paloalto NETWORKS | CORTEX

NOW FOR CLOUD

How to Plan for Tomorrow's SOC, Today

The Definitive Playbook for Transforming Security Operations with AI and Automation

Table of Contents

SOCs Are Challenged Like Never Before

Modern security threats are evolving at a faster pace than security technologies, while well-funded threat actors are investing in tools like machine learning (ML), automation, and artificial intelligence (AI). With over 750 million cloud-native applications in production[1] and a 66% increase in cloud-targeted attacks in the past year,[2] the challenge is particularly acute in cloud environments. SOCs built around legacy security information and event management (SIEM) weren't necessarily designed for the purpose of accurate detection, especially in dynamic cloud environments where attackers can exploit vulnerabilities, move laterally, and exfiltrate large amounts of data. As such, they aren't effective in leveraging ML for detection engineering that keeps pace with digital transformation, cloud initiatives, and advanced attack campaigns.

Challenges from legacy SOC environments can include:

- Lack of visibility and context, particularly across cloud workloads, control plane, and configurations.
- Increased complexity of investigations requiring manual correlation of events to stitch the full attack together.
- Inability to collect, process, and contextualize threat intelligence data across cloud and traditional environments.
- Alert fatigue and noise from a high volume of low-fidelity alerts across disparate cloud environments, both public and private.
- Lack of automation and orchestration for cloud-specific incident response.
- SOC is often disconnected from cloud teams and lacks runtime protection for cloud workloads.
- Inadequate real-time protection against container escapes, lateral movement, and privilege escalation in cloud environments.

These challenges underscore the critical need for an integrated security platform approach. Organizations can no longer afford to manage cloud security and SOC operations in isolation. A unified platform that combines cloud workload protection, threat detection and response, automation, and AI-driven analytics can help break down these silos, providing the comprehensive visibility and control needed to defend against today's sophisticated attacks while improving operational efficiency.

1. "The future of application delivery starts with modernization," IBM Security, April 10, 2024.
2. *Unit 42 Incident Response Report*, Palo Alto Networks, February 20, 2024.

Why SOC Platformization Is No Longer Optional

Modern security operations centers require platformization because the speed and sophistication of cyberattacks have created a critical mismatch between threat actors' capabilities and traditional fragmented security approaches. When security tools are stitched together from multiple vendors, each with its own management plane and data silos, organizations struggle to detect and respond to threats quickly enough. Platformization addresses this by unifying security capabilities under a single integrated platform with common data and management, enabling AI-powered automation to reduce response times to hours while eliminating the complexity and gaps created by point solutions.

A platform approach transforms security operations by providing:

Unified Visibility and Control

When powered by comprehensive data, AI, and automation, integrated platforms deliver:

- **Proactive application security**: Context-aware guardrails identify and prioritize vulnerabilities throughout development, reducing risk before code reaches production.
- **AI-powered runtime prevention**: Tools like the Cortex XDR® agent provide unparalleled runtime protection, achieving perfect efficacy in MITRE ATT&CK testing.
- **Cloud detection and response (CDR)**: AI-driven prioritization and investigation rapidly detect and mitigate attacks, automating remediation across the enterprise.
- **Streamlined DevSecOps**: Integrated automation capabilities eliminate manual workflows and enable fixes across code, cloud posture, and runtime environments.
- **Generative AI-powered productivity**: GenAI copilots accelerate workflows, boosting collaboration and efficiency across teams.

Operational Efficiency at Scale

- An integrated platform delivers measurable operational benefits:
- 90% of alerts are resolved through automation, dramatically reducing manual workload.
- Lightning-fast threat detection and response: 10-second MTTD, 1-minute MTTR (respond).
- Efficient incident management with 5-hour MTTR (resolution).
- Significantly reduced training overhead as teams operate on a unified platform.

Business Acceleration

Most importantly, a unified platform empowers organizations to move faster with less risk:

- Accelerated deployment of new cloud services with comprehensive visibility and built-in security.
- Lower total cost of ownership by consolidating tools and reducing operational complexity.
- Enhanced productivity across application, cloud, and security teams, enabling secure innovation at scale.

5 Steps Toward Creating a Future-Forward SOC

Step 1: Transform the Manual SOC Model

The manual SOC model, whether delivered as on-premises software or to the cloud, was built around the human analyst. SOC analysts pored through hundreds of alerts per day, triaged manually by collecting contextual data, and spent the bulk of their time on false positives and manual effort. As alert volumes grew and data became harder to integrate from more systems, the human-led approach broke down. Instead, the modern way to scale an effective SOC is with automation as the foundation and with analysts working on a small set of high-risk incidents.

