Deloitte.

# The Journey to Zero Trust with Deloitte and Palo Alto Networks

# Contents

# Deloitte's perspectives on Zero Trust

The Zero Trust concept represents a dramatic shift from the legacy castle-and-moat approach to cybersecurity, which focused on fortifying the perimeter to deter outsiders from accessing corporate data, while implicitly trusting insiders. In the past, well-constructed perimeter defenses were sufficient to deter intruders, when enterprise users, assets, and data resided within the walls of an organization's data centers and office spaces. Current challenges such as the growing scale, velocity, and impact of cyberattacks, an increasingly mobile workforce, enhanced regulatory oversight, and hyper-connected technology ecosystems spanning both on-premise and cloud environments require organizations to think differently about how to secure their enterprise while driving business agility.

Both a methodology and a mindset, Zero Trust recognizes there is no defensible perimeter that can effectively protect today's modern organization. Instead, the Zero Trust model advocates that security controls should always assume that malicious actors are already present, therefore the principle of "never trust, always verify" must be enforced. This enforcement should be grounded upon a risk-based access control posture that dynamically and continuously evaluates session parameters to enhance the fidelity of authentication and authorization decisions.

For a successful Zero Trust transformation, certain foundational capabilities and initiatives should be in place or enhanced along the journey, such as information technology (IT) asset management, vulnerability management, and data discovery. Gaining consensus from relevant stakeholders across each part of the business is an important component of a successful, business-aligned journey. Prior to setting off on a Zero Trust transformation, organizations should develop a clear understanding of the assets and data that exist in the enterprise environment, as well as where they reside, their classification and criticality, associated entitlements, and the contextual signals that should inform risk-based access control decisions.

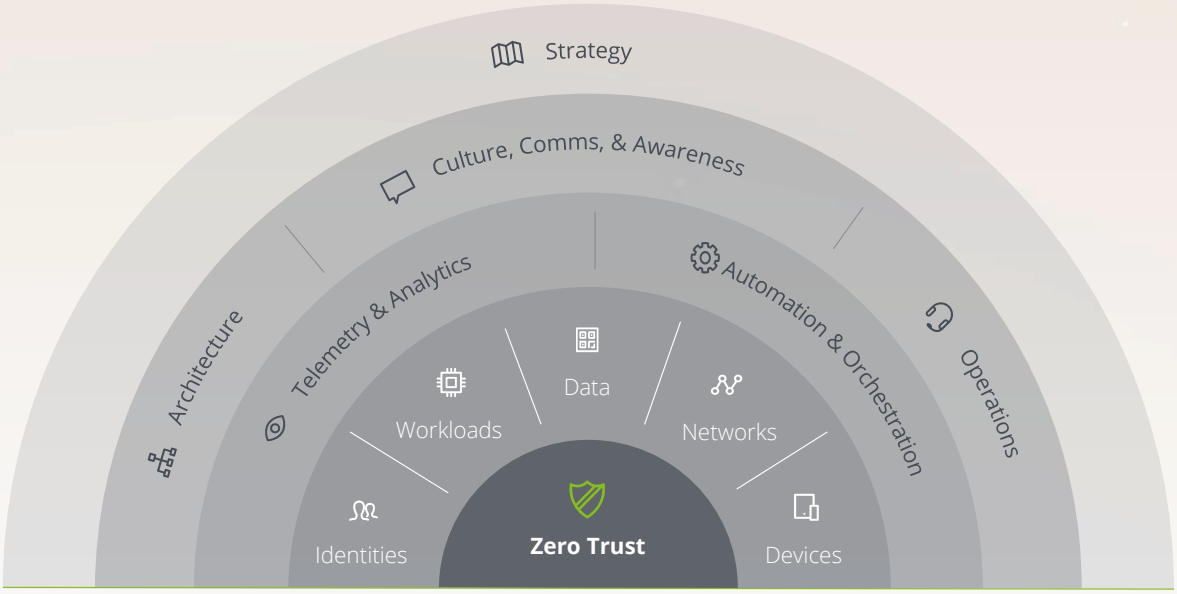
Implementing Zero Trust typically requires breaking down a company's IT security domains into its foundational elements. Rather than attempting to apply Zero Trust principles across the entire enterprise, business leaders should analyze existing capabilities against the framework, and develop an iterative and incremental plan to enhance maturity in alignment with business drivers.

