Whitepaper

Okta brings Zero Trust Identity and access to Defense Department networks

Department of Defense (DoD) organizations understand that secure Identity and Access Management (IAM) will grow more critical as the military transitions into a more modern information enterprise.

As the National Defense Strategy makes clear, to sustain its overmatch capabilities, the military will need to rely more heavily on secure, data-driven networks; collaboration with global alliances and partners; and new technologies like smartphones and cloud computing. These and other objectives all rely on having highly secure networks, protected by robust, modern IAM capabilities.

Tellingly, a key objective outlined in the National Defense Strategy is to build "a lethal, agile, and resilient force posture and employment," which requires forces to be more adaptable, flexible, and maneuverable to account for the uncertainty that exists in the changing global strategic environment. This means that supporting digital infrastructures must also be agile, fast, and secure to keep up with dynamic force deployments.

To achieve this, Defense organizations will need to evolve their security approaches beyond the traditional "defense in depth" tactics of firewalls and castle-and-moat-style cyber security architectures. These no longer keep pace with today's sophisticated cyber threats and they lack the adaptability and agility needed for today's force projection needs.

Moreover, this disproportionate reliance on traditional "defense in depth" approaches has left the IAM component of many networks a vulnerable gateway to attack. Many companies and government agencies have fallen prey to phishing and other forms of Identity-based attacks where employees are enticed to give away legitimate credentials. This opens the door for attackers to gain access to sensitive networks through non-privileged accounts and then to move laterally to sensitive data, resulting in high-profile data breaches.

The failure to adequately secure Identities is one of the most serious security issues facing Defense agencies. Industry analyst Forrester estimates that 80 percent of security breaches involve privileged credentials, and Verizon's 2022 Data Breach Investigations Report ranks privilege misuse only behind denial of service as the most prevalent cause of breaches and incidents.

Consequently, traditional tools and approaches to IAM expose DoD organizations to greater risk. For example:

- Defense organizations rely too heavily on Common Access Cards (CACs) to authenticate users when they access networks, applications, and data. CACs do not recognize or mitigate risk associated with attributes other than Identity, such as the user's device, location, network, time of day, or other online behavior.
- It often takes too long for new recruits or employees to gain the access privileges they need to sensitive networks so they can be productive from day one. Likewise, when military personnel or other employees leave their assignments or have a change in status, there are often delays in removing or adjusting their access privileges, creating potential security threats.
- Existing protections are insufficient to counter increasingly sophisticated, state-sponsored cyberattacks from Russia, China, Iran, and North Korea, as well as from insider threats.
- Existing protections are inadequate for protecting modern and future systems that rely heavily on cloud and mobile technologies. With traditional defenses, once an endpoint is breached, anyone can roam inside the cloud network.
- Existing protections could do more to protect third-party vendors and contractors and military partners and allies.

Defense leaders are already aware of the shortcomings of "defense in depth" security approaches and are exploring other security frameworks, such as Zero Trust architectures used by many best-in-class enterprises. The baseline capability to achieve Zero Trust is Identity, Credential, and Access Management (ICAM), as noted in the DoD Enterprise ICAM Strategy, "A secure, trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who and what is on our networks at any time."

Consequently, many Defense leaders are recognizing that Identity and access have emerged as the new perimeters to be defended. To achieve the National Defense Strategy objectives of a fast, agile, and secure force projection, they will need to adopt a Zero Trust security approach to IAM.

Zero Trust and Identity management: A game changer for DoD network security

Broadly speaking, Zero Trust means that everyone — whether internal or external to DoD — is assumed to be a security threat until they prove themselves otherwise. Once they are granted access to a DoD network and data, they must continuously demonstrate they do not pose a security threat through repeated authentications.

Zero Trust doesn't provide for default trust, such as by placing total reliance on passwords or CACs. Rather, risk is assessed continuously and in real time from many perspectives: the user, the network, the application, the time of day, whether the machine is trusted, and the user's online behavior, to name a few.

When effectively done, Zero Trust directs the right amount of security at the right places at the right time to identify and mitigate risk. This capability ultimately translates into more effective and secure data sharing across DoD networks, which means more speed and agility for DoD organizations that have business operations and missions to execute.

Many DoD leaders already understand the benefits of Zero Trust principles and have identified them as critical to future network security, especially those connected to the cloud and mobile endpoints at the battlefield edge. In fact, the DoD Digital Modernization Strategy notes that "the assumption Zero Trust makes — that you are compromised — is particularly suited to cloud infrastructures."

Okta delivers a modern, Zero Trust approach for Identity management and access control

Okta's Zero Trust security strategy builds on the concept of Identity and access as the new perimeters, taking a never-trust, always-verify approach to everyone operating within a network. The key is understanding that nothing is safe; there is no safe zone because every entity is exposed to all possible threats.

