XDR Myths, Misconceptions, and Musings

Insights from the Industry

It's a bird! It's a plane! It's a "new-ish" industry solution that's prone to numerous interpretations and definitions depending on whom you ask. In a nutshell, extended detection and response, or 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.

XDR entered the security lexicon in 2018 when Palo Alto Networks co-founder, Nir Zuk, introduced the concept during the Ignite USA conference keynote address. The idea was that the X could stand for "anything"—combining EDR, NDR, etc., to anything detection and response. The basic reason for creating XDR was to stop attacks more efficiently, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation.

The vision was to provide a seamless approach to 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).

While the majority of XDR solutions come primarily in two "flavors"—native (tightly aligned with other security tools in the vendor portfolio) or hybrid (relying on additional security tools from other vendors)—a lot of variation exists between vendor solutions claiming to offer XDR.

And, as one might expect, industry pundits offer a wide range of opinions about where we're at and where we're headed with XDR, most with valid arguments. Yet, rather than debate the nuances of individual offerings, nit-picking features and benefits, we thought we'd serve up a healthy discussion on the myths and misconceptions about XDR as we collectively strive to cut through the noise in the market.

Let's get started!

> **"There was no reliable, unbiased explanation for what XDR is and how it differs from a security analytics platform, which has led to confusion and disregard from clients who dismiss it as nothing more than yet another cybersecurity marketing buzzword."**[1]
>
> –Allie Mellen, Forrester Senior Analyst

Meet the Contributors

Eric Parizo, Managing Principal Analyst, Omdia Cyber

Eric supports Omdia's Cybersecurity Operations (SecOps) Intelligence Service research practice, guiding vendors, service providers, and enterprise clients. He provides thought-leading analysis on technologies, trends, and innovations in enterprise security operations centers (SOCs), and specifically the threat detection, investigation, and response (TDIR) lifecycle.

In addition to SecOps, he assists in supporting Omdia's Infrastructure Security Intelligence Service; contributes to Omdia Cyber's coverage of mergers, acquisitions, and other overarching market trends in North America; and oversees Omdia Cyber's social media efforts, including the Omdia research page on Dark Reading.

Eric has been covering, researching, or speaking on topics related to enterprise information technology for approximately 20 years. Prior to joining Omdia (formerly Ovum) in 2019, Eric spent four years at GlobalData (formerly Current Analysis), where his research focused on tracking and analyzing enterprise network security product segments, as well as top-tier enterprise security vendor technology and strategy.

Eric previously spent 15 years as a technology journalist and a multimedia editor at leading B2B publisher TechTarget, most recently serving as executive editor for the Security Media Group. He is a nine-time ASBPE award winner, the B2B publishing industry's most prestigious award for excellence.

Jon Oltsik, Senior Principal Analyst, ESG

Jon Oltsik is an ESG senior principal analyst, an ESG fellow, and the founder of the firm's cybersecurity service. With over 30 years of technology industry experience, Jon is widely recognized as an expert in all aspects of cybersecurity and is often called upon to help customers understand a CISO's perspective and strategies. Jon focuses on areas such as cyber risk management, security operations, and managed security services.

Jon was named one of the top 100 cybersecurity influencers for 2015 by Onalytica and is active as a committee member of the Cybersecurity Canon, a project dedicated to identifying a list of must-read books for all cybersecurity practitioners. Often quoted in the business and technical press, Jon is also engaged in cybersecurity issues, legislation, and technology discussions within the US government.

1. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection And Response," Forrester, April 2021.

Dave Gruber, Principal Analyst, ESG

Principal Analyst Dave Gruber covers endpoint security, application security, email security, and managed detection and response at ESG, where he helps product marketing and management leaders develop winning strategies in these highly competitive markets. Prior to ESG, Dave held executive leadership roles at successful endpoint and application security companies, most recently as the vice president of product marketing at Carbon Black through its IPO and as vice president of products at Black Duck Software (acquired by Synopsys), where he led product marketing and product management.

In his current analyst role, Dave researches the most pressing needs of CISOs and security teams, working together with endpoint, application, and email security vendors to develop successful product and go-to-market strategies, positioning, and messaging. Building on a strong technical background with early roles in enterprise application development, Dave became interested in figuring out why some products were more successful than others, which eventually led him to senior roles in software product management and product marketing.

