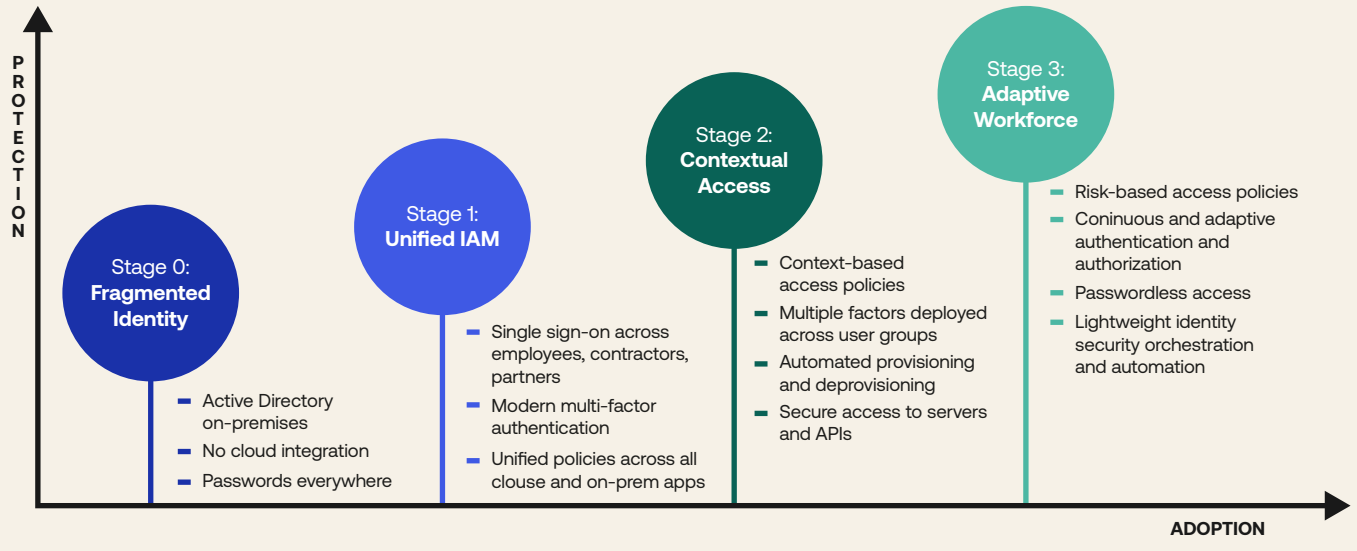


Making Identity the Foundation for Zero Trust

The Identity Defined Security Alliance (IDSA) states in their whitepaper that 'Zero Trust' begins with "identity" whose objective is to get access to "data". Identity is the "actor" in most transactions. Access to data includes retrieval, deletion and modification of data. An identity is not restricted only to human users, as processes often act on their own to access valuable data and must be considered as a valid "actor".'

By starting with an identity-centric approach to security organizations are able to ensure the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously—all without adding friction for the user. Ideally this begins with an identity and access management (IAM) solution.

Every organization will find themselves at various levels of adoption and maturity with many factors at play that need to be considered, zero trust doesn't happen overnight but it doesn't have to be complicated. As Okta has helped support many organizations to secure their identities and transform their business, there is a generalized maturity model that has been developed to provide guidance on areas of priority to ensure success.



Stage 0: Fragmented identity
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 identity and access management (IAM)
The first step to resolving the security gaps left open by these many fragmented identities is consolidating under one IAM system. This Stage 1 consolidation, via Universal Directory, SSO, and, for many businesses, the Okta Access Gateway (extending SSO to on-prem apps), 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 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 to unify their user identities. Okta Universal Directory, a cloud-based directory and meta-directory service, can serve as a single source of truth for IT organizations and act 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. With Okta Advanced Server Access, IT can extend the same access control to the server layer, bringing secure access management to the full breadth of on-premises and cloud resources IT needs to manage.

Stage 2: Contextual access
Once IT has unified IAM, the next stage in Zero Trust security is layering in contextbased 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

(i.e. do we recognize the device; what is it's security posture), location (i.e., have we seen this use here before), and network (i.e., are they in a known corporate network; are they trying to hide their IP address), 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 high risk attempts requiring users to use hardware tokens using a cryptographic handshake to securely authenticate to a service on top of a password or other second factor, while a low risk attempt may offer the option for a FIDO 2.0 or WebAuthn factor alone, no second factor or password required. 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.

Contextual Access Management

Furthermore, if a user leaves or changes roles within an organization, automated provisioning and deprovisioning ensures the user has access only to the tools needed to complete 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.