**Recognized as a leader.**

"Deloitte is ranked #1 in market share for security consulting services by Gartner for the 11th year in a row based on revenue."

**—Gartner, Gartner Market Share Security Consulting Services, Worldwide, 2022**

**Figure 1 - Deloitte's Zero Trust Framework**




Deloitte's perspective on this leading cyber framework is that it should be grounded upon strong foundational capabilities across five core domains: identities, workloads, data, networks, and devices.

**Identities** are the new "perimeter." A core component of a Zero Trust architecture is shifting to identity-based access control decisions based on user profile, entitlements, authorization, and acceptable usage patterns.

**Workloads** are applications or services hosted on legacy infrastructure or in cloud environments and containers. Workloads should be hardened, segmented, and monitored on a granular level with adaptive actions, such as limiting access or blocking uploads to specific applications.

**Data** lies at the heart of an effective Zero Trust strategy. Data should be discovered, inventoried, governed, classified, and tagged in a manner that can be used to inform access control decisions. Data should also be protected through obfuscation, encryption, and advanced data loss prevention mechanisms at each stage—at rest, in use, and in transit.

**Networks** carry traffic between identities, devices, and workloads, with controls that segment (block unintended network communications), monitor, and analyze activity, operating on the assumption that all network connection requests are inherently untrustworthy.

**Devices** include both known/managed endpoints, unmanaged ones (e.g., bring your own device - BYOD), and smart devices that connect to an organization's network and enterprise assets (e.g., Internet of Things - IoT). Devices should be subject to continuous assessment for risks and threats and to evaluate their compliance with defined security policies.

The next ring of the framework encompasses the enabling layer. These horizontals are the stitching that holds the core domains and their respective capabilities together.

**Telemetry & Analytics** systems collect data from relevant security controls into a centralized platform for event correlation and advanced analysis that can help detect suspicious and potentially malicious behaviors. As modernized controls are implemented, the associated telemetry should be ingested to enhance situational awareness of network and user access patterns. Threat intelligence should also be integrated to help enable a threat-driven security posture for the organization.

**Automation & Orchestration** capabilities help enable a more proactive security posture by automating detection, prevention, and response actions through integrated security controls. Security operations can become more productive and proactive in neutralizing threats when investigative tasks are automated in response to an ever-growing flood of security alerts.

Ultimately, strong capabilities across technical aspects of the core domains and enabling layers results in an agile and dynamic security foundation that is resilient to organizational change, and flexible enough to deal with the challenges imposed by modern business, workforce, and technology trends.

The governance layer of Deloitte's Zero Trust framework encompasses **Architecture** principles that should be defined and aligned to, **Culture Communications and Awareness** needed to socialize the potential impact on the end user experience, and the associated organizational change management updates to IT and security **Operations** that may be needed to manage new or modernized security controls.

Finally, the outer ring encompasses the organization's Zero Trust **Strategy**, which should be aligned to business drivers such that the journey is supporting the business, and not considered a science experiment or costly technology implementation.

# Palo Alto Networks: A leader in the Zero Trust technology space

Deloitte often forms strategic alliances with leading technology companies to provide innovative, tech-enabled solutions to meet our clients' needs.

**Recognized as a leader.**

"Palo Alto Networks' industry-leading, machine learning-based platform applies techniques that help customers handle sophisticated threats and meet end-to-end demands across network, endpoint, and cloud security. The company enables enterprises to go beyond standard threat protection by building a strong posture and resilience."

**—Rajarshi Dhar, Industry Analyst, Frost & Sullivan (February 2022)**

Here is what makes Palo Alto Networks' Zero Trust enterprise approach different:

- **It's broad.** No Zero Trust approach should just focus on a narrow swath of technology. Instead, it should consider the full ecosystem of controls that many organizations rely on for protection, as Palo Alto Networks' does.
- **It's actionable.** Adopting a Zero Trust model 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?
- **It's intelligible.** Non-technical executives can understand Palo Alto Networks' Zero Trust approach in a concise, easy-to-understand summary, in both business and technical terms.
- **It's ecosystem friendly.** Palo Alto Networks not only has an extensive technology portfolio in the market, but also works with a broad ecosystem of third-party vendors, integrating Application Programing Interfaces (APIs) without the need for custom code.

