

KuppingerCole Report

# LEADERSHIP COMPASS

By **John Tolbert**  
May 12, 2022

## Endpoint Protection Detection & Response

The KuppingerCole Leadership Compass provides an overview of a market segment and the vendors in the Endpoint Protection, Detection & Response (EPDR) market. It covers the trends that are influencing this market segment and the essential capabilities required of solutions in this space. It also provides ratings of how well these solutions meet our expectations. This report covers the previously distinct but now converged fields and product lines of Endpoint Protection (EPP) and Endpoint Detection & Response (EDR).



By **John Tolbert**  
[jt@kuppingercole.com](mailto:jt@kuppingercole.com)

# Content

|                                              |           |
|----------------------------------------------|-----------|
| <b>1 Introduction / Executive Summary</b>    | <b>4</b>  |
| 1.1 Highlights                               | 6         |
| 1.2 Market Segment                           | 7         |
| 1.3 Delivery Models                          | 8         |
| 1.4 Required Capabilities                    | 8         |
| <b>2 Leadership</b>                          | <b>10</b> |
| 2.1 Overall Leadership                       | 10        |
| 2.2 Product Leadership                       | 11        |
| 2.3 Innovation Leadership                    | 13        |
| 2.4 Market Leadership                        | 15        |
| <b>3 Correlated View</b>                     | <b>18</b> |
| 3.1 The Market/Product Matrix                | 18        |
| 3.2 The Product/Innovation Matrix            | 20        |
| 3.3 The Innovation/Market Matrix             | 21        |
| <b>4 Products and Vendors at a Glance</b>    | <b>24</b> |
| <b>5 Product/Vendor evaluation</b>           | <b>27</b> |
| 5.1 Comodo                                   | 28        |
| 5.2 CrowdStrike                              | 32        |
| 5.3 Cybereason                               | 36        |
| 5.4 ESET                                     | 40        |
| 5.5 Fidelis Cybersecurity                    | 44        |
| 5.6 Microsoft                                | 48        |
| 5.7 SentinelOne                              | 52        |
| 5.8 Sophos                                   | 56        |
| 5.9 Symantec (was acquired by Broadcom Inc.) | 60        |
| 5.10 WithSecure                              | 63        |
| <b>6 Vendors to Watch</b>                    | <b>67</b> |
| 6.1 AhnLab                                   | 67        |

|                                     |           |
|-------------------------------------|-----------|
| 6.2 Checkpoint . . . . .            | 67        |
| 6.3 Deep Instinct . . . . .         | 67        |
| 6.4 GoSecure . . . . .              | 67        |
| 6.5 Heimdal Security . . . . .      | 68        |
| 6.6 Infocyte . . . . .              | 68        |
| 6.7 Malwarebytes . . . . .          | 68        |
| 6.8 Tanium . . . . .                | 69        |
| 6.9 Trellix . . . . .               | 69        |
| 6.10 Trend Micro . . . . .          | 69        |
| 6.11 Webroot . . . . .              | 70        |
| <b>7 Related Research . . . . .</b> | <b>71</b> |
| <b>Methodology . . . . .</b>        | <b>72</b> |
| <b>Content of Figures . . . . .</b> | <b>78</b> |
| <b>Copyright . . . . .</b>          | <b>79</b> |

# 1 Introduction / Executive Summary

Malware is and will likely continue to be a top threat and thus a top concern among business and IT security professionals. The pace of malware development and delivery has only quickened since the last iteration of this report.

Malware comes in many forms: viruses, worms, rootkits, botnets, file-less malware, ransomware, and crypto-miners are prevalent in the wild. Malware is usually, and almost by definition, an exploitation of an operating system or application vulnerability.

Ransomware attacks are still popular and evolving. Ransomware is a form of malware that encrypts users' data, demanding that ransom be paid for the return of control or for decryption keys. The newest forms of ransomware are deployed similarly to an APT campaign, with staging of ransomware on various machines throughout an enterprise and exfiltration of data prior to ransomware detonation. Needless to say, paying the ransom only emboldens the perpetrators and perpetuates the ransomware problem. Moreover, in many cases the ransomware operators do not provide working decryption keys, so paying the ransom is purely a waste of money. Over the last couple of years, some attackers have used ransomware techniques and payloads for purely destructive purposes too -- rather than asking for ransom, these destructive "wiper" ransomware types simply delete or zero out data.

Much of the cybersecurity industry has, in recent years, shifted focus to detection and response rather than prevention. However, in the case of ransomware and wipers, detection is pretty easy because the malware announces its presence as soon as it has compromised a device. That leaves the user to deal with the aftermath. Once infected, the choices are to:

- Pay the ransom and hope that malefactors return control or send decryption keys (not recommended since it doesn't always work and incentivizes criminals)
- Wipe affected machines and restore data from backup
- In the case of wipers, there is no choice but to rebuild from backups

Restoration is sometimes problematic if users or organizations haven't been keeping up with backups, or if backups have been contaminated by malware. Even if backups are readily available, time will be lost in cleaning up the compromised computers and restoring the data. Thus, preventing ransomware infections is preferred. However, no anti-malware product is 100% effective at prevention. It is still necessary to have good, tested backup/restore processes for cases where anti-malware fails.

Ransomware attacks often arrive as malicious links or weaponized Office docs via phishing campaigns. Disabling macros can help, but this is not universally effective since many users need to use legitimate

macros. Ransomware can also come less commonly from drive-by downloads and malvertising.

Viruses are far more sophisticated than they were decades ago. Now viruses are generally polymorphic, meaning they alter their structure to try to avoid detection upon every iteration. Viruses infect files and usually need user interaction to initiate a compromise.

Worms are malicious code that spreads across unsecured networks, relying upon unpatched, compromised applications and unprotected ports.

Rootkits are low-level malware usually implemented like device drivers in operating systems. Rootkits allow bad actors complete control of affected machines.

Botnets are collections of controlled devices, often compromised by rootkits, that are used in large numbers to magnify other kinds of attacks, such as Distributed Denial of Service (DDoS) attacks, credential stuffing, account take-overs (ATOs), or other forms of cybercrime. Botnets can be composed of PCs, servers, smartphones, IoT devices, etc.

File-less malware is a malicious innovation that seeks to avoid signature-based anti-malware scanners by propagating between machines without being written and transferred as files. Instead, file-less malware is malicious code which spreads by process or memory injection. Once on a target device, file-less malware uses native tools like PowerShell or .NET to assemble and execute the malicious payload. File-less malware attacks are still on the rise.

Crypto-jacking is the unwanted execution of crypto-mining software on user devices. Crypto-jackers capitalized on the surge of cryptocurrency prices. Crypto-jacking incidents continue as cryptocurrency prices fluctuate, annoying device owners with increased power costs and depleted batteries in the case of mobile devices. Initially, some anti-malware solutions did not identify crypto-mining software as malicious since it could be built with freely available and sometimes legitimate code.

All end-user computers, smartphones, and tablets should have Endpoint Protection (EPP) clients installed, preferably with up-to-date subscriptions. Servers and virtual desktops should be protected as well. Windows platforms are still the most vulnerable, though there are increasing amounts of malware for Android. It is important to remember that Apple's iOS and Mac devices are not immune from malware, and as market share increases, particularly for Mac devices, the amount of malware for that platform will increase too.

Endpoint Detection & Response (EDR) solutions look for evidence and effects of malware that may have slipped past EPP products. EDR tools are also used to find signs of malicious insider activities such as data exfiltration attempts, left-behind accounts, and open ports. EDR solutions log activities centrally, allow administrators to examine endpoints remotely, and generate reports often complete with attribution theories and confidence levels.

Additionally, as part of the detection process, EDR also enables querying and evaluation of Cyber Threat Intelligence (CTI), event correlation, interactive querying of nodes across the customer environment, live memory analysis, and activity recording and playback. EPDR helps to automatically uncover attacks and enables security teams to understand what is happening from start to finish by consolidating all relevant information into a single view.

For the response phase, EDR solutions can provide alerts and reports, create attribution theories with confidence levels, update detection rules, shut down offending processes, delete or move files, automatic quarantine of assets suspected of having been compromised, and even rollback of compromised endpoints to known good states.

EDR solutions offer customizable levels of automation for investigations and remediation. The most functionally complete EDR solutions perform continuous monitoring, anomaly detection and categorization, proactively hunt for threats across an enterprise, and create cases then alert human analysts. When analysts take the case, they find up-to-date event lists, correlation across all affected nodes, timeline views, and pertinent CTI within their main screen.

Over the course of the last 5 or so years, EPP and EDR toolsets, and in some cases, vendors, have been converging into EPDR (Endpoint Protection Detection & Response).

EPDR solutions must be tightly integrated with other tools in vendor suites and should interoperate with security analytics tools such as Security Incident and Event Management (SIEM) and Security Orchestration Automation & Response (SOAR) tools. To achieve this integration, most EPDR suites support CEF, REST APIs, and syslog. Interoperability with IT Service Management (ITSM) solutions enables organizations to rely on a single system for ticket creation and management. Across the surveyed vendors, support for SIEM is widespread, with some support for SOAR, followed by limited interoperability with ITSM systems. A subset of EPDR solutions essentially outsource orchestration and automation to SOAR products.

XDR (eXtended Detection & Response) solutions are an emerging category of security tools that are designed to consolidate and replace multiple point solutions such as Endpoint Protection Detection & Response (EPDR), Network Detection & Response (NDR), Cloud Workload Protection Platform (CWPP), Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS), Distributed Deception Platforms (DDP), and Unified Endpoint Management (UEM). XDR solutions will also need to draw on telemetry from IAM systems, particularly User Behavioral Analytics (UBA) and Identity Governance and Administration. In our definition and view, XDR must encompass endpoint, network, and cloud aspects. This means that XDR solutions must have agents for endpoints, sensors for networks, and agents for cloud instances and containers.

The **MITRE ATT&CK Framework** is a comprehensive look at all the various TTPs that malicious actors use to compromise systems for the purpose of data exfiltration. Many security vendors contribute to MITRE ATT&CK and many of their tools map detections to the various steps and techniques to facilitate analysis within their product interfaces.

A number of different, independent testing regimes exist that vendors can participate in to demonstrate the effectiveness of their products. AV-Comparatives, AV-Test, and ICSA Labs run tests focusing on malware detection and prevention. They also run in-depth tests to simulate the kinds of scenarios business users encounter. MITRE.org has conducted four in-depth tests designed to show the efficacy of EDR solutions. KuppingerCole reviewed test results as published by these organizations for vendors examined below.

This Leadership Compass covers solutions that contain capabilities found in both EPP and EDR products.

## 1.1 Highlights

The top findings from this edition of the Leadership Compass on EPDR are:

- The majority of the products and services surveyed have interfaces that are aligned with MITRE ATT&CK, indicating its widespread acceptance as a standard for conceptualizing cyber-attack Tactics, Techniques, and Procedures (TTPs).
- The shift to vendor cloud-hosted management continues.
- Not all EPDR vendors offer a complete set of secondary protection functions, such as URL filtering, app controls, device controls, endpoint firewalls, and system file integrity monitoring.
- Malware detection models powered by Machine Learning algorithms are the norm, innovation is evidenced by those utilizing Deep Learning (DL), with behavioral detection models powered by Machine Learning (ML) algorithms varying in capability by vendor.
- The level of automation possible directly within EPDR products and interoperability with SOAR platforms varies within the field. Mature organizations will want to give extra consideration to these features.
- The evolution of EPDR into XDR has begun, and some vendors are well on their way, but many vendors have a long way to go on their roadmap for this to come to fruition.
- The Overall Leaders in EPDR are CrowdStrike, Cybereason, ESET, Microsoft, SentinelOne, Sophos, and Symantec (by Broadcom).
- The Product Leaders in EPDR are CrowdStrike, Cybereason, ESET, Microsoft, SentinelOne, Sophos, and Symantec (by Broadcom).
- The Innovation Leaders in EPDR are CrowdStrike, Cybereason, ESET, Microsoft, SentinelOne, Sophos, and Symantec (by Broadcom).
- The Market Leaders in EPDR are CrowdStrike, ESET, Microsoft, SentinelOne, Sophos, and Symantec (by Broadcom).

