Secureworks® | Taegis™ XDR

BUYER'S GUIDE

Extended Detection and Response (XDR)

Buyer's Guide Introduction

Extended Detection and Response (XDR) has been tabbed as the next big thing in cybersecurity. Research and Advisory firm Gartner, listed XDR as its top "Security and Risk Trend" in 2020 and as a top 10 "Security Project" for 2021[1]. Countless industry blogs have called XDR the "next evolution." As industry buzz continues to grow, IT and security leaders have quickly recognized XDR's potential impact to transform threat detection and response.

Advanced threat detection is in high demand.

83% of IT pros are increasing their budgets on threat detection and response technologies.[2]

Even though the solution is still in earlier stages of maturity, customer interest has grown quickly. XDR delivers centralized detection and incident response capabilities that help uncover complex attacks often missed by point solutions and legacy SIEMs.

The Solution

XDR initially emerged from customer demand for simpler security operations and advanced threat detection. As organizations struggle to effectively identify malicious actors and activity, the importance of quickly identifying emerging threats has become a necessity.

Top XDR Capabilities

42%

Visualization of complex attacks[2]

38%

Analytics to detect modern attacks[2]

31%

Improved mean time to detect (MTTD)[2]

[1] Gartner, Smarter with Gartner, 2020

[2] ESG, The Impact of the Modern SOC, 2020

With organizations facing security-operational challenges, the promise for increased efficiency, productivity, and automation is another attractive benefit of XDR.

As security solution providers race to position their offerings in the competitive XDR marketplace, IT and security leaders will need to look beyond industry hype to evaluate XDR vendors. This guide highlights 15 questions to answer before investing in an XDR product.

Understanding the Threat Landscape

As business transformation rapidly redefines where and how people work, the threat landscape continues to evolve as well. With millions of workers moving from a centrally located office building to a remote or home office, the attack surface has increased significantly. Perpetrators adapted quickly and attacks on home networks surged.

In addition, malicious actors are employing complex attacks that have become harder to detect. A recent study from the Ponemon Institute shows the impact of such sophisticated attacks:

- An average of 80% of successful breaches are new or unknown "zero-day attacks"[3]
- Zero-day attacks are expected to more than double in the coming year[3]

In this new reality, organizations that are not prepared to adapt to the threat landscape may feel the consequence for years to come.

Connecting Security Tools

Reactive security measures provide ineffective protection against today's emerging threats and targeted attacks. Security teams often fail to stay ahead of adversaries due to the time and effort needed to manage the large number of siloed security tools used to protect their infrastructure. Due to the lack of integration between these solutions, security analysts are often forced to invest time in manually stitching data from different tools and managing and troubleshooting disparate products, which distracts them from chasing real threats. Plus, security operations must overcome gaps in team staffing and skills shortages.

These operational deficiencies, as well as an inability to identify highly sophisticated and hidden threats, are characteristic of legacy SIEMs and point systems. Without a unified incident detection and response solution, most organizations struggle to stay on top of business trends with a poor security posture.

XDR Uplevels SecOps Effectiveness

58%

of IT pros believe XDR could improve the capabilities of security analysts.[2]

[3] Ponemon Institute, The Third Annual Study on the State of Endpoint Security Risk, 2020

XDR: A New Approach for a New Reality

XDR introduces a new evolution in threat detection and response. In essence, it picks up where EDR left off, extending detection and response beyond endpoints to include network and cloud environments. Analyst firm Gartner offers the following definition of XDR:

XDR "describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components."[4]

Over 90% of IT pros say tool integration is a top 5 priority as they build out their SOC tooling architecture, while 37% list integration as their top priority[2]. Unifying prevention, detection, and response between siloed products elevates threat visibility, enabling organizations to identify stealthy threats that commonly evade point solutions. The execution behind unified detection begins with the systemization of historic and real-time event data into common data formats within a central repository. With a complete picture of threat activity, XDR correlates telemetry and threat intelligence data to identify relationships and trends that indicate malicious activity. This benefits security teams by delivering faster detection and response with greater context and increased accuracy.

In sifting through the noise of alerts and keeping pace with a new wave of attacks, security operations work has never been more challenging. Each point solution requires separate management and expertise to operate. This complexity has taken a huge toll on the productivity of security teams. XDR consolidates multiple security components into a single detection and response solution which eliminates "swivel chair" scenarios and enhances analysts' efficiency. This also helps to uplevel the capabilities of junior analysts. XDR supports business transformation with improved operational productivity and enhanced threat detection.