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 adds a risk engine to the contextual responses from Stage 2 that goes beyond the discrete contextual access policies set in the previous stage. Now, IT can set policies based on their overall risk tolerance and allow risk scoring, based on those contextual signals, to determine whether to prompt for a second factor. This increases security and simplifies end-user experience, allowing for frictionless access, even passwordless authentication via Okta FastPass. Additionally, dynamic workflows provide identity-focused security orchestration and response capabilities to take automatic action-like quarantining or suspending accounts with suspicious or risky activity based on the organization's risk tolerance.

In Stage 3, trust is no longer assumed: here risk is 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. Most organizations today are between Stage 0 and Stage 1 of the Zero Trust maturity curve, but as they continue to adopt the "never trust, always verify" approach to their IT security, Okta continues to support additional features that enable stronger, simpler access management. Okta also offers a free Zero Trust Assessment tool to help organizations determine where they fall on this maturity curve and offers recommendations for which projects to tackle next.

Connecting the Security Ecosystem to Achieve Zero Trust

As all of the frameworks we've discussed have outlined, there is no single technology that solves for all challenges related to a Zero Trust strategy. Okta's policy engine enforces strong authentication to applications, helping to reduce risk of breach, and we also work closely with security partner technologies to offer additional insight and capabilities for managing the security of organizations. These partnerships focus on two key areas.

Risk scoring ecosystem

Today, Okta's Risk Engine comprises ThreatInsight and Risk-Based Authentication and serves as a central component of the access plane we discussed as a part of the Zero Trust and identity reference architecture earlier in this document.

Okta ThreatInsight, which launched in 2019 as a part of Okta's Insights Platform Service, serves as our threat detection and response system, which leverages data from the Okta customer network, admins and end-users to protect customers from identity attacks. Risk-Based Authentication launched in early 2020 and takes into account risk signals on IP, user, and device state to generate a risk score that can be evaluated against policy.

Additionally, Okta is also investing in ways to further integrate third-party risk signals (i.e., WAF, bot detection, fraud, or other threat feeds), to layer identity into the evaluation of security posture to provide higher confidence in risk assessment as well as expand options for enforcement: for example, step up authentication for a high-risk login instead of denying access.

Threat signal sharing and orchestration

Through the Okta Integration Network, Okta invests in and maintains deep integrations across components of the Zero Trust ecosystem. This expansive category of integrations supports a best-of-breed, vendor-neutral approach. Examples of integrations include:

- Skyhigh and Netskope as cloud security gateways for data security
- Palo Alto Networks and Cisco for network security
- VMware, CrowdStrike, Tanium and Carbon Black for endpoint security
- Splunk, Sumo Logic and IBM QRadar for analytics
- ServiceNow and Splunk/Phantom for orchestration

Our Spectra Alliance partnership with Crowdstrike, Netskope and Proofpoint provides a strategy and pre-integrated solutions for a comprehensive, best-of-breed approach to zero trust.