## 1.2 Market Segment

This Leadership Compass covers solutions that can detect and prevent malware from executing on endpoints, have built-in firewalls, perform URL filtering, application allow/deny listing, and the full gamut of typical EDR functions such as monitoring for IoCs, file analysis, registry analysis, alerting/reporting,

attribution theory creation, threat hunting, and remediation. Solutions which offer EPDR functions as part of a larger suite as well as specialized/standalone EPDR packages are considered. For standalone EPDR, interoperability with other components of security and IT environments will be addressed.

## 1.3 Delivery Models

EPDRs solutions are made of two primary components: agents on the endpoints and a management console. Endpoint agents are designed per operating system, such as Microsoft Windows versions 7, 8, 10; Windows Server 2008+; MacOS 10 and 11; the various flavors of Linux, Cloud Workloads, Virtual Desktops, and mobile devices. A few vendors maintain agents for deprecated Windows versions such as XP and Vista. Management consoles are used by administrators to deploy, monitor, activate/deactivate certain features, and push updates; by SOCs and management to get current status; and by analysts for investigations. Management consoles for on-premises deployment are usually Windows Server or Linux based. Most vendors offer management consoles as SaaS. Licensing is generally per endpoint.

## 1.4 Required Capabilities

This report describes the basic capabilities that all solutions should support in terms of use cases, which are:

- Detection and prevention of malware execution and subsequent compromise
- Secondary endpoint protection capabilities such as
  - Endpoint firewall
  - URL filtering
  - Application allow-listing/deny-listing
  - System file integrity monitoring
- Detection of IoCs such as
  - Registry and system file changes
  - Unusual use of network ports by applications
  - Contact with known bad IPs and URLs
  - Unusual process injections
  - Modification of module load points



- Integration of Cyber Threat Intelligence and sandbox services
- Alerting and reporting mechanisms
- Query interface for investigations and threat hunting
- Console for admins, analysts, and threat hunters
- Manual and automatic response functions
  - Run CTI queries
  - Collect forensic evidence
  - Run scripts to support threat hunting, incident response, and systems management
  - Create cases and open tickets
  - Alert SOCs and analysts
  - Terminate processes
  - Update detection rules based on findings
  - Delete or quarantine files
  - Remove registry entries
  - Isolate nodes
  - Rollback endpoints to known good states

## 2 Leadership

Selecting a vendor of a product or service must not be based only on the information provided in a KuppingerCole Compass. The Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

### 2.1 Overall Leadership



Figure 1: The Overall Leaders in Endpoint Protection, Detection, and Response

The Overall Leaders are (in alphabetical order):

- CrowdStrike

- Cybereason
- ESET
- Microsoft
- SentinelOne
- Sophos
- Symantec (by Broadcom)

## 2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.



Figure 2: The Product Leaders in Endpoint Protection, Detection, and Response

**Product Leadership** is where we examine the functional strength and completeness of services.

The EPDR field is a synthesis of EPP (NGAV plus secondary features) and EDR. In order to reach the product leader position, vendor entries must contain the majority of the key required functions defined in chapter 1. CrowdStrike, SentinelOne, Sophos, and Microsoft lead the field with solutions that are both comprehensive and advanced in terms of protective capabilities. Cybereason, ESET, and Symantec (by Broadcom) also place in the product leaders' section.

WithSecure (rebranding of F-Secure Business), Fidelis Cybersecurity, and Comodo are the challengers in

the EPDR field.

Product Leaders (in alphabetical order):

- CrowdStrike
- Cybereason
- ESET
- Microsoft
- SentinelOne
- Sophos
- Symantec (by Broadcom)

## 2.3 Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

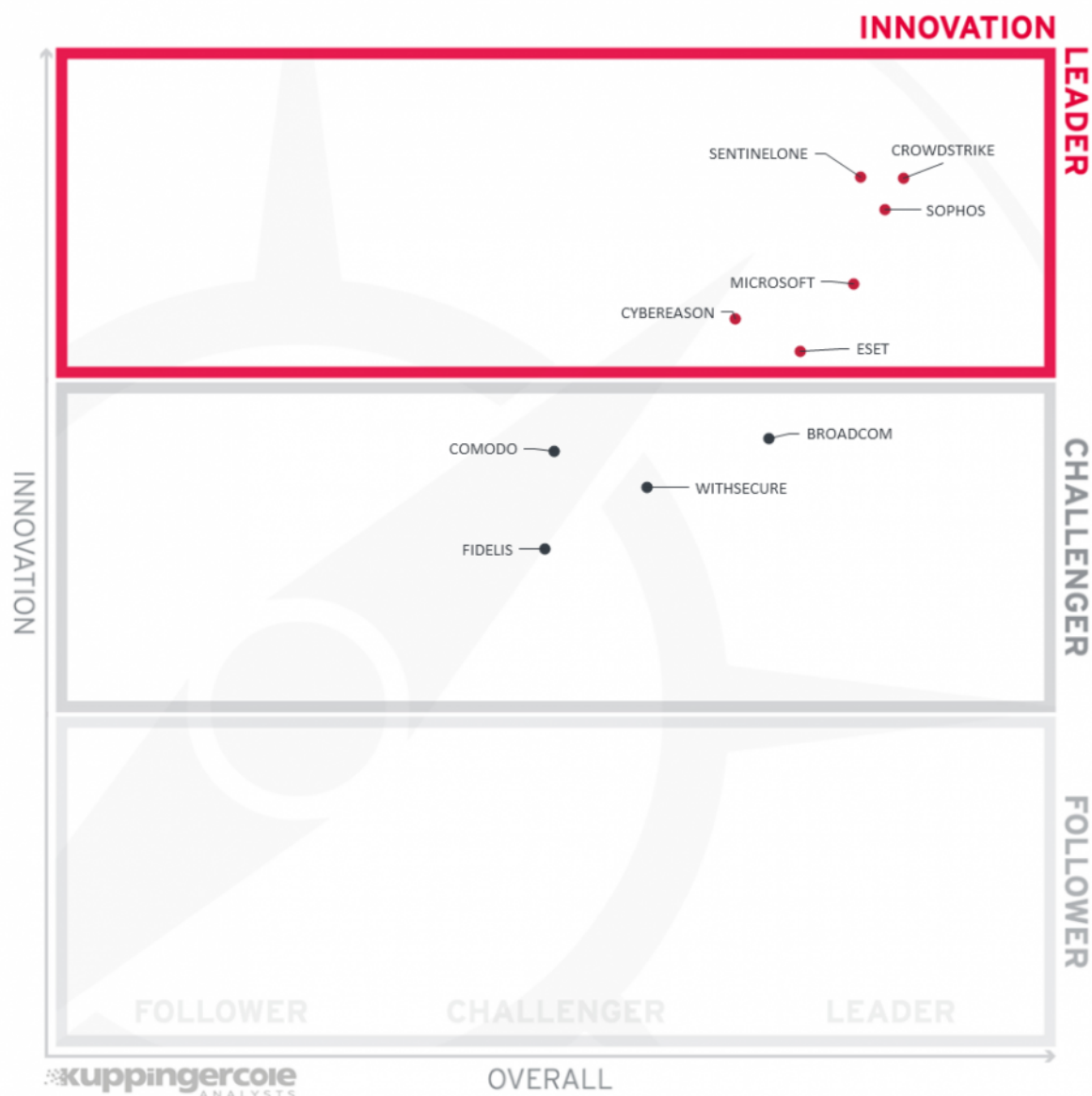


Figure 3: The Innovation Leaders in Endpoint Protection, Detection, and Response

Innovation in EPDR is characterized by the use of advanced malware identification technologies, the use of Deep Learning detection models, granularity in secondary EPP features such as application controls and URL filtering, intuitive interfaces for conducting investigations and threat hunts, the ability to construct playbooks for manual and automated remediation, workflow and case management, and integration with other parts of customers' security architecture.

CrowdStrike, SentinelOne, Sophos, Microsoft, Cybereason, and ESET are the leaders in EPDR innovation. Symantec (by Broadcom), Comodo, WithSecure, and Fidelis Cybersecurity are the challengers.

Innovation Leaders (in alphabetical order):

- CrowdStrike
- Cybereason
- ESET
- Microsoft
- SentinelOne
- Sophos

## 2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

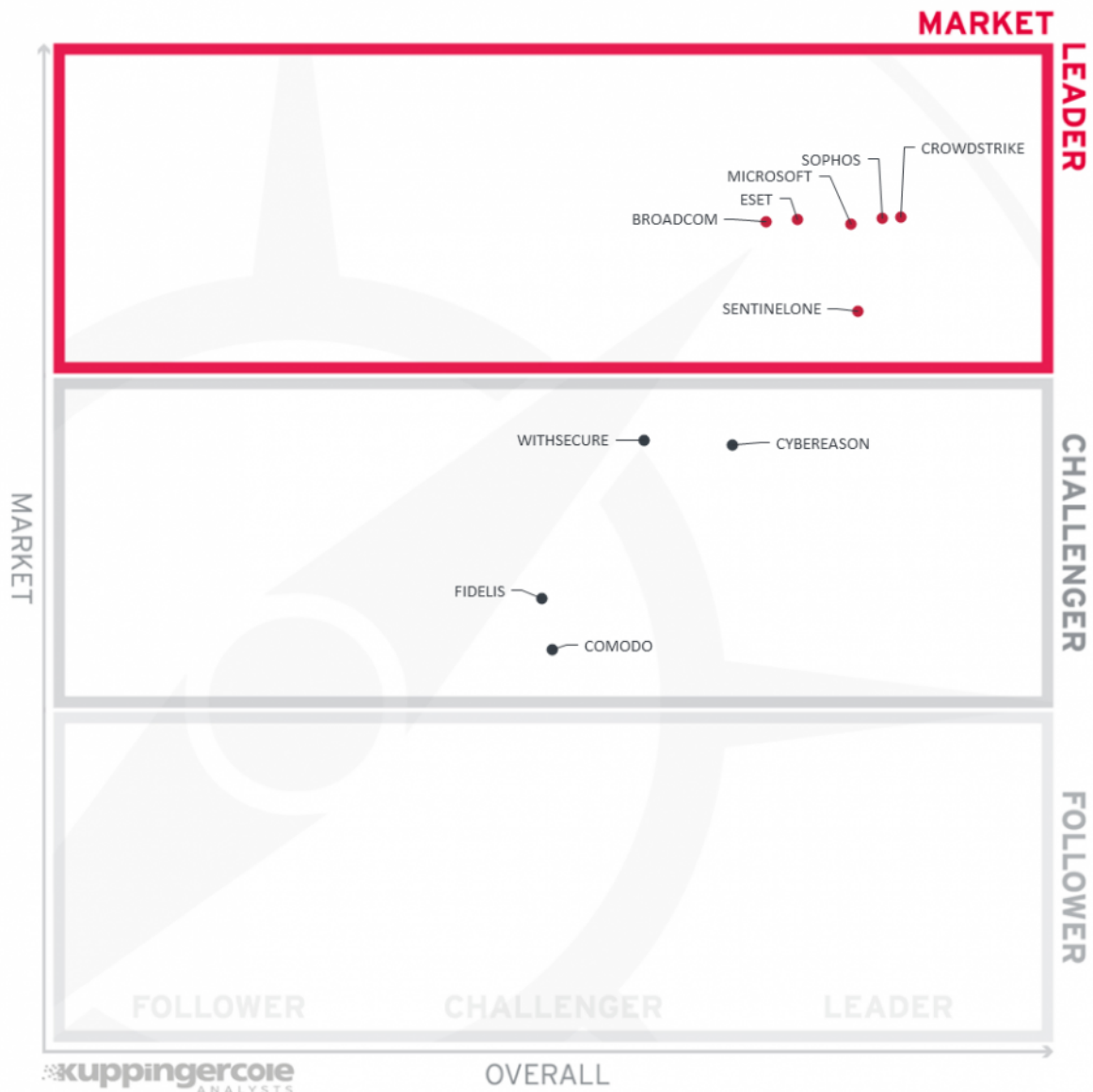


Figure 4: The Market Leaders in Endpoint Protection, Detection, and Response

The EPDR market is large, indeed all servers, desktops, laptops, tablets, and phones need EPDR solutions in the current threat landscape. Market leadership is determined by an amalgamation of metrics including numbers of enterprise and SMB customers, numbers of protected endpoints, geographic distribution of customers, vendor sales and support, and implementation partners, as well as overall vendor financial position.