Just as flying a commercial airplane no longer requires constant, hands-on control by the pilot, an automation-led SOC handles the bulk of low-risk, repeated alerts, analysis tasks, and mitigations. This frees the analysts to work on urgent, high-impact incidents while the underlying platform autopilots the SOC to safe outcomes, learning from each activity and offering information and effective recommendations to the captain at the controls. This is our vision for the autonomous SOC.

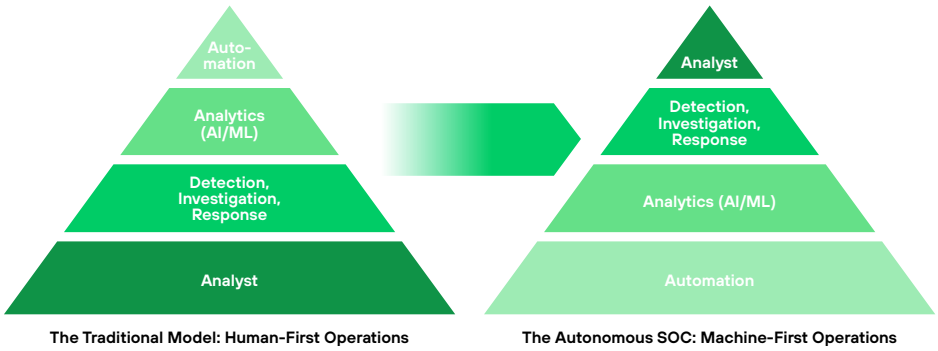

Figure 1: Human-first operations vs. machine-first operations

Ultimately, better data modeling and integration combined with automated analytics and detection ease the burden on security engineers who no longer need to build custom correlation rules to integrate data and detect threats. Unlike legacy security operations, the modern SOC leads with data science applied to massive datasets rather than only relying on human judgment and rules designed to catch yesterday's threats.

The modern SOC must be built with a different approach to solving modern threats by utilizing new architectures, data utilization, processes, and continuously updated knowledge of the threat landscape, such as:

- Broad and automated data integration, analysis, and triage.
- Unified workflows that enable analysts to be productive.
- Embedded intelligence and automated response that can block attacks with minimal analyst assistance.

Step 2: Auditing Your Environment Can Help Reduce the Security Risk of Tool Sprawl

Leonardo da Vinci once said, "Simplicity is the ultimate sophistication." Due to acquisitions, mergers, and a lack of standardization for similar security products, many organizations are burdened with a disparate swath of tools across their security stack. To put it simply, having too many tools results in too many issues. And with resources scattered across cloud environments and on-premises infrastructure, security teams struggle to maintain complete visibility of their attack surface. Effective security posture begins with a clear inventory: which cloud providers are connected, what services are being utilized from each CSP, and which assets have access to on-premises environments. Without this foundational understanding, organizations can't effectively map their true attack surface.

For some teams, tool sprawl can begin by deploying a point solution to fix a specific issue. Unfortunately, this piecemeal approach, combined with managing numerous agents, can (ironically) leave networks even more vulnerable, exposing gaps due to issues from a lack of interoperability and improper configurations across the various solutions.

One of the first steps an organization can take to reduce the security impact of tool sprawl is to audit protected systems and entities.

Identify precisely what is being protected and what is being prevented from happening. Is it intellectual property? Customers' personal information? By identifying as much as possible, whether software or physical assets, an organization can better prioritize protecting high-value and high-risk data.

Once an organization has a clear understanding of what is being protected, a logical next step is to identify solutions that can solve multiple needs if possible. As reported by Enterprise Strategy Group

(ESG) in a 2022 survey of 280 IT and cybersecurity professionals (from the US, Canada, Europe, Central/South America, Africa, Asia, and Australia), 22% report managing the complexity of too many disconnected point tools for cybersecurity a challenge, with 66% of respondents using 25 or fewer security products.[3] As things stand today, it's unnecessary to have sensors and enforcement happening across various tools, so organizations should consolidate where appropriate.

