Accelerating Your Zero Trust Journey in Financial Services

Implementing Key Industry Best Practices with Palo Alto Networks

Digital transformation is accelerating within the financial services industry with the continued adoption of the public cloud, the shift to a hybrid workforce, greater dependency on the internet, and an expanding ecosystem of third-party partners. At the same time, evolving regulatory emphasis on data privacy and operational resilience adds complexity to many digital transformation initiatives. Unfortunately, many financial institutions are still struggling with a poorly integrated, loose assembly of security point products that do not align with the strategic approach expected by board members and C-level executives.

Given this combination of tremendous change coupled with critical compliance and regulatory requirements, information security teams require a modern approach to security that fits these significant shifts. Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. A modern, holistic approach to security, such as Zero Trust, enables financial institutions to meet these challenges in a proactive manner for higher levels of security, reduced complexity, and increased operational resilience to minimize downtime and disruption to the business.

Zero Trust Today: A Modern Security Approach for Digital Transformation

As an industry, we've reached a tipping point: many users and apps now reside outside of the traditional perimeter. A hybrid workforce is a new reality—financial institutions must provide access from anywhere and deliver an optimal user experience. The days of managing implied trust by relying on a static, on-premises workforce are gone. Additionally, the growing financial services ecosystem drives more external access requirements for third parties, such as fintech and big tech.

At the same time, application delivery has firmly tilted in favor of the cloud, public or private, and has enabled development teams to deliver at an unprecedented pace. However, new architectures, delivery, and consumption models create more instances of implied trust, and an expanding catalog of apps creates a broader attack surface, while implied trust granted to microservices yields new opportunities for attackers to move laterally.

Infrastructure can be anywhere, and everything is increasingly interconnected, making the elimination of implicit trust even more critical. You can no longer simply trust IT equipment such as printers or vendor-supplied hardware and software because IT and workplace infrastructure are increasingly connected to internet-facing apps that centrally command and orchestrate them. Anything internet-facing, including retail bank branches, is a risk to your organization. Additionally, physical locations are increasingly run by connected things, including IoT, which typically have more access than they need. Traditional IT patching and maintenance strategies do not apply here—cyber adversaries know this is ripe for exploitation.

As financial institutions undergo their digital transformations, financial regulators maintain a watchful eye with a focus on data privacy, operational resilience, and third-party risk. Implicit trust is increasingly at odds with sound security practices in these areas.

Delivering the Zero Trust Enterprise

The biggest challenges to adopting a Zero Trust architecture have not been a lack of specific security tools but a simple lack of resources (talent, budget, interoperability, time, etc.), including limited knowledge of an application's dependencies. This then raises the specter of potential business impact as controls are implemented over existing applications. Consequently, running the most current security controls against a moving target—a dynamic threat landscape with multiple unknowns—has been a privilege reserved for a few well-resourced organizations. So, why would Zero Trust work this time for the financial services industry? As financial institutions continue their Zero Trust journeys, some comfort may be derived from their past experience with smaller-scale network segmentation efforts for PCI DSS and isolation of local SWIFT infrastructure.

On a larger scale, the Zero Trust enterprise is enabled through Palo Alto Networks extensive experience, and a comprehensive set of security capabilities to introduce consistent Zero Trust controls across the entire organization. As Forrester noted in the Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020, "Palo Alto Networks has essentially either procured, acquired, or built every tool or capability an organization could need to operate a Zero Trust infrastructure. Palo Alto Networks is assembling a robust portfolio to deliver Zero Trust everywhere—on-premises, in the data center, and in cloud environments."[1]

Instead of testing, running, and fixing multiple non-integrated security controls across all of your security domains, such as malware or DLP, you can rely on one single control, which you can deploy across your entire enterprise. Security by design becomes a reality as the cost of deployment, operations, and time-to-market are going down. Moreover, leveraging the network effect of telemetry from the entire enterprise and not just from one specific area means the time to respond and prevent cyberthreats goes down, leading to more resilient cybersecurity.