CrowdStrike, Sophos, ESET, Symantec (by Broadcom), Microsoft, and SentinelOne are the market leaders among the evaluated field. WithSecure, Cybereason, Fidelis Cybersecurity, and Comodo are the challengers.



Market Leaders (in alphabetical order):

- CrowdStrike
- ESET
- Microsoft
- SentinelOne
- Sophos
- Symantec (by Broadcom)

## 3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

### 3.1 The Market/Product Matrix

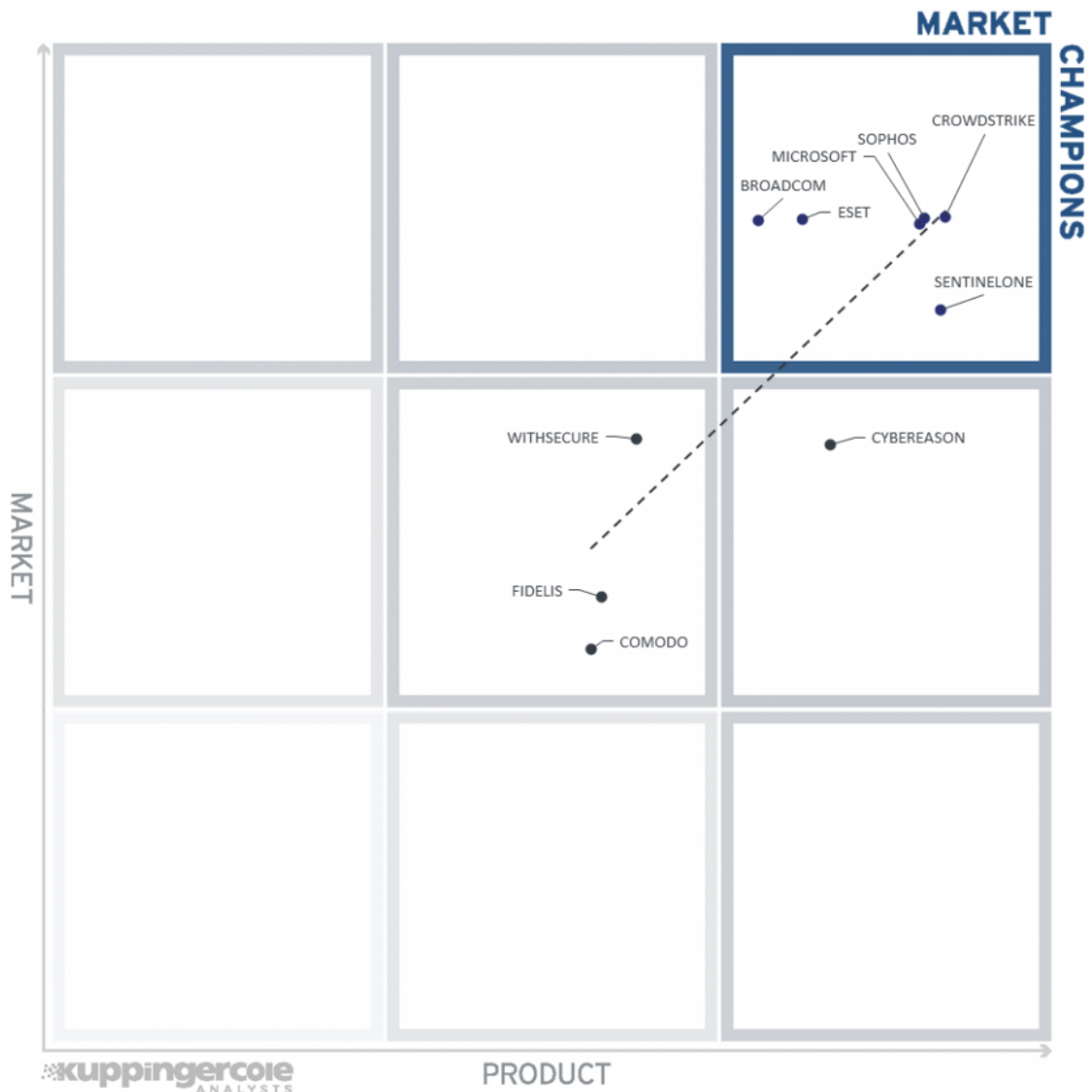


Figure 5: The Market/Product Matrix for Endpoint Protection, Detection, and Response

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

CrowdStrike, Sophos, ESET, Symantec (by Broadcom), Microsoft, and SentinelOne are the Market Champions in the top right square. The product strength correlates closely with market position.

Cybereason is in the center right, having a strong product and room for growth in market share.

WithSecure, Fidelis Cybersecurity, and Comodo are in the center of the chart.

### 3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a single exception. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

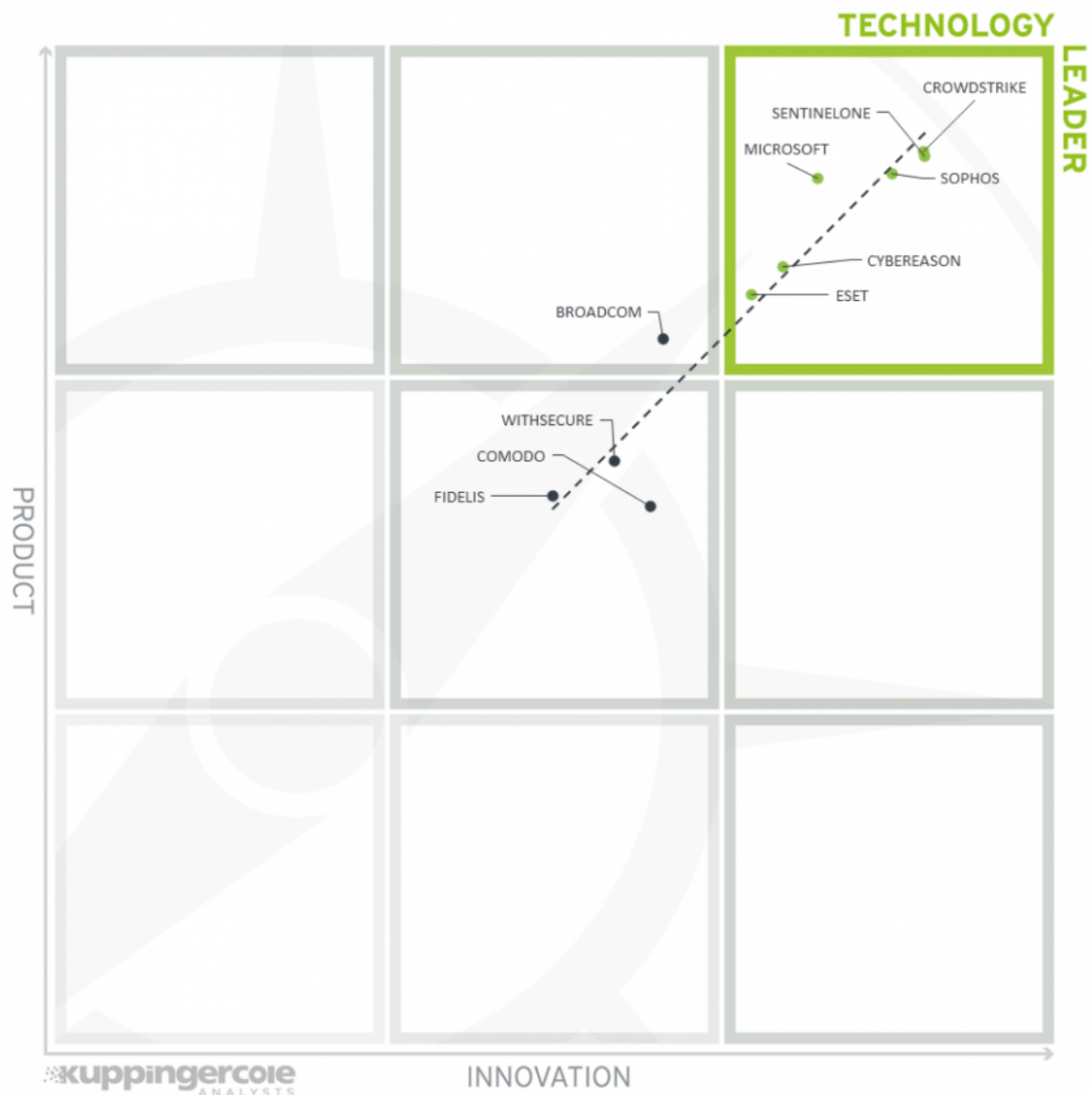


Figure 6: The Product/Innovation Matrix for Endpoint Protection, Detection, and Response

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Technology Leaders are CrowdStrike, SentinelOne, Sophos, Microsoft, Cybereason, and ESET. Symantec (by Broadcom) is in the top center, lagging a bit in innovation but with still a strong product. WithSecure, Fidelis Cybersecurity, and Comodo are found in the center.

### 3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

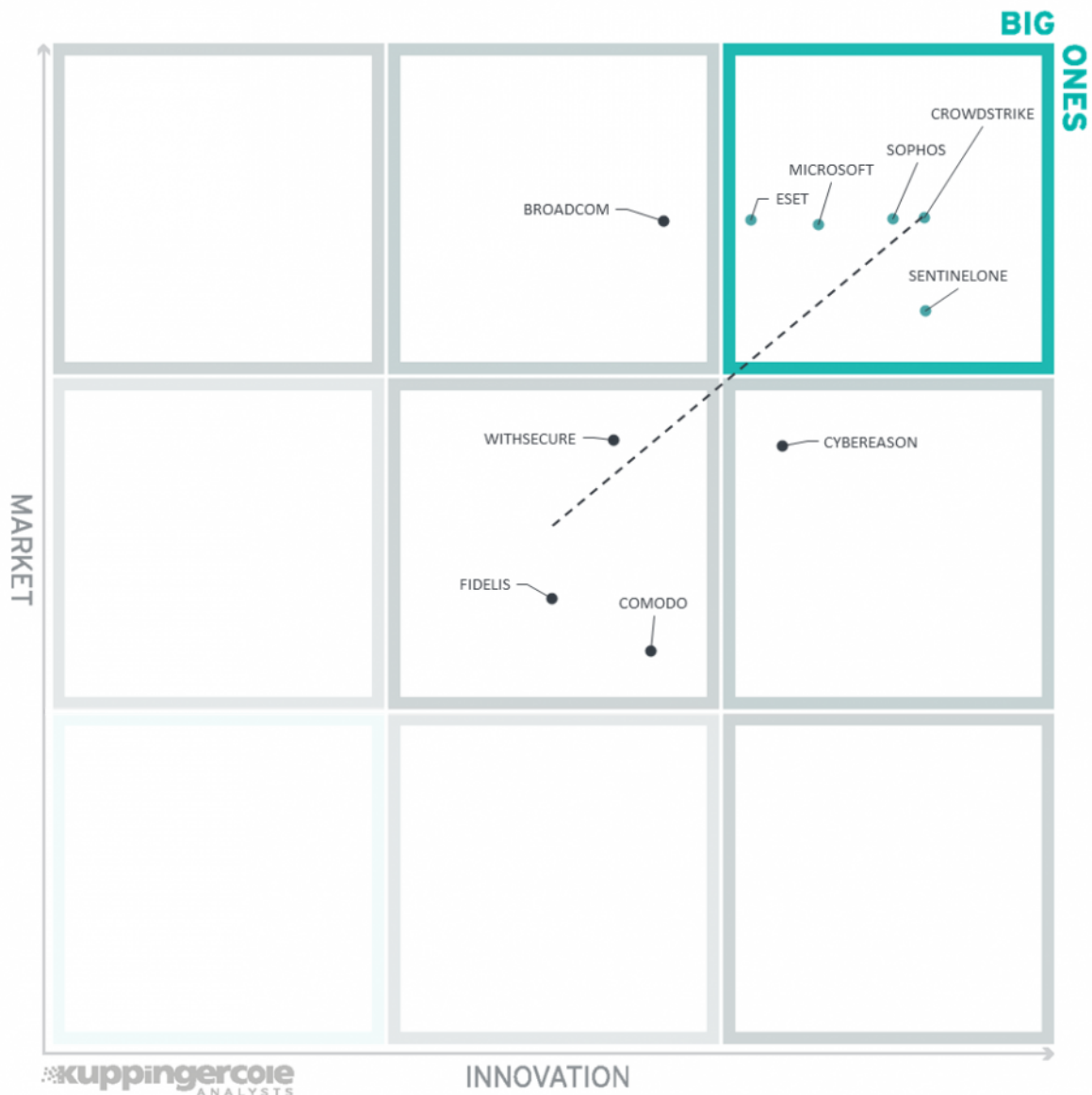


Figure 7: The Innovation/Market Matrix for Endpoint Protection, Detection, and Response

