FROST & SULLIVAN

Frost Radar™: Endpoint Security, 2025

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Authored by: Ozgun Pelit
Contributor: Jarad Carleton

KAE5-74
April 2025

© 2025 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- The average organization manages thousands of endpoints that have access to its corporate network. These endpoints are the most vulnerable and exploited part of any network.
- Endpoint security includes host-based software products that secure computing devices, such as laptops, desktops, tablets, servers, and smartphones, from malware, cyberattacks, and unwanted applications. Internet of things devices are endpoints that also require securing.
- Endpoint security consists of an endpoint protection platform (EPP) and endpoint detection and response (EDR). EPP is a software suite that includes antivirus, intrusion prevention, anti-malware, and other features; EDR is an advanced tool that detects threats, contains the incident, investigates with forensic and proactive hunting tools, and provides immediate response and remediation. Modern endpoint security combines EPP and EDR functions for superior performance.
- With limited resources to investigate detection alerts, organizations are more inclined to focus on protection, attack surface reduction, and identifying misconfiguration. Proprietary rollback capabilities of ransomware detection and response solutions will reduce the risk of ransomware attacks.
- Detection, auto-investigation, and setting and updating of security policies using AI is paramount for organizations facing resource challenges. AI offers the potential to substantially reduce the time to containment. Vendors are greatly improving threat detection capabilities by scanning exponentially more alerts using AI. In addition, generative AI offers multilingual communication and interface.
- To reduce overhead, technologies that enable scaling of effective policy management are paramount. This includes machine learning capabilities and automation to scale policy management across tens of thousands of nodes across hybrid and multicloud environments. To enable security teams to effectively manage device access policies, firewalls, and controls, vendors offer one centralized and integrated platform.

Growth Environment

- In 2024, enterprise spending on endpoint security solutions was projected to exceed $12.9 billion globally. Frost & Sullivan projects spending to reach $22.3 billion by 2028, achieving a compound annual growth rate of 14.7%.
- Digital transformation, remote working, internet of things devices, and bring-your-own-device (BYOD) practices are all factors driving the need for endpoint protection solutions and more extensive use of cloud-hosted consoles. BYOD requires regulation: each new device creates a potential threat to overall endpoint security, making it vital to register all devices on the network. Organizations can then regulate consistent endpoint security across all connected devices and maintain necessary security updates and patches.
- While enterprises experience a qualified cybersecurity staff shortage and reduced budgets, they face more sophisticated and multivectored attacks. Effective endpoint security reduces business risk and allows an organization to grow. Vendors providing automated tools, including unified management and integrated platforms, assist organizations with limited cybersecurity personnel.
- AI is an emerging technology that is enabling attackers to deploy more dangerous attacks. Security vendors can also leverage the technology to combat the influx in attacks. Organizations increasingly leverage ML and AI, including generative AI, to strengthen their security posture and reduce administrative overhead owing to a lack of security expertise to keep up with the fast-evolving security threats.

