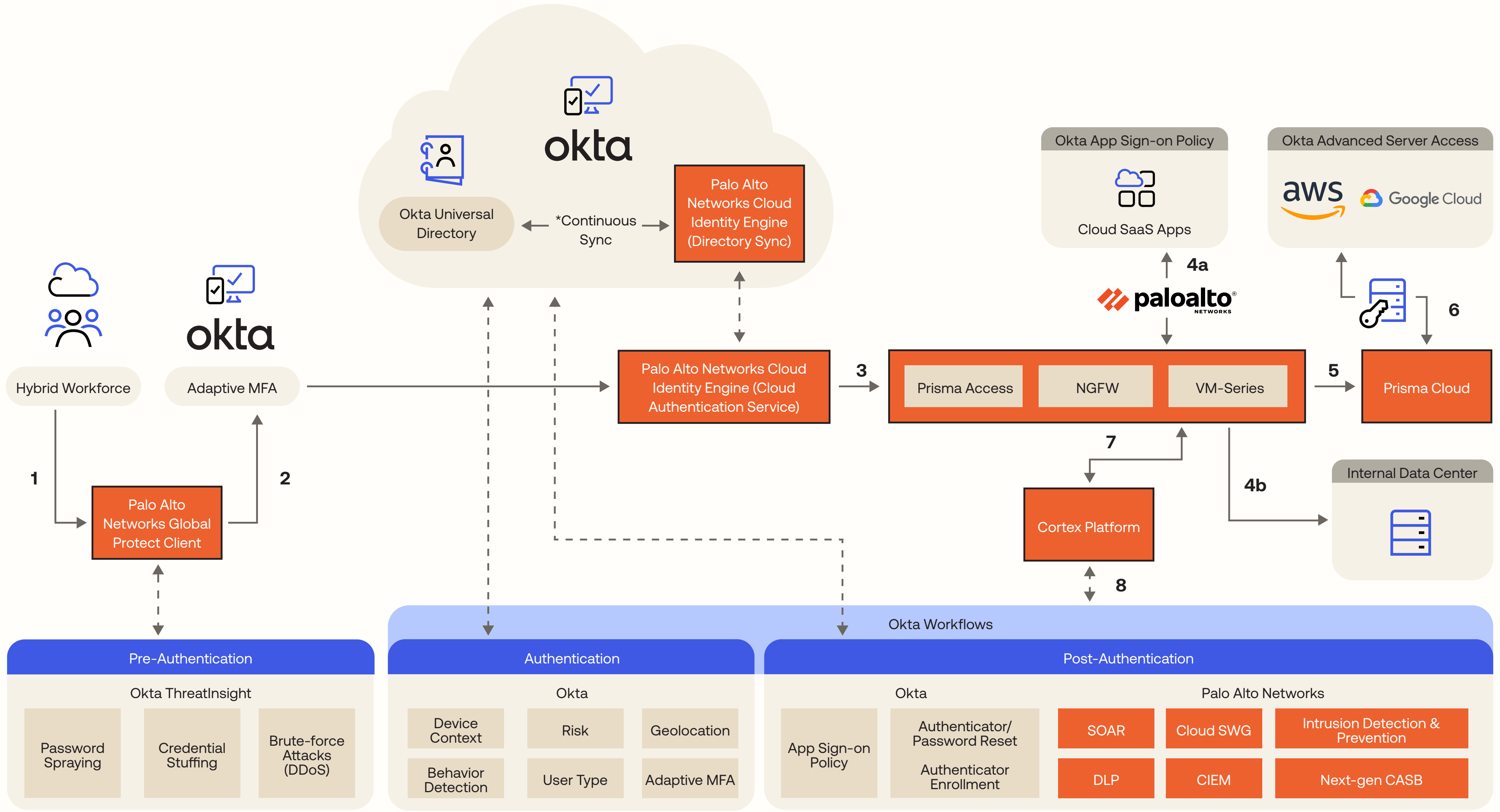

okta

Okta Universal Directory

*Continuous Sync

Palo Alto Networks Cloud Identity Engine (Directory Sync)

Hybrid Workforce

okta

Adaptive MFA

1

2

Palo Alto Networks Global Protect Client

Palo Alto Networks Cloud Identity Engine (Cloud Authentication Service)