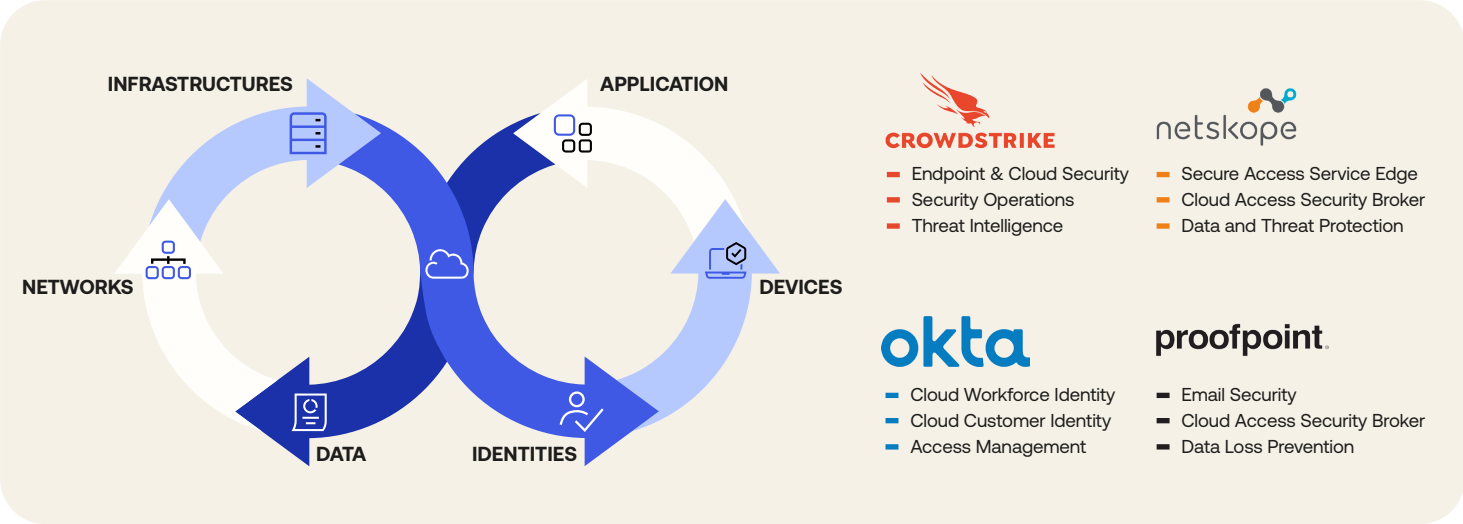


Figure: Secutiry coalition overview of Okta, CrowdStrike, Netskope and Proofpoint

In this example, organizations can leverage this joint solution to boost security in a few ways:

- Okta establishes Zero Trust to securely connect the right people to the right technologies for remote and on-premises teams, enabled by intuitive single signon and powered by adaptive multi-factor authentication.
- CrowdStrike protects all endpoints that access the enterprise, providing advanced threat hunting, next-generation antivirus protection, and tools for proactive incident response.
- Netskope provides web, cloud, and data-centric security to protect enterprise assets anywhere, and delivers contextual understanding that helps secure proprietary information everywhere.
- Proofpoint protects against today's complex people-based attacks, defending against phishing, malware, and other workforce attacks with deep visibility and behavioral training.

Case Study: GitLab Blazes an All-Remote, Open-Source Trail. Okta Helps Them Add Zero Trust to the List

GitLab makes collaboration software for the software development life cycle, and GitLab teams eat their own dogfood—building and developing the same online collaboration software that the company uses internally. Naturally, it is designed to allow people to work together asynchronously, from anywhere.

Since the company's inception, team members have been iterating and documenting all of its remote work processes in an online handbook which, like GitLab's core software, is an open-source project. While co-founder and CEO Sid Sijbrandij initially tried to get people to commute to a physical office space, he soon gave up the effort because it simply didn't add value.

Today, GitLab is scaling that all-remote model at an incredible rate, onboarding nearly 1,000 new employees in the past year. In the time of COVID-19, the company provides an exceptional example for other organizations to follow.

Can open-source embrace Zero Trust?
When Mark Loveless started as a senior security engineer at GitLab in 2019, he wasn't sure that striking a balance between open-source and Zero Trust was a realistic goal. Truthfully, he says, "I was horrified by this prospect." He was nevertheless inspired by the GitLab culture and its mission to "change all creative work from read-only to read-write"—building an inclusive and progressive world where "everyone can contribute."

GitLab is a unique company with a unique set of Zero Trust realities. "Google's BeyondCorp model was intended for somebody else, mainly Google," he says. "Not for us. We need something more open and flexible."

The company's rapid growth has made lifecycle management processes a big focus. Before, says Loveless, "we were kind of roughing it." Onboarding and offboarding were manual processes—"an absolute, massive time sink." When people left the company, deprovisioning got done with a hope and a prayer that critical access points weren't left open to attack.

GitLab's exponential growth adds to the challenge, and the company has an IPO scheduled for November 2020, which increases compliance and auditing requirements. "These are huge issues for us to overcome," he says.

GitLab also has asset management challenges because for the first several years of operation, everyone at the company used their own devices. "The company started buying employee laptops maybe two-and-a-half years ago," says Loveless.

For their Zero Trust initiative, the GitLab team is focusing on user and device identification, as well as on classifying data so that the team can create and enforce access control policies across systems. They're also looking to make sure all data in transit is encrypted, and they want to see robust logging data from all their systems, pulled together in one place.

Simplifying identity for users and admins

In eight months, Okta helped the GitLab team transform the way everyone at the company accesses their work. With Okta single sign-on and Okta adaptive multifactor authentication, the team standardized the access and authentication process and dramatically simplified IAM.

In the process, they reduced the IT friction the company was experiencing, so business leaders could adopt new technologies easily without adding risk. GitLab instituted an "MFA by default" policy and quickly achieved universal adoption. They enabled Okta ThreatInsights and Risk-Based Authentication, adding more authentication steps for high-risk applications.

The team also streamlined onboarding and offboarding at GitLab with Okta Lifecycle Management. When Loveless started at the company in February 2019, it took three weeks for him to gain access to all the applications he needed to get work done. Today, the company's human resources software, BambooHR, is tightly integrated with Okta. Provisioning actions begin the moment an HR team member makes changes in BambooHR.