[1] Chase Cunningham, *The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020,* September 24, 2020, https://www.forrester.com/report/The-Forrester-Wave-Zero-Trust-eXtended-Ecosystem-Platform-Providers-Q3-2020/RES157494

Palo Alto Networks: Over a Decade of Zero Trust Experience

As a pioneer in Zero Trust with thousands of customers and deployments, no one in security has more experience than Palo Alto Networks across the entire security ecosystem, including network, endpoint, IoT, and much more. We know security is never one size fits all. Here’s what makes our ZTE approach different:

- **Comprehensive:** Zero Trust should never focus on a narrow technology. Instead, it should consider the full ecosystem of controls that many organizations rely on for protection.
- **Actionable:** Comprehensive Zero Trust isn’t easy, but getting started shouldn't be hard. For example, what current set of controls can be implemented using security tools you have today?
- **Intelligible:** Convey your Zero Trust approach to nontechnical executives in a concise, easy-to-understand summary, both business and technical terms.
- **Ecosystem Friendly:** In addition to having one of the most comprehensive portfolios in the market, we work with a broad ecosystem of partners.

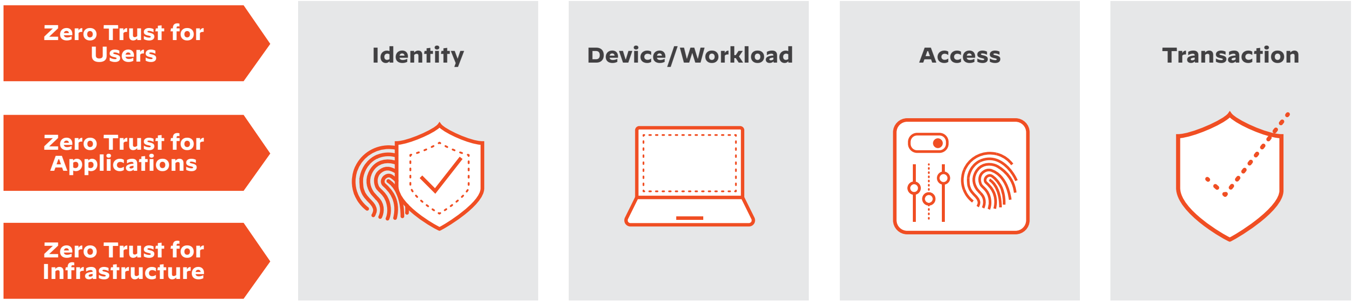


Figure 1: Each pillar requires validation across Identity, Device/Workload, Access, and Transaction

A Comprehensive Approach: Users, Applications, and Infrastructure

At its core, Zero Trust is about eliminating implicit trust across the organization. This means eliminating implicit trust related to users, applications, and infrastructure.

Zero Trust for Users

Step one of any Zero Trust effort requires strong authentication of user identity, application of least access policies, and verification of user device integrity.

Zero Trust for Applications

Applying Zero Trust to applications removes implicit trust with various components of applications when they talk to each other. A fundamental concept of Zero Trust is that applications cannot be trusted and continuous monitoring at runtime is necessary to validate their behavior.