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

The Big Ones in this edition of the EPDR Leadership Compass are CrowdStrike, Sophos, ESET, Microsoft, and SentinelOne. Symantec (by Broadcom) is in the top center. Cybereason is in the right center below the Big Ones, indicating opportunity for expansion. WithSecure, Fidelis Cybersecurity, and Comodo are in the center square.

## 4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Endpoint Protection Detection & Response Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.



| Product                                                       | Security                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Functionality                                                                       | Deployment                                                                          | Interoperability                                                                    | Usability                                                                           |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Comodo Advanced Endpoint Protection (AEP) Suite               |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| CrowdStrike Falcon Endpoint Protection                        |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Cybereason Defense Platform                                   |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| ESET Endpoint Security, Inspect, and LiveGuard Advanced       |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Fidelis Cybersecurity Endpoint (part of Elevate platform)     |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Microsoft Defender for Endpoint / Business                    |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| SentinelOne Singularity Platform                              |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Sophos InterceptX Advanced with XDR                           |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Symantec (by Broadcom Software) Endpoint Security             |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| WithSecure Elements Endpoint Protection, Detection & Response |                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |  |  |
| Legend                                                        |  critical  weak  neutral  positive  strong positive |                                                                                     |                                                                                     |                                                                                     |                                                                                     |

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product

| Vendor                                   | Innovativeness              | Market Position  | Financial Strength  | Ecosystem            |
|------------------------------------------|-----------------------------|------------------|---------------------|----------------------|
| Comodo                                   | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| CrowdStrike                              | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Cybereason                               | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| ESET                                     | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Fidelis Cybersecurity                    | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Microsoft                                | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| SentinelOne                              | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Sophos                                   | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Symantec (was acquired by Broadcom Inc.) | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| WithSecure                               | <div></div>                 | <div></div>      | <div></div>         | <div></div>          |
| Legend                                   | <div></div> critical        | <div></div> weak | <div></div> neutral | <div></div> positive |
|                                          | <div></div> strong positive |                  |                     |                      |

Table 2: Comparative overview of the ratings for vendors

## 5 Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

### Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC EPDR, we look at the following six categories:

- **Malware prevention:** evaluation of the combinations of different techniques and technologies employed by the solution to identify malicious code and prevent it from executing and achieving its goals.
- **Secondary EPP:** this category represents some of the additional security functions provided by EPP suites, including URL filtering, endpoint firewall, application controls, and system file integrity monitoring. Though we term these features "secondary", they are important, auxiliary capabilities that enhance protection from malware and subsequent compromise.
- **Compromise detection:** evaluation of the solutions' abilities to discover botnet activity, command and control traffic, port scans, tampering with security controls, reconnaissance, lateral movement, exfiltration, and other attacker TTPs.
- **Investigations:** evaluation of each solution's facilities for investigations and threat hunting, such as IoC creation, query construction and execution, memory and file system analysis, etc.
- **Responses:** analysis of actions available within the products' management consoles, such as alerting staff, process termination, deletion and/or quarantine of malicious files, node isolation, registry and file system rollbacks, etc. The Responses category also considers the availability of and organization of playbooks for customers to utilize for responses.
- **Management:** evaluation of management console functionality including SOC integration, dashboards, reports, and analyst/investigator interfaces.

## 5.1 Comodo

Comodo Security Solutions was originally founded in 1998. The company is headquartered in New Jersey. In 2018, the Comodo Enterprise Cybersecurity software group was established to focus on commercial solutions. Comodo has network and web security, IT service management, and consumer products and services. The product management console can be run on-site on Ubuntu, in AWS, and Comodo has SaaS options. Licensing is per endpoint.

Comodo AEP has agents for most every endpoint, including support for MacOS, Linux, Android, iOS, and legacy versions of Windows. AEP uses a mix of signatures and ML-based heuristics to scan code prior to execution. Known good code runs, known bad code doesn't, and unknown code gets special treatment: Comodo's Kernel API Virtualization creates a separate memory space and virtual file system in which it executes and observes unknown code, protecting endpoints from malware such as ransomware. If, for example, ransomware attempts to encrypt user files, Comodo's Kernel API Virtualization redirects the file operations away from the real data to the virtual file system. Unknown code is also dispatched to Valkyrie, Comodo's cloud-hosted sandbox and CTI platform. AEP also does URL filtering and can block downloads by file type. AEP has endpoint firewall, application control, and file monitoring features.

For investigations and threat hunting, Comodo has a drop-down list and regexp style query builder. Queries can be saved and edited. The interface has time and sequence-based correlation as well as a default process tree view. Map views in the interface and the ability to alert analysts and annotate cases are not included but are planned. The solution does record suspected malware activities for later investigations, but advanced features such as live memory and disk structure analysis are not present.

Its components can terminate processes, prevent deletion of on-disk backups, delete or quarantine files, add IPs to deny-lists, etc. Comodo's solution does not automatically create/route tickets and add CTI query results to tickets to expedite investigations.

YARA rule format is supported, but STIX and TAXII are not. Comodo uses a 3<sup>rd</sup>-party sandbox for its Valkyrie service. Comodo harvests and shares threat intel with 24 other cybersecurity vendors. Comodo interoperates with SIEMs via syslog and SOAR platforms over APIs. Comodo works with its own Dragon Enterprise ITSM; interoperability with other vendors' ITSMs can be configured over APIs. For customer administrator authentication, 2FA options such as Authy, Google, and Microsoft authenticators are supported.

Comodo asserts ISO 27001 and SOC 2 Type II compliance. The solution is missing some advanced features on the EDR side. Additional standards support would promote interoperability with other elements in customer security architectures. Comodo's response capabilities are targeted at front-end prevention of malware infection and damage. Their Kernel API Virtualization technology uses a somewhat different approach than others in the market. It is possible that this approach could be advantageous for organizations that have endpoints that are not always connected to the internet to receive signature and detection model updates from the vendor. Businesses that are looking for a tightly integrated ITSM for their EPDR and those looking for a managed EPDR offering may want to consider Comodo's extended suite of

endpoint and security tools.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ○ |
| Functionality    | ● ● ● ○ ○ |
| Deployment       | ● ● ● ● ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability        | ● ● ● ● ○ |

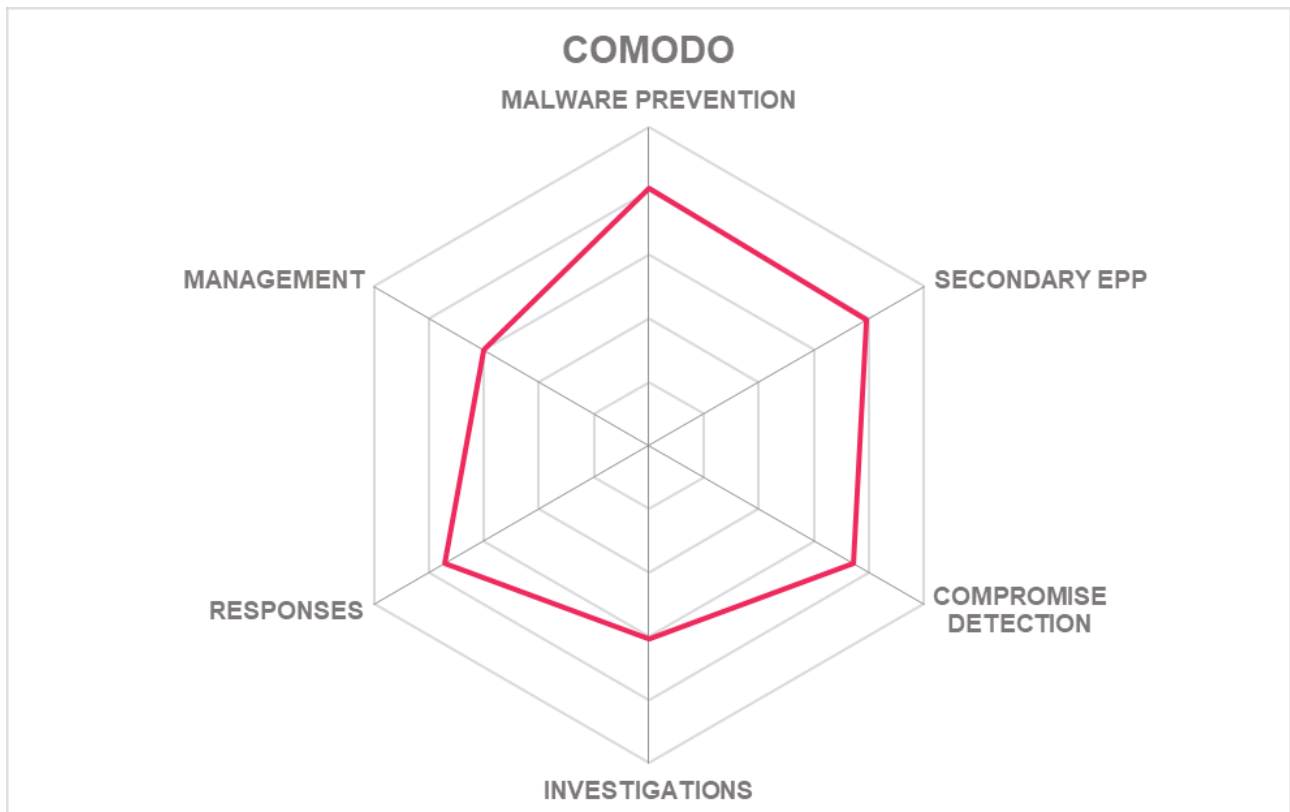
# COMODO

## Strengths

- Agents for most operating systems, including deprecated versions of Windows
- Kernel API Virtualization offers additional level of protection against malware and ransomware
- Includes endpoint firewall, application controls, URL filtering, and some system file integrity monitoring capabilities
- CTI sharing agreements with partners
- Multiple 2FA methods supported for customer admins

## Challenges

- Comodo has secure email/internet gateways, but the client doesn't interoperate with other vendor's URL filtering functions
- App control doesn't include browser extensions
- Console mapping to MITRE ATT&CK planned
- Advanced threat hunting and investigations features not available



## 5.2 CrowdStrike

CrowdStrike was founded in the Bay Area in 2011 as a cloud-native endpoint protection platform. The company went public in 2019. CrowdStrike has expanded their product offerings beyond EDR and has acquired several security specialist firms in recent years. In addition to endpoint security tools, CrowdStrike has cloud, identity, CTI, vulnerability management products and services. The management console is hosted by CrowdStrike. Licensing is per managed endpoint per year.