3

Okta App Sign-on Policy

Cloud SaaS Apps

4a

paloalto NETWORKS

Okta Advanced Server Access

aws

Google Cloud

6

Prisma Access

NGFW

VM-Series

5

Prisma Cloud

7

4b

Internal Data Center

Cortex Platform

8

Okta Workflows

Pre-Authentication

Okta ThreatInsight

Password Spraying

Credential Stuffing

Brute-force Attacks (DDoS)

Authentication

Okta

Device Context

Risk

Geolocation

Behavior Detection

User Type

Adaptive MFA

Post-Authentication

Okta

App Sign-on Policy

Authenticator/ Password Reset

Authenticator Enrollment

Palo Alto Networks

SOAR

Cloud SWG

Intrusion Detection & Prevention

DLP

CIEM

Next-gen CASB

## Okta & Palo Alto Networks ZTNA 2.0

**Palo Alto Networks Cloud Identity Engine (CIE) Directory Sync integration with Okta Universal Directory (UD) allows admins to create security policies based on Okta users and groups instead of IP addresses.**

***Okta UD continuously syncs Okta users and groups with CIE as a cloud-based directory.**

1. Users are required to first login through Palo Alto Networks GlobalProtect client before being provided network/internet access (ex. Always On Configuration).
2. Users are redirected to sign-in and perform Adaptive MFA through Okta. ThreatInsight provides a pre-authentication layer of security by blocking known malicious IP addresses at the edge layer.
3. Palo Alto Networks Cloud Authentication Services provides user authentication; after the user authenticates, the Palo Alto Networks solutions map the users and applies appropriate security policy.
4. Traffic inspection and SSL decryption of all user traffic is performed by Prisma Access, a physical next-generation firewall, or virtual VM-series to both cloud SaaS (4a) and internal on-prem apps (4b).
5. Prisma Cloud IAM Security is able to manage and provision access to AWS based on Okta roles and permissions while identifying risky relationships.
6. Okta Advanced Server Access (ASA) extends granular access controls to provide a Privileged Access Management (PAM) solution to Linux and Windows servers in AWS, GCP, and on-prem.
7. Palo Alto Networks Cortex (XDR, XSOAR) utilizes AI to aggregate data from multiple sources providing SOC teams with continuous device and trust verification on endpoints throughout an organization while automating incident response.
8. Okta Workflows provides an additional layer of low-code/no-code automation with out-of-the-box connectors and templates with security tools (Cortex) utilizing API calls.

okta | paloalto NETWORKS

# Security Integrations Playbook

## 1 Hybrid Workforce

Okta integrates directly with Prisma Access allowing your hybrid workforce to access apps securely from anywhere.

### How it works

- Work is an activity, not a location. Okta's deep integration with Palo Alto Networks allows your hybrid workforce to securely access their applications regardless of their locale with a Zero Trust and least privilege framework.
- With Okta, enforce Adaptive Multi-Factor Authentication (MFA) and Single Sign-On (SSO) for Prisma Access, Prisma Cloud, Panorama, and Captive Portal for some or all users based on granular security controls:
  - User Type (admin, group membership, etc.)
  - Device State (managed, unmanaged, jailbroken)
  - Device Platform (iOS, Android, macOS, Windows)
  - User's IP (geolocation, network zone, single/multiple IP addresses)
  - Risk (any, low, medium, high)
  - Behavior Detection (new city, country, device, velocity - impossible travel)
- Okta ThreatInsight provides an additional layer of security to Prisma Access by detecting malicious activity even before your end users authenticate through GlobalProtect preventing credential-based attacks such as:
  - Password spraying
  - Credential stuffing
  - Brute-force cryptographic attacks

### Customer stories

- Large Financial institution utilized both Okta and Palo Alto Networks platforms to modernize and implement Zero Trust Network Architecture (ZTNA) within their workforce environment.
  - 600+ legacy applications were successfully migrated to Okta while adhering to modern authentication protocols
  - Prisma Access protected the hybrid workforce through inline traffic inspection while Okta provided granular Adaptive MFA policies for SaaS applications
- National Healthcare provider utilized phishing resistant and hardware protected FIDO2 YubiKeys within their organization to provide as-needed access to their most sensitive applications with Okta's Adaptive MFA, Prisma Access, and Panorama.
- Large Energy organization reduced complexity within their environment by eliminating security point products, decreasing on-prem hardware by 50% by deploying Prisma Access with Okta SSO and Adaptive MFA.
- GlobalProtect is the #1 most utilized secure remote access solution within the Okta Integration Network (OIN).
  - Organizations save time, resources, and accelerate security initiatives by leveraging Okta's pre-built integrations with Palo Alto Networks
- See Okta & Palo Alto Networks out-of-the-box OIN offerings here:

## 2 Zero Trust & SecOps

Okta enriches Palo Alto Networks Cloud Identity Engine and Cortex, providing continuous trust and device verification with SecOps automation.