## Ease of deployment and management

Palo Alto Networks offers a comprehensive control set that an organization can deploy across the entire enterprise, instead of testing, running, and fixing multiple non-integrated security controls across domains. Security by design becomes a reality. Deployment, operations, and time-to-market costs are streamlined. And the time required to prevent and respond to cyber threats is decreased, leading to more resilient, operationally efficient cybersecurity.

## Solutions offered across multiple facets of Zero Trust

Palo Alto Networks' Zero Trust-aligned platforms help enable users to securely access workloads and data from a myriad of networks and devices. They offer value in a crowded security marketplace by eliminating implicit trust across organizations—from the core outward—with an approach that reaches across identities, workloads, and infrastructure. It's this comprehensive mapping of technology solutions and ecosystem integrations against the core domains and the enabling layer that makes Palo Alto Networks so well positioned.

### Visibility & Automation

Due to the sheer number of tools, integrations, and artifacts necessary to architect a Zero Trust environment, organizations should embed orchestration and automation into their framework wherever possible. It is critical to reducing the administrative burden on operations and security teams.

Palo Alto Networks' Security Orchestration, Automation, and Response (XSOAR) platform can be instrumental in facilitating these reductions. To develop an automation strategy fit for even the most complex scenarios, XSOAR is utilized in combination with both a security information and event monitoring (SIEM) platform, as well as the Cortex Data Lake. This integration enables several Zero Trust capabilities resulting from the machine learning and behavior analytics capabilities of the Cortex Data Lake. The XSOAR platform does more than orchestrate Palo Alto Networks' expansive suite of tools, however. It also builds a full operating picture by integrating with the security and incident response solutions of other vendors, and acting as a hub that ingests and enhances data. Organizations should leverage the Cortex product line and XSOAR toolset to enhance visibility and automation, resulting in greater cost efficiency and reduction of manual efforts, increased orchestration of incident response actions, and a more proactive cyber security posture.

### Identities

Users and their associated identities are essential components to Zero Trust and overall security posture. Palo Alto Networks has integrated User-ID capability into each of its firewall-based products, from Palo Alto Networks' Next

Generation Firewalls (NGFW), to Prisma Access. User-ID takes identity information from leading providers and uses it to drive the consistent application of security policy. User-ID is scalable, with reference architectures for distrusted information gathering and sharing across an enterprise feeding into a global policy. Combine this distributed architecture with the Panorama management platform to consistently apply security policies throughout an organization and realize a true Zero Trust architecture. Install the GlobalProtect agent to increase user clarity on remote devices, while significantly increasing the fidelity of information for on-premise ones.

Palo Alto Networks' Prisma Secure Access Service Edge (SASE) offering allows connectivity for devices, branches, and cloud systems, without the limitations of traditional Virtual Private Networks (VPNs). Zero Trust enablement with Prisma Access allows for policy decisions to be applied much closer to the ingestion of the traffic, saving the overhead of tunneling it to an enterprise data center for inspection. Prisma Access also ties into Panorama, allowing for the application of a consistent security policy without additional administrative overhead.

Finally, user behavior within Zero Trust must also be considered. From an analytics and automation perspective, Cortex XDR and Data Lake collect and build a user behavior profile. Then, when deviations occur, the risk score is elevated, and policies related to that score are applied. For example, if a user in the finance department suddenly starts attempting to access engineering shares, a behavioral anomaly indicator may trigger a security policy action that locks out the account or forces a step-up authentication.

**Workloads**

Prisma Cloud is a cloud workload protection solution that secures cloud-native applications across hosts, containers, serverless functions, and more. With both agentless and agent-based deployment options, it includes real-time protection for cloud workloads on public, private, and hybrid cloud environments, with integrated web application and API security for applications.