Falcon Endpoint Protection agents are available for Windows 7, 10, 11; Windows Server 2008+; all major Linux versions, MacOS, Android, and iOS. Falcon clients have 22 major endpoint security functions bundled into single agent. CrowdStrike can co-exist with other endpoint security solutions. Falcon uses advanced heuristics, ML detection (including Deep Learning algorithms), sandboxing with delayed execution malware prevention techniques. Falcon monitors client processes and memory to protect against malicious scripts and file-less malware attacks and prevent known exploits from executing. Falcon can audit and/or prevent volume shadow copy access for added ransomware protection. CrowdStrike reports that offline nodes have the same level of protection as those which are connected to their cloud. Suspicious code samples are automatically sent to CrowdStrike's cloud sandbox for analysis. Falcon does not do traditional URL filtering, but customer admins can manually configure file transfer restrictions if desired. Endpoint firewall features are present, but app controls are limited. Falcon does perform system file integrity monitoring and application inventories on endpoints.

Global and network maps feature in the top levels of the dashboard. CrowdStrike's analyst interface is its forte. The Falcon Console is intuitively laid out and yet customizable for each user if needed. Tool tips and right-click action context menus are abundant. Falcon creates cases and facilitates case management and investigations with automated correlation, threat intel updates, and assembly of IoCs for threat hunts. Analysts can quickly pivot from investigations and threat hunts to incident response. CrowdStrike provides root cause estimations and threat actor attribution when identified, allowing analysts to get the most updated info on the attackers. Advanced functions such as remote memory and disk examination and recording for forensic analysis are included. CrowdStrike runs its own sandbox in the cloud, and connectors are available for other sandbox services.

Email, Microsoft Teams, PagerDuty, Slack, and webhooks for generic services can be used for alerting. Code and no-code options (visual flow-chart style) can be used to customize workflows and playbooks. All relevant actions, such as process termination, node isolation, quarantining files, and full endpoint rollback can be automated or presented to admins and analysts within the console.

YARA format is understood directly, STIX and TAXII conversion is possible through MISP. CrowdStrike has its own high quality threat intel service which it uses, and they share CTI with unidentified partners. Customers can integrate other sources into the Falcon console for context enrichment. REST APIs and syslog are supported, and many connectors to other security tools, ITSM, and IAM solutions can be downloaded from the CrowdStrike Store. 2FA options for customer admin authentication include Duo Mobile and GAuth. SAML is also supported for federated authentication.



CrowdStrike has attested and/or certified to CSA Star Level 2, ISO 27001, SOC 2 Type 2, UK G-Cloud and Cyber Essentials. FedRAMP certification is reported to be in progress. Falcon omits some secondary EPP type features such as rules-based URL filtering and granular control over endpoint applications. Users cannot manually initiate scans, but most organizations would not consider that a drawback. The Falcon console is easy to understand and use, which makes it suitable for both highly experienced threat hunters and junior SOC analysts. CrowdStrike also has identity threat detection and prevention tools for the endpoint. Many connectors are available on the CrowdStrike Store to integrate with existing customer infrastructure. Organizations are interested in a cloud-hosted endpoint security solution with deep investigative capabilities and an emphasis on automation will want to put CrowdStrike Falcon on their shortlist for EPDR.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ● ● |
| Deployment       | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ● |
| Usability        | ● ● ● ● ● |



## Strengths

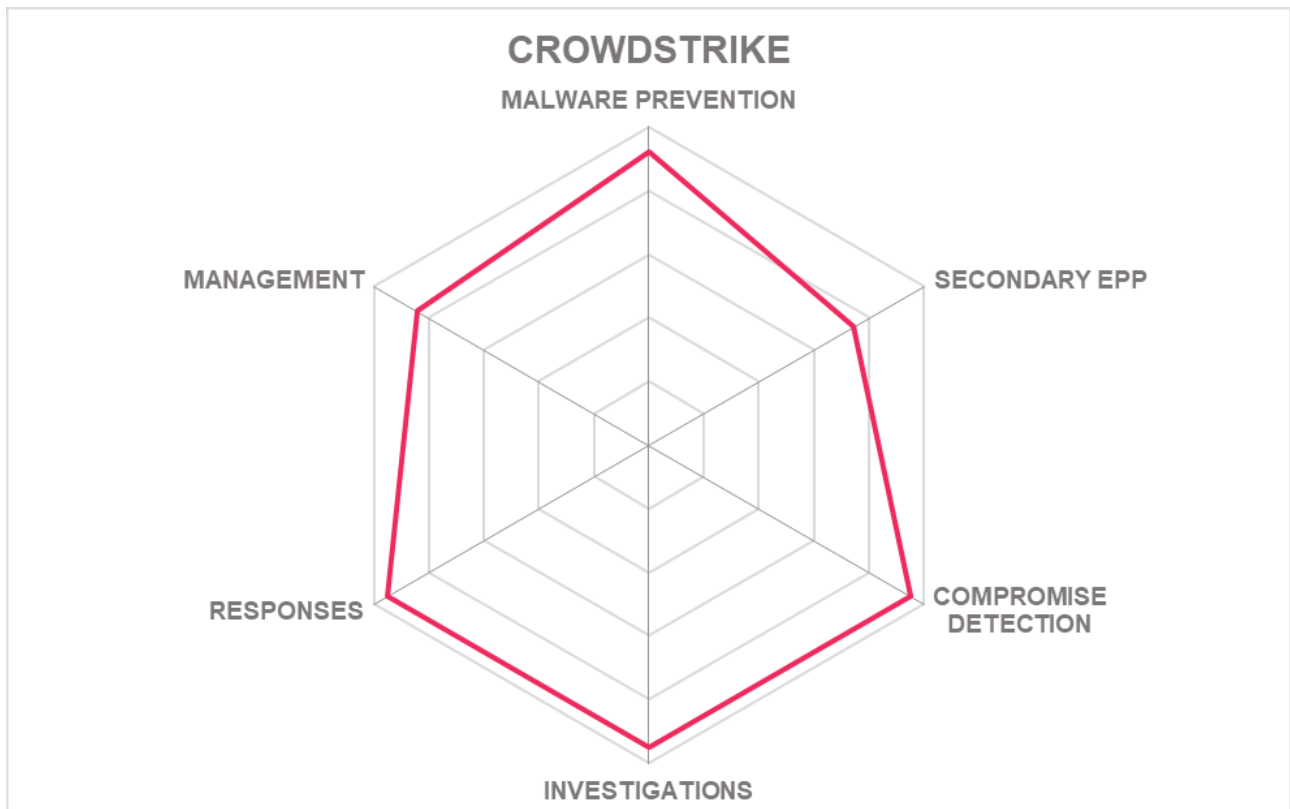
- Fully cloud-hosted management
- Comprehensive services for management
- Uses advanced Deep Learning detection algorithms
- Detection model updates do not require reboot
- Excellent, customizable investigation and threat hunting interface
- Identity threat detection and prevention options available
- Many connectors for IT management and security tools integration
- All major security certifications obtained

## Challenges

- User cannot initiate scans
- Missing URL filtering features: customers must manually configure file transfer restrictions
- Limited app controls
- Additional API authentication methods would enhance extensibility

## Leader in





## 5.3 Cybereason

Cybereason is a Boston-based, late-stage, high-valuation startup that was founded in 2012. Cybereason is focused on endpoint security and has been an early proponent for eXtended Detection & Response (XDR). In addition to full EPDR and nascent XDR functionality, Cybereason offers threat intelligence, MDR, and incident response services. The management console can run on-premises on CentOS, in public IaaS, and Cybereason hosts it as SaaS as well. Licensing is per endpoint.

Cybereason has agents for every OS, including MacOS, all Linux varieties, Android and iOS mobile, and legacy Windows versions. Its agents are compatible with other security tools. Cybereason leverages all conventional and advanced malware identification techniques with the exception of micro-virtualization. Their Defense Platform employs ML detection models, including Deep Learning algorithms, and both on-endpoint and cloud-based sandboxing for suspicious files. Cybereason protects the Volume Shadow Copy on Windows for more effective ransomware interdiction. Cybereason states that agents function autonomously even when disconnected from their cloud. Defense Platform contains an endpoint firewall but does not perform URL filtering. Application controls are based on allow/deny listing but are somewhat limited in capabilities with respect to the types of apps that can be governed by policies. File integrity monitoring can be enabled and can be used for any file types and locations.

Cybereason defines a connected set of attacks or suspicious events as a MalOp (Malicious Operation). Defense Platform's dashboards are intuitive to follow and use and are customizable. Customers can create different views and permissions for roles and users; for example, SOC manager, junior analyst, threat hunter, etc. Typical widgets include current activities, MalOp timelines, and process trees. The solution looks for all MITRE ATT&CK TTPs. Defense Platform assembles MalOps for analysts to investigate only when sufficient evidence warrants it. MalOps are pre-populated with all pertinent info, including event correlation and threat intelligence. The query builder takes a drop-down list approach and accepts regex input. Analysts can perform remote memory exams and annotate MalOps. Forensic evidence is automatically recorded for playback.

Email and Slack can be used for alerting. Cybereason makes recommendations on actions based on the context of the identified MalOp. The analyst interface enables a wide range of responses, including process termination, remote shell launch, registry remediation, file quarantine, and node isolation. For ransomware cases, rather than rolling back entire nodes to last known good state, Cybereason immediately restores any encrypted files to their uncorrupted states. Root cause analysis and attacker attribution theories are provided with confidence levels.

CyBox, STIX, TAXII, and YARA formats are supported. Cybereason primarily utilizes their own high-quality threat intelligence, and customers can configure some 3<sup>rd</sup>-party CTI sources and sandboxes if desired. For security and IT infrastructure integration, Defense Platform supports CEF, REST APIs, SNMP, and syslog, allowing connections to most SIEMs and some SOAR platforms. Packaged connectors are available on their marketplace to facilitate integration, such as ServiceNow for ITSM. Google Authenticator and SAML can be used for customer admin and analyst MFA.