> "Okta took the account creation process of onboarding from three weeks down to a minute. A new user is created in BambooHR. That profile information is immediately exported into Okta and from there we create accounts in all these other systems. It's pretty much all automated.
>
> Mark Loveless, Senior Security Engineer, GitLab

The same automation allows the team to remove access completely and automatically when someone moves on from GitLab. “It’s absolutely phenomenal,” says Loveless. “Lifecycle automation was a huge success story for us.”

A flexible Zero Trust foundation

To address these challenges, Loveless and team are reducing each problem to manageable chunks. They turned to Okta because they saw the opportunity to implement a centralized tool for managing identity—one they could connect easily to their growing portfolio of SaaS applications.

Okta provided a way for GitLab to proceed incrementally, while offering a solid foundation for a broad Zero Trust strategy. “Without a product like Okta, you really can’t achieve that model,” says Wise. “The fact that you get telemetry—better understanding of who’s logging in, where they’re logging in from, what operating system they’re using—those things are important whether you’re remote, or not.”

Okta’s flexibility was huge for GitLab. Because team members were so used to logging in from their personal devices, it was important to offer an array of authentication mechanisms.

“We had people who said, ‘What is this Okta Verify app? I don’t want to load a work app on my personal phone,’” says Loveless. “It was fine because we could offer them U2F (FIDO Universal 2nd Factor), YubiKey, or TOTP (Time-based One-Time Password). Having a product that supported all of that played a big part in addressing the concerns that people had.”

Leading with the user experience

In true GitLab style, the team began their Okta deployment by offering an open beta in April 2019, inviting staff members to opt in and gathering their feedback as the program progressed.

“The beta helped us engage people and get buy-in,” says Loveless. By May, the team was ready to move to an initial live deployment. They started with non-critical apps but included GitLab.com. “We were building up trust with users and also our own trust in Okta,” he says.

Critical app deployment began in July, and the team’s overcommunication habit was an important success factor. They had set up a dedicated Slack

channel during the beta, and that feedback and constant line of communication was critical for letting people know which apps were moving to Okta, and when.

To get universal buy-in, Loveless says it was important to sell the user experience benefits first. “Coming in and saying, ‘Hey, the security team wants you to do this security stuff because of security,’ wasn’t a good way to get users to jump on board,” he says. “We made it as transparent as possible. We were up-front about how everything worked and what we were trying to do, but we focused on the user experience,” says Loveless.

Getting into good compliance shape

Loveless says compliance reporting has also been “dramatically simplified,” paving the way for GitLab to become a public company. “Some of the auditing went from weeks to hours, simply because you can get to everything quickly and export it out,” he says.

Using Okta Universal Directory, the team was also able to eliminate shared accounts. “We’re grateful that we can put policies in place, create groups that they apply to, and grant access,” says Loveless.

GitLab has also used Okta to standardize its password policies, simplifying compliance with various data privacy laws around the world. Rather than having different standards for users in different locations, the team simply instituted one high set of standards that complies with all global privacy laws and pushed it out across the company.

Extending least-privilege access to infrastructure

As successes piled up, the security team’s case for Okta grew across GitLab and Okta became an integral part of the GitLab culture.

“The tipping point came when application owners started hunting us down,” says Loveless. “They’d hear from their co-workers, ‘Hey, if you put your app in Okta, you don’t have to create all the accounts anymore.’”

As a result, the security team has successfully cataloged its technology stack and put rules in place for application adoption. “Okta is part of our enterprise architecture initiative going forward,” says Wise. “If an application

doesn't adhere to Okta standards, it would have to be an unbelievable product, meeting a unique business need, for us to move forward with it."

Business champions appeared from across GitLab. "Our infrastructure team had a project coming up that would involve creating a lot of accounts," says Loveless. "They said, 'Hey, we've been using Okta for everything else. Could we use it for SSH access?'"

The team started a month-long pilot with Okta Advanced Server Access (ASA) and cut it short after two weeks because they didn't need to wait for full implementation. "Everyone was like, 'Oh, this'll work. We're fine,'" says Loveless. "It's a wonderful solution for creating accounts—wham-o!—just like that."

The GitLab team prefers Okta ASA as its method of securing SSH access because of the ability to scale across their elastic infrastructure fleets and automate account life cycles and policies. Whenever new infrastructure gets spun up, new accounts appear nearly instantaneously. Whenever a new user joins the team, they gain automated access in minutes. ASA also allows GitLab's DevOps-centric organization to move fast without breaking things.