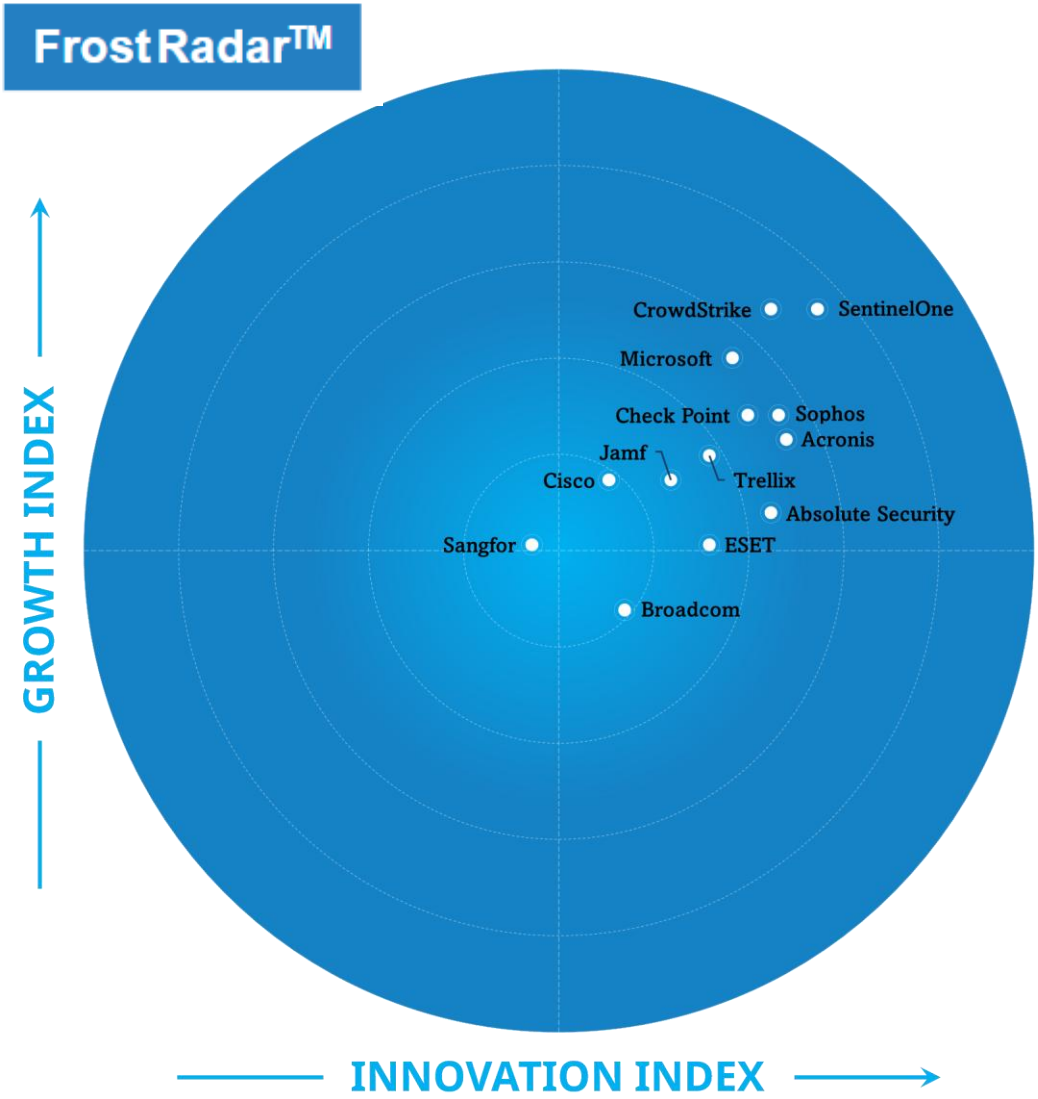
Growth Environment (continued)

- While many vendors already utilize AI technology in their products to a certain extent, widespread integration remains a work in progress. The symbiotic benefits of AI and cybersecurity go beyond just natural language processing (NLP) and generative AI, offering a broader scope, such as data contextualization, automated workflows, dynamic threat visualizations, and custom reports.
- An increase in connected devices creates a need for user and asset management features, taking into consideration device and account type and operating system in the business environment. Security solutions must constantly adapt to keep up.
- The restraint on market growth is vendors not investing to meet customers' performance and scalability needs. Vulnerabilities increase with the number of applications on each device. Various applications could be noncompliant with an organization’s security policies and are missing or have outdated OS patches. Endpoint security vendors must constantly push automatic updates and patches to organizational devices, which is difficult with the increase in zero-day attacks.

FROST & SULLIVAN

Frost Radar™: Endpoint Security

Frost Radar™: Endpoint Security



Frost Radar™ Competitive Environment

- Endpoint security is a saturated, mature, highly competitive, and crowded market with more than 40 vendors competing. Established endpoint security vendors continue to dominate the market and compete for a larger market share.
- In 2024, the top 5 vendors had a cumulative market share of 52%, up from 46.8% for 2023's estimation and reversing a declining trend observed in the market since 2019. Microsoft, CrowdStrike, and Trellix lead the endpoint market by revenue.
- SentinelOne has grown rapidly in the last few years and leads on the Frost Radar™ Growth and Innovation Indexes. The vendor's Singularity platform aims to help customers consolidate multiple security functions. This includes endpoint protection, EDR, network discovery, advanced incident response tools, vulnerability management, cloud workload security, and identity security.
- CrowdStrike is a leader on the Frost Radar™ Growth Index and a strong performer on the Innovation Index, with its above-industry-average growth rate and one of the largest market shares in endpoint security.
- Microsoft leads the endpoint security market with an estimated 16.5% share of global revenues. Microsoft's Windows OS has versions for small, medium, and large enterprises, each with built-in endpoint security—Microsoft Defender for Endpoint.
- Sophos, Trellix, and Check Point are strong performers, leveraging their broad security portfolios to generate multiple revenue streams and consolidated platform approaches.
- Acronis and ESET are well established in the SMB segment and pull most of their endpoint revenue from there.