Dave holds a BS degree in Computer Science from the University of Maine.

Zeus Kerravala, Founder and Principal Analyst, ZK Research

Zeus Kerravala is the founder and principal analyst of ZK Research. Zeus provides a mix of tactical and long-term strategic advice to constituents, including end-user IT and network managers, vendors of IT hardware, software and services, and the IT investment community.

Prior to ZK Research, Zeus was a senior vice president and distinguished research fellow with Yankee Group. Before Yankee Group, he had a number of technical roles, including a senior technical position at Greenwich Technology Partners (GTP). He has held numerous internal IT positions, including vice president of IT and deputy CIO of Ferris, Baker Watts LLC, and senior project manager at Alex. Brown & Sons, Inc. Kerravala is heavily quoted in the business and technology press and is a regular speaker at events including Interop and Enterprise Connect.

Bruce Hembree, Field CTO and Technical Director for Cortex, Palo Alto Networks

Prior to Palo Alto Networks, Bruce worked extensively with the U.S. Department of Defense and was a member of the Microsoft Digital Crimes Unit (DCU) in the takedown of some of the largest global threat ecosystems in internet history. The DCU is a small group of offensive-side personnel working with law enforcement agencies such as the FBI, Scotland Yard, Interpol, and foreign and domestic government entities doing takedowns of global internet threats, online organized crime, and botnets such as Citadel, Zbot, Conficker, Emotet, and Rustock, among others. The DCU was brought to the attention of the general public by inclusion in the Tom Clancy novel "Threat Vector" and the HBO special "The Perfect Weapon."

Bruce is a veteran of the U.S. Air Force and spent two years deployed to active conflict regions in support of global anti-terrorism efforts.

Gonen Fink, SVP, Cortex, Palo Alto Networks

Gonen Fink is a cybersecurity executive with more than 25+ years of entrepreneurial and leadership experience and demonstrated success in building teams, technologies, and products from inception to a leading position in multibillion-dollar markets. Gonen currently serves as senior vice president, Cortex products and head of Israel R&D center at Palo Alto Networks.

Gonen previously served as senior vice president of products at Palo Alto Networks, where he initiated and led the creation of Cortex XDR, the product that defined the XDR security category, positioned Palo Alto Networks as a category leader, and became an anchor of the company's cloud and AI security business.

He previously served as CEO of LightCyber (acquired by Palo Alto Networks in 2017), a behavioral analytics startup, where he led the company from the prerevenues stage to a leadership position in the network detection and response market. Earlier in his career, he was one of the first five employees of Check Point Software and filled various positions, including chief architect, vice president of products, and vice president of strategy; and played an instrumental role in building Check Point from an early stage startup to a multibillion-dollar firewall market leader.

Gonen was also a co-founder and CEO of Pythagoras Solar, a building-integrated pho-

tovoltaic (BIPV) company that invented and manufactured a revolutionary energy-generating transparent window. He has served as a board member, advisor, and investor in multiple startups including ForeScout Technologies (FSCT), SecureIslands (acquired by Microsoft), IntSights (acquired by Rapid7), and others. In 2014, he was named one of the most influential Israelis in tech worldwide.

Gonen holds a BS (summa cum laude) in Physics and Computer Science and an MA (summa cum laude) in Digital Philosophy from Tel Aviv University.

Michael Gregg, Chief Information Security Officer, State of North Dakota

The state CISO is responsible for establishing and leading the strategic direction of cybersecurity for the state and advising the governor and legislators on key cyber issues.

In Michael Gregg's two decades of experience, he has inspired people interested in becoming IT professionals as well as seasoned IT professionals through his 25 IT cybersecurity books, including *Inside Network Security Assessment*, *Hack the Stack*, *CISSP Exam Cram*, *Build Your Own Network Security Lab*, and *Certified Ethical Hacker Exam Prep*.

Michael developed high-level security classes and has been featured in newspapers, magazines, and on news programs such as MSNBC, *The New York Times*, Fox News, CBS News, etc. He also enjoys contributing his time and talents where there is a need to help others learn and grow by holding board, committee, and advisory positions for nonprofit organizations.

