Enabling a State-of-the-Art Healthcare SOC

Four Steps and Three Keys to Transform Healthcare Security Operations to Combat Advanced Attacks and Improve SOC Efficiencies

Table of Contents

Introduction: Healthcare Organizations Are Vulnerable Due to Legacy Systems and Outdated Software

During the global pandemic, a huge burden has been placed on healthcare organizations and their infrastructure. Health records and data have historically been attractive targets for bad actors, sold on the black market or dark web for money and/or further nefarious activity. Yet, with the recent attention placed on COVID-19 and the search for more information, attack methods like deploying ransomware are surging across the board.

Not only are healthcare organizations an attractive target during a health crisis, but they are also at an increased risk because of how they adapt and respond to radical changes in day-to-day operations. For instance, in some cases, the back-office staff is now working remotely from home offices, with a clear priority of adhering to compliance mandates such as HIPAA while keeping protected health information (PHI) safe.

In addition to risks associated with data compromise are risks to patient safety. Cyberattacks cause havoc on healthcare organizations that result in potential harm to patients from both the inability to provide the necessary care in a timely manner and the vulnerable connected medical devices that may negatively impact patients directly.

Protecting medical devices and the network they are connected to is of utmost importance in reducing risks to patient safety and privacy in today's connected health ecosystem. Also, with how data analytics is leveraged today to make important business and medical decisions, ensuring data integrity becomes a critical area for healthcare organizations as well.

Plus, newer technologies such as telehealth are being implemented and used more robustly due to shelter-in-place rules, requiring its own set of challenges as the medical community scales up to offer these nascent services. That said, telehealth—whose adoption was accelerated as a result of the pandemic—is here to stay and will continue to gain traction and acceptance to improve the patient experience, help expand coverage to rural areas, and improve hospital efficiency and outcomes.

> **"PHI is estimated to be worth 10–20 times the value of credit card data on the dark web and is sought after by criminals and nation-states alike."**
>
> — The Cybersecurity and Infrastructure Security Agency (CISA)

The April 2020 Healthcare and Cross-Sector Cybersecurity Report, authored by Lee Kim, the CSO of the Healthcare Information and Management Systems Society (HIMSS), offers this sobering introduction in their current report:

> *"Cybercriminals, state-sponsored actors, and others are now investing significant effort and time with COVID-19 phishing campaigns using means such as text messages, e-mails, social media messages, phishing websites, and advertisements. Both consumers and businesses of all types are targets.*
>
> *"The objective of these phishing campaigns varies, such as money (business e-mail compromise), stealing (including in regard to email accounts and popular web conferencing platforms), and more.*
>
> *"While phishing remains a significant threat during the pandemic, criminals are also heavily engaged in financial fraud (including economic stimulus payments), intellectual property theft, distributed denial of service campaigns, and more. In summary, criminals are capitalizing on current events and are preying on fear and concern of individuals with respect to the pandemic."*[1]

Not only are healthcare entities at risk due to increased activity and exposure across the threat landscape, but they are also vulnerable due to the use of legacy systems and software. Additionally, the healthcare industry is challenged with managing countless tools keeping systems compliant and up-to-date to avoid risk exposure or, worse, compliance violations.

Although most healthcare organizations have been able to meet the increased capacity and bandwidth demands as a result of pandemic, many struggled to scale out security capabilities and adapt to a quickly changing business environment.

Healthcare, as with other industries, also suffers from the problem of security tool sprawl. This problem is amplified by how the industry has traditionally taken a "best-of-breed" approach when it comes to security tool procurement. This has led to added complexity and efforts required to optimize and maintain efficient security operations.

According to a report from Palo Alto Networks and Unit 42 that checked 1.2 million devices used in thousands of healthcare organizations in the US, over 83% of healthcare systems run on outdated software, with 56% of devices operating on Windows 7.[2] In January 2020, Microsoft stopped supporting

1. Lee Kim, *HIMSS Healthcare and Cross-Sector Cybersecurity Report*, HIMSS, May 1, 2020, https://www.himss.org/resources/himss-healthcare-and-cross-sector-cybersecurity-report.
2. *2020 Unit 42 IoT Threat Report*, Unit 42, March 10, 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

Windows 7. While systems using the older version may appear to run normally, users will not receive security updates or bug fixes, making the endpoints running on older versions even more vulnerable.

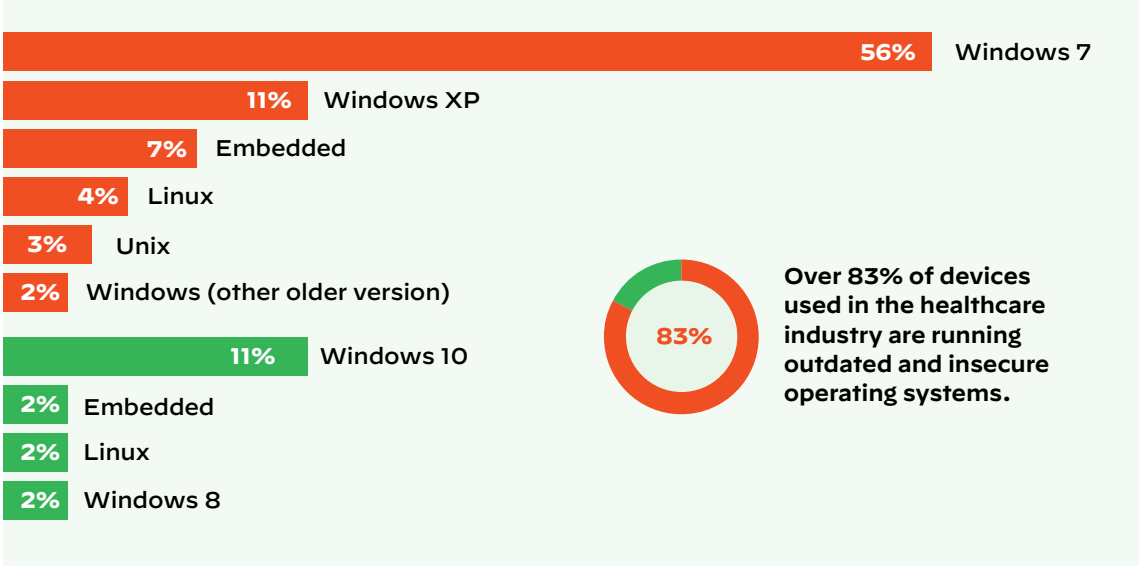


Figure 1: Operating systems used by the US healthcare system in 2020

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 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. Plus, the cost to maintain SIEMs extends beyond the initial investment, including infrastructure and personnel who have to continually tune and optimize SIEM functionality.

Challenges 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

"COVID-19 refocused security teams on the value of cloud-delivered security and operational tools that don't require a LAN connection to function, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and securing new digitization efforts to minimize person-to-person interactions."[3]

— Gartner

Unique Challenges for Healthcare

In 2020, the healthcare sector saw a jaw-dropping 41.4 million patient records breached in 758 incidents, fueled by a 42% increase in hacking according to the Protenus Breach Barometer, which analyzes breaches reported to the Department of Health and Human Services, the media, or other sources.[5]

"By 2024, 80% of all modern SOCs will leverage tools using machine learning, up from less than 10% today, but it won't significantly reduce industry-wide average attacker dwell time."[4]

— Gartner

3. Christy Pettey, "Gartner Top 9 Security and Risk Trends for 2020," Gartner, May 24, 2021, https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020.
4. Ibid.
5. Jessica Davis, "UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack," Health IT Security, October 5, 2020, https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack.

Telehealth and Telemedicine Get Ready for Prime Time

With the arrival of a global pandemic and the resultant stay-at-home orders instituted across the globe, physicians and medical teams turned to telemedicine and/or telehealth to communicate and stay connected to their patients. Having the ability for real-time, face-to-face audio/video communication allows patients and their doctors to connect from remote locations.

Telehealth is a bit different from telemedicine in that it refers to a broader scope of remote healthcare services, including non-clinical services, while telemedicine refers specifically to remote clinical services. While the American Medical Association outlines some areas where telemedicine can offer new ways to deliver care, these technologies can easily expand attack vectors, especially with the increased adoption of the cloud for both services and health data storage and processing. Today, telemedicine can provide:

- Real-time, audio-video communication tools (telehealth) that connect physicians and patients in different locations.
- Store-and-forward technologies that collect images and data to be transmitted and interpreted later.
- Remote patient-monitoring tools such as blood pressure monitors, Bluetooth-enabled digital scales and other wearable devices that can communicate biometric data for review (which may involve the use of mobile health apps).
- Verbal/Audio-only and virtual check-ins via patient portals, messaging technologies, etc.

Endpoints in Healthcare

Healthcare organizations are replete with endpoint devices. Besides the conventional computing devices, there are electrocardiogram and MRI machines, IV pumps, blood pressure monitors, and implanted defibrillators, to name a few. Most (if not all) of these operate with network and sometimes internet connectivity, making them that much more vulnerable to compromise. As such, security practitioners in healthcare face two main challenges: optimizing seamless and safe access to medical devices and protecting their critical data.

Case in point, in October 2021, the FDA issued their most serious type of recall (Class I) for all remote controllers used with a particular insulin pump citing significant security concerns. According to the FDA,

> *"An unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially record and replay the wireless communication between the remote and the insulin pump. Using specialized equipment, an unauthorized person could instruct the pump to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis, even death."*

Connected medical devices can make up 74% of the devices on a hospital's network, yet these devices are typically invisible in the eyes of traditional endpoint and network security solutions.[6] The reasons are twofold: first, connected medical devices that have gone through regulatory approval are generally sensitive to unaccounted-for voltage and performance fluctuations and simply cannot support a security agent installation. Second, they are often managed and secured by a different team in the hospital, such as clinical engineering, biomedical engineering, and/or medical technology management, compared with the rest of the data network where traditional IT management and security resides.[7]

As a result, challenges can result from the shared ownership wherein IT owns the connectivity, non-IT teams like Biomed or clinical engineering own the device lifecycle management, and the vendor/manufacturer owns patching, etc.

Beyond securing modern medical devices, healthcare orgs also often have to support many antiquated systems due to hospital devices and/or systems having a very long lifecycle, such as MRI machines, and general technical debt for IT. Technical debt in healthcare orgs often stems from hospital IT having inadequate testing or staging environments while being expected to keep unrealistic uptime requirements to make necessary changes and upgrades.

6. *The Forrester New Wave™: Connected Medical Device Security, Q2 2020, Forrester, June 11, 2020, https://www.forrester.com/report/The-Forrester-New-Wave-Connected-Medical-Device-Security-Q2-2020/RES157303.*
7. Ibid.

Four Steps Toward Creating a Future-Forward SOC

Step 1: Auditing Your Environment Can Help Reduce the Security Risks Associated with Tool Sprawl

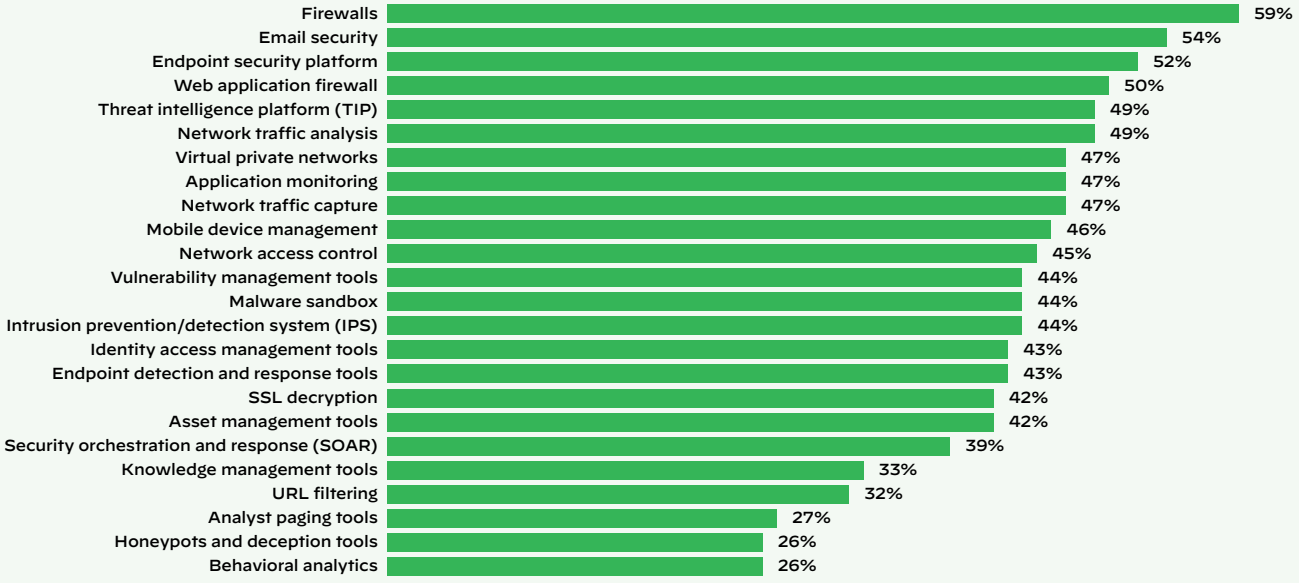
Leonardo da Vinci once said, "Simplicity is the ultimate sophistication." Due to acquisitions, mergers, and a lack of standardization for similar security products, many healthcare organizations are burdened with a disparate swath of tools across their security stack. To put it simply, having too many tools results in too many issues. And with resources both in cloud environments and on-premises, security IT teams are challenged with complete visibility of their attack surface.