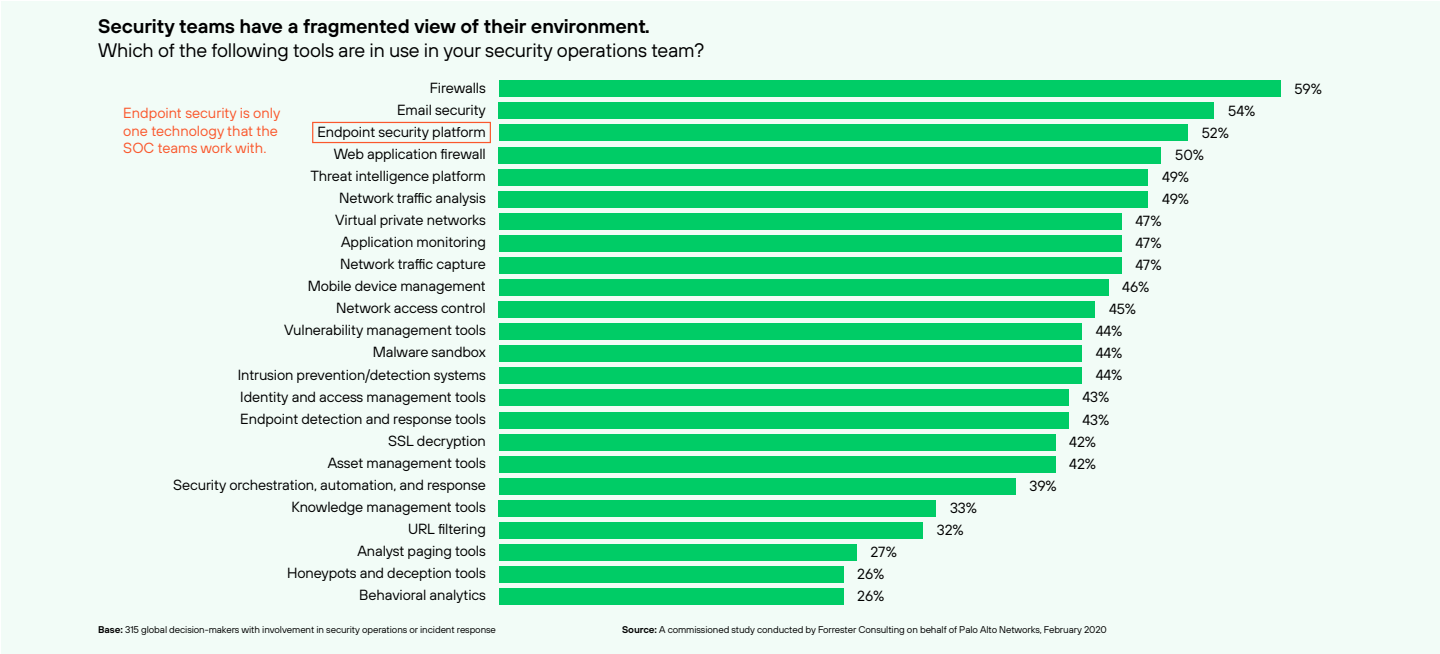

Figure 2: Tools security operations pros use, self-reported to Forrester[4]

Step 3: Automate Workflows

Security leaders must consider whether a tool requires a human to configure or run it. Must an expert interpret or triage the result? Are people needed to test things? 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 crucial to achieving optimal outcomes for a smooth SOC transformation.

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.

3. *Cybersecurity Process and Technology Survey*, ESG, June 2022.
4. *The State of Security Operations*, Forrester Consulting study commissioned by Palo Alto Networks, February 2020.

How Automation Makes Life Easier in the SOC (and Cloud)

- **Accelerate incident response**: Automate manual tasks to reduce response times and improve accuracy across both traditional and cloud threats, including container escapes and privilege escalation attempts.
- **Standardize processes**: Implement replicable workflows to standardize incident response and automate routine cloud configuration checks and compliance monitoring.
- **Unify security operations**: Enable orchestration of workflows across disparate security products and cloud tools, enabling unified incident response.
- **Increase productivity**: Free analysts from routine tasks for strategic work through automated correlation of cloud and traditional security events.
- **Maximize investments**: Coordinate across multiple products efficiently through automation, extracting more value from existing security tools.
- **Streamline incident handling**: Speed resolution through automated ticket management and stakeholder notification across key ITSM platforms and communication tools.
- **Strengthen cloud security**: Enable continuous monitoring, automated threat response, and streamlined collaboration between cloud and SOC teams.
- **Improve overall posture**: Reduce security and business risk through comprehensive automation across cloud and traditional environments.
- **Enable team collaboration**: Automate incident routing between SOC, CloudSecOps, and DevOps teams while facilitating real-time communication and coordinated response through integrated collaboration tools and automated incident follow-up and tracking.

Step 4: Augment People with ML-Driven Intelligence

A key component in modern SOC transformation is ensuring that security teams leverage both machine learning and artificial intelligence to augment and complement humans in security. ML and AI can significantly reduce the time teams spend processing massive amounts of data to generate critical security insights. By automatically detecting anomalous patterns across multiple data sources and providing alerts with context, ML and AI today deliver on their promise of speeding investigations and removing blind spots in the enterprise.

This works by training ML models, using them to detect patterns among and across the data, and then testing and refining the processes. ML and AI techniques can gather, integrate, and analyze data and interrogate it 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.

