Architecting the Zero Trust Enterprise

The Benefits of Adopting a Holistic Approach to Zero Trust

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction.

The Zero Trust Model has become increasingly top of mind for executives who need to keep up with digital transformation and adapt to the ever-changing security landscape. Unfortunately, many organizations are still struggling with a poorly integrated, loose assembly of point products that do not align with the strategic approach expected by board members and C-level executives.

Deployed properly, the Zero Trust Enterprise is a strategic approach to cybersecurity that simplifies and unifies risk management under one important goal: to remove all implicit trust in every digital transaction. This means regardless of the situation, user, user location, device, source of connection, or access method, cybersecurity must be built in by design in every network, connection, and endpoint to address the modern threat landscape.

By becoming a true Zero Trust Enterprise, organizations enjoy more consistent, improved security and simplified security operations that effectively lower costs.

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—businesses 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.

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 is a risk to your organization. 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.

Delivering the Zero Trust Enterprise

The biggest challenge to adopting a Zero Trust architecture has not been a lack of specific security tools but a simple lack of resources (talent, budget, interoperability, time, etc.). Running the most current security controls against a moving target—a dynamic threat landscape—has been a privilege reserved for a few well-resourced organizations. So why would Zero Trust work this time for the masses?

The Zero Trust Enterprise is enabled through Palo Alto Networks extensive experience and 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 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.

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.

1. Chase Cunningham, *The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020*, Forrester Consulting, September 24, 2020, https://start.paloaltonetworks.com/2020-forrester-ztx-report?utm_source=social&utm_medium=blog&utm_campaign=-FY21Q1%20Forrester%20Zero%20Trust%20eXtended%20Wave%20report.

- **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.

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.

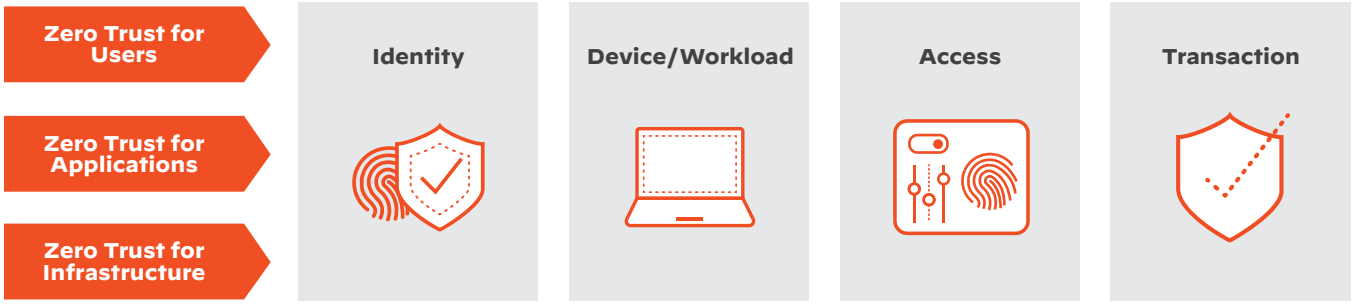

Figure 1: Each pillar requires validation across Identity, Device/Workload, Access, and Transaction

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.

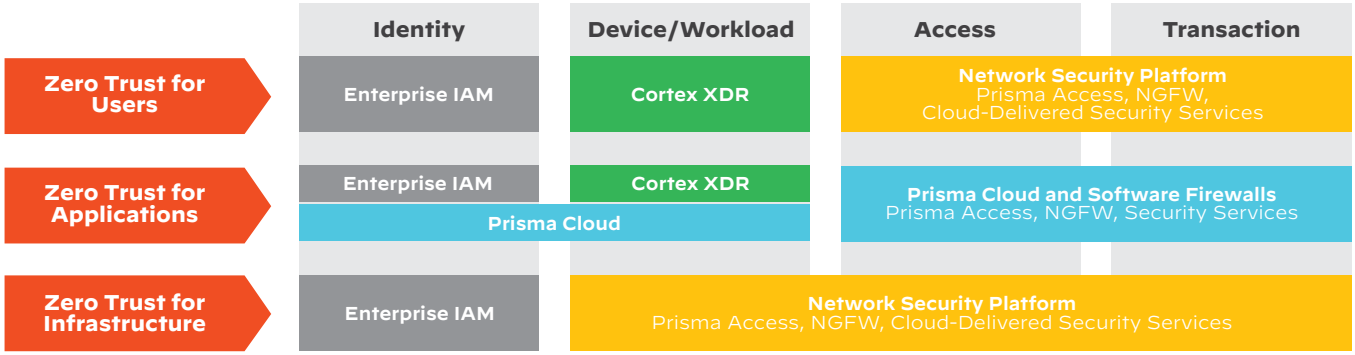

Figure 2: A comprehensive approach across users, applications, and infrastructure

The Role of the Security Operations Center (SOC)

The 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.

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