Ryan Kramer, Enterprise Infrastructure Architect, State of North Dakota

Ryan Kramer is the enterprise infrastructure architect with North Dakota Information Technology. He has 17 years of experience with the state, and he and his team are ultimately responsible for the design and architecture of not just STAGEnet, a statewide network that supports over 252,000 daily users throughout North Dakota, but the architecture of other infrastructure components, including, storage, compute, unified communications, and security.

Let's Talk About XDR

In less than five years, XDR has gained momentum and increased adoption, with Gartner predicting, "By year-end 2027, XDR will be used by up to 40% of end-user organizations."[2]

Lauded as a key security and risk trend, it has emerged to improve accuracy and productivity for security practitioners struggling to stay ahead of advanced emerging threats. The following myths or misconceptions represent a cross-section of themes and industry "buzz" seen in and around conversations in the security community.

We encourage anyone considering an XDR solution to proceed with an open mind, invite discourse, and take advantage of the numerous third-party reports and evaluations available in the market, including MITRE ATT&CK.

"When I coined the name XDR, the X stood for 'anything' combining EDR, NDR, etc., to anything detection and response."

–Nir Zuk, CTO and Co-Founder, Palo Alto Networks

Myth 1: XDR Is Just Marketing Hyperbole

Eric: It's easy to assume hyperbole with any emerging cybersecurity technology that has yet to establish a track record of success. But XDR really is a unique, positively disruptive approach to security operations.

XDR is a purpose-built solution designed to conduct holistic threat detection, investigation, and response (TDIR) as a unified process across key areas of the IT estate, including endpoints, networks, and clouds. Unlike most other TDIR solutions, analytics and machine learning are at the core of XDR, serving to enhance and orchestrate detection and investigation capabilities, while the single-pane-of-glass approach ensures that even amid the most complex threat events, the start-to-finish process is smooth and efficient for SOC analysts to manage.

Bruce: We all get too much marketing hype noise. It makes it easy to filter out things that actually have value. XDR is one of those cases.

2. Craig Lawson, Peter Firstbrook, and Paul Webber, *Market Guide for Extended Detection and Response*, Gartner, November 8, 2021.

Internally, in the Palo Alto SOC, it became a necessary evolution to move away from SIEM. It was slow, expensive, and the solution was sold based on the volume of data stored. We found that SIEM was only as good as the engineer and the query that was written against the data that they had at the time the query was run. ML and automation changed that detection and response mechanism for us. It also saved us a pile of money and time.

Zeus: XDR is a fundamental rethink of networking to address the security concerns of a world that is becoming increasingly dynamic and distributed. IT pros have much less control over infrastructure than in the past. Apps are in the cloud, users are mobile, SD-WANs use the public internet, and business units are making their own decisions on applications.

This has created a number of "blind spots" with siloed security tools, like EDR and NDR. XDR brings full visibility across all the elements of an attack, not just ones found on a specific device, such as an endpoint. It also brings the analytics that are necessary to interpret the data across the numerous data sources that compromise the platform. Also, because XDR sees every enforcement point, it can respond and block the threat faster across a wide range of attack vectors, not just an endpoint or network node.

Ryan: For us, security has always started with visibility. With the size and scale of the network I architect, it is impossible to secure every corner of it. What I can do is instrument as much as possible to gain the visibility, and therefore the ability, to stop the attacks.

XDR is the major component of our network suite that allows for that. Much like the first time we deployed a Palo Alto Networks NGFW, XDR gives us a similar revelation into all the data we were missing previously.

Myth 2: XDR Is EDR on Steroids

Eric: While it's true that many of today's nascent XDR solutions are built on top of a core EDR product, XDR is much more. In reality, XDR takes the best parts of existing TDIR solutions like EDR, SIEM, and SOAR and builds upon them.

XDR automatically gathers data from key sources, stitches it together to create a single, cohesive data set to cross-correlate likely threats and anomalies, and it applies orchestration and automation to key processes like preinvestigation data enrichment and remediation response.

It's not on steroids, but XDR can be a much-needed shot in the arm to enterprise SOC programs struggling with today's traditional disconnected stack of best-of-breed tools.