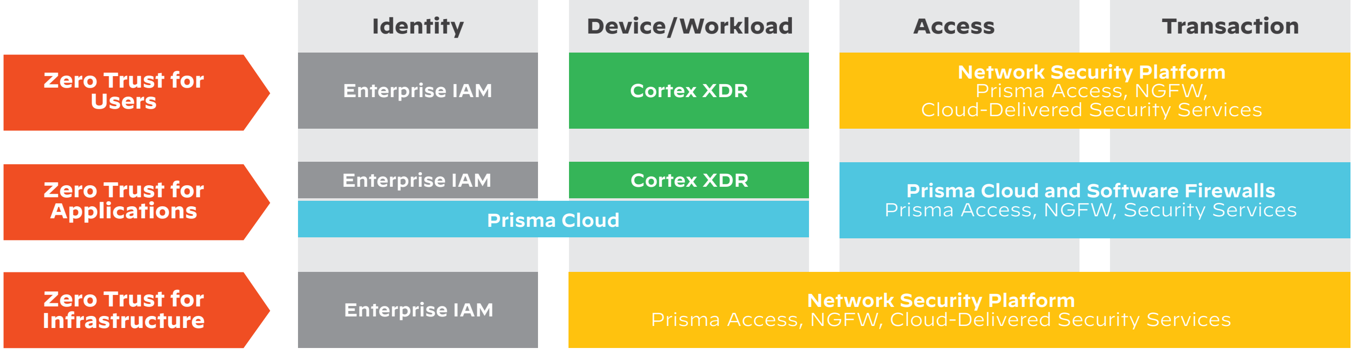
Zero Trust for Infrastructure

Everything infrastructure-related—routers, switches, cloud, IoT, and supply chain—must be addressed with a Zero Trust approach.

For each of the three pillars, it is critical to consistently:

- **Establish identity using the strongest possible authentication.** The request is authenticated and authorized to verify identity before granting access. This identity is continuously monitored and validated throughout the transaction.
- **Verify the device/workload.** Identifying the enterprise laptop, a server, a personal smartphone, or a mission-critical IoT device requesting access, determining the device's identity, and verifying its integrity is integral to Zero Trust. The integrity of the device or host requesting access must be verified. This integrity is continuously monitored and validated for the lifetime of the transaction. Or, in the case of applications and cloud infrastructure, identifying the requested device or microservices, storage or compute resources, partner and third-party apps before granting access.

- **Secure the access.** Enterprises need to ensure users only have access to the minimal amount of resources they need to conduct an activity, restricting access to, for example, data and applications. Even after authentication and checking for a clean device, you still need to ensure least privilege.
- **Secure all transactions.** To prevent malicious activity, all content exchanged must be continuously inspected to verify that it is legitimate, safe, and secure. Data transactions must be fully examined to prevent enterprise data loss and attacks on the organization through malicious activity.



	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Enterprise IAM	Cortex XDR	Network Security Platform Prisma Access, NGFW, Cloud-Delivered Security Services	
Zero Trust for Applications	Enterprise IAM Prisma Cloud	Cortex XDR	Prisma Cloud and Software Firewalls Prisma Access, NGFW, Security Services	
Zero Trust for Infrastructure	Enterprise IAM	Network Security Platform Prisma Access, NGFW, Cloud-Delivered Security Services		

Figure 2: A comprehensive approach across users, applications, and infrastructure

The Role of the Security Operations Center

The security operations center (SOC) continuously monitors all activity for signs of anomalous or malicious intent to provide an audit point for earlier trust decisions and potentially override them if necessary. Using broad enterprise data collected from network, endpoint, cloud, and much more, the SOC uses behavioral analytics (UEBA), threat hunting, anomaly detection, correlation rules in the SIEM, and more to double-check all trust decisions. The SOC can do this because they have a wide view of the entire infrastructure versus a subset of information such as separate firewall or endpoint telemetry. When this information is examined across the entire infrastructure, the SOC has the ability to discover things that would normally go undetected in individual silos.

Summary

What are the benefits of becoming a Zero Trust enterprise? By taking a holistic, platform-based approach to Zero Trust, organizations can secure their digital transformation initiatives while enjoying increased levels of overall security and significant reductions in complexity. This provides value in the areas of data privacy, operational resilience, and third-party risk management—all of which are enablers of digital transformation for financial institutions.

Please visit www.paloaltonetworks.com for more information on Zero Trust and on solutions for Financial Services.

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

parent_wp_zero-trust-journey-in-fsi_020122