### How it works

- Okta Universal Directory (UD) is a metadirectory where user attributes and schema information (assigned apps, groups, devices) are aggregated and stored regardless of the user's source directory location (ex. Workday, Active Directory, LDAP, csv).
  - Okta UD integrates directly with Palo Alto Networks Cloud Identity Engine (CIE) where security policies within Prisma Access and Next-Generation Firewalls (NGFW) can be created utilizing Okta user and group data vs IP addresses
  - CIE continuously syncs with Okta UD (via read-only access) providing a single-pane-of-glass for identity ensuring your user attributes and application access policies are accurate and up to date
- Palo Alto Networks Cortex XDR integrates directly with Okta by ingesting and analyzing authentication data, providing your organization with increased visibility into shadow IT and user-based attacks. This integration provides security teams the ability to:
  - Detect compromised accounts and malicious insider activity on privileged accounts that may have higher levels of access throughout the network
  - Enhance threat hunting during active investigations by utilizing Okta system logs within Cortex XDR queries to identify lateral movement by bad actors
  - Terminate processes, quarantine suspicious files, isolate endpoints, and update IP addresses/domains to block lists
- Palo Alto Networks Cortex XSOAR integration with Okta's API-first architecture allows your security teams to automate incident response, run playbooks, and even proactively disable user accounts within Okta if a credible threat is found.
- Okta Workflows provides an additional layer of security and automation to SecOps teams by replacing scripts/code with powerful identity-based logic and connections.
  - Immediately prompt suspicious users for step-up authentication
  - Suspend suspicious accounts during an active investigation
  - Log and share lifecycle events
  - Send, receive, and authorize API calls to 3rd party SaaS API endpoints
- Workflows Use Case: Executive Locked Out
  - User is a member of "Executive" group within Okta UD
  - User status is changed to "Locked Out" due to numerous failed login attempts defined by Okta login policy
  - Workflows is triggered and creates a ServiceNow ticket through API integration
  - Slack message is sent to SecOps admin and/or channel
- See Okta Workflows and Palo Alto Networks Cortex XSOAR templates and playbooks here:

## 3 AWS & GCP Security

Okta's integration with Prisma Cloud provides visibility, governance, and control to both AWS and GCP by aggregating Okta user activity across platforms.

### How it works

- Prisma Cloud IAM Security is a Cloud Infrastructure Entitlement Management (CIEM) platform tool that is able to:
  - Calculate effective permissions to assigned users, workloads, and data within multiple cloud environments (ex. AWS, GCP, etc.)
  - Monitor and detect excessive and unused privileges with out-of-the-box security best practices and policies
  - Automatically adjust IAM permissions to reduce security risks
  - Identify rules and actions needed to achieve least privilege entitlements
- For AWS, Prisma Cloud IAM Security integrates with Okta by ingesting Single Sign-On (SSO) data that is utilized to view and map entitlements within Okta to:
  - AWS IAM roles
  - AWS IAM policies
  - AWS IAM groups
  - AWS IAM resource based policies
  - AWS service control policies
- See how Okta protects AWS environments here:
- Okta Advanced Server Access (ASA) provides an additional layer of security to both AWS Elastic Cloud Compute (EC2) and GCP Compute Engine instances. ASA extends the power of Okta's identity and access controls to provide:
  - Just-in-Time (JIT) passwordless authentication to Linux and Windows servers
  - End-to-end lifecycle automation of servers, user, and group accounts
  - Fine-grained role-based access controls (RBAC) and command-level permissions
- Okta ASA provides a seamless and secure Privileged Access Management (PAM) solution to admin and DevOps teams regardless of where their Linux and Windows servers are hosted (on-premise, cloud).
  - Centralized directory service for users and groups
  - SaaS control plane to manage access controls
  - Ephemeral client certificate architecture
  - SSH and RDP tooling integration
  - Server user and group account management
  - Sudo entitlements management
  - Integrates with Terraform, Chef, Puppet Ansible, etc
- See additional information on Okta Advanced Server Access here: