Building the Zero Trust Enterprise

Establishing Strong Identity Best Practices with Palo Alto Networks and Okta

Why Zero Trust Now?

Zero Trust is a strategic approach to cybersecurity that simplifies risk management to a single use case: the removal of all implicit trust for users, applications, and infrastructure.

For years, organizations implemented layer upon layer of defenses—firewalls, antivirus software, two-factor authentication, intrusion prevention systems, URL filters, sandboxes, and more—to protect what was inside of their security perimeter. Essentially, they've been playing a game of whack-a-mole, trying to deflect threats and risks as soon as they emerge but never quite catching them all or ever getting ahead of them.

This approach to security was never truly effective. Now, it's even less relevant because organizations can no longer inherently trust what's inside of their security perimeter.

Organizations have been racing to add tools and technologies to meet new and intensifying demands, such as the need to transform the network to support a hybrid workforce or move more data center applications to the cloud. Under pressure to evolve quickly, many enterprises have been forced to take an ad hoc approach to digital transformation instead of a thoughtful, holistic one. The result? They've inadvertently created an IT environment that is much more fragmented, complex, porous, and murkier than ever before—an ideal habitat for threats and risks to thrive.

A Unique Opportunity to Rethink and Rebuild Security

As organizations look to expand digital transformation further and prepare for the future of work, they should step back to evaluate their current IT environment and how they're securing it. Most will discover—and likely be surprised to find—that they have 100 or more disparate point solutions for security, from application firewalls to secure web gateways deployed across the enterprise. Yet, despite all of this coverage, security gaps abound.

A parallel and complementary journey to their digital transformation process, the Zero Trust journey can help organizations reduce complexity in their IT environment while achieving better overall security and risk management. Zero Trust is a way to secure all users, all the time, wherever they're located and whatever they're trying to do, using one approach. Zero Trust also provides a strategic framework—a North Star—to help guide the organization's security approach and purchasing decisions for the future.

A key component of a comprehensive Zero Trust strategy is identity and access management (IAM). In a Zero Trust environment, only "least-privileged" access is granted following the authentication, authorization, and verification of users, apps, and infrastructure. This guide will expand on the importance of establishing strong identity best practices, which can help your organization to accelerate both its Zero Trust and digital transformation journeys. It will also explain how Zero Trust Network Access (ZTNA) fits into the overall Zero Trust journey, and how Palo Alto Networks and Okta are together helping to enable ZTNA 2.0, which overcomes the limitations of legacy ZTNA solutions and makes the transition to a broader Zero Trust architecture easier.

Who Is This White Paper for?

The information detailed herein is intended for the following IT executives and professionals who play a vital role in helping their organizations transition to a Zero Trust approach to security:

- **Chief information officers (CIOs)** and heads of infrastructure who want to invest resources strategically in Zero Trust solutions that can expand the capabilities of their teams and help the business maintain compliance without increasing IT complexity
- **Chief information security officers (CISOs)** who are tasked with finding cohesive, flexible, scalable, and seamless solutions for implementing Zero Trust that are leading-edge but also customizable and cost-effective
- **Security architects and engineers** who understand the value of Zero Trust security and want to help implement solutions that won't create friction or undermine their teams' ability to ensure optimal network performance
- **Network security engineers and architects** who are responsible for implementing the systems that make security seamless and seek Zero Trust solutions that can fit within existing infrastructure and won't be disruptive

The Role of Identity Within a Zero Trust Strategy

Zero Trust leads to better security outcomes because it requires the deployment of the most rigorous security checks, which are applied to everyone and everything that can access the environment—users, applications, and infrastructure—continuously throughout every stage of a digital interaction. The following framework shows how IAM is foundational to achieving Zero Trust for those three pillars of a Zero Trust architecture (ZTA).

Zero Trust is achieved across the three pillars of users, apps, and infrastructure by:

- **Verifying identity** to determine who is requesting access. Requests are authenticated and authorized to verify identity prior to granting access. Identity is continuously monitored and validated throughout the transaction stage (e.g., downloading or uploading files).