SentinelOne

INNOVATION

- Achieving 100% detection and zero delays across all steps and operating systems in the MITRE ATT&CK 2024 Enterprise Evaluations, SentinelOne's Singularity Platform delivered top-tier performance by detecting all 16 attack steps and 80 substeps, proving the platform’s defense against advanced real-world cyber threats.
- Combining a cloud-native and AI-native approach, SentinelOne boasts AI/ML capabilities self-contained in the agent, allowing it to take response actions quickly. SentinelOne’s lightweight agent is designed for minimal user impact and architected to limit kernel interactions, reducing the risk of kernel panics and allowing for a more resilient architecture. The unified agent also allows for protection against endpoint and identity-based attacks with a single platform.
- With behavioral AI and automation built into the system, SentinelOne’s solution autonomously responds as soon as a threat is detected. With its patented one-click remediation piece and its unique deception/interception capabilities, the vendor’s offering reverses all changes made by an attacker to their pre-infected state within minutes.

SentinelOne (continued)

GROWTH

- SentinelOne is a leader on the Frost Radar™ Growth Index, with rapid and sustained growth performance over the period studied.
- Technology-driven differentiation, key business strategies with its channel and partner network, as well as its go-to-market model are drivers behind SentinelOne's growth performance. The vendor substantially expanded its total addressable market from endpoint security to identity, cloud, SIEM, and exposure management, adding numerous capabilities with Purple AI, experiencing exponential growth.
- SentinelOne's endpoint security platform supports a large ecosystem of technology partners and other security solutions, integrating endpoint and identity alerts from third parties as well. Such integration and standardization significantly enhance user experience and onboarding of new customers, with great impact on the vendor's growth performance.

SentinelOne (continued)

FROST PERSPECTIVE

- SentinelOne is the best performing vendor on the 2025 Frost Radar™ and a leader on both the Growth and Innovation indexes. Frost & Sullivan applauds the vendor's technology-first approach, close attention to market needs and megatrends, sustained sales relationships with its global partners, and strategic roadmap.
- Built on the Singularity Data Lake, in April 2024 SentinelOne released Purple AI as an add-on to its endpoint security solution, accelerating threat detection and incident response for security analysts. Together with its Singularity Ops Center and vulnerability management offerings, as well as its roadmap to improve its behavioral and static AI models, the vendor's endpoint security offering will continue to significantly increase efficiency and ease of use for human analysts.
- To sustain its growth and expand its platform approach in endpoint security, the vendor should continue its investments and R&D on credential protections, capabilities against identity-based attack vectors, and exposure management offerings.

Best Practices & Growth Opportunities

Best Practices

1. Streamlined processes, consolidation, and automation of common analyst workflows are improving the mean time to investigate. Best practices include solutions that go beyond EPP/EDR into XDR with capabilities to integrate SOC experience with unified alert management and unified asset inventory.

2. Automated response and rollback capabilities against ransomware attacks are a key functionality that vendors offer. These capabilities allow organizations to quickly recover from ransomware attacks by restoring systems to a preinfected state without manual intervention. This process typically involves backing up data and system configurations, enabling a seamless restoration of affected systems. By automating the rollback, businesses can minimize downtime and reduce ransomware's impact on operations.

3. Many organizations struggle to keep pace with the complexity of cyber threats and require highly skilled security analysts to detect attacks and trace how adversaries gained access. For a comprehensive view on threat hunting and investigations, analyzing telemetry from various security layers, including endpoint, network, email, and identity security, on an ongoing basis is crucial.

Growth Opportunities

1. While AI has introduced new risks and challenges, endpoint security vendors can leverage AI technology using enhanced detection capabilities and automated responses to combat cyber criminals. It is important for customers to choose a security vendor with differentiating AI capabilities, but to be cautious of those that are grandiose about their capabilities.

2. Implementing an effective MTD strategy that complements endpoint security is essential for organizations of all sizes. If implementation is not done correctly, an organization could experience a catastrophic cybersecurity incident that would harm customer experience, operations, and revenue.

3. A defensive plan including prevention technology and a response method for a potential attack is an effective strategy for detecting and mitigating zero-day attacks. Organizations must prepare for attacks because vulnerabilities are present in every environment. Worst-case scenario preparedness allows security teams to mitigate a security event if an attack penetrates a network.

FROST & SULLIVAN

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a compan s revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

GI3

GROWTH PIPELINE™
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGATRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders

Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com

© 2025 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.