Whitepaper

Enabling Zero Trust through the Okta Security Identity Commitment

Contents

Executive Summary

The term “Zero Trust” was first coined in 2010 by Forrester researcher John Kindervag to conveniently encapsulate the growing need for a “never trust, always verify” security ideal.

This security paradigm gained a major boost in May 2021, with Executive Order (EO) 14028 “Improving the Nation’s Cybersecurity” — which pushed United States government agencies to adopt Zero Trust cybersecurity principles and adjust their network architectures accordingly.

In recent years, Zero Trust has progressed rapidly from cool philosophy, to stretch goal, to everyday business reality — with Okta’s The State of Zero Trust Security 2023 revealing that:

- 61% of all organizations now have a defined Zero Trust security initiative in place
- 35% plan to implement one within the next 18 months
- 91% of respondents said that Identity is important to their Zero Trust strategy

Identity and Access Management (IAM) is an important element of any security strategy, and Zero Trust is no exception. In fact, “Identity” is the first of five key pillars within the Zero Trust Maturity Model (ZTMM) developed by the Cybersecurity and Infrastructure Security Agency (CISA) to assist agencies as they implement zero trust architectures. The Identity subsection of the model specifically notes that:

- Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.
- Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities.
- Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

As part of the Okta Secure Identity Commitment (OSIC), we have recently introduced a number of features that support Identity-powered Zero Trust initiatives, including:

- ID Token Expiration
- Enable MFA for the Admin Console
- Govern Okta Admin Roles
- Enforce an Allow-listed Network Zone for APIs
- Allow admins to detect and block requests from anonymizing services
- Bot Detection v4
- Enforce ASN binding for Auth0 admin sessions

The features listed above don't constitute an exhaustive list, but instead are included to highlight particular functionality that may not be as well known as the foundational featuresets within Okta's workforce and customer Identity solutions.

Introduction

In recent years, two trends have driven dramatic change in how Identity is regarded and, by extension, in the demand for Identity solutions:

1. **Identity is now the primary enterprise security entry point** for all workforce and consumer applications.
2. **The volume and complexity of cyber attacks has grown**, with a range of threat actors — including ransomware groups, nation-state actors, and malicious insiders — developing advanced tactics, techniques, and procedures (TTPs) to bypass defenses and evade detection.

As a world-leading independent Identity company, Okta is at the forefront of dealing with Identity attacks. Accordingly, in February 2024, we launched the Okta Secure Identity Commitment to:

Provide market-leading secure Identity products and services

Harden our corporate infrastructure

Champion customer best practices to help ensure they are best protected

Elevate our industry to be more protected from Identity attacks

The benefits of an Identity-powered Zero Trust strategy aren't limited to improved security operations (SecOps). Organizations embracing this paradigm are able to leverage Identity management across their entire IT infrastructure to:

- Enable new operational efficiencies
- Deliver better workforce and customer experiences
- Support compliance objectives

Identity and Zero Trust

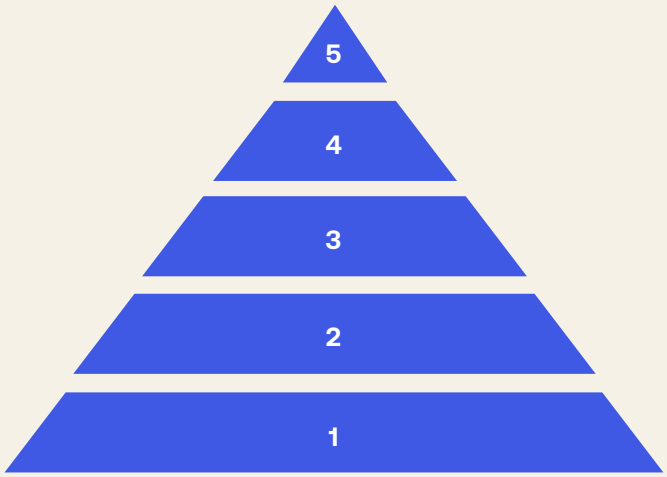
No security strategy — whether pertaining to members of the workforce or to customer-facing resources — is complete without applicable safeguards against Identity threats.

In short, the more identities you manage, the broader your risk landscape, and an Identity-powered strategy that gives the right people the right level of access to the right resources at the right time should be the end goal.

Traditionally, Identity and Access Management (IAM) fell under the purview of IT teams, but today — in response to the significant role Identity plays in managing cyber threats — that control has largely shifted to the security team.

Because every organization is on its own path (see figure, below), there's no silver bullet when it comes to achieving a Zero Trust security architecture — but Identity remains at the heart of any successful adoption.