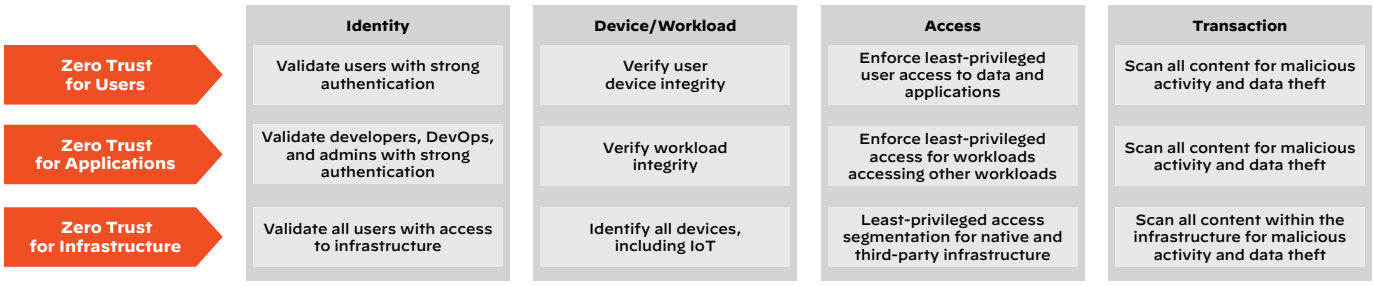

Figure 1: Overview of the Zero Trust approach to security

- **Verifying the device or workload.** Also core to Zero Trust is identifying an enterprise laptop, a server, a personal smartphone, or a mission-critical Internet of Things (IoT) device that is requesting access and then verifying its integrity. The integrity of the device or host is continuously monitored and validated for the lifetime of the transaction. As for workloads, the requested device or microservices, storage or compute resources, and partner or third-party applications must be identified prior to granting access.
- **Securing access.** Even after user authentication and confirmation of device or workload integrity, enterprises must ensure users have least-privileged access—that is, access to the minimal amount of resources, such as data or apps that they need to conduct the activity they are authorized to perform.
- **Securing all transactions.** Finally, all content exchanged in a Zero Trust environment must be continuously inspected to verify that it is legitimate, safe, and secure. Data transactions must be fully examined to avoid enterprise data loss and prevent attacks on the organization through malicious activity, including by insiders.

Because IAM is foundational to a ZTA, organizations must assess their current IAM practices before they can embark on a Zero Trust journey. The following are some questions about identity security to help make that assessment. They're based on The Five A's of Enterprise IAM—authentication, authorization, administration, audit, and analytics—which constitute a holistic approach to identity management operational controls.[1] These are just some examples of questions that your organization might need to consider:

- What solutions are we using to authenticate users (e.g., MFA, SSO) before we apply additional processes for authorization to access certain data and applications? (Note: The authors of The Five A's of Enterprise IAM emphasize that authentication is not the same as authorization; it is the next step after authentication. Authorization is a user's right to perform a function based on their authentication.)
- Can we apply granular, role-based access control (RBAC) as well as access our network with a single-pane-of-glass view to create and enforce our security policies?
- Can we manage large numbers of cloud accounts and resources, and govern permissions for them effectively?
- Can we detect instances of improper or suspicious credential usage? When that activity is detected, are other security controls set to trigger automatically?
- Do we have advanced tools in place to provide visibility into and pinpoint user-based threats and analyze user behaviors?
- Are we able to audit our IAM approach to ensure that it's effective? Are we collecting the right data for that process?
- Are we employing identity analytics tools that use artificial intelligence and machine learning to provide insights and recommendations that allow us to enhance our security and compliance?

Once you have a better idea of where your organization stands today with IAM and where it needs to be, you can start to implement a Zero Trust framework and begin your evolution to become a Zero Trust enterprise (ZTE). That means taking Zero Trust principles, making them actionable, and effectively rebuilding security to keep pace with digital transformation and the modern threat landscape.

1. Morey J. Haber and Darran Rolls, *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*, page 11, Apress, 2020.

The Need to Secure Access for Remote and Hybrid Teams

Another question today's enterprises must consider, even if they aren't looking to become a ZTE, is this: Are we currently equipped to enable seamless, secure access for remote and hybrid teams? They must also assess whether their current approach to securing these workers is adequate, especially if they are using first-generation ZTNA solutions.

In recent years, many organizations have turned to ZTNA to modernize their access infrastructure. ZTNA is a category of technologies that provides secure remote access to apps and services based on defined access control policies.

However, ZTNA 1.0 approaches fail to secure hybrid workforces adequately. For one, they violate the principle of least privilege. They don't apply fine-grained application, user, and device-based access controls to limit exposure and reduce the attack surface. Also, they only validate connections between users and apps once, which means trust is only verified once. In other words, once a user passes the initial authentication hurdle, they're essentially free to roam inside the network.