Bruce: From the development side, it was much more than just EDR. It was the ingest and normalization of a significant array of data types at exabyte scale to give machine learning something useful for advanced analytics.

The level of detail is so excruciating that it takes substantial cloud resources just to receive and prepare the data to be useful, much less actually involve it in advanced analytics.

Michael: In a previous shop, we used a traditional EDR product that did not utilize machine learning. XDR is light-years ahead of these products.

With XDR, you don't have to wait for an update and can have assurance that even if a device is not connected to the internet, you still have coverage.

Myth 3: XDR Will Replace SIEM

Eric: XDR is not a direct replacement for SIEM, but it can be deployed in lieu of SIEM or alongside SIEM. XDR won't be able to take in the wide variety of disparate data sources that a SIEM can, meet top-tier SIEM performance benchmarks, or address key business demands, like comprehensive compliance management and business reporting. However, XDR has the potential to strongly benefit not only organizations that have implemented and been unable to realize the expected outcomes of SIEM-based threat detection and response architectures, but also those for which SIEM is too expensive, complex, and time-consuming.

Omdia sees XDR being deployed increasingly as a SIEM alternative, serving to democratize enterprise-grade TDIR for budget-conscious and less-sophisticated security organizations, and alongside existing SIEMs to add more advanced TDIR capabilities without requiring the cost and complexity of replacing a legacy SIEM.

Bruce: Some orgs may choose to keep SIEM for use cases they have custom-developed internally. For many orgs, it can fulfill and replace the *promise* of what SIEM was originally designed to do. For us, here at Palo Alto, it fulfilled everything we needed and gave us the ability to deal with alerting at a scale and speed that most SOC engineers would find intriguing.

"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."[3]

– Allie Mellen, Senior Analyst, Forrester

Myth 4: XDR Eliminates the Need for SOAR Solutions

Eric: Not necessarily. XDR will have orchestration and automation abilities like a SOAR system, but its focus will be on a limited set of threat response scenarios, such as ransomware or suspicious end-user activity.

However, SOAR systems will be able to offer a broader set of orchestration and automation capabilities across a broader set of security and nonsecurity systems. While XDR will prove easier and faster than SOAR for core TDIR use cases, large enterprises that have come to rely on SOAR for advanced orchestration activities, especially those beyond security, will likely continue to do so.

Bruce: SOAR is critical. We prefer to keep our automation agnostic from our security platform so that it can be useful in multiple automation cases. The impact across our entire organization has been felt by our willingness to use automation in places where it changed the way we do business.

Gonen: XDR doesn't eliminate the need for SOAR, as SOAR can be used to orchestrate and automate various SOC operations, from threat intel management, alert enrichment, response steps, and collaboration around incident investigation, ticketing, and more.

However, it is worth noting that a good XDR solution that relies on multiple data sources can autonomously perform many tasks that SOAR systems are designed to do. For example, SOAR may be used to enrich an incoming firewall alert with information from endpoint telemetry, and from threat intel feeds through an alert enrichment playbook that integrates with EDR systems and threat intel feeds. A true XDR, on the other hand, will be ingesting all those data sources and stitch them together so that the firewall alert will be automatically enriched prior to being presented to the user, without the need to write custom playbooks.

Ryan: XDR and SOAR are complementary and could never replace one another.

In our environment, SOAR has a much larger place in the enterprise that spans well beyond the endpoint role of XDR, and I have a vision to take SOAR outside of the security space. In fact, the true benefit of XDR comes from a well-developed SOAR solution working behind the scenes, and without a SOAR, you risk creating a higher signal-to-noise ratio for the analyst.

Myth 5: XDR Means You Don't Need Zero Trust

Bruce: I would not agree with this statement. XDR is simply a telemetry-ingest ethos. It is about using everything you have. Insider threat, supply chain, and all of the other vectors for attack still exist, but with XDR, you now actually have a solid chance of detecting and preventing them.

Gonen: XDR is focusing on detection and response, as well as endpoint prevention, but it doesn't replace the need for network-based Zero Trust.