Top Criteria for Evaluating XDR Vendors

Improvement of security efficacy and operational efficiency

The ideal XDR solution should provide centralized prevention, detection, and incident response capabilities to address unknown, sophisticated threats, and it should boost operational productivity. XDR should also include automated correlation and alert validation, eliminating alert fatigue and allowing security teams to place more focus on threats that matter.

To gain a better understanding of threat protection capabilities, organizations must evaluate a vendor's ability to continuously refresh their XDR solutions with intelligence on attacker activity.

[4] Gartner, Innovation Insight for Extended Detection and Response, 2020

5 Questions to Ask a Potential Vendor

- What kind of threats and malicious activities can your solution detect?
- What sources of threat intelligence do you use?
- Do you map alerts to the MITRE ATT&CK Framework?
- How effective is your XDR solution at stopping attacks (e.g., ransomware) before damage occurs?
- What technologies do you use to identify anomalies and find indicators of compromise?

Open Architecture

There are primarily two type of XDR solutions: closed, or proprietary, XDR and open XDR. Proprietary XDR is characterized by vendors that have unified their own suite of security solutions on a centralized XDR management platform. This approach requires customers to "rip and replace" their existing security controls and, possibly, sacrifice efficacy with vendors that have gaps in their product portfolio.

Open XDR consolidates best-of-breed security products, as opposed to single-vendor solutions, into a centralized management and analytics hub. When researching XDR vendors, ensure their solution interoperates with your existing security tools and provides flexibility to accommodate third-party products your organization may require in the future.

Data Aggregation and Retention Cost

40% of IT pros believe improving data ingestion to keep up with real-time data sources will help improve security efficacy and efficiency for their organization[2]. With the acceleration of digital transformation, XDR must be able to centralize, correlate, and analyze terabytes of real-time and batch data. Siloed security creates blind spots that leave data in gaps across your ecosystem. A primary requirement for XDR is the ability to centralize and normalize data into a central repository for analysis[5].

Vendors that build their XDR solutions on cloud-native platforms ease integration of data from multi-vendor products while providing the scalability to meet business demands for an increasing volume of data.

Data ingestion and retention cost is another issue to consider. You do not want to be forced to decide which potentially relevant data to erase because retaining it is too costly. So, choose the vendor accordingly.

[5]Gartner. Innovation Insight for Extended Detection and Response, 2020

5 Questions to Ask

- Will I need to change my infrastructure or deploy new technology? Do I need to adapt to the vendor's technology stack?
- What environments does your solution cover (i.e., Cloud/Endpoint/Network/All)? Do you look at them separately or all together?
- Can you centralize and analyze data from my existing security technology?
- Which log sources do you collect and retain? Can you directly search your log information?
- How do you collect, store, process, and analyze the huge amounts of data you bring in?
- How much would it cost to ingest and retain data and for how long?

Prevention, Detection, and Response to Known and Unknown Threats

Endpoints are often the first line of defense for many organizations working to protect themselves in today's complex threat landscape. The ability to prevent known and unknown threats on the endpoint automatically is instrumental to stopping numerous attacks while reducing the investigations load and bringing prevention data into the XDR equation. Next-generation, machine-learning driven prevention (NGAV) helps detect advanced and novel threats while minimizing the impact on the performance of endpoints. Plus, prevention solutions with local machine-learning models can ensure endpoints are protected even when offline, without requiring frequent signature upgrades. With effective prevention, security teams can leverage XDR to focus on attacks that bypass endpoint security. The unification of prevention, detection, and response capabilities in XDR helps improve and accelerate threat detection and investigation.

5 Questions to Ask

- Does your solution deliver unified prevention, detection, and response capabilities?
- Does your solution ingest and analyze prevention/NGAV data?
- Can remediation be performed on the endpoint via the XDR console?
- Does the prevention portion of your solution automatically block advanced threats such as zero-day and polymorphic malware at the endpoint?
- How much does the prevention/NGAV portion of your solution impact the performance of end-user machines?
- Can your product ensure endpoint protection when the device is offline?