Palo Alto Networks pioneered and recently introduced ZTNA 2.0 to address the deficiencies of ZTNA 1.0 approaches by connecting all users and apps with fine-grained access controls and providing behavior-based continuous trust verification after users connect to reduce the attack surface dramatically. ZTNA 2.0 provides a truly cloud native architecture built to secure today's digital enterprises at cloud scale and deliver exceptional performance and user experiences. Being completely software-based and hardware neutral, ZTNA 2.0 ensures auto scaling to keep up with changing hybrid workforce and evolving business demands without requiring manual interactions or processes.

ZTNA 2.0 is only available with Palo Alto Networks Prisma Access. Using the combined capabilities of Prisma Access and Okta, organizations can deploy ZTNA 2.0 confidently, taking a streamlined, cloud-first approach to securing their users, systems, and data.

While ZTNA and Zero Trust are different, they are intertwined. Solving the secure connectivity challenges of today's remote and hybrid workforces with ZTNA 2.0 can provide organizations with a logical entry point to a broader and more secure Zero Trust strategy.

End-to-End Zero Trust: Palo Alto Networks and Okta

Today, most vendors confine Zero Trust to the security use cases their products address, such as endpoint, network, or access use cases. While no single vendor provides everything to enable a ZTA, Palo Alto Networks offers a full suite of products and solutions that can help your business achieve Zero Trust security. Our integrations with industry-leading technology partners can also make it easier for your organization to undertake the Zero Trust journey.

Unlike niche vendors that offer only a partial solution to Zero Trust, Palo Alto Networks is uniquely positioned to deliver a broader, higher quality, and integrated set of capabilities. Below is an overview of our ZTE framework, showing where our various products come into play to help enable and support a Zero Trust approach.

The products supporting our Zero Trust enterprise framework include:

- **Prisma® Cloud**, for securing infrastructure, applications, and data across hybrid and multicloud environments.
- **Cortex XDR®**, the industry's first extended detection and response (XDR) platform that spans all data sources to stop modern, sophisticated attacks.

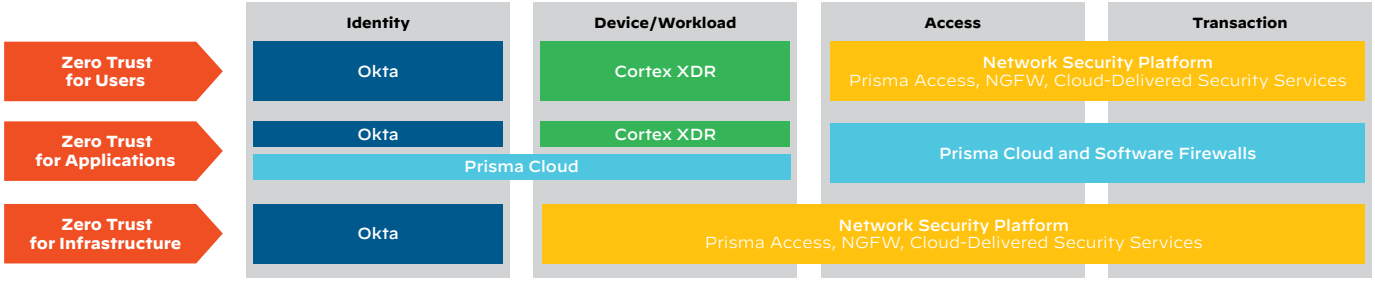

Figure 2: An overview of the Zero Trust enterprise framework from Palo Alto Networks and Okta

- **ML-Powered Next-Generation Firewalls (NGFWs)**, which, being powered by machine learning, can inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of their location or device type.
- **Prisma Access**, which seamlessly extends consistent, centralized, and best-in-class security controls to every user and location.

Cloud Identity Engine: Securing Access for the Right Users

Recently, Palo Alto Networks introduced the industry's first Cloud Identity Engine to help organizations easily authenticate and authorize their users across enterprise networks, clouds, and applications, irrespective of where their identity stores live.

