Integrated Security for Zero Trust

Bring simplicity, speed, and advanced protection to your cloud environments with a unified solution from AWS, Okta, and Palo Alto Networks

Navigating the complexity of Zero Trust adoption

Zero Trust security has become crucial for protecting distributed workforces and resources. However, in their quest to implement the framework, organizations often struggle with complicated tool integration, fragmented implementation approaches, and cross-functional alignment. These obstacles make developing a holistic, streamlined security strategy difficult.

16%

of early Zero Trust adopters who implemented without a broader strategy reported achieving all their expected outcomes.

A scalable, holistic security solution from three industry leaders

By combining the cloud scalability of Amazon Web Services (AWS), the power of identity from Okta, and next-generation security from Palo Alto Networks, organizations can simplify Zero Trust implementation across diverse environments. Using a suite of robust integrations, organizations can more easily implement Zero Trust principles to effectively manage cloud infrastructure, user identities, and network security—while also improving productivity and operational agility.

- ✓ Secure access and support workforce mobility for users everywhere, from managed and unmanaged devices to workloads across environments.
- ✓ Gain cost efficiency, eliminate tool sprawl, and reduce manual effort by consolidating tools and automating workflows.
- ✓ Facilitate compliance with flexible configuration, data retention, and vulnerability alerts using solutions providers that hold a long list of industry and government certifications and authorizations.

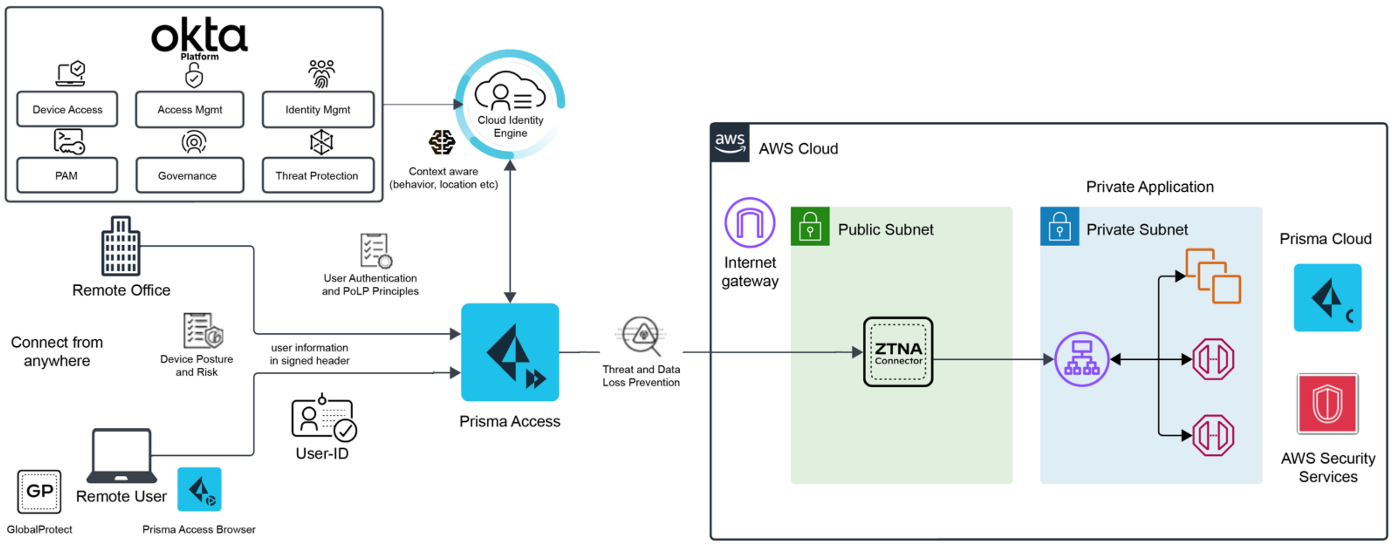
Comprehensive protection across your entire digital landscape

Secure. Simple. Scalable.

Unify protection across identity, devices, networks, data, applications, and workloads with cloud-native security that leverages automation, AI-driven insights, and user-friendly tools.

- Deploy quickly, scale seamlessly, and centralize data across environments with **AWS**.
- Implement an identity-first approach using fine-grained access controls and workload-to-workload authentication with **Okta**.
- Segment networks, monitor continuously, and prevent breaches with **Palo Alto Networks**.

Zero Trust Network Access for Private Applications



- **Continuous monitoring**
- **Multi-factor authentication (MFA)**
- **Real-time threat detection**
- **Least privilege access**
- **Microsegmentation**

Enforce Zero Trust to safeguard data with AWS as the secure cloud where private applications reside, Okta Adaptive MFA for identity verification, and Palo Alto Networks Prisma Access and Prisma Access Browser for securing identities, access, and managed and unmanaged devices. Together, these prevent implicit trust, enforce least-privilege access, and continuously monitor your data.

Unify visibility to detect threats and correlate identity events with cloud activity across environments by aggregating security logs from AWS services, identity data from Okta, and security insights from Palo Alto Network into Amazon Security Lake for centralized analysis.

Assess user risk post-authentication and automate responses by integrating Okta’s Identity Threat Protection with Palo Alto Networks through the Shared Signals Framework (SSF). AWS enforces these security policies to ensure only trusted users and devices access sensitive workloads.

Secure the continuous integration and continuous deployment (CI/CD) pipeline on AWS by applying strong identity verification and least-privilege access control. Okta manages developer authentication through single sign-on (SSO) and MFA, while Palo Alto Networks provides continuous security monitoring and policy enforcement, keeping access to AWS resources compliant and authorized throughout the development lifecycle.

Take the easiest path to Zero Trust with AWS, Okta, and Palo Alto Networks

Ready to adopt Zero Trust, without the headache? Get started by visiting Okta and Palo Alto Networks in AWS Marketplace.