Prisma Cloud's approach to securing cloud workloads and applications includes:

- Detection of vulnerabilities, compliance issues, and anomalous behavior
- Integration of vulnerability management to continuously monitor, identify, and prevent threats across the application lifecycle
- Enablement of collaboration between development and security teams by integrating and automating security in developers' tools and workflows across the application lifecycle

**Data**

Protecting enterprise data is at the core of a sound Zero Trust strategy. Palo Alto Networks' Enterprise Data Loss Prevention (DLP) offers a cloud-based service that uses supervised machine learning algorithms to sort sensitive documents into financial, legal, healthcare, and other categories for document classification to guard against exposure data loss and data exfiltration. These patterns can identify sensitive information in traffic flowing through an organization's network, and protect them from exposure. Enterprise DLP protects sensitive data by preventing file uploads and non-file-based traffic from leaking to unsanctioned web applications and monitoring uploads to sanctioned web applications. Enterprise DLP is integrated with other Palo Alto Networks products such as their Next-Generation Firewalls (NGFW), Prisma Access, Next-generation CASB, Prisma Cloud, and Cortex XSOAR.

Prisma Access protects the hybrid workforce with the superior security of ZTNA 2.0, while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access protects all application traffic with best-in-class capabilities, while securing both access and data to reduce the risk of a data breach dramatically. With a common policy framework and single-pane-of-glass management, Prisma Access secures today's hybrid workforce without compromising performance, and is backed by industry-leading SLAs to ensure exceptional user experiences.

Managing sanctioned SaaS applications and preventing unsanctioned SaaS applications is another critical capability for data protection. Palo Alto Networks' Next-Generation CASB offers an integrated Cloud Access Security Broker (CASB) solution that addresses the challenges of protecting the growing adoption of sanctioned and unsanctioned SaaS applications and maintaining compliance consistently in the cloud, while stopping threats to sensitive information, users, and resources.

NG CASB includes:

- SaaS Security Inline to discover and manage risks posed by unsanctioned SaaS applications
- SaaS Security API and Enterprise DLP to prevent exposure of sensitive data within SaaS apps, including secrets commonly shared within collaboration apps
- SaaS Security Posture Management (SSPM) to help detect and remediate misconfigured security settings in sanctioned SaaS applications through continuous monitoring

### Networks

Palo Alto Networks' Zero Trust methodology takes the data, applications, assets, and services (DAAS) concept and suggests creating a micro perimeter around each DAAS element based on its criticality. NGFW utilizes a full gamut of tools, including User-ID, App-ID, Device-ID, and Content-ID, coupled with robust reporting capabilities within the platform to address identification and discovery, helping to identify the DAAS elements used most frequently, as well as the way they are accessed. Shrinking the perimeter to the smallest surface around the asset enables a far more granular and robust security posture from a protection standpoint. Network segmentation has traditionally been enforced at layers two and three, utilizing virtual local area networks (VLANs) and manually created access control lists (ACLs). A Zero Trust approach, however, should encompass layer-seven visibility in order to fully protect the DAAS. A robust network segmentation capability should also be informed by the contextual signals of each request when enforcing access control decisions. For example, an organization may wish to allow email access from anywhere, but limit access to financial or personally identifiable information (PII) data types to connection requests sourcing from physical corporate locations. Finally, the ability to block or isolate devices from the network is a critical capability to operationalize a full Zero Trust methodology.

