A Practical Guide to Adopting Zero Trust in the SOC

Mature Your Zero Trust Strategy with Visibility into Critical Assets and Continuous Monitoring

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

Table of Contents

Introduction

The purview of the SOC has traditionally been focused on the perimeter, yet perimeter-centric strategies for security don't work anymore. The location of security infrastructure and systems extends beyond the traditional network perimeter to the public/private cloud and to every connected device or endpoint. Each of these requires some level of visibility and control over respective activity and behavior to prevent compromises and breaches. With the advent of embedded systems, IoT, and (nearly) ubiquitous wireless connectivity, our collective attack surface knows no bounds. As such, our trust decisions need to be reevaluated to secure modern enterprise ecosystems.

Factors fueling the expanding attack surface include the tsunami-like shift to remote and hybrid work launched by the pandemic, applications and data moving off-premises, cloud migration, and the continued growth of connected "smart" devices.

The concept of Zero Trust has been around for a while and was introduced by Forrester Research Analyst John Kindervag as a way of addressing threats that were circumventing traditional security models. This new model assumed previously "trusted" infrastructure was in fact compromised and potentially hostile and completely changed the way we think about IT security.

Generally speaking, Zero Trust relies on strict and continuous verification and validation for every person, device, or entity attempting to access network resources. The primary goal is to prevent successful breaches or corruption of data, applications, and business-critical systems from attacks and exploits.

The principles in Zero Trust are designed to reduce exposure and unauthorized access across the threat landscape. They've been thoughtfully developed to address the security of critical applications and sensitive data across an enterprise organization. These principles can easily become a part of any security strategy. Some of them include:

- **Multifactor authentication (MFA)**: A security protocol that requires individuals to be authenticated with more than one required security procedure. Typically, this is a combination of things one knows (e.g., passwords or a PIN); things one has, such as a fob, badge, etc.; and physical markers, such as biometrics, voice recognition, or fingerprints.

1. *The State of Hybrid Workforce Security*, Palo Alto Networks, August 25, 2021.

- **The policy of least privilege**: A policy in which end users are given the minimum amount of access they need to carry out their jobs. This helps reduce pathways and exposure to malware, attackers, and the chances of data exfiltration.
- **Microsegmentation**: A network is divided into separate segments or "secure zones" in data centers or in cloud deployments that require different access credentials to help isolate users, devices, and even workloads. This also helps limit lateral (or east-west) movement in internal networks if breached.

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

Zero Trust starts with verifying and validating your users' identities.

- All elements in your security architecture need to be able to block or allow access based on a verified user.
- You need to be able to verify user identity everywhere in your security architecture where you block and allow access.

Applying Zero Trust to applications requires a very similar approach.

- We need to address the identity of users trying to access applications.
- We also need to validate access between applications and workloads and validate the transaction to ensure the content related to applications is not malicious regardless of where these applications are in a private cloud, public cloud, etc.

Apply this same rigor when looking at infrastructure by validating the identity of users connecting to the infrastructure.

- IoT presents a significant security risk due to a lack of built-in security, so validating identity can secure all devices including IoT.
- Continuously discover and monitor all internet-connected assets and changes to existing assets to ensure full visibility of exposure risks.
- The same principles around "access" and "transactions" are also used.
- Apply least-privileged access and segmentation, as well as monitor the transactions of native and third-party supply chain infrastructure.
- Scan all content within the infrastructure for malicious activity and data theft.

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privileged user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, DevOps, and admins with strong authentication	Verify workload integrity	Enforce least-privileged access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to infrastructure	Identify all devices, including IoT	Least-privileged access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

Figure 1: Building a Zero Trust Enterprise requires a holistic approach across users, applications, and infrastructure

APPS ARE EVERYWHERE

80% of organizations have a hybrid cloud strategy,[2] and the average organization uses 110 SaaS apps.[3]

A Holistic Approach to Zero Trust: The Role of the SOC

Zero Trust is an ongoing process that requires continued evolution and refinement as each organization's business requirements change and subsequent technology shifts occur—especially during digital transformation initiatives. As such, continuous monitoring of the threat landscape should be a core requirement in any Zero Trust journey. Additionally, monitoring needs to go beyond any single security tool to broaden visibility. This makes the role of the SOC critical in the continued audit and maintenance of any Zero Trust security posture.

Specifically, the SOC plays a key role in:

- Continuous verification of Zero Trust policies
- Identifying gaps in your Zero Trust posture
- Limiting attack impact through automated enforcement
- Speeding investigation with automated threat data collection
- Continuous discovery of critical assets

As a case in point, an organization might implement MFA to correctly identify users and grant access to applications. The SecOps team can analyze a user's activity with machine learning, behavioral analytics, and human insights to detect insider abuse and disable a rogue user's account to mitigate damage. Even with a mature Zero Trust implementation that secures users, applications, and workloads, organizations still need a SOC for threat detection, response, automation, and risk management.

