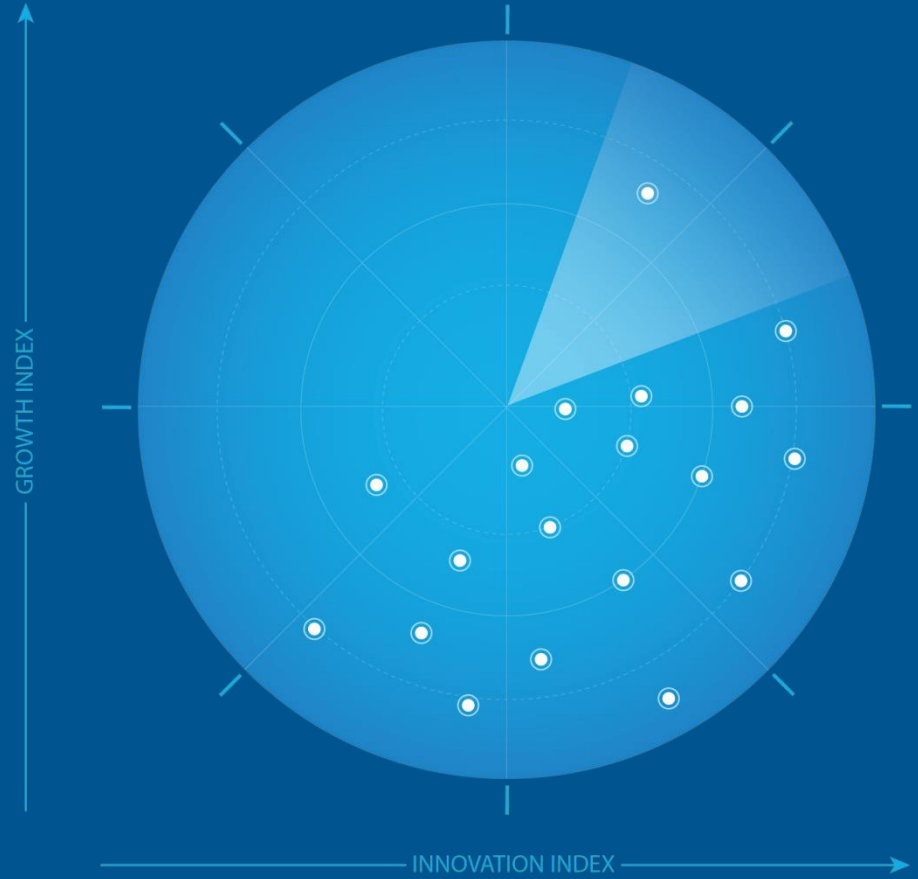


# Frost Radar™: Endpoint Security, 2023

Authored by: Sarah Pavlak

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



October 2023

FROST & SULLIVAN

# Strategic Imperative and Growth Environment



# Strategic Imperative

The endpoint security market fluctuates. Changing work environments and continuously evolving cyber threats drive the market's technological advancement. Addressing new endpoint security product use cases and applications helps market leaders maintain a competitive edge and sustain growth.

- The threat landscape is changing because cyberattacks are more lucrative, and new cybercriminal groups are emerging. Enterprise attack surfaces are expanding because more individuals use their devices and connect remotely. Attackers exploit remote working environments with various endpoint devices, lacking proper security management.
- Some organizations lack the resources or expertise to defend against cyberattacks targeting IoT devices. Some outdated IT security methods cannot recognize IoT endpoints as entry points for attack, offering cyber criminals an open door to the corporate network. Some unmonitored IoT devices send unencrypted messages within and outside a corporate network, allowing hackers to intercept sensitive data. Endpoint security solutions can detect this through continuous data collection and behavioral analytics.
- Remote work and bring your own device (BYOD) add to the challenges of protecting endpoints because of the increase in the number of devices and an organization's lack of physical control over them.

Source: Frost & Sullivan

# Strategic Imperative (continued)

- Endpoint security paired with network security solutions deliver on the ideal of a holistic, zero-trust security architecture—the future of security portfolios. Some vendors already offer such integrated solutions, and more will embrace the strategy in the next few years.
- Organizations know they must improve their cybersecurity posture. Security technologies and the threats they aim to thwart are becoming more sophisticated and complex, prompting enterprises to employ advanced technologies such as extended detection and response (XDR) as a consolidation strategy.