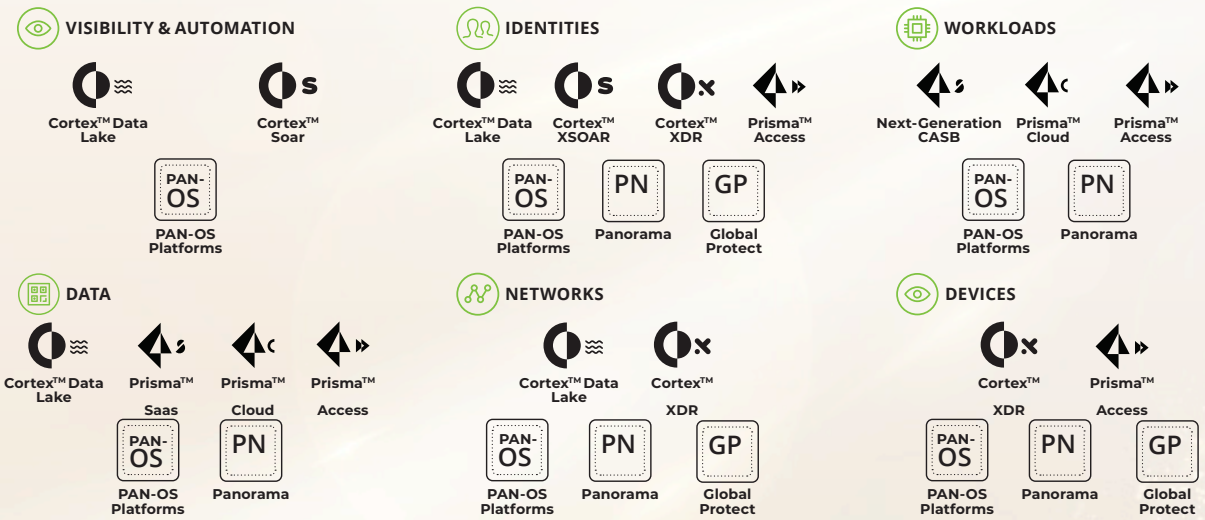
Unified policy management from Panorama, Cortex XDR, Prisma Access, and GlobalProtect toolsets enables isolation (and recovery) of hosts and devices that need to be contained based upon policy, or in response to a potential threat.

### Devices

Protecting the infrastructure that supports an application is another area associated with application security. Palo Alto Networks can support application security via Cortex XDR installed on the supporting infrastructure with the Prisma Cloud Compute edition, providing runtime defense for hosted applications. Their Prisma Cloud Compute edition is also able to ensure that repositories and sources used to build the application are secure, providing an integrated security baseline.

In addition to validating that a user attempting to access the DAAS is authorized, it is important to know that the device and method being used to access it are approved, as well. Palo Alto Networks utilizes the NGFW to validate the access attempt against the security policy. Using the Device-ID capability, it can identify device type, firmware version, and other critical information about the device initiating the access attempt. Upon validation of device type, device compliance checks are used to ensure that the device security posture (e.g., firmware, patch level, installed applications) is aligned with the defined security policy.

**Figure 2. Mapping of Palo Alto Networks' technologies to Deloitte's Zero Trust Core Domains and Enabling Layer shown on figure 1**