Michael: Does XDR mean you don't need Zero Trust? In my opinion, the best security posture is a layered approach so that you can truly get "defense in depth." By adding multiple layers of defenses that include technical, physical, and administrative, you can better protect yourself from threat actors and move from a responsive to a detective/preventive model. XDR will help in the journey.

"By 2023, at least 30% of EDR and SIEM providers will claim to provide XDR, despite them lacking core XDR functionality."[4]

– Gartner

Myth 6: XDR Generates Too Much Noise to Use

Bruce: Potentially true if implemented poorly. The efficient application of well-trained machine learning with advanced analytics means that it is possible to evolve beyond what ML has brought to security ecosystems in the past.

3. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection And Response."
4. Craig Lawson, Peter Firstbrook, and Paul Webber, *Market Guide for Extended Detection and Response*.

When coupled with SOAR, you generate the system that has the detailed data to detect threat, respond to it efficiently, and make large volumes of telemetry useful without overwhelming the engineers trying to use the system.

Michael: Will XDR generate noise when it is first deployed in an environment? Yes, because it may very well be detecting malware the others missed!

All products need to be tuned to some degree. When we deploy XDR, we place it first in a limited environment and verify there are no false positives or needed exclusions. Using this multistep approach has helped us ensure a smooth implementation and deployment. Once deployed, we rarely see a false positive, and there is little to no noise.

Ryan: We desperately needed to do automation and to have a tool that filtered through all the noise. Cortex is doing exactly that. We're seeing the noise going away, and we're getting to the important alerts that we hadn't seen previously.

Myth 7: All XDR Products Operate on the Same Principles

Eric: Definitely not. Omdia sees two distinct types of XDR solutions: Open XDR and Comprehensive XDR.

Comprehensive XDR is a single-vendor platform with integrated TDIR capabilities across endpoints, networks, and cloud deployments. Comprehensive XDR solutions require little integration, providing more ease of use and higher efficacy than a mix of third-party solutions. And Comprehensive XDR solutions are designed to foster a closed loop for the detection, alerting, investigation, and the actions that analysts initiate to actually stop the threat and remediate affected systems.

Open XDR, alternatively, relies on a combination of its own and third-party data to detect threats, conduct investigations, and initiate response actions. It can cover any number of IT estate regions and offers the flexibility to enhance enterprise TDIR capabilities within SOC architectures with a variety of existing best-of-breed tools.

Bruce: I don't believe they do. They tend to play to their strengths. The secret sauce in this sort of system is removing latency from the entire kill chain. From detection to action on a target, low latency and high confidence come from the degree of integration and threat research that is built into the DNA of the system. They may have similar traits in some cases, but the actual implementation and design concept produces very different end-state products.

Gonen: That's not the case. When evaluating XDR products, one should take a look at what data sources can be ingested to the product and whether the tool ingests raw telemetry data that can be used for detection and machine learning, or it ingests only a small number of alerts, which makes it an alert aggregation tool.

Myth 8: I'm Working Myself Out of a Job Using XDR

Bruce: Very frequently, people ask me, "Am I working myself out of a job (by using this technology)?" That's simply not the case. You're not working yourself out of a job. You're working yourself into the job that you actually wanted in the first place. That is a critical distinction.

Instead of being constantly overwhelmed and hence allowing a threat actor additional dwell time inside your network, ML, automation, and XDR produce a low-latency detection, prevention, and remediation cycle. That is key to getting the threat actor out as soon as possible.

Prevention is always our first focus, but there is no such thing as an impenetrable defense. Eventually, someone's going to get through. How you respond and how long they have on that endpoint to do their work is the best place to focus once prevention has been subverted. It's the place where you've really got to focus. How well do you respond?

The autonomous SOC is not going to happen without humans in some form. You're not going to be able to take the people out of it. Instead, you're going to be able to provide SOC analysts the tools they need to work efficiently at scale. Which is why speed is key—removal of that dwell time.

Right now, across our close to 17 billion events per day in our SOC, our time for detection in our SOC at Palo Alto Networks is 10 seconds, and our time for response is one minute. If something does require manual intervention from a human, then you've got to be able to get in there and do something about it quickly. That's where we're at.