# Growth Environment

- In 2023, enterprise spending on endpoint security solutions is projected to exceed \$12.2 billion globally. Frost & Sullivan projects spending to reach \$22.3 billion by 2027, achieving a compound annual growth rate of 16.2%.
- In response to cyberattacks' increasing severity and sophistication, the endpoint security market has had strong double-digit growth over the last five years. A growth driver is organizations migrating to the cloud—transitioning from on-premises to cloud-delivered solutions.
- Continued growth in endpoint devices, BYOD, and IoT device connectivity will increase enterprise web traffic and enterprises' need for endpoint protection capabilities. More devices on the network will require scaling and more security services. Some vendors offer endpoint protection platforms (EPP).
- Many organizations have shifted to hybrid workspace environments after a period of fully remote work at the start of the COVID-19 pandemic. However, that has opened them to new risks and forced IT security to counter unknown threat vectors as users work outside traditional network security perimeters.



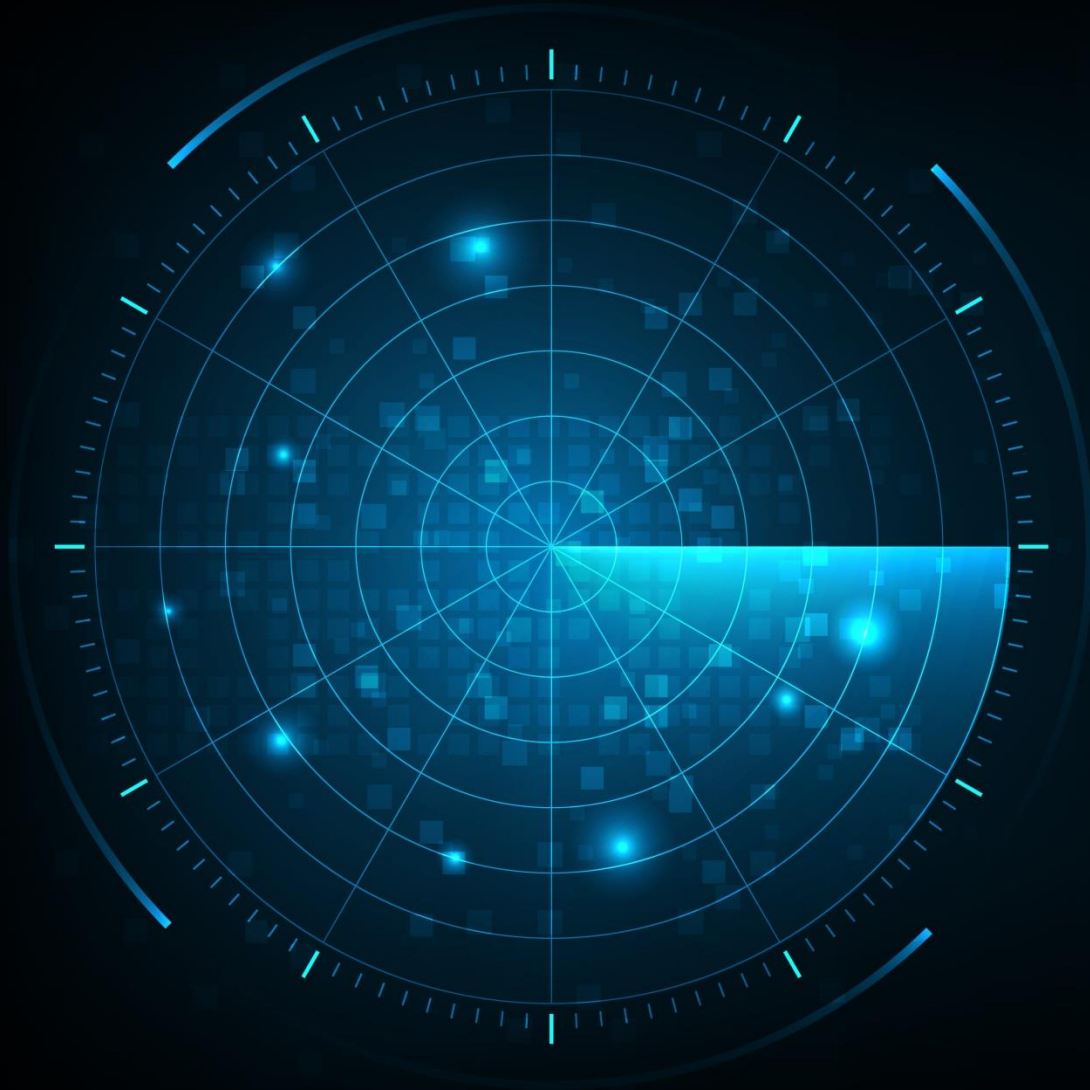
Source: Frost & Sullivan

# Growth Environment (continued)

- Secure access service edge (SASE), zero trust, and platform integration will enhance endpoint security's efficacy and value. These factors will contribute to industry growth.
- The banking, government, healthcare, and manufacturing industries have experienced novel and previously unseen types of cyberattacks during the pandemic years. These industries remain vulnerable, driving the need for better endpoint security solutions.
- Threats will continue to evolve and challenge existing endpoint security solutions. Ransomware will remain a prominent threat, and endpoint security vendors will innovate and deliver new solutions to counter advanced threats.