The Identity-powered Zero Trust journey



5. Evolved Model

Fully embracing the concept of least privileged access.

4. Elevated Model

Leveraging Identity as a central control point across security.

3. Maturing Model

Mitigating risk and optimizing resources.

2. Emerging Model

Balancing user experience and security.

1. Traditional Model

Incorporating identity into the security stack.

In this document, we want to share how some of the features recently introduced under the Okta Secure Identity Commitment support Identity-powered Zero Trust strategies. The features presented herein don't constitute an exhaustive list, but instead are selected to highlight particular functionality that may not be as well known as the foundational featureset.

To place the features in an illustrative context, we've grouped them under four Zero Trust themes from the NIST Cybersecurity Framework 2.0:

1. Periodically re-authenticate users, services, and hardware based on risk [PR.AA-03]
2. Restrict access and privileges to the minimum necessary [PR.AA-05]
3. Restrict network access to each resource to the minimum necessary [PR.IR-01]
4. Monitor network communications to identify changes in security postures [DE.CM-01]

Periodically re-authenticate users, services, and hardware based on risk

FUNCTION - PROTECT (PR)

Safeguards to manage the organization's cybersecurity risks are used

Category Identity Management, Authentication, and Access Control	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
Subcategory PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties Ex: Restrict access and privileges to the minimum necessary (e.g., zero trust architecture)

Source: NIST Cybersecurity Framework

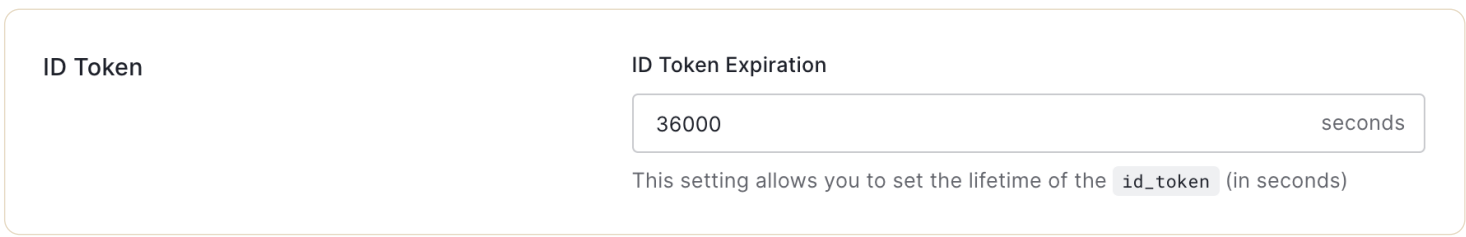
ID Token Expiration

Applies to: Customer Identity Cloud

ID tokens are used in token-based authentication to cache user profile information and provide it to a client application, thereby providing better performance and experience. The application receives an ID token after a user successfully authenticates, then consumes the ID token and extracts user information from it, which it can then use to personalize the user's experience.

Under Application Settings, the ID Token Expiration value allows you to configure the lifetime of an ID token, balancing security (shorter lifetime) with convenience (longer lifetime). The default value of the ID token is 36,000 seconds — equivalent to 10 hours.

Learn more



Restrict access and privileges to the minimum necessary

FUNCTION - PROTECT (PR)

Safeguards to manage the organization's cybersecurity risks are used

Category Identity Management, Authentication, and Access Control	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
Subcategory PR.AA-03	Users, services, and hardware are authenticated Ex: Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures)

Source: NIST Cybersecurity Framework

Enable MFA for the Admin Console

Applies to: Customer Identity Cloud & Workforce Identity Cloud

Multi-factor authentication (MFA) with strong secondary factors is a proven way to substantially strengthen defenses against account takeover attempts, whether such attempts make use of known (i.e., stolen) credentials or brute force techniques.

Within the Customer Identity Cloud, MFA was an optional requirement for Auth0 administrators, to avoid imposing incremental authentication friction for organizations comfortable operating without this layer of defense. In response to the evolving threat landscape, MFA is now mandatory for all admins with a username/password-based login or third-party social login.

Within the Workforce Identity Cloud, Super Admins should enable mandatory MFA for all admins who access the Okta Admin Console. After this feature is enabled, the MFA policy for the Admin Console is enabled by default. The next time an admin signs in, they're prompted to set up MFA for access to the Admin Console. Admins who haven't enrolled in MFA are prompted to enroll for the first time.

Learn more

Govern Okta Admin Roles

Applies to: Workforce Identity Cloud

As Identity-based attacks move closer to critical IAM infrastructure, standing access to sensitive administrator privileges in Okta can present a target for malicious actors.