ML techniques can be used to read the digital markers from devices, such as desktop computers, mail servers, or file servers, and then learn the behavior of different types of devices and detect anomalous behavior. For example, an ML model establishes behavioral baselines for applications in your environment by learning their normal patterns across multiple dimensions:

- File system interactions (which files and directories are typically accessed)
- Process behavior (expected parent-child relationships and process trees)
- Network communications (usual connection patterns, protocols, and destinations)
- Resource utilization (standard CPU, memory, and I/O patterns)

When the ML model detects anomalous behavior—such as an application accessing unauthorized files, spawning unusual processes, or establishing unexpected network connections—it can trigger alerts for potential security incidents. This approach is particularly effective at identifying living-off-the-land attacks where malicious actors hijack legitimate applications.

Precision AI® by Palo Alto Networks takes this capability further by combining multiple AI approaches into a unified system. It leverages machine learning for accurate prevention and prediction, deep learning to build real-time predictive models, and generative AI to simplify user experience through human-readable insights. This proprietary system helps security teams trust AI outcomes by using rich data and security-specific models to automate detection, prevention, and remediation with unprecedented accuracy while reducing false positives.

At a high level, ML and AI techniques can:

- **Integrate**: Enable the data to tell a story about what is happening.
- **Analyze**: Extract insights about the problem space and make predictions.
- **Automate**: Accelerate human decision-making and automate system-level action, workflows, and decision-making.
- **Learn**: Continuously adapt to new threats and attack patterns.
- **Enhance**: Augment human expertise to improve security outcomes.

Step 5: Optimize Security Teams

Beyond investing in security solutions and tools, the most important factor in any successful SOC remains the human element. While machine learning and automation will undoubtedly improve outcomes like response times, accuracy, and remediation overall—especially for low-level, repetitive tasks—attracting, training, and retaining security personnel, including engineers, analysts, and architects, must be baked into any cohesive SOC transformation strategy. By leveraging automation technologies, organizations can be more efficient at protecting the business.

According to the Bureau of Labor Statistics, the number of individuals employed within the cybersecurity sector is slated to grow by 31% between 2019 and 2029.[5] Additionally, the National Center for Education Statistics (NCES) shows the number of new cybersecurity programs has increased by 33%, while cybersecurity job postings have grown by 94% in the past six years.[6]

In concert with filling critical roles is adopting cybersecurity awareness training to ensure employees, contractors, and in some cases, partners are well versed in helping to prevent breaches. Stolen credentials, phishing attacks, and social engineering require people to execute campaigns so building a cybersavvy team holds long-term value. As the noted cryptographer and computer security professional Bruce Schneier says, "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

Cortex: The Bedrock for SOC Transformation

Laying a foundation to build a resilient and effective SOC starts with taking the above five steps and considering the following five technology "keys" to help inform your security operations strategy.

Key 1: Power Up Your Risk Management Function by Understanding Your Attack Surface

One foundational component of a SOC transformation is a strong risk management function. Identifying what you're trying to protect and prevent from being attacked is a logical first step in a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with identification, you can prioritize what's at risk and analyze what it would take to mitigate each risk.

5. *Occupational Outlook Handbook, Information Security Analysts*, U.S. Bureau of Labor Statistics, April 9, 2021.
6. *CISO Benchmark Study*, Cisco, March 2019.

A critical step to informing any risk management function is to have a clear understanding of one's attack surface—you can't protect what you can't see.

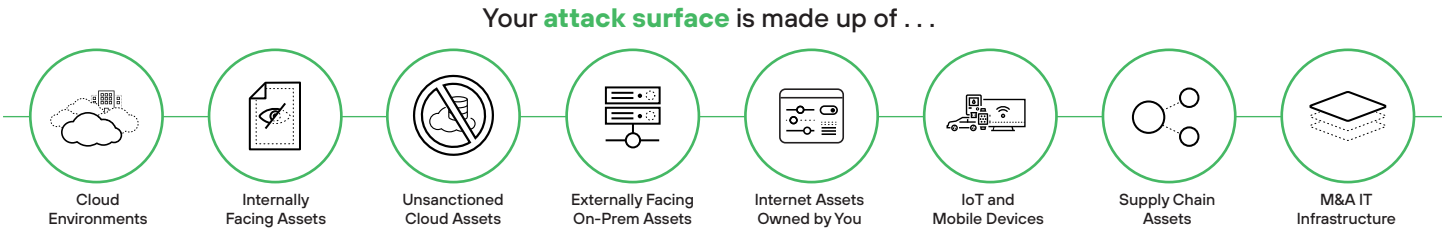

Figure 3: Components of the attack surface

Yet, whether one chooses to deploy attack surface management (ASM) solutions or perform proactive assessments like penetration testing or vulnerability scanning, there's clearly a need to identify both product and operational requirements to determine the best fit. Both product and operational requirements can include functionality, feature, capability, and evaluation criteria to help summarize the features and capabilities you might expect in an ASM solution or tool.