Tool sprawl often begins by deploying a point solution to fix a specific issue in a specific department. For example, a radiology department elects to keep the radiologists home during the pandemic because they can access image files from anywhere as long as they have a secure internet connection and screen. 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? Patients' 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 ESG (Enterprise Strategy Group), in a 2019 survey of 406 IT and cybersecurity professionals (US and Canada), 42% of respondents used between 10 and 25 security tools, with another 26% using between 26 and 50 security tools.[8] As things stand today, it is unnecessary to have sensors and enforcement across various tools, so organizations should consolidate where appropriate.

Security teams have a fragmented view of their environment.
Which of the following tools are in use in your security operations team?



Base: 315 global decision-makers with involvement in security operations or incident response
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

Figure 2: Tools security operations pros use, self-reported to ESG

8. *ESG Research Report: The Rise of Cloud-Based Security Analytics and Operations Technologies*, ESG, December 23, 2019, https://research.esg-global.com/reportaction/Cloud-BasedSecurityAnalytics2019/Marketing.

Step 2: Automate Workflows

Security practitioners must consider whether a tool requires a human to configure or run. Must an expert interpret or triage the result? Are people needed to test things? Security teams 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 achieve 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 SOAR solution can help orchestrate actions across the product stack for faster and more scalable IR.

1–5 Year Prediction on Automation Takeaways

New SOC operations can start using automation from day one, while more established organizations will have to re-tool 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.

Manual Alert Investigations Plague Teams

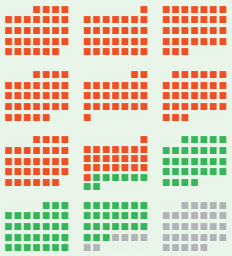
One area that is a continued sticking point for SOC teams is managing the number of alerts. Deploying solutions that can automate a range of tasks, decisions, and workflow associated with alert triage (alert prioritization/ranking, causal event correlation, and enrichment) can help streamline investigations.

Even after deploying a SIEM, or other solutions for better security insights and visibility, SOC teams are often flooded with low-fidelity alerts generated by their security controls. A 2019 survey of CISOs reported that "over 41% see more than 10,000 and that some claim to see more than 500,000 alerts daily."[9]

As one would expect, these types of numbers are not sustainable. The overwhelming number of false positives creating "noise" is often a result of a combination of poorly tuned algorithms, legacy detection tools, and/or configuration errors. These issues, combined with a lack of correlation from disparate tools and operations often done in silos, don't always enable the consolidation of event data. Even the use of SIEM or log management tools requires tuning or customization to accurately correlate alerts. What further muddies the waters is that even though tools may trigger alerts, they are not necessarily malicious. As such, many low-fidelity alerts go ignored.

329 days on average to identify and contain a data breach.

In their 2020 Cost of a Data Breach Report, IBM Security reported that healthcare ranks at the top (worst) when it comes to the average days it takes to identify (236 days) and contain (93 days) a data breach incident.[10]



Step 3: Augment People with ML-Driven Intelligence

A key component in a modern SOC transformation 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 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. ML 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.

Supervised machine learning techniques can be used to fingerprint devices, such as desktop computers, mail servers, or file servers, and then learn the behavior of different types of devices and detect anomalous behavior. The promise of machine learning is having the ability to determine causal inferences around what is happening in an environment and letting the *software* direct next steps instead of relying on human interaction. For instance, flagging "bad" actions based purely on behavior and interactions within the joined datasets, so it can then propagate a decision to the rest of the network with explicit instructions such as instructing an agent to contain it or a firewall not to communicate with it.

9. *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.
10. *Cost of a Data Breach Report*, 2020, IBM Security, July 28, 2021, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

At a high level, machine learning 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, automate system-level action, workflows, and decision-making.

Step 4: Optimize Security Teams

Beyond investing in security solutions and tools, the most important factor in any successful SOC will remain 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, needs to be baked into any cohesive SOC transformation strategy. By leveraging automation technologies, organizations can be more efficient at protecting the business at hand.

