FROST & SULLIVAN

2024 COMPETITIVE STRATEGY LEADER

IN THE GLOBAL EXTENDED DETECTION AND RESPONSE INDUSTRY

Secureworks®

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Secureworks excels in many of the criteria in the extended detection and response space.

The Three Promises to Revolutionize Cybersecurity

Extended Detection and Response (XDR) is a rapidly growing security solution category that promises to deliver comprehensive detection and response against cyber threats across the entire customer ecosystem. Over the past few years, XDR has become an established platform, showing high adoption across every region and industry vertical. According to Frost & Sullivan's Voice of the Enterprise Security Customer survey, 36% of global organizations were leveraging XDR for their security operations in 2023, with a further 32% planning to invest in XDR by 2024.

This success is the result of XDR addressing many customer pain points through three core aspects that define it and allow it to stand out from other cybersecurity solutions. The first is the promise of cross-layered detection and response, provided by XDR's visibility across the entire environment, and its ability to correlate, analyze, and match threat data to create an attack story. Secondly, automation plays a big role in how XDR protects business-critical assets, from playbooks and detections powered by machine learning to generative AI that helps train and guide analysts in the threat investigation process. The third one is the promise of integration with disparate security controls, including third-party data sources, tools, and solutions.

With these three core promises, XDR aims to address organizations' needs and use cases. These include dealing with highly sophisticated cyberattacks in today's ever-changing threat landscape, alleviating the effects of the growing cybersecurity workforce gap, supporting analysts by allowing them to focus on the business-critical tasks and alerts, and providing flexibility for customers looking to leverage their existing

security investments.

XDR has significantly evolved since its inception, especially in the way vendors deliver on the three core aspects / promises. Many of the top competitors in the market have shifted their approach and strategy, gradually extending visibility across additional environments, finding new ways of delivering meaningful automation, and, most importantly, increasing the number and depth of third-party integrations.

Secureworks: Continued Success in a Fiercely Competitive Market

Atlanta-based Secureworks has been in the cybersecurity business for over 25 years, providing security services and products for more than 4,000 customers across more than 70 countries. Secureworks became part of Dell Technologies in 2011, and went public in 2016, with its revenue performance improving steadily ever since. In the XDR market, the company has had 82.7% growth in the 2022-2023 period and is projected to grow at 61.4% CAGR for the 2022-2025 period, almost twice as fast as the market average.

Secureworks unveiled its cloud-based multi-purpose Taegis™ platform in 2019 when the XDR market was still in its infancy. The platform serves as a single-pane-of-glass tool for Taegis XDR, Taegis VDR (focusing on vulnerability management), and Taegis ManagedXDR. Taegis provides visibility into the endpoint, network, cloud, identity, email, container, apps, and log environments, ingesting and correlating alerts, telemetry, and threat intelligence to deliver comprehensive threat detection and response. Secureworks' portfolio also includes EDR, NGAV, threat hunting, log management, OT security, and other products and services, delivered by a team of more than 300 security analysts.

To aid XDR detection, Secureworks provides its own threat intelligence, gathered by the Counter Threat Unit™ (CTU™) from its extensive customer ecosystem and 3,000 annual testing and IR engagements. The CTU is a team of more than a hundred world-class researchers and incident responders, and Secureworks is one of four companies certified by the US and UK governments for IR in critical infrastructure, specifically the NSA's Cyber Incident Response Assistance and the National Cyber Security's (NCSC) Cyber Incident Response Standards. The CTU also supports Secureworks in the discovery of new attack techniques and patterns that the company leverages to proactively protect customer environments.

Secureworks' portfolio is tightly integrated and works as a well-oiled machine that improves customer security outcomes, thanks to a strategy that includes market growth and expansion initiatives, flexibility, technology innovation, and an effective approach to XDR solutions.

Strategic Investments to Multiply the Value of Human Capital

Secureworks has always been at the forefront of innovation and the most relevant megatrends of the XDR space. Taegis employs artificial intelligence and machine learning to eliminate false positives, increase detection rates, and reduce analysts' mean time to respond to security incidents. The company recognizes the tremendous importance of meaningful automation, with the understanding that sometimes machine learning and artificial intelligence are not sufficient to provide the support customers require.