In the *Cortex Xpanse Attack Surface Threat Report*, we outlined some key findings from our research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, the Cortex Xpanse® research team monitored scans of 50 million IP addresses associated with 50 global enterprises to understand how quickly adversaries can identify vulnerable systems for fast exploitation.

One interesting discovery was that nearly one in three vulnerabilities they uncovered were due to issues with the Remote Desktop Protocol (RDP),[7] which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new work-from-home protocols due to the COVID-19 pandemic. Other findings include:

- **Adversaries work nonstop**: In a game of never-ending "cat and mouse," threat actors were found to conduct a new scan once every hour, whereas global enterprises can take weeks.[8]
- **Adversaries jump on new vulnerabilities**: Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVE) released between January and March and launched scans within 5 minutes of the Microsoft Exchange Server zero-day security update.[9]
- **Vulnerable systems abound**: On average, global enterprises present a new serious exposure every 12 hours or twice daily. Issues included insecure remote access (RDP, Telnet, SNMP, VNC, etc.), database servers, and exposures to zero-day vulnerabilities in products such as Microsoft Exchange Server and F5 load balancers.[10]
- **Cloud comprised the most critical security concerns**: Cloud footprints were responsible for 79% of the most critical security issues found in global enterprises, reiterating the inherent risk of cloud-hosted/based services, compared to 21% for on-premises.[11]

Takeaway: Advancements in scanning technologies allow attackers to locate attack vectors quickly and easily, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution can provide a continuous assessment of an organization's external attack surface.

7. *2021 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, May 2021.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid.

Key 2: SOAR—Orchestrating Across Your Product Stack for Efficient Incident Response

When it comes to SOAR, solutions running a playbook outlining automated response workflows may come to mind, yet an effective SOAR strategy goes beyond just leveraging automation to streamline and eliminate manual tasks. Workflows can be orchestrated via integrations with other technologies and automated to achieve desired outcomes, such as:

- Incident alert triage
- Threat qualification
- Incident response
- Threat intel curation and management
- Compliance monitoring and management

According to the SANs State of Automation in Security Operations survey, phishing vulnerability response and data enrichment are popular targets for automation, with most respondents targeting 50–75% of their incident response to be handled via automation.[12] A comprehensive SOAR solution that addresses all aspects of incident management needs to provide comprehensive out-of-the-box integrations of commonly used tools in the SOC, best practice playbooks to aid in automating workflows, as well as integrated case management and real-time collaboration to enable cross-team incident investigation.

Last but not least, the ability to serve as a central repository for threat intelligence (both internal and external) enables automated correlation between indicators, incidents, and intel so security analysts and incident responders get enriched strategic intelligence for added insight into threat actors and attack techniques.

SOAR solutions continue to build toward becoming the control plane for the modern SOC environment, potentially becoming the control plane for various security operations functions. To achieve this end, SOAR platforms are starting to integrate threat intelligence, vulnerability management, cloud security, network security, etc., directly into the platform and expanding automation to use cases beyond the SOC. Leading security vendors are also embedding SOAR and incident management capabilities into their products, which are preprogrammed and optimized for the specific technology.

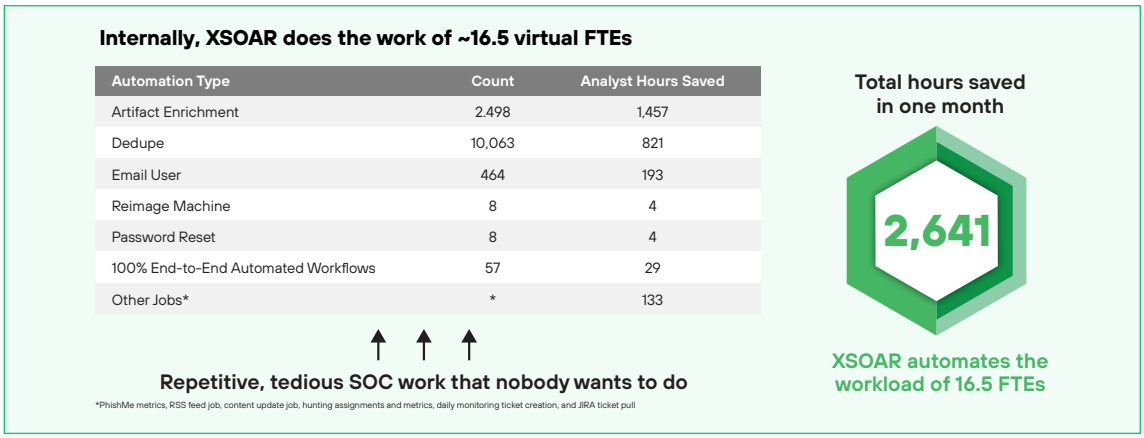

Figure 4: Top automation time savers

Takeaway: At the heart of any SOAR solution is the ability to set priorities and build streamlined workflows for security events that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes, as well as provide a single platform for minimizing complex incident investigations, orchestrating across the entire product stack of a SOC.