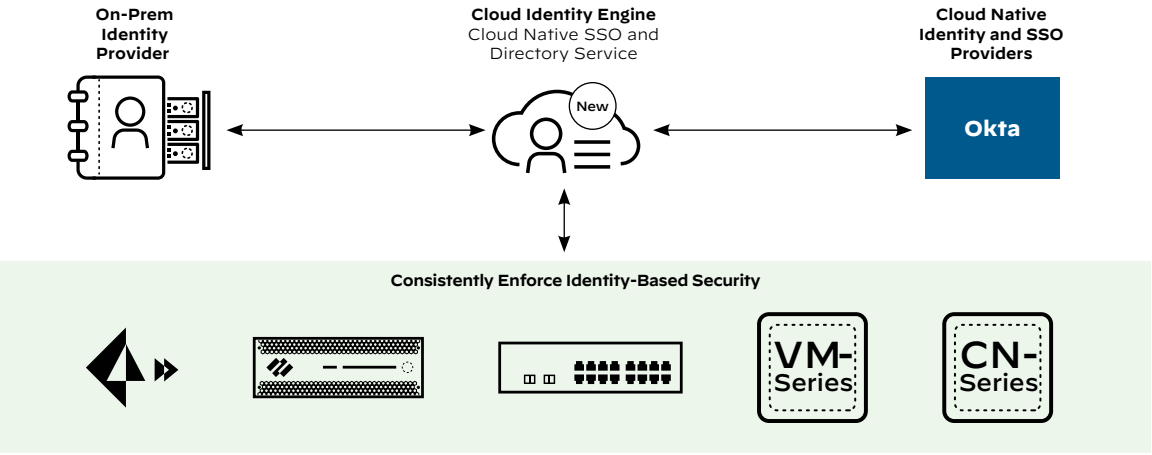

Figure 3: Overview of Palo Alto Networks Cloud Identity Engine

The authentication component of the Cloud Identity Engine allows you to configure a profile for a SAML 2.0-based identity provider (IdP) that authenticates users by redirecting their access requests through the IdP before granting access. When you configure an authentication policy and the authentication portal on a Palo Alto Networks firewall, users must log in with their credentials before they can access the requested resource.

The Cloud Identity Engine application works with leading identity providers, including MFA and SSO providers, to help you rethink Zero Trust. In the following sections, we'll look at how Palo Alto Networks and our technology integrations with one of those providers, Okta, can help you design and implement your security to achieve Zero Trust.

Enabling Zero Trust Best Practices with Palo Alto Networks and Okta

Palo Alto Networks and Okta partner to offer several integrations that help organizations enable Zero Trust by addressing the foundational step of validating identity for users, apps, and infrastructure. (See the sidebar for a list of integrations.)

The following is a look at various security challenges that some of our integrations can help to solve. Implementing these solutions can help organizations take advantage of the opportunity to rethink and rebuild their security as they lay the groundwork for and embark on their Zero Trust journey.

Applying Strong Authentication to Secure a Hybrid Workforce

Today, many enterprises require MFA to enhance security for their critical systems or to meet compliance requirements for mandates such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). However, it's often difficult, disruptive, and time-consuming to rearchitect application login processes to add MFA.

The Prisma Access and Okta integration protects today's remote and hybrid workforces with the superior security of ZTNA 2.0, while providing exceptional user experiences from a simple, unified security product.

Select Palo Alto Networks and Okta Integrations

Prisma Access and Okta SSO
Secure remote access.

NGFW and Okta Identity Cloud
Prevent credential theft and abuse.

Cortex XDR and Okta Identity Cloud
Detect compromised accounts and malicious insider activity.

Prisma Cloud and Okta SSO
Seamlessly integrate Okta users and permissions into AWS.

For more details on these integrations, see this page.

The modern architecture of Prisma Access combined with Okta's Single Sign-On and Adaptive MFA makes it easy for users to log in from anywhere, from any device, securely. They enjoy a simple, convenient identity management and secure connection experience whether they're accessing the internet, SaaS apps, or public, hybrid, or private clouds. And instead of needing to remember different passwords and authentication schemes for various apps, they can enter a single set of credentials, or even use passwordless authentication.

With this Palo Alto Networks and Okta technology integration, your organization can also quickly and easily set MFA policies across the network without taking critical resources offline or disrupting your users. You can configure Prisma Access to enforce MFA for some or all users and applications without having to change existing applications to meet security requirements.

Okta's Adaptive MFA solution is part of the Okta Identity Cloud, and it uses robust risk signals (e.g., from an IP address, device, or geography) to inform security teams of potential risks around authentication attempts. This integration also provides the flexibility to set policies to step up MFA if high risk is detected or offer a passwordless experience if the risk is low.