Ryan: Absolutely not! There are very few consistencies in technology; one of those is the increasing scale and intensity of the threats that attack us on a daily basis. XDR (and SOAR) is an opportunity for a security analyst to do their job more effectively, more efficiently, and more importantly, to do high-

er-value work. Tedious operations, such as pulling files or quarantining an infected machine, are now single-click operations; the analyst doesn't need to deal with the low-level operations that are happening behind the scenes.

Myth 9: XDR Can Replace All Other Detection and Response Tools

Dave: XDR may, over time, be able to deliver a high percentage of the capabilities that other detection and response tools deliver, but other tools will likely continue to support additional use cases outside of what XDR provides. This leaves room for other security operations tools, including SIEM, SOAR, EDR, and NDR tools, to persist for many years to come. While many are optimistic that XDR may, over time, provide an opportunity to reduce investment in these tools, most plan to continue to leverage multiple tools for at least the short term while investing in XDR to strengthen detection and response programs.

Bruce: No. You still need the firewalls. You still need automation. You still need attack surface management (ASM). You still need identity management. You still need solid security hygiene across the org. XDR does not solve everything, but it has functionality that augments most security processes in an organization if implemented well.

Jon: Maybe. For example, a customer may replace their current EDR with an XDR endpoint sensor/actuator as part of a replacement process. This type of replacement is not common, however. It's more likely that XDR is an architecture and strategic direction where customers are focused on vendor consolidation and security technology integration. In the near term, XDR will be used to improve threat detection in support of existing controls and analytics solutions.

> **"Data is a precious thing and will last longer than the systems themselves."**
>
> –Tim Berners-Lee

Myth 10: There Is a Single Definition of What XDR Solutions Must Provide

Jon: This statement is patently false, and those that promote it are doing security professionals a disservice. In fact, XDR is an evolving architecture that combines existing security controls and analytics with new controls and analytics in a tightly integrated architecture. Different users and vendors bring different components to XDR, so it must be flexible and be able to accommodate these differences.

Dave: While many have attempted to put XDR in a box with a definitive definition, the truth is that XDR is more about an approach than a list of specific features. With an objective of helping security teams more rapidly detect and respond to all types of threats across their diverse private and public IT infrastructure, XDR embraces the need to aggregate, correlate, and analyze signals from every potential attack vector, bubbling up the cleanest, most precise view of threat activity to help facilitate and automate rapid threat mitigation.

Choosing the right XDR solution requires careful attention to many things, including scalability, customization, openness, automation, workflow support, out-of-the-box integrations, and reporting. The size, scope, and security maturity of the purchasing organization will impact all of this. Ultimately, there is currently no one-size-fits-all for XDR, as security strategies and needs vary widely across different organizations.

Bruce: Not that I've yet seen, and I work with the gent that literally created the term.

Our Take on XDR

Eric: Omdia believes XDR technology has already initiated what will be a significant shift in SecOps technology architectures. XDR solutions will soon be able to deliver better TDIR outcomes with greater ease, consistency, and lower cost than the myriad best-of-breed, ad hoc SOC technology architectures widely used today. This will lead to rapid growth in XDR adoption across organizations of all sizes, including those with no or limited existing SOC technology architectures, as well as those that have implemented SIEM/SOAR-based architectures.

While Open XDR solutions may prove popular in the early going, over time, Omdia sees steady growth in Comprehensive XDR solutions because of preintegrated telemetry, cross-correlated semiautomated investigations, and coordinated, validated response across multiple areas of the IT estate.

Zeus: It's critical for businesses to embrace the concept of XDR today. The cybersecurity industry has been built on the concept that point products placed at strategic locations will protect an organization's critical assets and data. The reality is that model has never worked, is not working, and will never work.

> **"We're entering a new world in which data may be more important than software."**
>
> –Tim O'Reilly

What's required is business to consider lateral movement of breaches to be the biggest cyberthreat today. An endpoint could be breached and then laterally spread to other systems. A traditional EDR tool might find the breach on the endpoint but would have no concept of where it migrated to. The only way to find breaches and track the movement of it is with XDR, as it operates across the infrastructure. CISOs must shed legacy thinking and make XDR a priority.