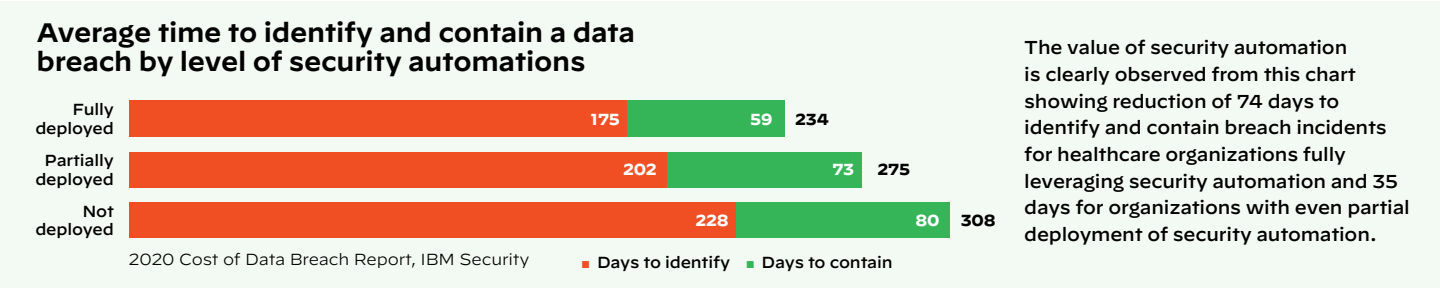


Figure 3: The value of security operation

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.[11] 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.[12]

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 cyber-savvy 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."

SOCs Can Come in Many Flavors

At Palo Alto Networks, our SOC story is highly optimized in that we actively chose to break away from the traditional four-tier SOC approach, ranging from Tier 1 analysts who monitor, prioritize, and investigate SIEM alerts to Tier 4 SOC managers responsible for recruitment, security strategy, and reporting to management. Taking more of a hybrid approach, the Palo Alto Networks SOC team follows this general philosophy:

- Staff the SOC with 80% of people who have previous SOC experience.
- Cross-train the SOC team in all domains, including alert triage, incident response, threat hunting, and others.
- Provide a well-funded annual training budget for all analysts.

Our rationale is that we can:

- Maintain a nimble team, able to pivot between responsibilities (and tiers).
- Support business continuity.
- Provide a more engaging atmosphere and reduce staff burnout.
- Promote an environment of continuous learning.
- Provide greater coverage with less staff by relying on the right technology to get the job done.

11. *Occupational Outlook Handbook*, U.S. Bureau of Labor Statistics, December 31, 2021, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
12. Integrated Postsecondary Education Data System (IPEDS), National Center for Education Statistics (NCES), last visited July 19, 2019, https://nces.ed.gov/ipeds/.

ASM, SOAR, and XDR: Together, the Bedrock for SOC Transformation

Laying a foundation to build a resilient and effective SOC starts with taking the above four steps and considering the following three 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 to have a strong continuous risk management function. Identifying the "things" you are trying to protect and what is exposed that allows it to be attacked is a logical segue into a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with identification, the ability to prioritize what's at risk makes it easier to analyze what it would take to actually mitigate each risk.

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.

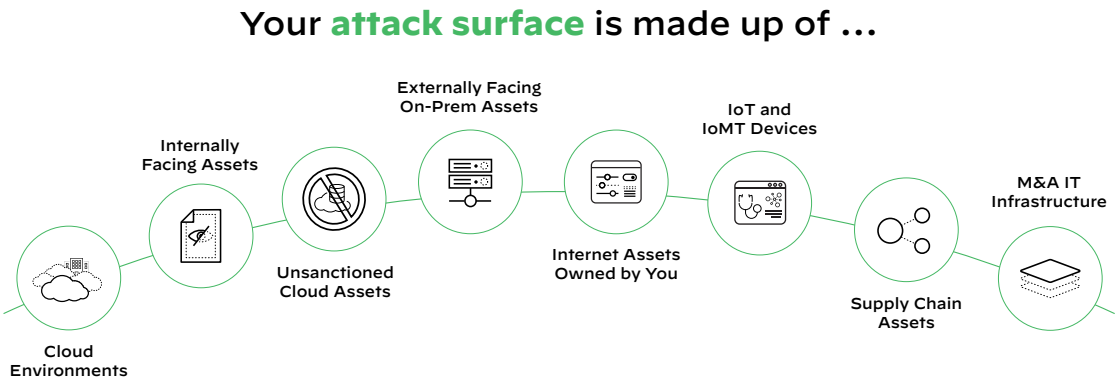


Figure 4: Components of your attack surface

Whether one chooses to deploy ASM solutions or perform proactive assessments like penetration testing or vulnerability scanning, what is clear is the need to identify both product and operational requirements to determine the best fit. Both product and operational requirements can include functionality, feature(s), capability, and evaluation criteria to help summarize the features and capabilities you might expect in an ASM solution or tool.