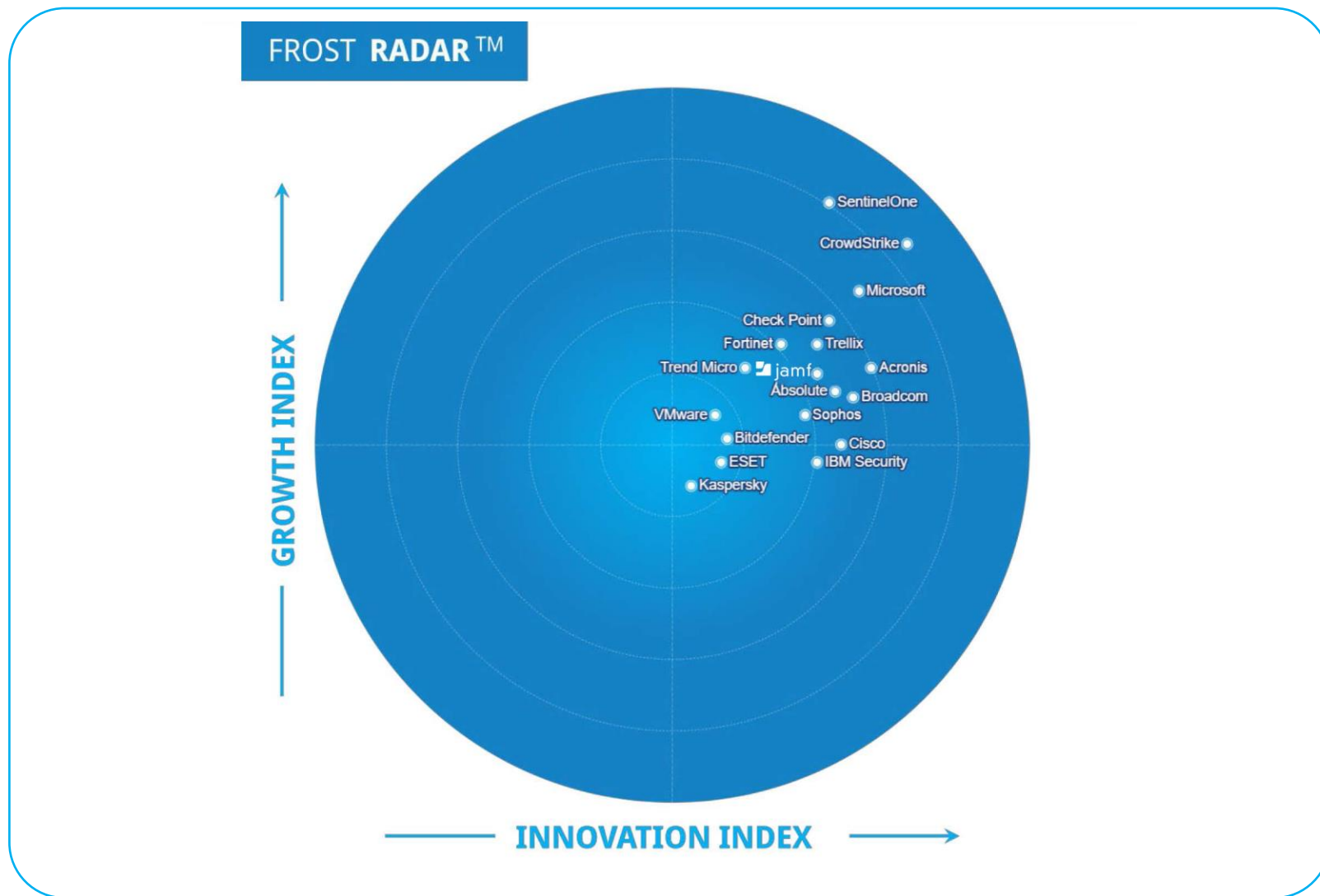
Source: Frost & Sullivan



**Frost Radar™**

**Global Hiring  
Platform Market**

# Frost Radar™: Endpoint Solutions, 2023



Source: Frost & Sullivan



# Frost Radar™

## Competitive Environment

- In a competitive field of more than 50 participants globally in the endpoint security space, Frost & Sullivan independently plotted 18 growth and innovation leaders in this Frost Radar analysis.
- Security vendors continuously innovate and expand endpoint security features and functions to make their technologies more competitive and better able to counter increasingly sophisticated cyberattacks.
- Vendors recognize the shift to platform service consolidation and are making their technologies capable of merging with broader solution suites. The ability to offer unified device security is a significant factor as customers seek to consolidate their security solutions and reduce the management overhead of an expanded security perimeter.
- The endpoint security market is saturated, mature, highly competitive, and crowded. The technology is becoming commoditized, but vendors are developing functions and features to counter new threats and adjust to changing standards.