Applying to both outside attackers that breached the network and malicious insiders already within, Okta's Zero Trust Reference Architecture combines and analyzes risk signals across devices, Identities, networks, geographies and resources. Everyone without exception is required to provide appropriate methods of authentication based on that risk posture and at each step of the way to access applications, servers, APIs, and machines.

That's why every Zero Trust strategy must start with the foundational elements of IAM and put trusted Identities at the core of security. In a perimeterless environment where every entity and every transaction must be protected against all threats, only Identity authorization and authentication can give organizations assurance of who is accessing the network and what exactly they're accessing.

It means taking advantage of proven capabilities, such as IAM tools, data governance, analytics, Identity-as-a-Service (IDaaS), and role based access control.

Okta's industry-leading Zero Trust Reference Architecture serves as the foundation to secure critical DoD resources from cloud to ground by delivering a comprehensive access management platform for DoD personnel, stakeholders, and partners. Further, Okta integrates closely with top security vendors across all layers of the Zero Trust stack, from endpoint security to ZTNA network protection to monitoring and automation tools. This capability means that Defense networks — whether based at a local data center or deployed in the cloud and delivered across countless mobile devices — are secure wherever and whenever they are deployed and accessed, advancing the goals of the National Defense Strategy.

The Okta Identity Cloud helps DoD organizations manage their extended enterprise by making it possible for them to:

- Embrace the secure cloud, at scale — while also extending the same strong authentication to on-prem apps.
- Reduce the complexity of managing separate password and authentication policies across on-premise and cloud resources.
- Provide a consistent and seamless access experience for end users, eliminating password fatigue and improving onboarding time.

Okta features include:

- Single sign-on (SSO) to provide a unified authentication experience while Universal Directory provides one place to manage all users, groups, and devices across on-prem and cloud resources.
- Lifecycle management to automate the control of a user Identity from creation to deletion, ensuring the right people have access to the right resources, and that accounts are automatically deleted when the user leaves.
- Adaptive multi-factor authentication to mitigate the risk of Identity attacks (such as phishing), and universal policies can be applied across cloud apps as well as gateways to on-prem resources such as VPNs, Application Delivery Controllers, or resources leveraging LDAP.
- Native integration with any on-premises app that uses SAML or OAuth authentication, and can provide an on-prem RADIUS agent for any application that uses RADIUS as its authentication mechanism. Okta can also support cloud-based LDAP authentication, minimizing or completely removing the need for on-prem LDAP servers.
- DoD Impact Level 4 conditional Provisional Authorization, FedRAMP High Authorization to Operate (ATO), and FedRAMP Moderate ATO. Okta is also committed to continuing investments in this area as well. In addition, Okta is compliant with FIPS, HIPAA, and other government certifications.
- Ability to work with PIV/CAC credentials.

- A SaaS platform, so it is quick and easy to improve or fix capabilities and inject new functionality.
- More than 7,000 pre-built integrations to applications and infrastructure providers, including tight integrations with many top SaaS platforms used in government, including ServiceNow, SailPoint, Netskope, and Office 365.

Case study: CDO Technologies

Tasked with advancing the privacy of 5 million U.S. Air Force users, CDO Technologies relied on Okta to raise the Air Force's security position by transitioning its entire Human Resources (A1) data center to the cloud, including 33 systems and 200 applications. Due to extensive experience, industry expertise, and proven capability, CDO chose Okta to assist with security, user experience, and value delivering the following benefits:

- Centralized IAM across 33 systems and 200 applications
- The ability to tailor information access according to user location
- Streamlined auditing and reporting tools
- Improved user experience anywhere in the world with simple, streamlined multi-factor authentication (MFA)
- Robust tools for analyzing user behavior across a broad portfolio and uncovering anomalies as they occur
- The ability to hand over the administration of individual applications to owners throughout the organization

Read the full case study:
www.okta.com/customers/cdo-technologies

Why Okta

Okta is a recognized industry leader in Identity and Access Management (IAM). Gartner has recognized Okta as a Leader in the "Magic Quadrant for Access Management, November 2022" for the sixth year in a row. Okta is also placed highest on the "Ability to Execute" axis for the second year in a row.

Conclusion

At Okta, we apply a deep and thoughtful understanding of Zero Trust principles to the complex challenge of Identity and Access Management. With our Okta Identity Cloud, we deliver an industry leading, highly scalable solution that dramatically strengthens and streamlines security for Defense Department organizations as they modernize their digital enterprises.

About Okta
The Okta Identity Cloud is an independent and neutral platform that securely connects and enables government and defense agencies to achieve simple and secure access from any device at any time, allowing its workforce and citizens to accelerate their missions with modern, Zero Trust Identity. Okta holds FedRAMP ATO and has been named a leader in both the Gartner Magic Quadrant for Access Management and Forrester Wave Identity-As-A-Service (IDaaS) for Enterprise reports. Many agencies are using Okta to fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work. For more information visit okta.com/dod.