Building on frictionless authentication

The GitLab security team is currently evaluating endpoint management solutions, including Okta device trust. "We're getting to the point where we can control those assets better," says Wise. They're also looking at Okta Workflows, to achieve the next level of lifecycle efficiencies.

As they proceed, the team is moving toward centralizing all user and group profiles in Universal Directory. "We've never had a server farm where we run Microsoft Active Directory or LDAP," says Peter Kaldis, IT manager at GitLab. "More and more, Okta is our directory for everything."

With that project complete, Loveless says the team will be able to create and enforce granular security policies and meet customer compliance requirements even more easily.

He also dreams of building a completely passwordless environment for GitLab. "If I had a career goal, it would be to end the password," he says. "The

fact that we have a second factor is because the first factor is insecure, so why have the first factor?"

Between GitLab's cutting-edge DNA and Okta's identity management expertise, Loveless has more hope than ever of achieving that goal. "It could happen in my lifetime," he says.

When it comes to more immediate achievements, Okta has already met one overriding criteria: "In our security department, we leave things better for end users than when we started," says Loveless. "Any solution needs to make things easier. If it's very hard or extremely complex, then we look for a better solution."

With Okta, the team now has frictionless authentication that users don't have to think about. "It's like muscle memory," he says. "When they get out of their car, they automatically lock the door. That's how we want the identity process to work here."

What's Next with Okta and Zero Trust

Identity's role in a Zero Trust context is all about ensuring the right people get the right level of access to the right services in the right context—and with the least amount of friction. To achieve this, we've explored how organizations can leverage identity solutions to secure access to their cloud and on-prem applications, APIs, and infrastructure resources, and also walked through the roadmap to deploying these tools in your organization.

A lot of work has gone into determining the likelihood a person is who they say they are when they attempt to access a service (and whether they should have access to the app, API, or infrastructure they're requesting), but the next question is: What if their risk profile changes after the initial authentication? While that initial decision is still critical, the next step is asking, "How can we recheck trust throughout a session's lifecycle, and then do something about it if things change?"

Productivity and Security through Zero Trust

The future of Okta and Zero Trust

While protections at the authentication layer—such as MFA, device fingerprinting, location checks, etc.—are valuable at the time of authentication, it's also important to have frequent checks after the initial authentication. In a cloud and mobilecentric world, most people access both corporate and personal apps from a variety of different devices. And login sessions across apps can often last for hours, days, or even weeks (especially in the case of

native mobile applications). When your device is stolen, or you log into an app on a shared computer, the initial MFA prompt becomes meaningless if your app session remains active. A bad actor could open up the app and easily access your data.

This is why Okta is building toward continuous authentication, to help solve this problem by sharing more risk signals between the identity provider and the service provider. If a change is detected, your identity provider should be able to take an action, such as prompting for re-authentication or ending the session.

Today, Okta has laid the foundation to provide continuous visibility into multiple contextual aspects in order to establish and adapt trust controls for application-level access. We are focusing on these pillars in areas of on-going investment:

- Achieving visibility into device posture through Okta Devices to enhance our initial and continuous security posture evaluation.
- Building Okta Risk Engine into a signal hub for identity security posture for each end user, ingesting signals from a best-of-breed network of ecosystem partners and leveraging data to build machine learning models.
- Passwordless authentication into any resource, from any device with Okta FastPass.
- Orchestration and flexible enforcement through Okta Hooks and Workflows, onprem apps via Okta Access Gateway and infrastructure access through Advanced Server Access.

None of this will happen overnight, but we believe there's tremendous value in developing an industry-wide solution to meet the rising threats of our digital world. What's clear is that to be successful, it will take collaboration across the entire service provider and security ecosystem, including network, endpoint, application, data security, and identity, as well as development and runtime security vendors.

Conclusion and Resources

As the most common aggregation point through which enterprises interact with their customers, partners, and employees, identity platforms must take the lead in pushing security boundaries. Okta continues to proactively invest in our own products to meet today's security challenges and accelerate organizations' journeys from the real-time, contextual-based access decisions of today, towards a future of true continuous access and automated Zero Trust remediations.

There's no silver bullet for Zero Trust. But starting with identity as the foundation positions organizations well to begin on this path. For more information about how Okta is supporting the next frontier of Zero Trust security, visit Okta.com/Zero-Trust.

Additional Resources

- Zero Trust Assessment Tool
- 2021 State of Zero Trust Report
- Spectra Alliance

References

Kindervag, Forrester Research: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, 2010

Ward, Byers, Google, BeyondCorp: A New Approach to Enterprise Security, 2014

Cunningham, Forrester, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem, 2018

Whitepaper

Getting Started with Zero Trust Access Management

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871