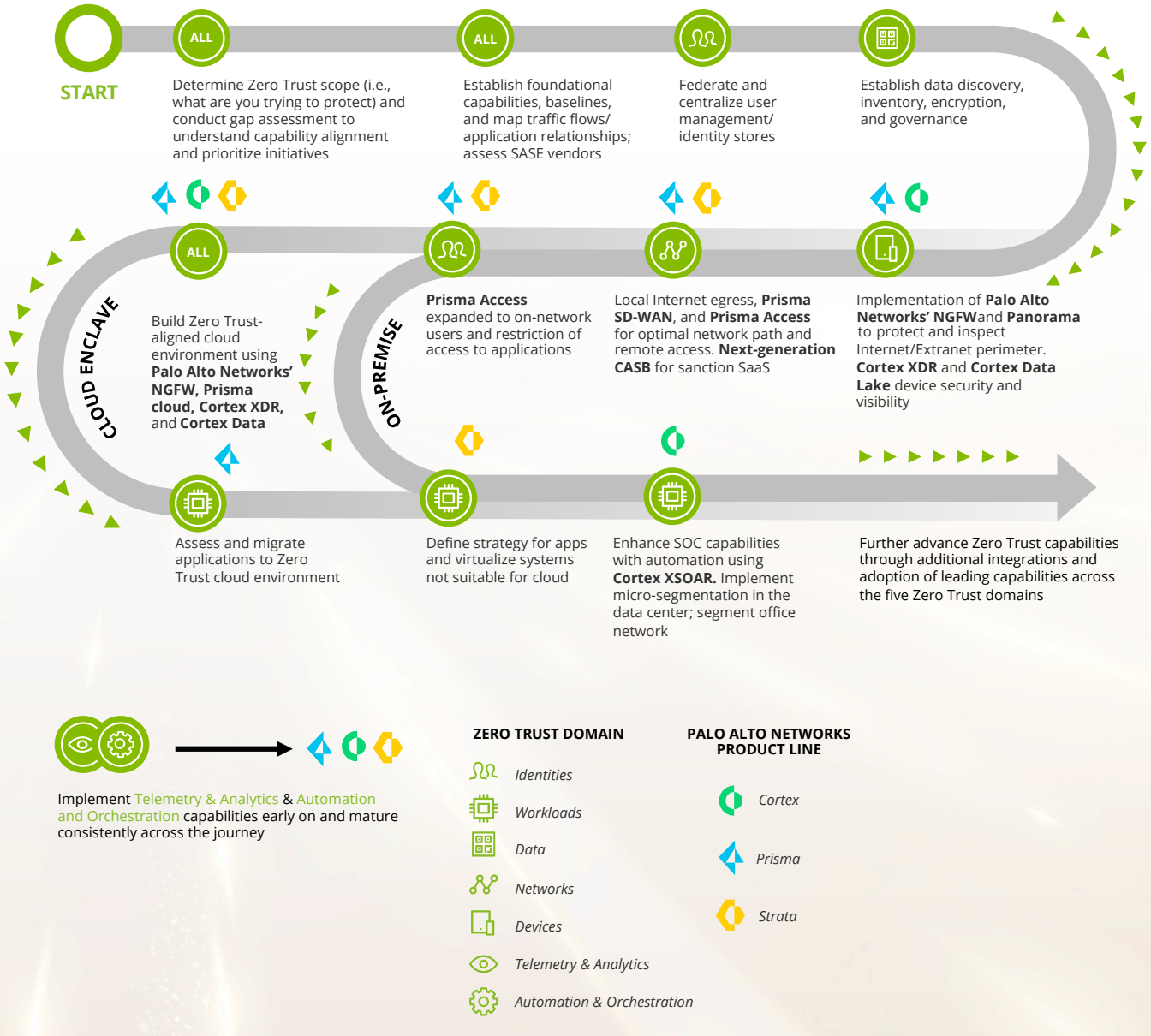

Source: Deloitte Development LLC

## An illustrative Zero Trust adoption journey

There are many approaches to implementing the Zero Trust solutions described. The approach for each organization will vary based on their current state, requirements, and desired target state.

Figure three illustrates a multiphase Zero Trust adoption journey for an organization with a mobile workforce that is on a path of cloud migration, with hybrid cloud and on-premise environments as their target state.

**Figure 3. An illustrative multi-phase journey towards Zero Trust leveraging Palo Alto Networks technologies**




Source: Deloitte Development LLC

# Deloitte and Palo Alto Networks: Working together for Zero Trust enablement

Through their alliance in promoting and implementing Zero Trust solutions as a leading cyber practice, Deloitte and Palo Alto Networks are working together to help organizations realize their desired outcomes for enterprise modernization and digital transformation initiatives. Deloitte's industry scale and cybersecurity experience, combined with Palo Alto Networks' technology portfolio, make it possible to deliver an array of differentiated joint offerings that are tailored to each organization's Zero Trust journey.

**Pilot and accelerated launch**. These services are designed to facilitate and accelerate Zero Trust adoption through a distinct blend of industry-leading cyber technology platforms, intellectual property (IP) assets, and professional services.

| Typical Deloitte Services | Associated Outcomes |
|---|---|
| • Define strategy and success criteria for pilot<br>• Identify in-scope use cases for Zero Trust pilot<br>• Leverage Palo Alto Networks product lines for rapid assessment to inform gap analysis and/or roadmap development, and to expose client to Prisma product functionality<br>• Define Zero Trust roadmap with Palo Alto Networks product adoption and/or expansion and integration opportunities<br>• Build and configure POC/pilot environment leveraging Palo Alto Networks' product stack | • Zero Trust solutioning workshop<br>• Current-state Zero Trust capability gap analysis<br>• Zero Trust adoption roadmap, including Palo Alto Networks' product mapping<br>• Prioritized use cases and requirements<br>• High-level target-state design, including mappings and integrations to Palo Alto Networks' product stack |

**Minimum secure cloud (MSC).** A cloud environment should be built with Zero Trust foundations in place to establish the capability to migrate workloads to the new secure cloud environment.