Learn more about this integration.

Extending Strong Authentication and Access Controls to Cloud Applications

More organizations are deciding to maintain remote or hybrid workforces for the long term—making the move to a ZTA even more essential for these businesses. Zero Trust is the most effective approach to secure these workforce models, which are challenging to manage by nature and rely heavily on the cloud. To achieve Zero Trust, organizations need accurate, granular context about users, such as where they're logging in from, what workstation they're using, and which resources they're trying to access.

Here again, the integration of Prisma Access and Okta technologies can help. Prisma Access is a modern architecture for remote and hybrid workforces because it offers an always-on connection for a range of operating systems and devices, eliminating the need for users to start a VPN or log in to a secure web gateway. It's cloud-delivered, scales with demand, and inspects all traffic for threats 24/7.

With Okta's Single Sign-On and Adaptive MFA, users logging in from anywhere, and from any device, enjoy a simple, convenient identity management and secure connection experience whether they're accessing the internet; SaaS apps; or public, hybrid, or private clouds. Users only need to enter a single set of credentials, or even use passwordless authentication, rather than remember different passwords and authentication schemes for different applications.

Additionally, with centralized, identity-driven security policies, IT can provision access only to the resources a particular user needs; and workers, no matter their location, can seamlessly get access to the tools they require to be productive. Prisma Access can also be configured to apply additional security policies to authenticated users, such as preventing them from visiting websites associated with phishing or hacking.

Learn more about this integration.

Securing SaaS Applications and Reducing Credential-Based Attacks

Every organization is embracing the convenience of the cloud, and many are picking up the pace of migrating applications and data from their in-house data centers to SaaS applications. In 2020, SaaS apps accounted for 70% of companies' total software usage,[2] and according to recent research from Okta,[3] most organizations have 88 apps deployed on average.

While app use continues to expand both rapidly and exponentially, the number of IT staff responsible for securing apps isn't increasing in most organizations. IT team members who are charged with securing apps face the added challenge of working with disparate security tools that don't integrate well and provide little or no visibility into the IT environment.

Meanwhile, the rise of remote and hybrid work is creating more security risks for enterprises, with workers using their own devices to log in to sanctioned and unsanctioned applications and data stores, both in the cloud and on-premises. Also, users are top targets for malicious actors seeking to steal credentials and then use those compromised passwords to authenticate applications and steal data.

2. "Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021," Statista, 2022, https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/.
3. *Businesses at Work*, Okta, March 2021, https://www.okta.com/sites/default/files/2021-03/Businesses-at-Work-2021.pdf.

Prisma Access from Palo Alto Networks works with Prisma SaaS to safely enable SaaS application adoption. Prisma SaaS is a multimode cloud access security broker (CASB) service. By using both Prisma solutions together, your organization can address its CASB needs and also gain deep visibility into SaaS risks, data protection, leakage prevention, data governance, compliance assurance, advanced threat prevention, and much more. When you have Okta integrated with Prisma Access as well, you can easily set up MFA for identifying and authenticating remote users.

An additional benefit of this integration is that because Prisma Access, Prisma SaaS, and Okta remote access services are all based in the cloud, they can be deployed quickly. They also can scale with demand while reducing both on-premises hardware and the operational load on your network and security teams.

Learn more about this integration.

Leveraging Identity Information for Continuous Monitoring

The integration of Palo Alto Networks Cortex XDR and Okta technologies is crucial to building identity-based security, which is vital for developing a Zero Trust approach to security.

With this integration, security teams have increased visibility into authentication data, powerful threat-hunting capabilities, and expanded rapid response. They can surface, prioritize, investigate, and respond to stealthy threats, including targeted attacks, insider abuse, and risky user behavior, more rapidly. Authentication logs also help to unearth unusual user activity like credential abuse.

Cortex XDR integrated with Okta Identity Cloud helps your organization to focus its security posture and investments around user identity and behavior to provide safe, reliable access to all users while quickly eliminating threats. AI-driven analytics for root cause analysis in Cortex XDR can also cut investigation time for security teams by 88%.

Learn more about this integration.

Integrating Users and Permissions into Amazon Web Services

Again, remote and hybrid workforces are heavily reliant on the cloud. Most businesses today use some form of SSO, like Okta, to manage the way users interact with public cloud services. This approach is an effective way to centralize access to cloud accounts, especially across a large number of users and services. However, the mapping between SSO users and IAM roles can become challenging because users can have multiple roles that span several cloud accounts. Organizations also often lose visibility into how IdP permissions translate to cloud entitlements.