Gonen: XDR is a new technology that, within less than four years, became a de facto standard for detection and response. While not all XDR tools are the same, there's a broad agreement that XDR is changing the way companies do detection and response and replaces a lot of the traditional tools used to perform this operation

You say "Tomāto;" I say "Tomäto."

Enterprise Strategy Group: "XDR is an integrated suite of security products spanning hybrid IT architectures, designed to interoperate and coordinate on threat prevention, detection, and response. In other words, XDR unifies control points, security telemetry, analytics, and operations into one enterprise system."

Forrester: "The evolution of 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, 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."

Gartner: "XDR is a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components."

Ready to Kick Some XDR "Tires"? Know What Questions to Ask

Distinguishing between the various options available on the market to determine whether a solution is true XDR as opposed to another vendor hopping on the XDR bandwagon requires due diligence and sorting through the noise. The following specifications (while not exhaustive) can help provide clarification when reviewing the different solutions available in the market:

A *true* XDR solution:

- Should provide stitching of key data automatically, rather than table joins, simple correlation, or manual queries
- Natively stitches together network, endpoint, identity, and cloud data into a single "story" or integrated log record for cross-data analytics
- Applies intelligent, advanced logic to show the complete story of an incident in a single view
- Automatically maps evidence and artifacts to the MITRE ATT&CK framework
- Provides a built-in capability to perform deep forensic analysis
- Is backed by world-class security research and security services teams

Does the Solution Take a Prevention-First Approach?

While XDR is defined as "extended detection and response," its strength lies in the ability to prevent attacks and block, disrupt, and contain threats and attacks before any damage occurs. For all other activities, XDR provides a deep level of integration with devices to build a complete record of communications and endpoints and knows how users interact with all applications and data to detect attacker TTP (techniques, tactics, and procedures).

Does the Solution Base Detections on Identity, Endpoint, Network, and Cloud?

Can the solution detect attacks based on identity, cloud, and network data, including between unmanaged devices? Some endpoint-only "XDR" vendors will say they see network data when what they really mean is network traffic coming from the endpoint agents instead of getting data from network security devices like NGFWs. A true XDR will analyze data from at least these sources, correlate with threat activity, and tag with MITRE ATT&CK TTPs to help provide a more detailed picture of adversarial movement.

Does the Solution Have Native Investigation and Response Capabilities?

A *true* XDR solution:

- Uses security analytics to automate response recommendations
- Allows for native response actions on the endpoint
- Can support but does not require integrations with other tools like SOAR for response
- Enables response across endpoint, network, and cloud enforcement points vs. endpoint only
- Allows native support for ad hoc searching across all third-party data sources using analyst-optimized investigative and hunting methods
- Optimizes triage and investigations by surfacing all related malicious artifacts, hosts, users, and correlated alerts mapped to MITRE ATT&CK
- Can provide smart recommendations for targeted response actions based on MITRE ATT&CK

The Mission of Cortex XDR

"Empower organizations to know about and stop all attacks by ingesting, integrating, and analyzing every data source to encompass the entire environment, and leveraging multi-layer cross-data analytics for higher fidelity detection, continuous learning for automated investigation and response, and all threat context and insight in one place."

By all accounts, XDR is continuing to gain momentum and adoption with security practitioners despite variations in definition and capabilities. As organizations remain unsatisfied with their ability to correlate security data across all products and services, stay ahead of threat alerts, and uncover the root causes of attacks, XDR is a solution that helps meet those needs. That said, it's important to differentiate between vendor strategies for delivering XDR, including longer-term roadmaps and overall vision.

Consider Cortex XDR

At Palo Alto Networks, we have a steadfast commitment to providing best-in-class security solutions, and Cortex XDR—as the first XDR product in the industry—continues to lead by example by adding robust, new third-generation capabilities such as forensics, identity analytics, and cloud security.

Resources

To learn more about Palo Alto Networks extended detection and response capabilities, please visit our Cortex XDR webpage.

Read XDR For Dummies, our guide to help you understand what XDR is and isn't, the current state of detection and response, and 10 must-have XDR capabilities.

XDR RFP Checklist

Our RFP checklist includes requirements within nine key categories to help you evaluate the quality of the platforms you're considering. Use this checklist as a starting point and tailor it to your company's needs to ensure you're able to identify vendors that can best support your organization.

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