As a first step, organizations should establish the need for Zero Trust controls across users, applications, and infrastructure. The SOC has the best vantage point to ingest a broad set of security telemetry, perform continuous monitoring, and validate and verify Zero Trust controls.

SOC Transformation: A Critical Step in Modern Zero Trust

In order to implement Zero Trust, SOC teams have to be aggressive when tuning their detection alert settings, which results in higher alert volumes. Multiply this across the average 30 or more tools that the SOC uses, and it becomes

2. *2021 State of the Cloud Report*, Flexera, March 2021.
3. "Average number of SaaS apps used by organizations worldwide 2015-2020," Statista, February 16, 2022.

inevitable there will be a deluge of low-fidelity alerts and noise cluttering analysts' dashboards.

For instance, while we have tools that can create alerts, they require analysts to either confirm if an alert is legitimate or close it as a false positive. As a result, SOC analysts can spend inordinate amounts of time investigating and validating a *single* alert. Plus, they may end up using numerous other—and often siloed—tools just to gather enough information to decide if an alert should be escalated.

These types of practices lack the useful context needed to assist in diagnosing problems, which can result in even more time chasing down related data and sifting through logs while hoping to correlate alerts that may or may not be related. With this combination of a lack of consolidation of suspicious activity, tool sprawl, and even gaps in security staffing, organizations need a better way forward to defend and protect their critical infrastructures.

Modern security threats are also evolving at a faster pace than security technologies. While well-funded threat actors are investing in new tools like machine learning, automation, and artificial intelligence, SOCs built around legacy security information and event management (SIEM) fail to provide a flexible and scalable solution that keeps pace with digital transformation, cloud initiatives, *and* advanced attack campaigns. Security analysts struggle to identify, manage, and remediate critical threats when faced with overwhelming challenges, such as noisy false positives, event storage (volume and cost), poor investigation workflows, the adoption of hybrid and multicloud architectures, and the proliferation of devices and endpoints.

Figure 2: Traditional approaches to security aren't working

Issues from legacy SOC environments can include:

- Lack of visibility and context
- Increased complexity of investigations
- Alert fatigue and "noise" from a high volume of low-fidelity alerts generated by security controls
- Lack of interoperability of systems
- Lack of automation and orchestration
- Inability to collect, process, and contextualize threat intelligence data

A Way Forward: Embracing AI, Automation, and Orchestration

When embarking on a Zero Trust journey, an organization first needs to define a unified security policy. This typically starts with identifying critical assets and deploying a Zero Trust architecture with strict, least-privileged access policies across users, applications, and infrastructure.

Automate Workflows

Security leaders must consider whether a tool requires a human to configure or run. Is an expert needed to interpret or triage the result? Are people needed for testing? Security leaders can identify repeatable, low-level tasks that can work with human decision-making to help accelerate incident investigations.

While advancements in machine learning and artificial intelligence hold great promise, retaining the human element for knowledge transfer in either direction is imperative to achieving optimal outcomes for a smooth SOC transformation. As automation capabilities begin to mature, humans can and should own smaller and smaller pieces of workflows.

One-to-Five-Year Prediction on Automation Takeaways

New SOC operations can start using automation from day one, while more established organizations will have to retool and figure out where the move to automation can begin. This is a good three-year goal for an established organization: to move 50% of SOC work into the hands of automation. By year five, most SOC teams can be closer to 75% of activities automated yet continue to rely on human engineers for other activities like threat hunting.

With too many manual processes involved in security operations and incident response (IR), including numerous threat feeds to monitor, investing in automation capabilities such as those in a security orchestration, automation, and response (SOAR) solution can help orchestrate actions across the product stack for faster and more scalable IR.

Augment People with Machine Learning-Driven Intelligence

A key component to rearchitecting your SOC for Zero Trust is to ensure that security teams are leveraging machine learning to its full potential to augment and complement humans in security. Advanced analytics and AI can significantly reduce the amount of time that teams spend processing massive amounts of data in the enterprise to come up with critical security insights. By automatically detecting anomalous patterns across multiple data sources and automatically providing alerts with context, machine learning today can deliver on its promise of speeding up investigations and removing blind spots in the enterprise.

This works by training machine learning models, using them to detect patterns among and across the data, and then testing and refining the processes. Machine learning techniques can gather, integrate, and analyze data and interrogate the data to reduce the amount of time and knowledge needed for a human to perform these tasks. This also minimizes the challenge for a SOC team trying to find threat context and evidence across multiple layers of security that are embedded in data.