Cybereason is [annually audited](#) for ISO 27001, 27017, 27018 and SOC 2 Type 2 adherence. Cybereason regularly takes part in multiple independent tests for product effectiveness and performance. URL filtering functions are not present, and app controls are not as granular as some other solutions. More integrations with adjacent security and IT tools such as SOAR and ITSM solutions would be beneficial. Cybereason aims to make security analysts more efficient by automating as many elements of an investigation as possible. The admin/analyst interface is well-designed, customer configurable, and provides playbook recommendations based on MalOp context. Organizations that are looking for full EPDR solutions with excellent threat hunting facilities should consider Cybereason.

|                  |   |   |   |   |   |
|------------------|---|---|---|---|---|
| Security         | ● | ● | ● | ● | ● |
| Functionality    | ● | ● | ● | ● | ○ |
| Deployment       | ● | ● | ● | ● | ● |
| Interoperability | ● | ● | ● | ● | ○ |
| Usability        | ● | ● | ● | ● | ● |



## Strengths

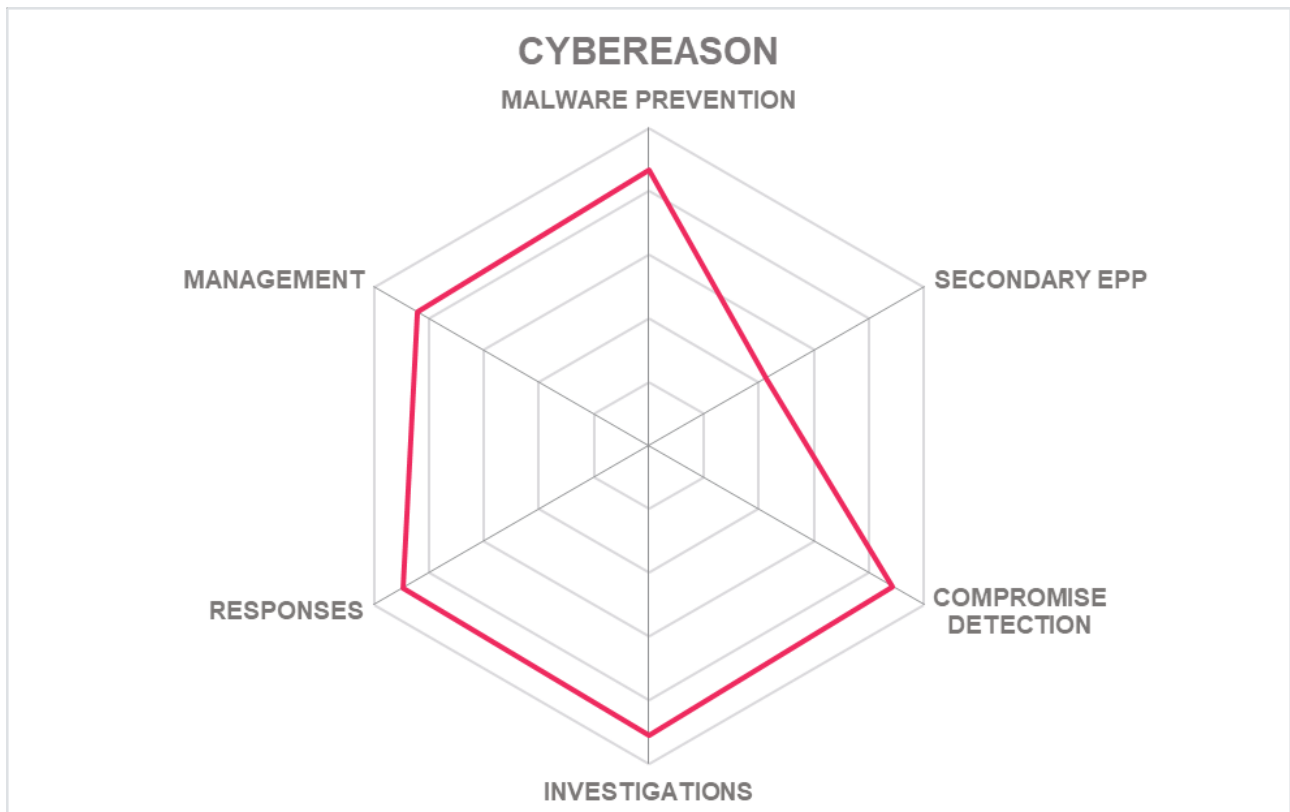
- Excellent OS support for agents
- On-device sandboxing improves offline detection effectiveness
- Uses advanced Deep Learning-based detection models
- Highly customizable and easy-to-use analyst interface
- Investigations are expedited due to automated collection of forensic evidence and threat intelligence
- ISO 27001 & SOC 2 Type 2 audited and certified

## Challenges

- No URL filtering
- Coarse-grained app controls
- Additional MFA options would be useful
- Additional connectors for SOAR and ITSM would promote interoperability with security infrastructure

## Leader in





## 5.4 ESET

ESET, headquartered in Bratislava, was founded in 1992. ESET has been in the malware prevention business for a long time, and has other security products for email security, file server security, full-disk encryption, cloud office security, DLP, and authentication. The ESET Protect console is hosted by ESET, or, if preferred, can run on customer sites on any Windows or Linux host, as a virtual appliance, or in any major IaaS environment. ESET offers subscription-based licensing.

ESET has agents for most operating systems, including MacOS, all Linux variants, Windows XP to Windows 11, and Windows Server 2008+, and iOS. Android is supported in the ESET Endpoint Security for Android product, which also functions as an MDM. Agents have not been tested for compatibility with similar software. ESET employs the most common malware identification and prevention techniques, with the exception of micro-virtualization. ESET was a pioneer at the application of Machine Learning detection models for malware prevention. Their solution employs a regularly tuned, multi-layer set of unsupervised, supervised, and Deep Learning algorithms. ESET has both sophisticated and granular URL filtering for enterprise clients. ESET's endpoint firewall features include endpoint application traffic monitoring, botnet, and DDoS protection. App controls are rules-based and must be configured by customers or ESET services. File integrity monitoring includes baselining functions, and file types beyond critical system files can be watched.

ESET looks for all MITRE ATT&CK techniques and has been involved in both testing and defining it. Analysts drill down from dashboards on events in a timeline view, which are prioritized by severity and context. Threat hunting capabilities are extensive, but the workflow and interface could be optimized. Analysts can create custom IoCs for threat hunts and search across an enterprise, but live memory analysis and disk inspection are not possible currently. Eight hundred detection rules ship with the solution, and customers can add detection rules manually by editing XML. ESET Inspect does record suspicious activity for playback by analysts.

ESET Inspect ships with some playbooks, and customers can edit rules within although there is no GUI for playbook design. ESET does make remediation recommendations. A wide range of response tasks are present, such as terminate process, isolate host, quarantine files, stop VSS deletion, etc. Suspicious code is automatically sent to LiveGrid for analysis. ESET has reported the LiveGrid renders quick sandbox verdicts. Rollback of registry entries or full node configurations is not available. ESET can make root cause and attribution theories.

ESET supports CyBox, STIX, TAXII, and YARA formats. REST APIs and syslog support facilitates interoperability with ITSM, SIEM, and SOAR platforms, although this must be configured and/or coded by the customer or professional services. SAML is supported for federated authentication. ESET Secure Authentication (separate product) comes with the ESA mobile app, which supports push notifications and time/event-based OTP. Other MFA options available via an ESET Business account include hardware tokens, Authy/Google/Microsoft authenticators, and FIDO authenticators.

ESET has obtained ISO 9001, 15408, 27001, and 27018 and UK Cyber Essentials Plus certifications. SOC



2 Type 2 has not been achieved yet. ESET has excellent and consistent results in malware detection tests. ESET Inspect provides strong malware prevention and a good baseline of EDR functionality, although workflows could be improved. The analyst interface could use some updates to include additional query features and a playbook editor. Agents are available for every OS running today. ESET publishes much threat research and contributes to the cybersecurity community. Documentation in and support for many languages makes ESET a top EPDR contender for companies with global operations.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ● ○ |
| Deployment       | ● ● ● ● ● |
| Interoperability | ● ● ● ● ○ |
| Usability        | ● ● ● ● ○ |



## Strengths

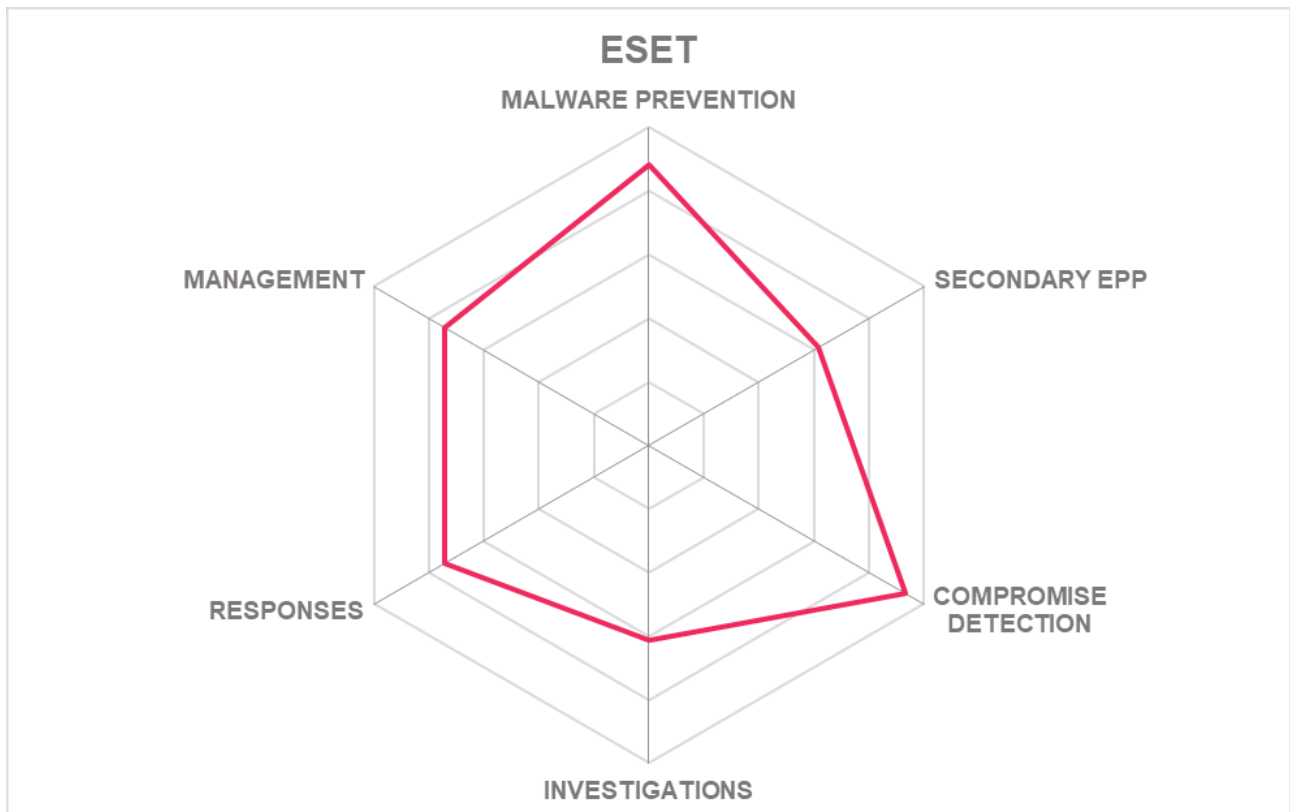
- Broadest language support (39) for documentation and technical assistance
- Participates regularly in independent malware detection testing
- UEFI scanner detects lowest levels of malware on UEFI images and disk partitions
- Early adopter of ML and DL for malware detection
- URL filtering, endpoint application traffic monitoring, and botnet/DDoS protection
- Advanced file integrity monitoring
- ISO 9001, 27001, and 27018 certified

## Challenges

- SaaS is not SOC 2 Type 2 certified yet
- Coarse-grained app control requires manual configuration and maintenance
- Analyst interface could be modernized
- Registry and full node rollback not available
- No playbook editor

## Leader in





## 5.5 Fidelis Cybersecurity

Fidelis Cybersecurity was founded in 2002 and is headquartered in Bethesda, MD, outside Washington, DC. They are a privately held company. Fidelis Endpoint contains EPDR functionality and is widely used for forensic investigations and incident response. It is part of their Elevate platform, which also offers Network Detection & Response (NDR) and Distributed Deception Platform (DDP) capabilities. Fidelis Cybersecurity also has cloud, server, and container security solutions. The Fidelis Elevate console can be run on-premises, in IaaS, and Fidelis Cybersecurity hosts it as SaaS. Multiple MSSPs run Elevate for their customers as well. Licensing is per node, with additional fees to increase EDR data storage for SaaS customers.

Fidelis Endpoint has agents for Windows 7, 8, and 10; Windows Server 2008+; most Linux types except Debian; and MacOS 10+. There are no mobile agents. Windows 11 support is expected in 2Q2022. Anti-virus functions are OEM'd from another vendor as an add-on, and many Fidelis Cybersecurity customers use their EDR in conjunction with Microsoft Defender. No compatibility testing has been done. The endpoint protection features employ a mix of signature and ML-enhanced process and memory behavioral analysis techniques to identify potentially malicious code prior to execution. Exploit prevention is built-in. Suspicious code is sent to their cloud-hosted sandbox for evaluation; therefore, optimal detection requires internet connectivity. Micro-virtualization is not used, nor does this solution scan browser content prior to user-initiated downloads. URL filtering can be provided by the Elevate platform but is not present in the Endpoint. App controls, endpoint firewall, and system file integrity monitoring features are not available.