Source: Frost & Sullivan

# 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.

Source: Frost & Sullivan

**Companies to Action:**  
**Companies to Be Considered First for**  
**Investment, Partnerships, or Benchmarking**

# Company to Action: Jamf

## Innovation

- According to Jamf, Apple systems and devices require unique security solutions, so it focuses on protecting the Apple platform and preserving the native Apple experience. It is the only vendor in the endpoint security market developing “Apple-first” solutions.
- Zero-touch deployment allows for devices to be pulled into management and secured from the first time they are powered on. This requires no administrator interaction on the hardware.
- Jamf’s endpoint security solution, Jamf Protect, provides real-time detection of malicious applications and scripts and recommended user actions, consistent vulnerability management, threat prevention, and policy control and security reporting across all Mac and mobile platforms including MacOS, iOS iPadOS, and Android. Additional web threat protection includes these platforms and extends to Windows and Chromebooks.
- Over the past few years, Jamf has dramatically expanded its configuration and auditing framework to help customers meet complex compliance standards. Jamf has also enhanced the richness of its endpoint telemetry for export to third-party log collection and analytics tools.

Source: Frost & Sullivan

# Company to Action: Jamf (continued)

## Innovation

- Jamf's endpoint security solutions provide consistent policy enforcement and support for both company-issued and personal devices.
- Jamf's Trusted Access is the only solution specifically built for Apple devices that combines device management, identity and access, and endpoint security.



# Company to Action: Jamf (continued)

## Growth

- Jamf has invested significantly in endpoint risk assessment integrations with modern security policy frameworks, including conditional access policies, zero-trust network access (ZTNA) policies, Microsoft Device Compliance, AWS Verified Access, and Google BeyondCorp access rules. The company plans to continue improving Mac and mobile EDR capabilities to combat evolving sophisticated threats.
- Jamf's growth strategy is differentiation as the only Apple-first security solution provider. This includes continuing its leadership status in Mac management and security, focused on the customer experience. The company has seen above-average revenue growth and a net retention rate exceeding 100%, which will likely continue as organizations continue to invest in Apple devices.
- Jamf's R&D team regularly monitors developments in the Apple ecosystem to ensure Jamf products, specifically those in device management and identity and endpoint security, can support new updates and features on Apple product release days.

Source: Frost & Sullivan

# Company to Action: Jamf (continued)

## Frost Perspective

- Jamf should continue to capitalize on its unique value proposition in the endpoint security market. Jamf should add security awareness training programs, which are not as prevalent as in other markets, such as email security, into its business strategy and service suite. Phishing training to defend against user-initiated risks could attract more customers and be a gateway into other markets.
- Continuing to expand its unique product portfolio with more integrations will set the company up for a merger or acquisition opportunity with a more prominent endpoint security vendor.
- Focusing on Mega Trends directly related to growth opportunities, such as extending its reach into network security and further into ZTNA will increase Jamf's customer base for those working specifically with Apple devices and looking for a multi-tiered security strategy.



## Key Takaways

# Key Takeaways

1

Stand-alone endpoint security solutions can be too complex for some organizations to manage effectively. Unifying EPP and EDR within a single cloud-based platform allows these complementary solutions to protect endpoints comprehensively. Enterprise attack surfaces have grown. Threat risk is one of several trends (including technological innovation and platform consolidation) driving EDR and XDR adoption.

2

The migration from EDR to XDR is accelerating and generating attention: XDR offers a unified suite of EDR and related security technologies and provides broader, extended visibility into all phases of an attack on an endpoint. This allows security teams to monitor any changes to the environment, thwart an attacker, or launch a manual investigation at any attack stage.

3

Many customers have too many siloed security solutions. This patchwork complicates security administration, makes communication between solutions difficult, and can create significant security gaps. Customers want fewer, better, and more comprehensive security solutions.



# Key Takeaways

4

End-to-end visibility solutions (platforms or suites) ensure better endpoint security and an easier means to locate and address any security issues that may arise. They are also easier to administer, offering single-pane-of-glass monitoring and unified security policy development. A customer aims to access an integrated, secure cloud solution that supports zero trust access.