12. Mark Orlando, *The State of Automation in Security Operation: A SANS Survey*, SANS Institute, June 13, 2024.

Key 3: XDR Fills the Detection and Response Void

The term "XDR," short for "extended detection and response," was coined by Nir Zuk, CTO and co-founder of Palo Alto Networks, in 2018. The basic reason for creating XDR was to stop attacks more efficiently, detect attacker techniques and tactics that can't be prevented, and help SOC teams better respond to threats that require investigation. The approach is to pull disparate telemetry together from multiple (and in some cases, complementary) sources, including EDR, network firewalls, identity providers, cloud infrastructure, and other extended sources to enrich attack context.

XDR lets security teams stop attacks more efficiently and effectively by consolidating siloed tools, streamlining processes, and providing greater visibility for threat detection and investigations. Teams can eliminate blind spots, reduce investigation times, and ultimately improve security outcomes using XDR. And with XDR's ability to stop attack sequences at critical stages such as execution—before persistence techniques result in broader lateral damage—security teams finally have a solution to "head attacks off at the pass."

Factors driving the adoption of XDR include endpoint security transformation, simplified visualization of complex attacks across the attack lifecycle, response automation, advanced analytics, and machine learning-based threat detection. XDR is becoming the foundation of security operations' modernization, providing superior endpoint protection, more robust analytics, and faster response capabilities—especially when one considers that organizations may use up to 45 security tools on average, while responding to an incident requires coordination across approximately 19 tools.[13]

XDR combines alert integration, normalization, and correlation that can be expanded with SOAR for automated investigation and remediation.

XDR Fills the Detection and Response Void

Up until XDR, correlating telemetry from endpoints with other event data was an exercise in sifting through large volumes of data in a SIEM. Stitching disparate events together is resource-intensive and dependent on seasoned analysts to determine which data sources to use and writing detection rules to uncover threats. As a result, SOC teams find themselves spending significant time analyzing data manually, writing rules, and subsequently verifying the accuracy of every alert. All of this effort takes away from the time needed to investigate real attacks that could be progressing to a breach at any moment.

Impeded by this nonstop version of security whack-a-mole and an increase in attack sophistication and frequency, forward-thinking security organizations are taking advantage of all the efficiencies gained from an XDR approach to security architecture. These organizations are seeing their mean time to detect (MTTD) transform from a manual effort that takes days—to AI-driven analytic detections in real time, shifting the advantage from adversary to defender.

Viewing threats through the lens of the endpoint is not enough. Organizations must unify endpoints with cloud and network data through a single source of truth powered by AI and analytics.

Takeaway: Cortex XDR can be utilized in multiple permutations of SecOps architecture, providing enterprise threat detection and response with prevention capabilities that start with EDR/EPP as a baseline. From XDR, the SOC can advance to Cortex XSIAM®, which converges XDR, CDR, SOAR, SIEM, attack surface management, and more into a single AI-driven security operations platform.

13. *2020 Cyber Resilient Organization Report*, IBM Security, June 2020.

Key 4: Securing the Cloud—Bridging the Gap Between Cloud Security and SOC Operations