Outpace and Outmaneuver Adversaries with Secureworks Taegis™ XDR

As cyber threats become stealthier and more sophisticated, many businesses and governments have a hard time keeping pace. With limited visibility into their hybrid IT environments, understaffed security teams, and growing cost and complexity of managing disparate security tools, organizations need an extended detection and response (XDR) solution that unifies their existing security infrastructure. Specifically, they need a solution that derives actionable, focused insight and provides a single console to investigate and rapidly respond to threats in a highly automated fashion.

Improve the effectiveness and efficiency of security operations with Taegis XDR cloud-native SaaS that incorporates the security operations know-how and in-depth knowledge of the threat landscape that have made Secureworks an industry leader for over 20 years.

- Gain holistic visibility and control over endpoint, network, and cloud environments by aggregating telemetry from across your organization's security fabric
- Detect advanced threats with AI-powered analytics and comprehensive threat intelligence from the Secureworks Counter Threat Unit™
- Accelerate investigations and incident response with all the data, threat-hunting tools, and automated playbooks at your fingertips in one easy-to-use cloud console

Unify Prevention, Detection, and Response

Combine the award-winning detection and response capabilities of Taegis XDR with next-generation endpoint prevention of Taegis NGAV for an intuitive, comprehensive prevention, detection, and response solution

Detect Threats Faster and More Accurately

Leverage Taegis NGAV to automatically stop threats coming from the endpoint. Rely on Taegis XDR's advanced analytics engine, continuously updated with threat indicators, countermeasures, and purpose-built analytics from Secureworks Counter Threat Unit™ to detect sophisticated attacks anywhere in your environment. Spend less time dealing with false positives and get to real threats sooner with validated and prioritized alerts

Modernize Security Operations

Get a holistic view of your security infrastructure and perform all investigations within Taegis XDR, without having to manually stitch data or bounce between tools. Reduce mean-time-to-respond (MTTR) to minutes with response-action recommendations and automated playbooks informed by Secureworks' 1,400 customer incident response engagements per year

Secureworks®

In Their Own Words: What customers and analyst firms are saying about Taegis XDR

"XDR combines security analytics with additional advanced tools previously unavailable to us. It's picked up threats we wouldn't have seen. XDR isn't just the next generation of SIEM, it's an evolution."

David Levine
VP Corporate & Information Security, CISO
Ricoh USA, Inc.

"Our biggest security challenge was the ability to identify and respond to an event quickly. Secureworks Taegis alerted us to suspicious activity and gave us specific, actionable recommendations on the first night we went live. We had never been alerted so quickly and it was a critical first step in driving a stronger security posture for our team."

Dr. Faisal Jaffri
Global IT Director
GKN Wheels and Structures

"In addition to analyzing, correlating, and visualizing telemetry from multiple security controls using proven tooling that Secureworks' own teams have been using for years, Secureworks Taegis XDR further adds rich threat intelligence and proven counter measures developed by their expert threat and response teams."

David Gruber
Senior Security Analyst
ESG

"Taegis NGAV is a mature product, ready to be used in a wide set of deployment scenarios, ranging from small environments to multinational enterprises."

"With its solid performance, convincing detection capabilities against in-the-wild malware, SOC-ready console and feature set, Secureworks Taegis NGAV is a trustworthy addition to any IT security arsenal."

Efficacy Assessment of Secureworks Taegis NGAV (August 2021) - MRG Effitas

Key Features of Taegis XDR:

- Comprehensive attack surface coverage including endpoint, network, and cloud environments
- Machine and deep learning-driven analyses of telemetry and events from multiple attack vectors enriched by threat intelligence
- High-fidelity alerts augmented with all the context and data you need, when and where you need them
- Single-click response actions and automated playbooks
- An open XDR solution offers extensive pre-built and easy-to-create custom integrations with 3rd-party security tools

Secureworks®

Free Trial: Secureworks Taegis XDR

START YOUR FREE TRIAL

XDR is a cloud-native solution that combines advanced analytics and data modeling with unrivaled threat intelligence to help detect both known and unknown threats. We're putting the power in your hands with a free trial experience. Get started today to discover how you can improve your SOC efficiency.

Click the link above to place the power of Taegis XDR in your hands. The free trial entails the following:

- No credit card or sales call required: Trial registration is completely self-service
- Get started within minutes: Access the platform immediately upon sign-up
- Use your own data: Set up the trial with your own data to detect known and unknown threats in your environment
- 14 days of access: Explore at your leisure and experience XDR via self-paced missions
- Leverage pre-loaded demo data: Understand how XDR helps you detect, investigate and respond to a demo living off the land attack

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.