In the 2021 Cortex Xpanse Attack Surface Threat Report, Palo Alto Networks outlined some key findings from their research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, their 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 exposed assets they uncovered was due to unnecessary use of the Remote Desktop Protocol (RDP), which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new WFH protocols due to the COVID-19 pandemic. Other findings in this report include:[13]

- **Adversaries scan more frequently than companies.** 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.
- **Adversaries scan within 15 minutes of new vulnerabilities.** Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVEs) released between January and March and launched scans within five minutes of the Microsoft Exchange Server zero-day security update.

13. *2021 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, May 2021, https://start.paloaltonetworks.com/asm-report.

- **Exposed systems presented every 12 hours.** Cortex Xpanse discovered that, 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.
- **The cloud comprised almost 80% of the global enterprise 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.

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 is the best way to provide a continuous assessment of an organization's external attack surface in a cost-effective, repeatable, and scalable manner.

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

Gartner defines security orchestration, automation, and response (SOAR) as "solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format."[14] 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

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. 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.

How a Security Company Automates Security

Cortex XSOAR is leveraged within the Palo Alto Network SOC to minimize the repetitive and time-consuming tasks discussed in the above sections. Below is a snapshot of top automation "timesavers" for the month of February 2021.

Automation Type	Times Ran	Hours Saved
Artifact Enrichment	1,195	697.08
Dedupe	12,744	1,062
Email User	822	342.5
Password Reset	4	1.67
GCP Remediation	34	17
Other Jobs*	*	74.73

Repetitive, tedious SOC work that nobody wants to do

*PhishMe metrics, RSS feed job, content update job, hunting assignments and metrics, daily monitoring ticket creation, and JIRA ticket pull

XSOAR automates the workload of 13.72 FTEs

Figure 5: Top automation timesavers

14. Claudio Neiva, Craig Lawson, Toby Bussa, and Gorka Sadowski, *Market Guide for Security Orchestration, Automation and Response Solutions*, Gartner, 21 September 2020, https://www.gartner.com/en/documents/3990720-market-guide-for-security-orchestration-automation-and-r.

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, with the potential of becoming the control plane for various security operations functions. To achieve this end, SOAR solutions are starting to integrate threat intelligence and expanding automation to use cases beyond the SOC. Leading security vendors are also embedding SOAR and incident management capabilities in their products, which are preprogrammed and optimized for the specific technology.

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.

Key 3: XDR—The Next Logical Evolution of EDR

The product vision for "XDR," short for "extended detection and response," was created by Nir Zuk, CTO and co-founder of Palo Alto Networks, in 2018. The reason for creating XDR was to stop attacks more efficiently at the endpoint, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation. The vision is to automate many of the SOC analyst tasks, like writing detection logic; gathering evidence and building an incident from alerts; enriching the incident with identity and threat information; and pulling disparate telemetry together from multiple (and in some cases, complementary) sources, including EDR, network traffic analysis (NTA), user and entity behavior analytics (UEBA), and indicators of compromise (IoCs).

XDR lets security teams stop attacks more efficiently and effectively, eliminating blind spots, reducing investigation times, and ultimately improving security outcomes. 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 off attacks at the pass."

In the MITRE ATT&CK® Round 3 testing, the Cortex® XDR™ results against TTPs used by Carbanak and FIN7 blocked 100% of attacks in the protection evaluation on both Windows and Linux endpoints, achieved 97% visibility of attack techniques, which represents the best detection rates of any solution that also got a perfect protection score.[15] Of the attack techniques used, Cortex XDR identified 86% with an analytics detection, defined by MITRE as detections that provide additional context beyond telemetry.[16] Legacy endpoint vendors that only provide EDR/ESS/NG-AV solutions scored poorly in protection efficacy, visibility, and techniques detection.