Secureworks' solution for this is twofold. Its first step was to spearhead the collaborative approach to XDR by developing an in-built feature that lets customers connect with a Secureworks SOC analyst who is familiar with their environment in less than 90 seconds of submitting the request. This service puts the combined knowledge of Secureworks' experts within the customer's grasp and significantly simplifies

working with an XDR solution. The advice customers get from Secureworks' analysts goes far beyond basic support questions, it can include best practice workflows, help with threat investigation or threat hunting, and more. This feature provides extended value, adding a service component to the Taegis XDR platform, which greatly enhances customer experience.

Secondly, Secureworks invests a significant portion of its R&D budget to enhance the Taegis platform with additional AI and ML capabilities, mostly related to assisted threat investigation to enable faster triage, visualization of key contextual information about threats, and an innovative threat scoring system. As part of its AI research, Secureworks' roadmap includes leveraging generative AI to set up a security assistant for the Taegis platform.

While many players are transitioning from a mostly native (i.e., integrating their own portfolio of security products) to a mix of hybrid and open approaches to XDR (i.e., focusing on the integration of third-party tools and solutions), Secureworks embraced the vendor-agnostic vision early in its XDR journey. Taegis XDR ingests telemetry and alerts from over 100 third-party integrations out of the box and allows customers and partners to create their own integrations via open APIs. This data is parsed by Taegis, which categorizes it according to over 20 event types that the solution analyzes when seeking threats.

As its technology innovation strategy shows, Secureworks keenly understands that the key aspect of meaningful automation and artificial intelligence capabilities should be how these technologies interact with the most important element in any security strategy, the analysts.

Enabling Growth Through a Customer-Oriented Approach

Secureworks' success in the market cannot be explained fully by its focus on innovation and technology. The company's prime target for Taegis XDR is organizations that have a 24/7 SOC and want to increase security efficiency. However, Taegis ManagedXDR, which is delivered through the Taegis XDR platform, aims at less mature organizations that need support in establishing and maintaining a strong security strategy. This creates upselling opportunities for both mature and less mature organizations, driving robust organic growth for Secureworks.

To help drive revenue growth, its pricing strategy is transparent, allowing customers to plan ahead if they need to expand the protected surface. Secureworks' pricing is based on the number of endpoints, and includes all product functionality, advanced APIs and integration support, the Taegis EDR agent, and threat intelligence among other features.

Even if the lion's share of Secureworks' revenue comes from North American organizations, the company is cognizant of the importance of expanding into other regions. To support its significant presence in the EMEA market, Secureworks has a data center in Europe, which enables customers in the region to comply with data residency requirements. As part of its APAC expansion, Secureworks has recently localized Taegis XDR in Japan, where it has a sizeable customer base. The localization allows the vendor to deliver the solution itself, support, and all adjacent services – including MDR, in either English or Japanese. Localization efforts multiply customer value, improving collaboration by removing potential communication barriers and showing commitment to the relationship with local organizations.

Conclusion

Secureworks is a force to be reckoned with in the XDR market, an innovation powerhouse that understands and leverages megatrends to unlock growth opportunities. Taegis XDR's features enable security professionals to focus on the truly important alerts, provide avenues for them to seek an expert's help, and allow the customer to leverage its existing cybersecurity investments, promoting collaboration and increasing cyber resilience. By establishing a SOC in Europe and localizing Taegis XDR for Japan, Secureworks shows a customer-first approach that enhances and empowers their professional relationship. These initiatives are part of a strategy that places the human element where it should be, at the forefront of the cybersecurity industry. With its strong overall performance, Secureworks earns Frost & Sullivan's 2024 Global Competitive Strategy Leadership Award in the extended detection and response market.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Award recognizes the company with a stand-out approach to achieving top-line growth and a superior customer experience.

Best Practices Award Analysis

For the Competitive Strategy Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes Best Practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

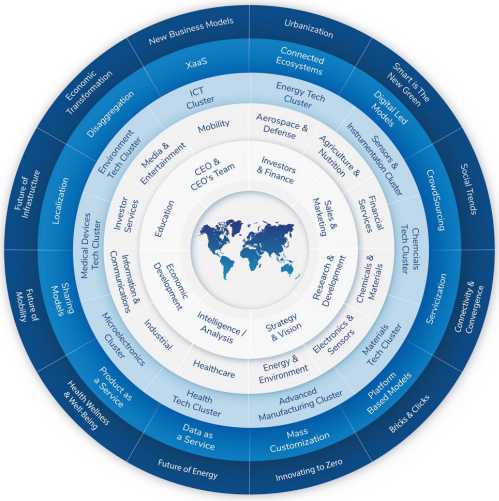
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)