At a high level, machine learning techniques can:

- **Integrate**: Enable the data to tell a story about what is happening.

"We treat all the use cases the same in the most extreme way that we can. We don't give anyone any discounts just because we can assume something about them based on where they are, who they are, what they're trying to do, and so on. It turns out that that approach leads to a much simpler infrastructure because all of a sudden we don't need to buy different equipment or different solutions, different technology for securing users, depending on the situation or the securing applications based on the situation.

We can use one architecture, one system, one solution, one technology to secure all users all the time, wherever they are, whatever it is they're trying to do because we're going to run them through the same security checks and the same is true for securing applications and so on. ***That's the idea behind the Zero Trust Enterprise.****"*

—Nir Zuk, Co-Founder & CTO, Palo Alto Networks

- **Analyze**: Extract insights about the problem space and make predictions.
- **Automate**: Accelerate human decision-making; enrich incident data; and automate system-level action, workflows, and decision-making.

Achieve Comprehensive Zero Trust Faster with the Cortex Suite of Products

You can begin or accelerate your SOC journey by deploying the Cortex suite of products: Cortex XDR, Cortex XSOAR, and Cortex Xpanse, which seamlessly work together as a force multiplier across your security operations.

Better together, SOC teams can experience immediate high-level advantages:

Cortex XDR: Helps keep your organization safe from attack by delivering leading endpoint protection and enterprise-wide threat detection and response across network, cloud, endpoint, and virtually any data source. Patented behavioral and machine learning-based analytics pinpoint evasive threats and provide the intelligence you need to respond before a breach can occur.

Cortex XSOAR: Provides a single platform for SOC teams to manage all their incidents and threat intelligence feeds. With over 800+ prebuilt integrations for security tools used in the SOC and thousands of automated workflow scripts or playbooks, XSOAR enables SOC teams to be as aggressive as they need to be in their alert settings to implement Zero Trust, without worrying about the flow of alerts impacting analyst workload. As a result of using XSOAR to automate their SOC operational processes, a US electric utility company was able to reduce the number of cases by 30% within the first month of operations.

Cortex Xpanse: Offers a complete, accurate, and up-to-date inventory of an organization's global, internet-facing cloud assets and misconfigurations to continuously discover, evaluate, and mitigate risks on an external attack surface and evaluate supplier risk or assess the security of M&A targets.

While each product brings its own unique features and benefits, when combined, the positive results increase exponentially. These three products help lower the risk and impact of breaches with a comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities, bar none.

With end-to-end native integration and interoperability, SOC teams can close the loop on threats with continual synergies across the

Cortex ecosystem. All three products work in concert to monitor the threat landscape and provide the most robust detection, response, and investigation capabilities:

- Cortex XDR and Cortex Xpanse provide ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network, including remote workers.
- Cortex XDR can leverage Cortex XSOAR to automate malware investigation and response.
- Cortex Xpanse and Cortex XSOAR work together to automatically enrich incidents using Xpanse asset information and automate remediation of newly discovered assets.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive automated incident response workflows.