As an evolution of existing threat detection and response solutions, XDR includes features such as:

- Integrated threat intelligence
- Network analysis
- Machine learning-based detection
- Investigation response orchestration
- Dynamic deployment
- Integrated sandbox (WildFire®) capabilities

Factors driving the adoption of XDR include simplified visualization of complex attacks across the kill chain, presenting information within the MITRE ATT&CK framework, more robust automation, advanced analytics, and machine learning.

XDR's value is gaining momentum by the need in the market for tighter third-party integrations, better 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.

15. "Detection and Protection Categories," ATT&CK Evaluations, MITRE Engenuity, April 20, 2021, https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/#detection-categories.
16. Ibid.

XDR Fills the Detection and Response Void

XDR combines the SIEM-like features of alert integration, normalization, and correlation with SOAR-like automated investigation and remediation.

Forrester defines XDR as:

The evolution of endpoint detection and response (EDR), which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management (IAM), cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.[17]

Up until XDR, correlating telemetry from endpoints with other event data was an exercise in sifting through large volumes of data and false positives cluttering analysts' dashboards. Stitching disparate events together is resource-intensive and dependent on seasoned analysts to determine if alert escalations are warranted. As a result, SOC teams could find themselves wasting time trying to verify the accuracy of low-fidelity alerts while compromising the time needed to investigate legitimate alerts.

Impeded by this nonstop version of security "whack-a-mole" and an increase in attack sophistication and frequency, forward-thinking security organizations are beginning to position themselves to take advantage of all the efficiencies gained from an XDR approach to security architecture.

According to Forrester analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[18] In a recent blog post, Mellen explains further:

> *"XDR will compete head to head with security analytics platforms (and SIEMs) for threat detection, investigation, response, and hunting. Security analytics platforms have over a decade of experience in data aggregation; they apply to these challenges but have yet to provide incident response capabilities that are sufficient at enterprise scale, forcing enterprises to prioritize alternate solutions. XDR is rising to fill that void through a distinctly different approach anchored in endpoint and optimization.*

"The core difference between XDR and the SIEM is that XDR detections remain anchored in endpoint detections, as opposed to taking the nebulous approach of applying security analytics to a large set of data. As XDR evolves, expect the vendor definition of endpoint to evolve as well based on where the attacker target is, regardless of if it takes the form of a laptop, workstation, mobile device, or the cloud."[19]

Takeaway: XDR can address SIEM use cases by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments.

Better Together, End to End: Cortex XDR, Cortex XSOAR, and Cortex Xpanse

Securing the endpoint is not enough. Organizations must unify it with cloud and network data through a single source of truth driven by comprehensive data and deep analytics.

Let's face it. We understand most of our customers and potential customers don't want to be systems integrators. Nor do they want to "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 to the analytics required by modern SOCs.

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 the security analyst with the tools they need to keep their data safe so they can focus more on what matters and less on mundane tasks.

Palo Alto Networks Security Operations Center Mission Statement: Defend our information and technology resources, intellectual property, and ability to operate by disrupting our adversary's ability to conduct their operations and achieve their desired outcomes.

17. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection And Response," Forrester, April 28, 2021, https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/.
18. Ibid.
19. Ibid.