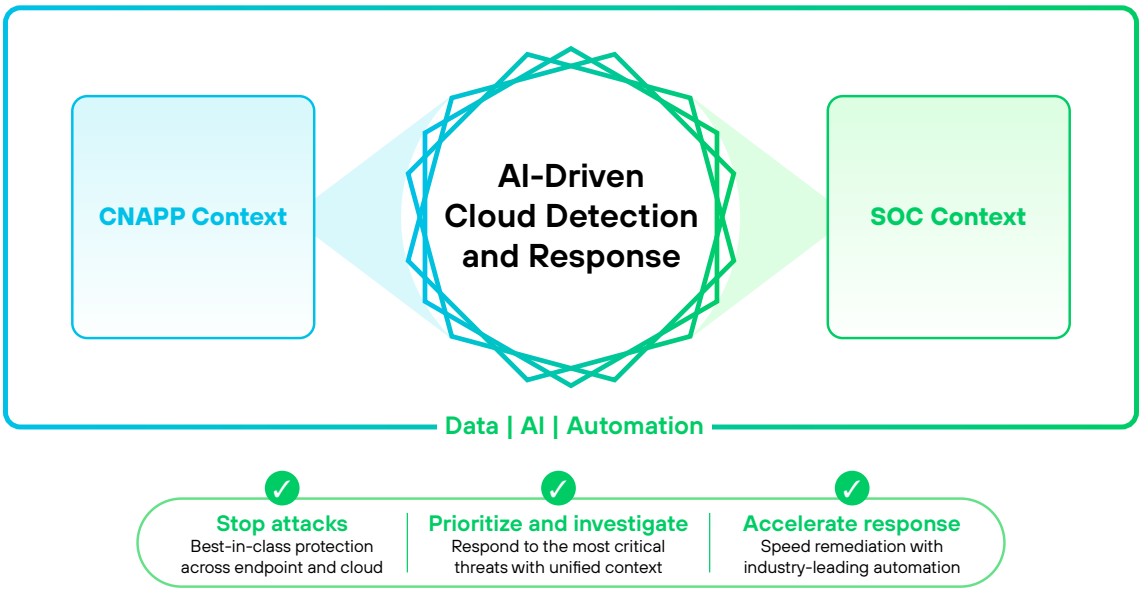

Figure 5: Bringing cloud security into the greater security ecosystem with AI-driven CDR for best-of-breed protection

Today's security teams often operate in silos, with cloud security and SecOps teams working on separate platforms with disconnected workflows. This siloed approach creates dangerous delays in incident response and leaves organizations vulnerable to sophisticated cloud attacks. Traditional security tools lack visibility into cloud-native services and configurations, while the scale and dynamic nature of cloud environments generate thousands of alerts that teams struggle to prioritize effectively.

A typical cloud attack scenario illustrates these challenges: An attacker exploits a zero-day vulnerability in a container running a customer-facing website, uses container escape techniques to break out to the host system, then moves laterally through the infrastructure using stolen access tokens. Traditional solutions scatter indicators of compromise across data silos, causing security teams to miss the attack even when they detect these indicators.

SIEM tools monitor cloud logs but require security analysts to manually parse and correlate findings to make sense of the data. This scenario highlights why traditional approaches aren't enough—without real-time protection at runtime, attackers can move through cloud infrastructure long before teams detect their presence.

The growing challenges in cloud security include:

- Cloud workloads face increasing threats including container escapes, cryptomining, and reverse shell attacks.
- Traditional security tools miss up to 80% of cloud-native attack patterns due to lack of runtime visibility.[14]
- A 66% increase in cloud attacks in the past year.[15]
- Too many tools: 16+ is the average number of cloud security tools used by an organization, which adds more complexity with point products.[16]

14. *Unit 42 Attack Surface Threat Report*, Palo Alto Networks, September 14, 2023.
15. *2024 Unit 42 Incident Response Report*, Palo Alto Networks, February 20, 2024.
16. *The State of Cloud-Native Security Report*, Palo Alto Networks February 2024.

Cortex® Cloud Detection and Response (CDR) addresses these challenges through three core capabilities:

- **Prevention at runtime**: Leveraging the XDR agent with a 100% prevention score in the MITRE ATT&CK Evaluations[17]
- **Accelerated threat detection**: Using machine learning models trained for cloud-specific threats, reducing detection times from weeks to minutes
- **Automated response**: Implementing automated playbooks for high-confidence attack scenarios with immediate response actions

Takeaway: Cortex CDR transforms cloud security operations by providing real-time protection, AI-powered threat detection, and automated response capabilities—enabling organizations to secure their cloud environments while breaking down operational silos between security teams.

CDR combines cloud-native security with SOC operations through unified visibility, detection, and automated response across hybrid environments.

The Cortex platform enhances CDR's capabilities by integrating with XDR for comprehensive threat detection, XSOAR for automated response actions, and XSIAM for AI-driven analytics. This integration provides organizations with unprecedented visibility while reducing the complexity of managing multiple security solutions.

Key 5: XSIAM—The AI-Driven SOC Platform to Accelerate Response and Outpace Threats

The traditional SIEM-centered security operations model is no longer sufficient for today's threat landscape. While SIEM solutions have served security operations for years, their reliance on human-driven detection and manual remediation can't keep pace with modern cyberthreats that execute end-to-end attacks in hours.