The EDR features are based on continuous behavioral collection which are evaluated near real-time against the various high quality Fidelis Cybersecurity threat intelligence feeds to detect potential malicious activity. The dashboard and analyst interface are designed to expedite investigations and facilitate incident response: threat hunters will find it intuitive to use. Customization is possible if needed. The analyst interface features timeline and process tree views and supports regexp searches. Cases must be manually created, but Fidelis Cybersecurity performs automated CTI queries and updates open cases. Fidelis Endpoint allows definition of custom IoCs for searches and derives variants based on pertinent threat intel. Remote memory and disk analysis are available within the console. Incident recording and playback are not available. The solution contains many response scripts which can be edited and triggered either manually or automatically. Root cause and attribution predictions are not made.

Email, Microsoft Teams, and Slack are used for alerting. Scriptable responses include collect detailed forensics, kill processes, isolate nodes, delete files, etc. The ability to stop mass file name or extension changes is not included.

Fidelis Elevate supports YARA rule and STIX formats. It relies on Fidelis Cybersecurity's CTI sources, which includes Reversing Labs feeds. Elevate integrates with other components of customer security architectures via CEF, LEEF, REST APIs, and syslog; a connector for Palo Alto XSOAR is available. Fidelis Cybersecurity professional services can build connectors for other systems if desired. Google Authenticator, LDAP, RADIUS, OIDC, and SAML can be used for authentication and federation. Various roles with

different privileges are available, and integration with PAMs is possible via LDAP.

Fidelis Endpoint is part of their forward-looking XDR platform, Fidelis Elevate. This Active XDR Platform attained leader ratings in multiple categories in recent KuppingerCole Leadership Compasses on [NDR](#) and [DDP](#). They have not pursued ISO or SOC 2 certification yet. Fidelis Endpoint omits some secondary EPP type functions such as app controls and system file integrity monitoring. Other secondary EPP functions are present within their platform, such as URL filtering. Their product emphasis is on the EDR aspect. The analyst interface is well thought-out and easy to navigate. Forensic investigators and incident responders will find it to be an efficient tool. Organizations with mature SOCs and security teams looking for EDR and incident response platforms will want to consider Fidelis Cybersecurity Fidelis Endpoint and Fidelis Elevate platforms.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ○ ○ |
| Deployment       | ● ● ● ○ ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability        | ● ● ● ● ○ |

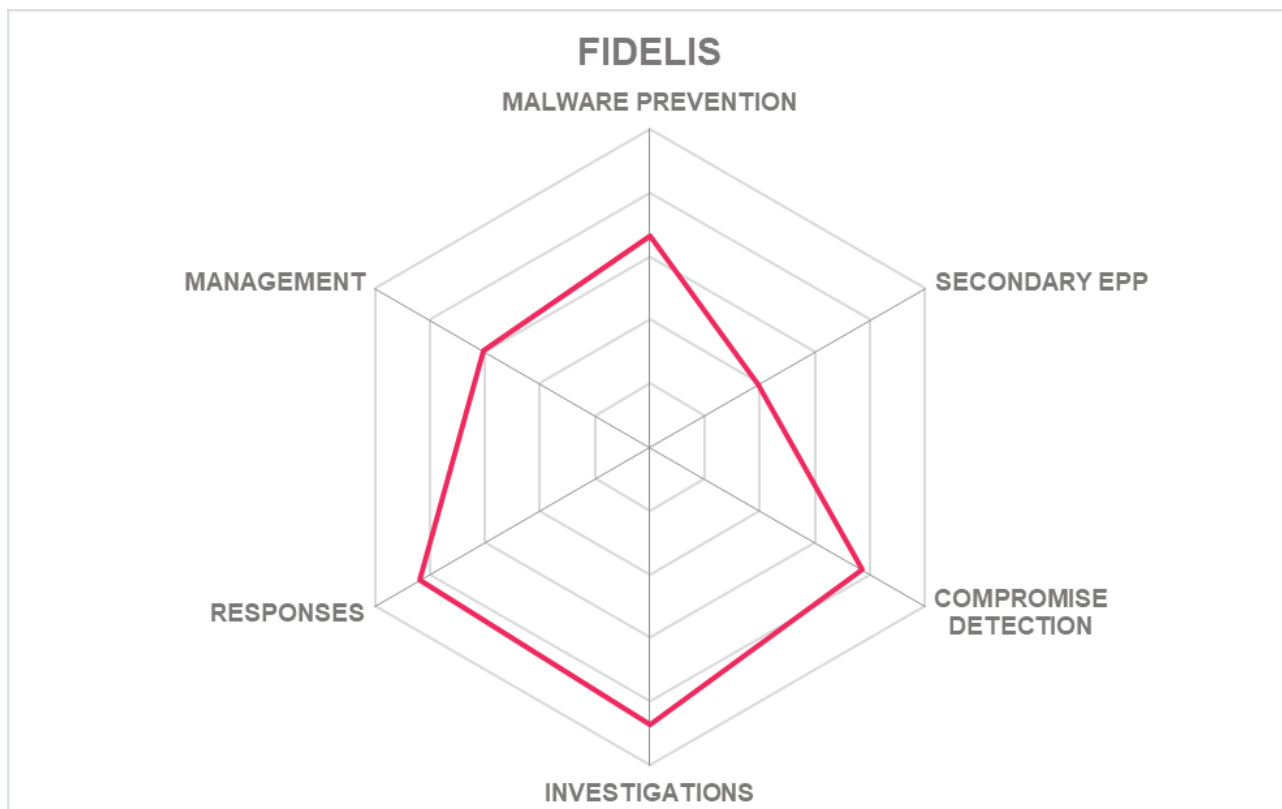


## Strengths

- Intuitive analyst interface for investigations and threat hunting
- Built-in high-quality Fidelis threat intelligence and cloud-hosted sandbox
- Integration with Fidelis' NDR and DDP
- Support for multiple MFA types and SAML federation

## Challenges

- Lacks ISO and SOC 2 certifications
- No agents for mobile
- Does not scan browser content
- Missing endpoint firewall, app controls, and system integrity monitoring



## 5.6 Microsoft

Microsoft was founded in 1975 and is headquartered in Redmond, WA, with many offices around the world. Microsoft offers a wide variety of hardware and software products and services. Microsoft first created Defender for Windows, but it has grown to support many other operating systems. Customers can host the console on-premises, in IaaS, and Microsoft offers it within their Azure cloud also. Licensing is per endpoint, with multiple tiers of service.

Defender agents are available for Windows 7-11, Windows Server 2012+, all major Linux types, MacOS, Android, and iOS. If running another EPP tool on Linux, Microsoft recommends switching Defender to passive mode. The EDR components can function side-by-side with other NGAV or EDR tools. Optimal detections require internet connectivity to their sandbox. All browsers except Apple Safari are supported. Defender does scan content in browsers prior to downloading. Defender uses the full array of detection techniques, including signatures, process and memory analysis, and micro-virtualization. Starting with Windows 10, Exploit Prevention includes Arbitrary Code Guard (Edge), Controlled Folders Access, and Attack Surface Reduction, which, if configured, enable strong protection against file-less malware and ransomware. Defender and the sandbox service are powered by a range of ML and DL neural network detection models. Microsoft includes a robust URL filtering service, but it does not block files by type. The endpoint firewall can work in stealth mode, shielding nodes from ICMP queries and DDoS attacks. Application and device controls are comprehensive. System file integrity monitoring is handled by Windows kernel for that OS.

Defender's EDR functions look for all types of malicious activity post-compromise. The dashboard is intuitive for analysts and well-designed for SOCs. The dashboard shows incidents by severity, devices and risks, compliance levels, etc. Analysts can dive into incidents from the timeline view. Incidents are automatically created and updated. A drop-down style query builder and regexp searches are permitted for investigations and threat hunting. Remote disk/memory analysis and activity recording/playback are possible within the analyst interface.

Email, SMS, Slack, and other Webhook-enabled means are used for alerting. All expected response actions are available, such as process termination, file quarantine, node isolation, registry rollback, and full endpoint rollback. Playbooks cover most remediation use cases, and customers can extend playbooks via a low-code visual workflow editor.

Microsoft uses their own high-quality threat intelligence and supports CTI exchange through Sentinel. Syslog support enables SIEM connectivity. REST APIs allow integration with ITSM and SOAR platforms. Multiple MFA options can be used to secure customer access to consoles, and AD and/or Azure AD can be used for granular authorization.

As a leading cloud hosting provider, Microsoft is ISO 27001/27018 and SOC 2 Type 2 certified. Microsoft Azure hosting environment is a CSA Trusted Cloud Provider. Microsoft participates in and does well in multiple independent testing scenarios. Defender is a highly capable EPDR solution across all covered operating systems. It is most effective on Windows 10+ systems with the Edge browser. Support for



deprecated OSes is not available. With support for most common operating systems, easy-to-use administrative and analyst interfaces, effective malware detection and remediation, Defender is a contender for any enterprise. Organizations running modern Microsoft OSes should put Defender on the short-list for consideration.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ● ○ |
| Deployment       | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability        | ● ● ● ● ● |



## Strengths

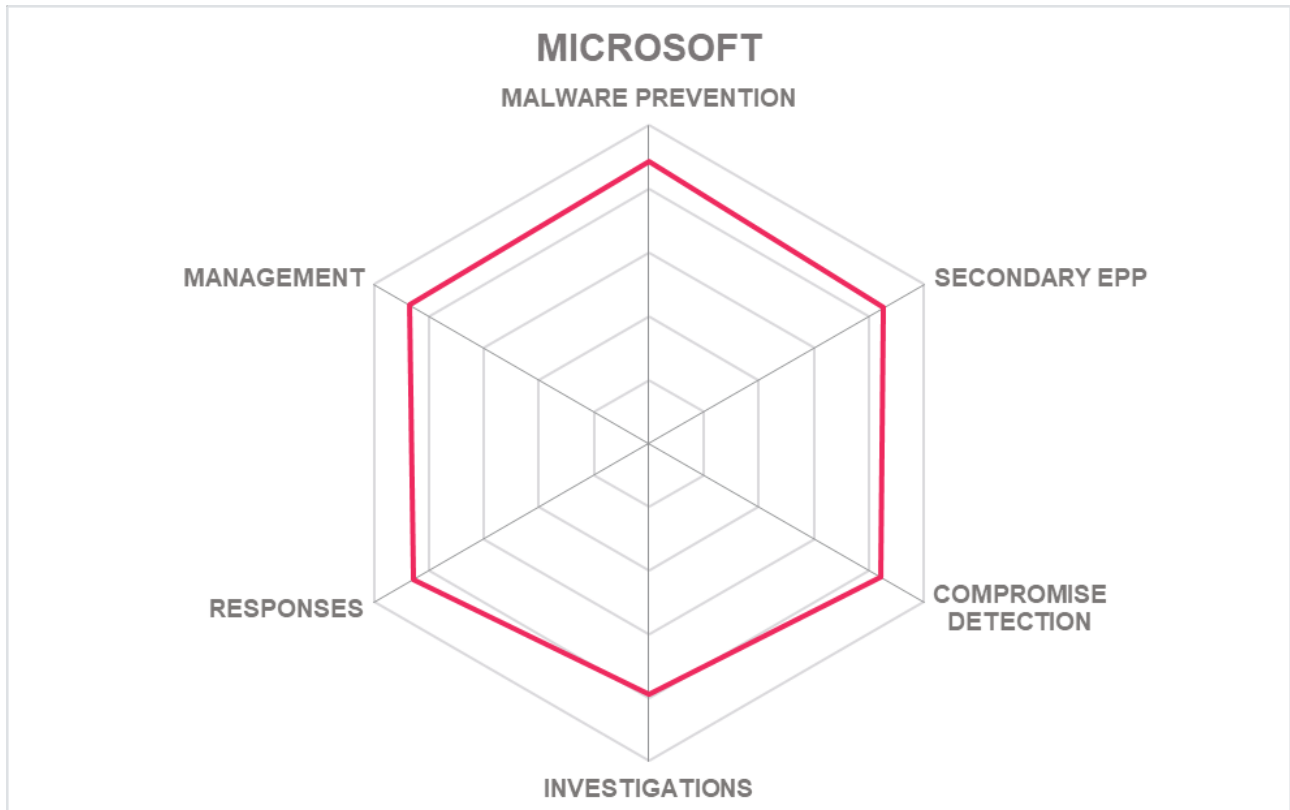
- Compatible with other EPDR tools
- Employs all available malware identification techniques
- Exploit Guard provides advanced controls for file-less and ransomware protection on Windows 10+ machines
- Intuitive analyst interface for more efficient investigations
- Full range of response actions
- Visual playbook workflow editor
- ISO 27001, SOC 2 Type 2, and CSA Trusted Cloud Provider