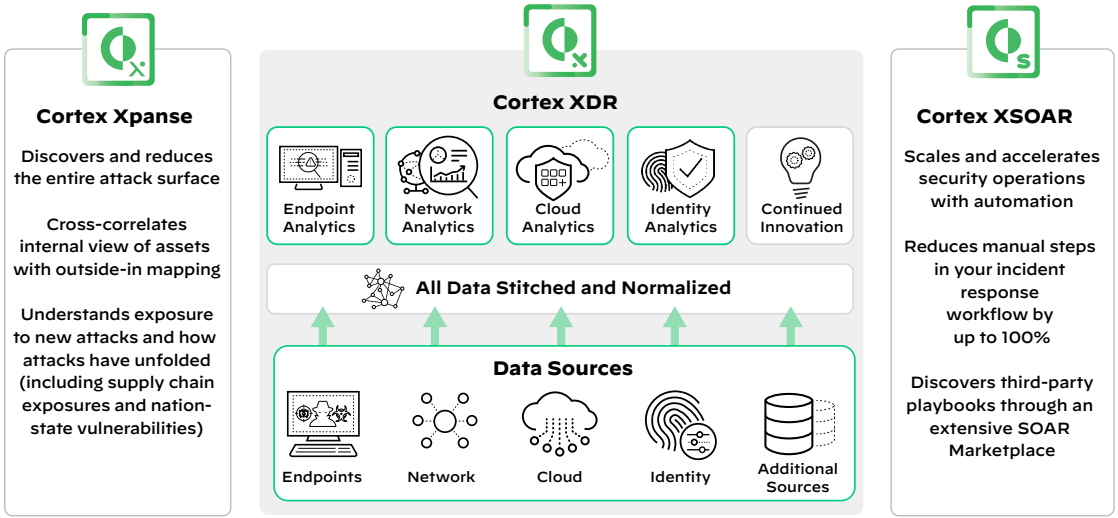

Figure 3: The Cortex suite of products

What's Next? Future-Forward with XSIAM

While Cortex products address key SOC requirements for visibility, protection, and automation, most organizations still depend on SIEM as a core component of SecOps. But SIEM products have failed to deliver on the promise of effective centralized threat detection and response, burdening analysts with endless alerts and manual processes. Security teams are in need of a central platform that incorporates and automates multiple security functions into a single foundational solution with visibility into enterprise-wide security data.

Extended security intelligence and automation management (XSIAM) is purpose-built to address this need, harnessing the power of AI-driven automation to radically improve security outcomes, and transform the manual SecOps model. By building an intelligent data foundation and automating unified SOC functions, XSIAM accelerates response, outpaces threats, and dramatically streamlines analyst activities.

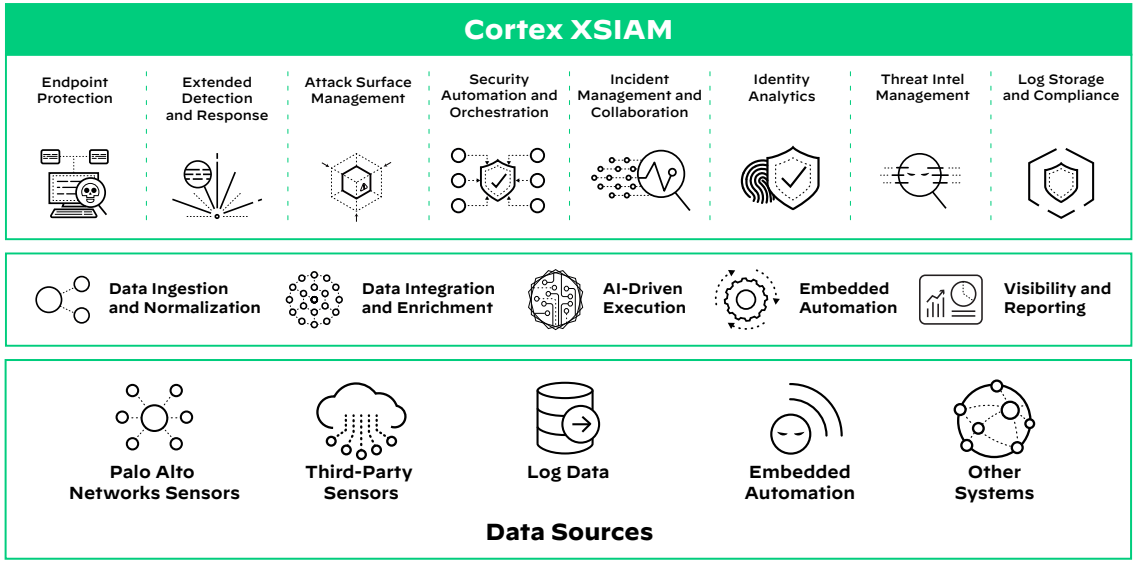

Figure 4: XSIAM is the AI-driven platform for the modern SOC

XSIAM is designed to be the center of SOC activity, replacing SIEM and specialty products by unifying broad functionality into a holistic and automated solution. XSIAM is revolutionary in the way it operates, using intelligent automation to transform the analyst-driven model of today's security products. With XSIAM, organizations can consolidate security data and tools, automate activities, and eliminate security gaps, delivering dramatically better protection and streamlined operations.

Powered and Protected by Cortex

Palo Alto Networks is committed to bringing the newest and most advanced and integrated security solutions to the market. We invite you to take a look at our solutions, reach out, and talk to us. We're here to help you learn more, do more, and secure more.

Visit our product pages for more information:

Cortex Xpanse
Cortex XSOAR
Cortex XDR
Cortex XSIAM

Visit our Cortex portfolio page.

More Zero Trust Resources

Digital transformation is accelerating with key shifts such as the expanding hybrid workforce and continued migration of applications and data to the cloud. As we make this transformation, InfoSec teams have the opportunity to adopt a modern Zero Trust approach that fits these significant shifts.

Enjoy our resources to learn more:

Read our blog, "Building the Zero Trust Enterprise: The Role of the SOC"
Download our "Architecting the Zero Trust Enterprise" whitepaper.

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

cortex_ebook_practical-guide-to-adopting-zero-trust_092022