Cortex XSIAM—extended security intelligence and automation management—reimagines security operations through an AI-first approach. It unifies critical security functions into a single platform:

- Single SOC UI simplifies and accelerates SOC analyst work
- Eliminates data silos through analytics with full context
- AI-powered defense to stop threats from days to minutes
- Automated operations to accelerate SOC workflows

XSIAM's proven impact is demonstrated in Palo Alto Networks own SOC, where it processes over a trillion monthly events while surfacing only the most critical incidents requiring human attention. XSIAM unifies best-in-class security operations functions, including SIEM, EDR, XDR, SOAR, CDR, ASM, UEBA, and TIP. XSIAM centralizes all of your security data and uses AI models designed specifically for security. With XSIAM, organizations can automate data integration, analysis, and response actions, enabling analysts to focus on the incidents that matter.

Takeaway: XSIAM represents a transformation from human-centric to AI-driven security operations. By consolidating multiple security functions and automating routine tasks, organizations can dramatically improve threat detection and response while reducing costs and complexity. The platform's success in production environments validates its ability to transform security operations for the AI era.

The Cortex Suite

Let's face it. We understand that most of our customers and potential customers don't want to be systems integrators. Nor do they want to be run ragged performing manual, repetitive tasks. An array of siloed tools requires massive time and costs to maintain. Numerous and disparate solutions can limit security outcomes by introducing complexity and fractured visibility for the analytics required by modern SOCs.

17. *MITRE ATT&CK Enterprise 2024 Evaluations*, MITRE, December 2024.

And while we can't add hours to the day, we can help our customers optimize, reduce TCO, and integrate with more third-party tools than any other security provider for next-level operations. Beyond these results, is the ability to equip security analysts with the tools they need to keep their data safe so they can focus more on what matters and less on mundane tasks.

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

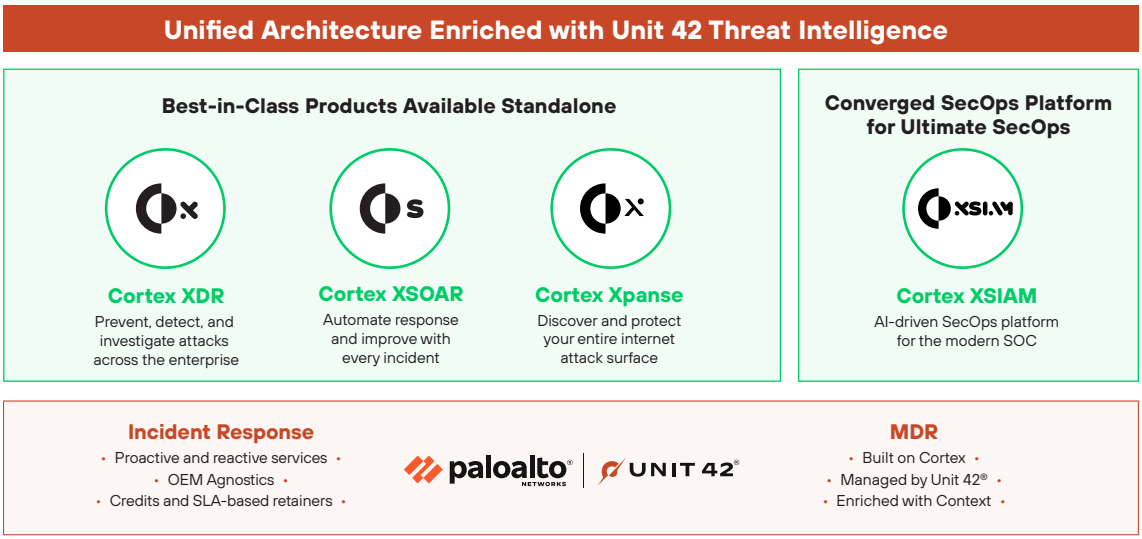

Figure 6: The Cortex solutions for flexibility and growth

The Cortex suite offers integrated solutions for a platform approach:

- **Cortex Xpanse**: Continuously monitors and secures your external attack surface by discovering and evaluating internet-facing assets and misconfigurations.
- **Cortex XSOAR**: Single platform for incident management with 900+ integration packs, enabling orchestrated security workflows and automated threat intelligence.
- **Cortex XDR**: Provides world-class EDR for Windows and Linux, automating evidence gathering and investigation timelines to speed response for analysts at all levels.
- **Cortex CDR**: Integrates with Cortex XDR for comprehensive threat detection, XSOAR for automated response actions, and XSIAM for AI-driven analytics.
- **Cortex XSIAM**: AI-driven platform that transforms SOC operations by unifying SIEM, EDR, XDR, SOAR, and other security functions into a single platform. Automates analysis and response, letting analysts focus on critical incidents.

Let us show you how Cortex can help you secure more while doing less.

Visit our product pages for more information:

Cortex Xpanse | Cortex XSOAR | Cortex XDR | Cortex CDR | Cortex XSIAM

Interested in scheduling a demo? Get started today.

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_ds_how-to-plan-for-tomorrows-soc-today_040125