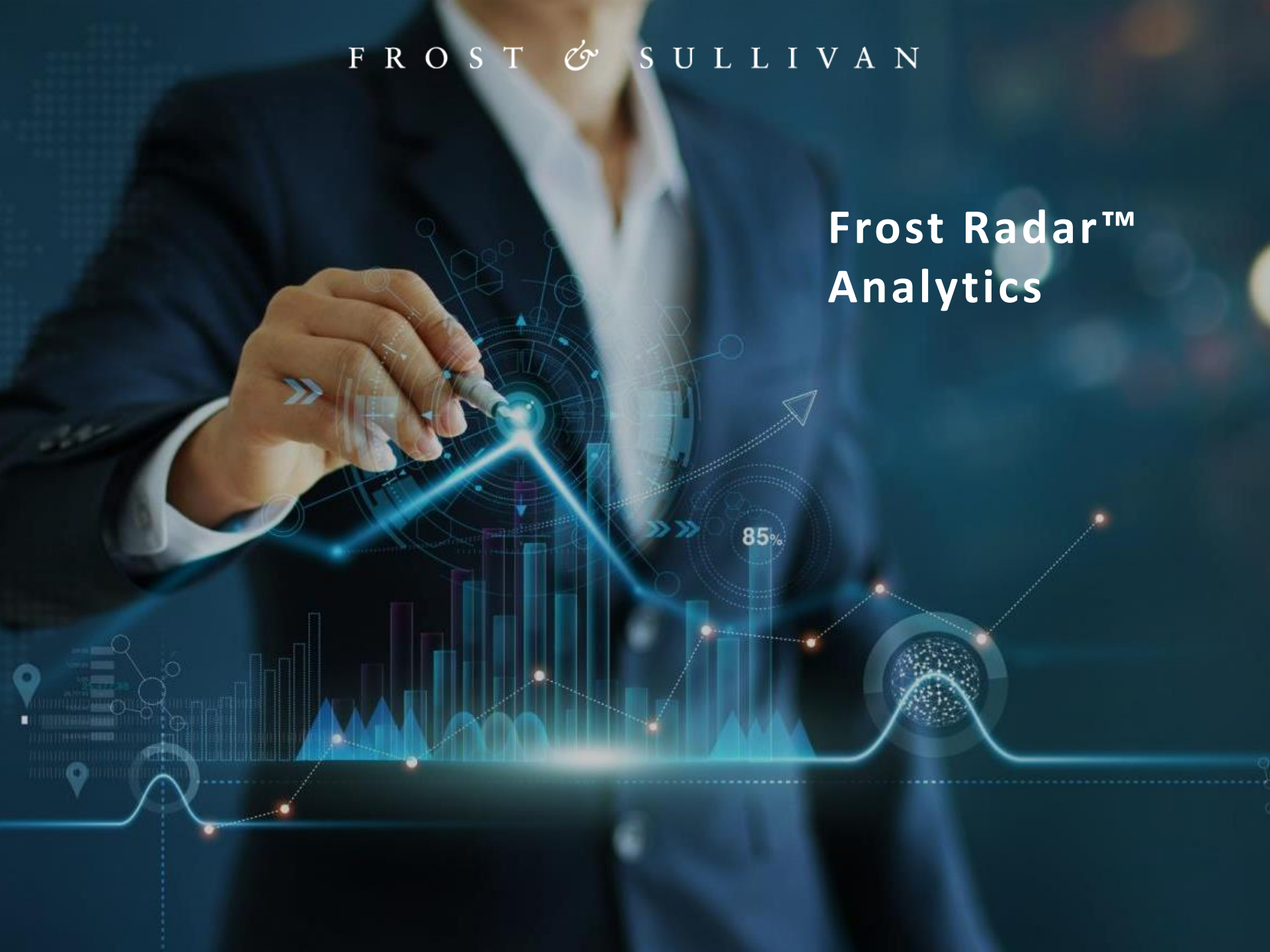
5

Deploying a security suite that combines endpoint security capabilities is better for customers than a piecemeal, multivendor, point-solution approach. To gain and preserve momentum in the market, EDR vendors must consider these considerations and pursue integrated platform development strategies.



FROST & SULLIVAN

# Frost Radar™ Analytics



# Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

## VERTICAL AXIS

**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.

## GROWTH INDEX ELEMENTS

- **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 company'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

## HORIZONTAL AXIS

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

## INNOVATION INDEX ELEMENTS

- **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: MEGA TRENDS 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 Mega Trends 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.

# 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](mailto:permission@frost.com)

© 2023 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.