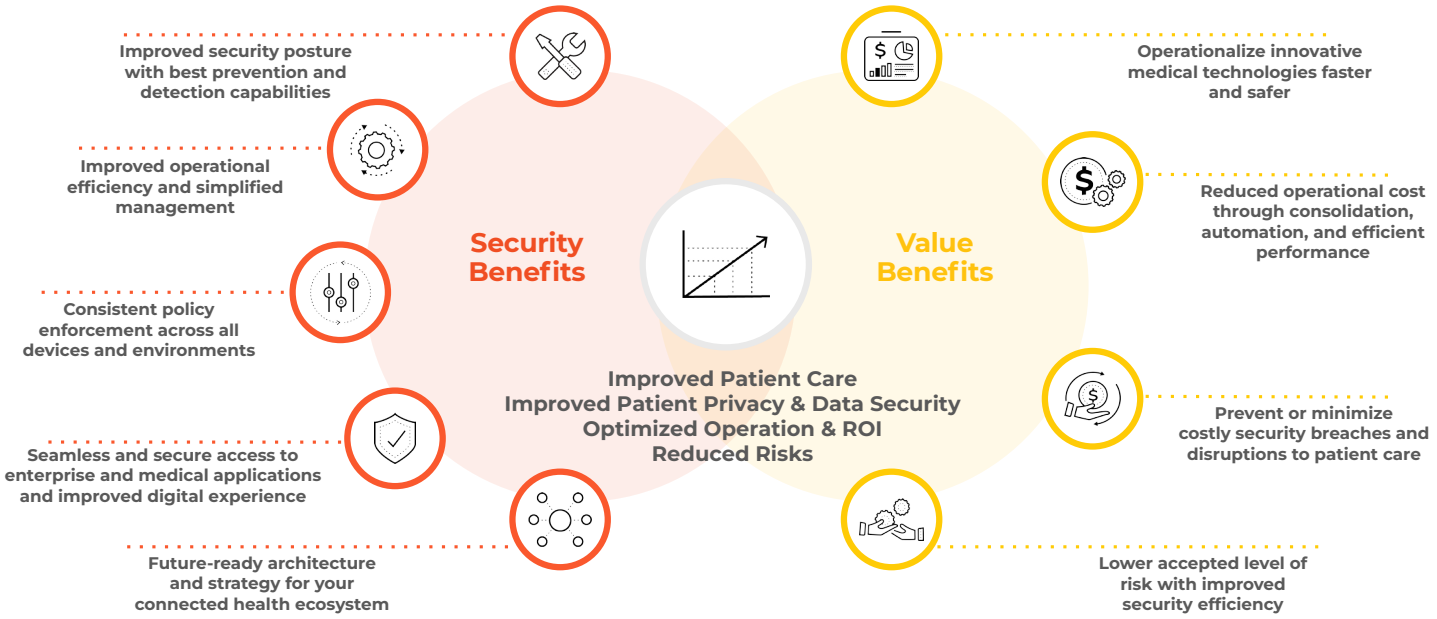


Figure 6: Clinical and IT outcomes achieved with our portfolio

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. Immediate high-level advantages include:

Cortex XDR: Cortex XDR can stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts with:

- AI-driven local analysis and ML-based behavioral analysis that is updated regularly
- A suite of endpoint protection features such as device control, host firewall and disk encryption
- A range of protection modules to protect against pre-execution and post-execution exploits

Once you prevent everything you can at the endpoint, Cortex provides detection and response that focuses on incidents by automating evidence gathering, grouping associated alerts, putting those alerts into a timeline, and revealing the root cause to speed triage and investigations for analysts of all skill levels.

Cortex XSOAR: Cortex XSOAR provides end-to-end incident and security operational process lifecycle management, helping companies accelerate security operations, reduce the time it takes to investigate and respond to security alerts and incidents and handle more incidents. Security teams of all sizes can orchestrate, automate, speed incident response and any security workflow or security process across their environment by leveraging the extensive vendor integration and 725+ pre-built integration content packs to maximize enterprise integration coverage.

> **"Threat actors do not wait till the afternoon. They will process malicious IPs at 3 a.m. on a Saturday. With the XSOAR automation, we are guaranteed we have IPs dropped almost in real time, 24 hours a day, 365 days a year."**
>
> —Security and Infrastructure Engineering Director, World-Class Cancer Hospital and Research Center

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

While each standalone product brings its own unique features and benefits, when combined, the positive results increase exponentially. These three products help lower the risk and impact from 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, security 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 prevention, detection, response, and investigation capabilities:

- Cortex XDR provides endpoint security and EDR to block sophisticated attacks using AI-driven analysis and a range of protection modules.
- Cortex XDR and Cortex Xpanse provide ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network.
- Cortex XDR and Cortex Xpanse leverage Cortex XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

Conclusion

Healthcare organizations face unique security challenges, including the need for context-based security tools for specialized medical devices and applications. As such, healthcare is a prime target for cybercriminals with rich sources of sensitive private information that can be monetized by threat actors or exploited to hold organizations at ransom, impacting patient care.

In addition, the industry suffers from its use of legacy systems with extremely long lifespans and vulnerable yet critical medical systems and devices that can directly impact patient safety. Adoption and expansion of new medical technologies and the connected health ecosystem are also expanding attack surfaces and complexities for healthcare organizations in managing enterprise cyber risks. Amidst these growing challenges, healthcare organizations need to adopt a robust cybersecurity strategy enabling integrated, programmatic approaches to security operations with optimum efficiency and efficacy. This balanced approach will enable healthcare organizations to provide improved patient experience throughout the continuum of care.

Powered and Protected by Cortex

Driven by innovation to protect and defend our customers' most valuable resources, Palo Alto Networks is committed to bringing the newest and most advanced security solutions to 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

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