To strengthen defenses against such attacks, Govern Okta Admin Roles empowers you to deliver zero standing privileges for Okta admins by leveraging core governance functionality within the Workforce Identity Cloud:

- **Entitlement management:** Bundle entitlements across custom and out-of-the-box admin roles. Administrators can create sets of permissions to capture necessary business processes without over-permissioning across administrator actions.
- **Access requests:** Provide access to Okta administrator roles via self-service access requests. Administrators can build admin-role-specific flows with multiple approvals and documented justifications.
- **Access certifications:** Perform ongoing reviews of existing access to administrator roles. Administrators can create recurring multi-level reviewer campaigns designed to prevent any accumulation of elevated or privileged administrator access.

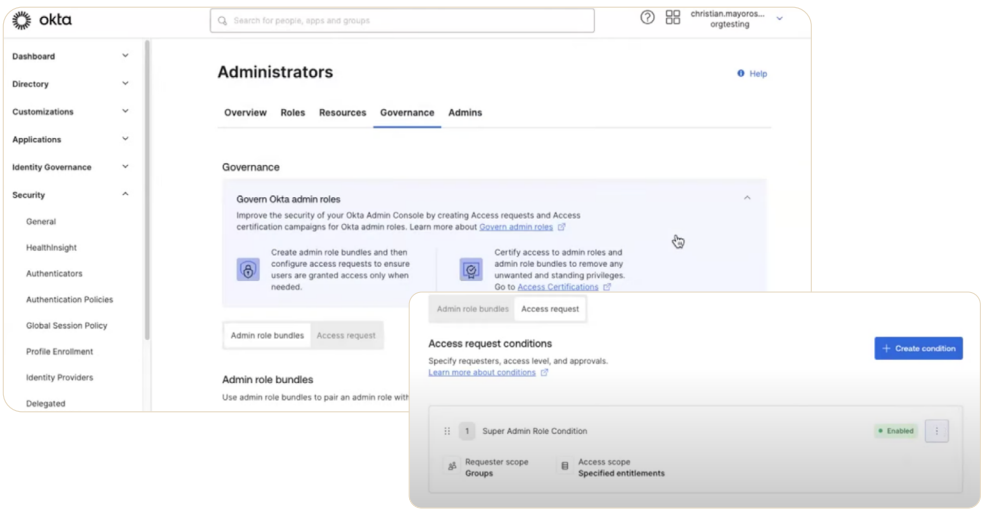
Govern Okta Admin Roles builds on custom admin roles by enabling every Workforce Identity Cloud customer to govern administrator access in privilege and time.

IT teams can ensure only select users can request the right level of admin access in Okta, and can time-bound that access for whatever task a user is accomplishing — guardrails that help organizations minimize and monitor standing privilege without impacting productivity.

Security and risk teams can review any standing administrator access through automated campaigns to give the appropriate reviewers the ability to validate any access and take action. Combining Govern Okta Admin Roles with admin role assignments reporting gives security and IT teams visibility and automated remediation capabilities through the Workforce Identity Cloud.

Learn more

Watch a demonstration



Restrict network access to each resource to the minimum necessary

FUNCTION - PROTECT (PR)

Safeguards to manage the organization's cybersecurity risks are used

Category Technology Infrastructure Resilience	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience
Subcategory PR.IR-01	Networks and environments are protected from unauthorized logical access and usage Ex: Implement zero trust architectures to restrict network access to each resource to the minimum necessary

Source: NIST Cybersecurity Framework

Enforce an Allow-listed Network Zone for APIs

Applies to: Workforce Identity Cloud

To restrict attackers and malware from stealing SSWS tokens and subsequently replaying them to gain unauthorized access, you can specify from where you allow connections to originate:

- **Any IP:** Allow connections from any IP address or network zone.
- **In any network zone defined in Okta:** Allow connections if they come from any network zone defined in your Okta org.
- **In any of the following zones:** Allow connections if they come from network zones that you specify. Enter text that matches the name of the network zone you want to select. Okta presents results that match what you enter. Select a name. Repeat this step to add more network zones.
- **Not in any network zone defined in Okta:** Allow connections if they don't come from any network zone defined in your Okta org.
- **Not in any of the following zones:** Allow connections if they don't come from network zones that you specify. Enter text that matches the name of the network zone you want to select. Okta presents results that match what you enter. Select a name. Repeat this step to add more network zones.