| Typical Deloitte Services | Associated Outcomes |
|---|---|
| • Gather requirements and define target state based on Deloitte's Zero Trust framework<br>• Define cloud service provider (CSP) environment and high-level architecture<br>• Develop target-state design for MSC, aligned to Zero Trust principles<br>• Build and configure CSP environment and Palo Alto Networks components to facilitate migration of targeted applications and/or workloads, data, users, etc.<br>• Select and onboard the first set of MSC applications and services, test, tune, and go live | • Use case and MSC platform design guide<br>• Technical requirement specifications<br>• Low-level design<br>• Handover of live operating environment<br>• Postproduction support |

**Phased implementation rollout and use case expansion.** Focuses on the next steps after a successful pilot and/or MSC rollout by expanding the implementation roadmap aligned to the desired final state.

| Typical Deloitte Services | Associated Outcomes |
|---|---|
| • Identify and prioritize expanded use cases (both CSP and on premise) and align with corresponding Palo Alto Networks' technologies for enablement<br>• Develop implementation roadmap and/or milestones<br>• Build and configure capabilities to support expansion<br>• Enable and integrate new in-scope capabilities and platforms into telemetry and analytics, and automation and orchestration platforms (e.g., Cortex)<br>• Enable and integrate new in-scope capabilities into future Palo Alto Networks product releases | • Use case and MSC platform design guide<br>• Technical requirement specifications<br>• Low-level design<br>• Handover of live operating environment<br>• Postproduction support |

**Zero Trust as a Service (ZTaaS).** Zero Trust, available as a managed service:

| Typical Deloitte Services | Associated Outcomes |
|---|---|
| • Leverage existing Deloitte managed services with the integration of additional Palo Alto Networks products to expand managed Zero Trust capabilities<br>• Stand up and operate client-specific target-state environment that is architected to align to Zero Trust guiding principles including in multi-cloud deployment scenarios | • Service definition<br>• Operations guide(s)<br>• Service level agreements (SLAs)<br>• Metrics and reporting |

# Trust in your ability to change

Implementing a Zero Trust model is hardly a three-month sprint. Still, companies that had begun adopting the Zero Trust model amid the COVID-19 pandemic in 2020 clung to it as a priority. In a Deloitte poll published in September 2020, 37.4% of respondents at organizations adopting Zero Trust said COVID-19 had accelerated their journeys, with 35.2% reporting that it had not slowed their efforts.[1]

Similar to broader transformation efforts, a Zero Trust journey may also take years to fully optimize, and could face similar impediments, such as resistance to change and analysis paralysis. As with many transformation initiatives, it is useful to achieve and showcase quick wins. These can include reducing costs by requiring that Zero Trust principles and security requirements be part of strategic IT and application transformation programs, including cloud migrations, network transformations, virtualization and serverless initiatives, and digital transformation initiatives.

The path to Zero Trust may feel daunting—even never-ending—which may discourage some organizations from getting started. However, the journey is just as important as the destination. With every step, organizations embracing Zero Trust adoption move further out of reach of lurking cyber attackers that may be eager to infiltrate their enterprise.

1. Deloitte, "Zero Trust cybersecurity: Never trust, always verify," September 2, 2020.

# Authors

**Andrew Rafla**
Principal
Risk & Financial Advisory
Deloitte & Touche LLP
arafla@deloitte.com

**Henry Li**
Managing Director
Risk & Financial Advisory
Deloitte & Touche LLP
henli@deloitte.com

**Ferenc Spala**
Specialist Leader
Risk & Financial Advisory
Deloitte & Touche LLP
fspala@deloitte.com

# Palo Alto Networks Alliance Leaders

**Kieran Norton**
Principal
US Cyber & Strategic Risk
Deloitte & Touche LLP
kinorton@deloitte.com

**Jane Chung**
Managing Director
US Cyber & Strategic Risk
Deloitte & Touche LLP
jachung@deloitte.com

Deloitte.

## About this publication

This publication contains general information only and Deloitte and Palo Alto Networks are not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte and Palo Alto Networks shall not be responsible for any loss sustained by any person who relies on this publication.

Product names mentioned in this publication are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this publication.

## About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.