This integration allows you to seamlessly integrate Okta users and permissions into AWS. Prisma Cloud integrates with Okta to ingest SSO data, enabling organizations to view effective permissions and overly permissive roles to Okta users and correlate results with cloud identities like IAM users and machine identities.

With Okta integrated into Prisma Cloud, you can map current entitlements to AWS IAM roles and continuously enforce least-privileged access. Together, they can also quickly discover Okta entities across multiple AWS accounts with intuitive Resource Query Language (RQL).

Learn more about this integration.

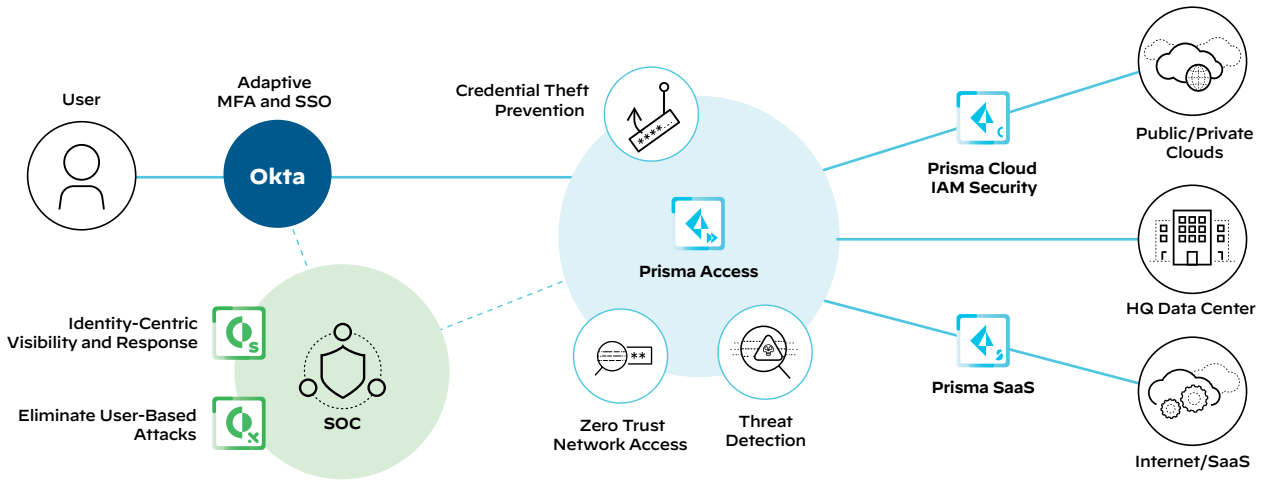

Figure 4: Context-aware, continuous validation to secure remote and hybrid workforces with Palo Alto Networks and Okta

Palo Alto Networks and Okta: Accelerating Your Zero Trust Journey

It will take time to become a Zero Trust enterprise, but the journey is well worth it because you can rebuild your security approach for the better. When that journey is supported by the right technology solutions, you can get to your destination faster and more confidently. With Zero Trust as a North Star to guide all of your security decisions, you'll be able to:

- Reduce risk by eliminating implicit trust for users, applications, and infrastructure.
- Adopt a simplified, consistent security posture that is less expensive to manage.
- Achieve better security outcomes by deploying the most rigorous security checks.
- Make it easier for security operations staff to double-check the trust decisions made by infrastructure and override them if signs of anomalous or malicious intent are detected.
- Accelerate your organization's digital transformation journey by ensuring that security and risk management are at the heart of every initiative.

Palo Alto Networks and Okta technology integrations, such as the examples outlined in this guide, can help you address IAM gaps and strengthen what you're already doing well so that you can complete the foundational step of validating identity to secure your users, applications, and infrastructure and build a Zero Trust architecture. Now, with the Cloud Identity Engine app from Palo Alto Networks—which works with Okta and other MFA and SSO providers—you can write security policy based on users and groups, not IP addresses, to help secure your assets by enforcing behavior-based security actions.

Zero Trust means you trust nothing, and you must validate everything. Ultimately, by doing both, you can enable business everywhere.

Learn more about the Palo Alto Networks and Okta integrations here.

Read more about the Zero Trust enterprise here.

Get more details on ZTNA 2.0 here.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com