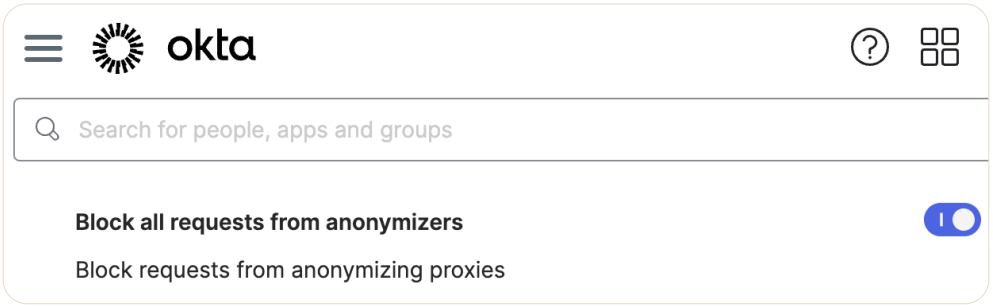
Learn more

Allow admins to detect and block requests from anonymizing services

Applies to: Workforce Identity Cloud & Customer Identity Cloud

In response to an observed increase in the frequency and scale of credential stuffing attacks — facilitated by the broad availability of residential proxy services, lists of previously stolen credentials, and scripting tools — we have empowered customers to block, prior to authentication, access requests originating from anonymizing services.

Learn more



Monitor network communications to identify changes in security postures

FUNCTION - DETECT (DE)

Possible cybersecurity attacks and compromises are found and analyzed

Category Continuous Monitoring	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
Subcategory DE.CM-01	Networks and network services are monitored to find potentially adverse events Ex: Monitor network communications to identify changes in security postures for zero trust purposes

Source: NIST Cybersecurity Framework

Bot Detection v4

Applies to: Customer Identity Cloud

Bot Detection, with Okta AI, has proven capable of filtering bots targeting authentication systems. Importantly, these defensive capabilities are achieved without introducing unnecessary user friction — by carefully training and continually tuning the AI at the heart of the Bot Detection feature, we can ensure that human users are rarely presented with a CAPTCHA, preserving seamless experiences.

Importantly, there's considerable evidence that this efficacy is a very strong deterrent, as some of our largest customers saw their 90-day average of bot traffic drop by nearly 90% after enabling this Attack Protection feature.

The latest version of our Bot Detection capabilities introduces enhancements for signup-based attacks, third-party data to improve efficiency, and edge-based component signals.

Learn more

Enforce ASN binding for Auth0 admin sessions

Applies to: Customer Identity Cloud & Workforce Identity Cloud

In response to more secure forms of authentication, adversaries are targeting session cookies as an alternative way to gain access into protected applications and environments.

Typically extracted from browsers via infostealers and other malware, or through adversary-in-the-middle attacks, session cookies are like golden tickets that allow cybercriminals to impersonate legitimate users without raising any alerts. If an attacker steals a session cookie and injects it into their browser, they can often access the same session as the legitimate user (for as long as the session remains active).

While session hijacking can be somewhat scaled, the approach is more likely to be used as part of a targeted attack against particular users (e.g., admins) in high-value organizations.

To help prevent hijacking of established sessions, Okta will automatically revoke an Okta Admin Console session if the ASN (Autonomous System Number) observed during an API or web request differs from the ASN recorded when the session was established.

Learn more (Customer Identity Cloud)

Learn more (Workforce Identity Cloud)

Within the Workforce Identity Cloud, customer administrators are also able to automatically revoke an administrative session if the IP address observed at session creation changes during an active session within the following Okta products:

- Workflows Admin
- Okta Access Requests (Inbox)
- Okta Privileged Access (OPA)
- Okta Admin Console

Conclusion

The term and concepts of Zero Trust have been circulating around the cybersecurity community for nearly 15 years, but CISA's efforts to create a Zero Trust Maturity Model, and programmatic expansion from NIST have helped bring measurable security controls into the equation.

Security professionals (and the security-minded) can now make the logical connections between these security controls and the benefits your Identity provider offers.

Okta can help

Okta's goal is to simplify the approach to Zero Trust through integration of an Identity solution across your entire technology ecosystem.

To that end, we encourage you to take our Zero Trust Assessment to get personalized recommendations on how to tackle the Zero Trust journey with Identity to secure your organization.

We also recognize that there's no silver bullet or single-vendor solution for Zero Trust, and that Identity itself is 'only' one of five key pillars within CISA's Zero Trust Maturity Model. To support expansive security initiatives, Okta integrates with solutions across your security stack, including:

Network Security

Extend SSO and authentication policies to provide secure access across your corporate network.

→ Learn more

Cloud Access Security Brokers

Use your cloud traffic and application usage patterns to improve compliance, threat protection, and data loss prevention.

→ Learn more

Unified Endpoint Management

Deliver the right access to the right user, on the right device, at the right time by combining Okta with endpoint management and security technologies.

→ Learn more

Security Analytics

Expand your view across cloud, mobile, and on-prem systems to amplify correlation and enforcement opportunities.

→ Learn more