## Challenges

- System file integrity monitoring is not available for non-Windows OSes
- File transfer control is not built-in, but is available as Purview DLP (add-on)
- Support for oldest Windows versions not present

## Leader in





## 5.7 SentinelOne

SentinelOne was founded in 2013 and is headquartered in Mountain View, CA. The company had a successful IPO in 2021. Their products and services are centered on endpoint security and advanced XDR powered by full-stack data ingestion and analytics. The company's strategic vision is an integrated endpoint security platform to replace multiple types of endpoint and network security tools with a single solution to prevent, detect, analyze, and respond to cyberthreats across all enterprise IT assets, on-premises and in the cloud. Customers can run the console on-premises, in IaaS, and SentinelOne hosts it as SaaS in multi-tenant / multi-site architecture. MDR, Digital Forensics, and Incident Response (IR) services utilize this platform. Licensing is per endpoint and per workload node for cloud.

SentinelOne has agents for Windows XP to Windows 11, Windows Server 2008 to Server 2022, MacOS, all Linux flavors, Android, Chrome, and iOS. Agentless methods are available for Kubernetes cloud workloads and Docker containers. SentinelOne agents can run in AWS, Azure, and GCP IaaS instances. Virtualization environments from VMware, Citrix, Oracle, and Microsoft are supported. Agents scan browser content prior to user downloads. Agents can co-exist with other vendors' products through an exclusion system. SentinelOne engages all malware identification methods except micro-virtualization. SentinelOne uses static and behavioral ML and DL detection models, and that logic runs on the endpoint agent itself. Constant connectivity to SentinelOne cloud is not required for optimal detection capabilities. URL filtering is present but is limited to allow/deny list rules. The agent serves as an endpoint firewall for Windows, Mac, and Linux. App controls in Windows OSes are limited to customer-maintained allow/deny lists of filenames and types; no application reputation service is included. Application control is available for Linux and Kubernetes workloads. System file integrity monitoring is on by default.

SentinelOne Storyline? automatically monitors, correlates events, initiates cases with relevant threat intel for analysts, and stores data for up to a year. A full attack storyline can be visualized immediately in alignment with MITRE ATT&CK, showing timelines and process tree views. The query interface accepts regexp and allows for customization of IoCs. Customers can define and automate threat hunt and responses. Root cause analyses and attribution theories can be generated. Remote memory analysis and disk analysis are available.

Customers are alerted in console, via email, Slack, and SNMP; other methods are planned. SentinelOne Singularity STAR is highly capable in the response action and automation area: permitting all pertinent steps to be automated, from collection of forensic evidence to full node rollback. Hundreds of playbooks are available and can be further edited using a wizard and/or the S1 query language (S1QL).

STIX and YARA formats are understood. SentinelOne pulls in multiple CTI sources and automatically sends previously unknown code samples to 3<sup>rd</sup>-party sandboxes for dynamic analysis. CEF, REST APIs, and syslog enable interoperability with most SIEMs and many SOAR platforms. A connector for ServiceNow ITSM is available on the marketplace. RBAC is definable within the console. TOTP-based MFA is used for authentication, and SAML is supported for federation.

SentinelOne is SOC 2 Type 2 certified and is FedRAMP authorized (moderate). Though URL filtering is

available for iOS, Android, and Chrome OS, slight improvements to URL filtering / application controls for other OSes would be helpful. Independent tests show that SentinelOne is good at preventing malware as well as discovering all known MITRE ATT&CK TTPs. SentinelOne's Storyline? makes it easy for SOC managers to follow events and for analysts to run investigations and take actions. In fact, SentinelOne permits any possible remediation to be automated if the customer chooses. Full node rollback to last known good state is an option. SentinelOne Singularity should be near the top of the short-list for any organization looking for EPDR.



## Strengths

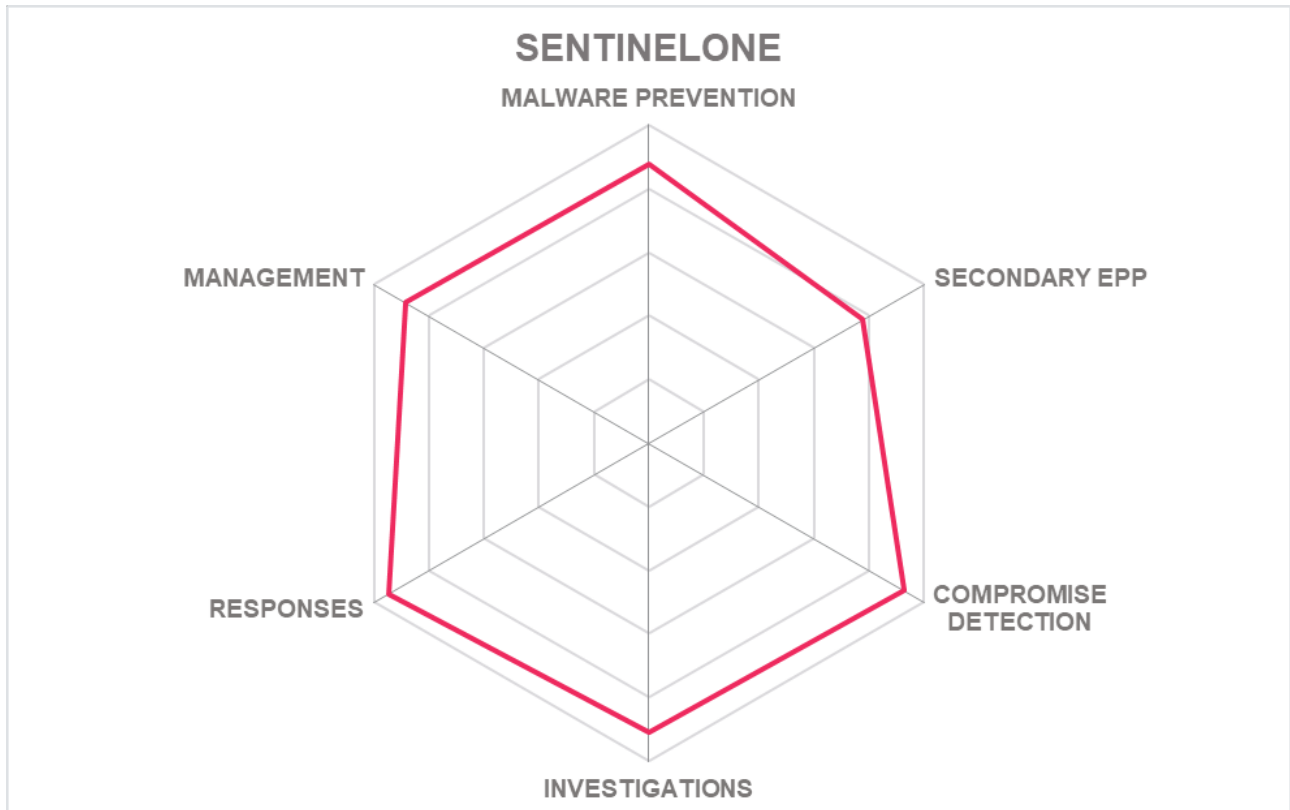
- Agents support a comprehensive list of operating systems
- Autonomous agents effectively protect offline nodes; perform network discovery, peer-to-peer agent installation push, and suspicious device blocking
- Excellent analyst interface makes investigations and incident response easier
- Automated, proactive threat hunting via Singularity STAR
- Ships with many playbooks, and customers can create more
- Consistently good independent test scores
- Singularity is part of their full IR platform, which is utilized by IR and MDR firms
- SOC 2 Type 2 and FedRAMP-Moderate certifications

## Challenges

- URL filtering by allow/deny list only, not by category or reputation
- Does not block file transfer by file type
- App control features need expansion
- Additional MFA methods would be useful

## Leader in





## 5.8 Sophos

Sophos was founded in 1985 in the UK. The company was acquired by Thoma Bravo in 2020. Sophos is a pureplay cybersecurity solution, with a strong focus on the endpoint. Sophos also offers solutions for encryption, Unified Threat Management, cloud security, firewalls, Zero Trust Network Access, and email and web security gateways. Sophos hosts the management interface as SaaS across multiple regions. Sophos offers full managed detection and response services. Per-user with multiple devices or per-device licensing options are available.

Sophos has InterceptX agents for Windows 7-11, MacOS, and all main Linux variants. Agents can scan content in browsers prior to downloading. It is best to not run other agent-based security tools when running InterceptX. Sophos uses all available malware prevention methods except micro-virtualization. Sophos employs a proprietary endpoint backup process that makes it resilient against ransomware attacks on the Windows Volume Shadow Service. When suspicious code is encountered, it is sent to their cloud sandbox for analysis. Sophos utilizes multiple ML detection models, including sophisticated Deep Learning algorithms. URL filtering can be applied by user/group policy, and downloads can be prevented by file types. Basic endpoint firewall capabilities can be enhanced by automating queries. Application controls are reasonably granular but do not permit browser extension exclusions. System file integrity monitoring is built-in.

Sophos' dashboard and analyst interface provides the standard features, and it has a highly functional visual query editor which can accept SQL style commands as well as regexp input. This allows knowledgeable admins to conduct investigations and threat hunts more easily. More than 500 SQL queries ship with the product, and more are added regularly. InterceptX automatically creates cases for suspicious events, inserts relevant CTI, and generates IoCs for threat hunts. Remote memory/disk analysis and activity recording/playback are possible.

Email and SMS are used for alerting customers. Sophos has robust response capabilities, including process termination, node isolation, and rollback of registry changes, file changes, and entire nodes if needed. Playbooks are provided but customization is handled by Sophos' services. Root cause and attribution theories are generated for incidents.

YARA rule format is supported, but STIX/TAXII are not. Third-party sandboxes are not utilized. They both leverage and share with partners the CTI they discover. REST APIs, SNMP, and syslog are supported, enabling connections to any SIEM, most SOAR platforms, and multiple ITSM products. A limited number of MFA options are present, and support for SAML is planned.

Sophos has obtained SOC 2 Type 2 certification. Sophos is an affiliate member of Cyber Threat Alliance. Sophos publishes not only on threat research but also on how to use advanced Deep Learning technology to discover and thwart malware. Sophos aims to turn InterceptX into a full SASE client, offering secure routing over SD-WAN as a VPN upgrade as well as DLP, CASB, NGFW, and other core services. Enhancements to a few secondary EPP functions and MFA and identity federation support are needed. The analyst interface is their primary differentiator: its design allows good sys admins to become more effective



at forensic investigations and threat hunting. Sophos InterceptX is a feature-rich solution that should be on the short-list for any organization considering upgrading their EPDR.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ● ● |
| Deployment       | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ● |
| Usability        | ● ● ● ● ● |



## Strengths

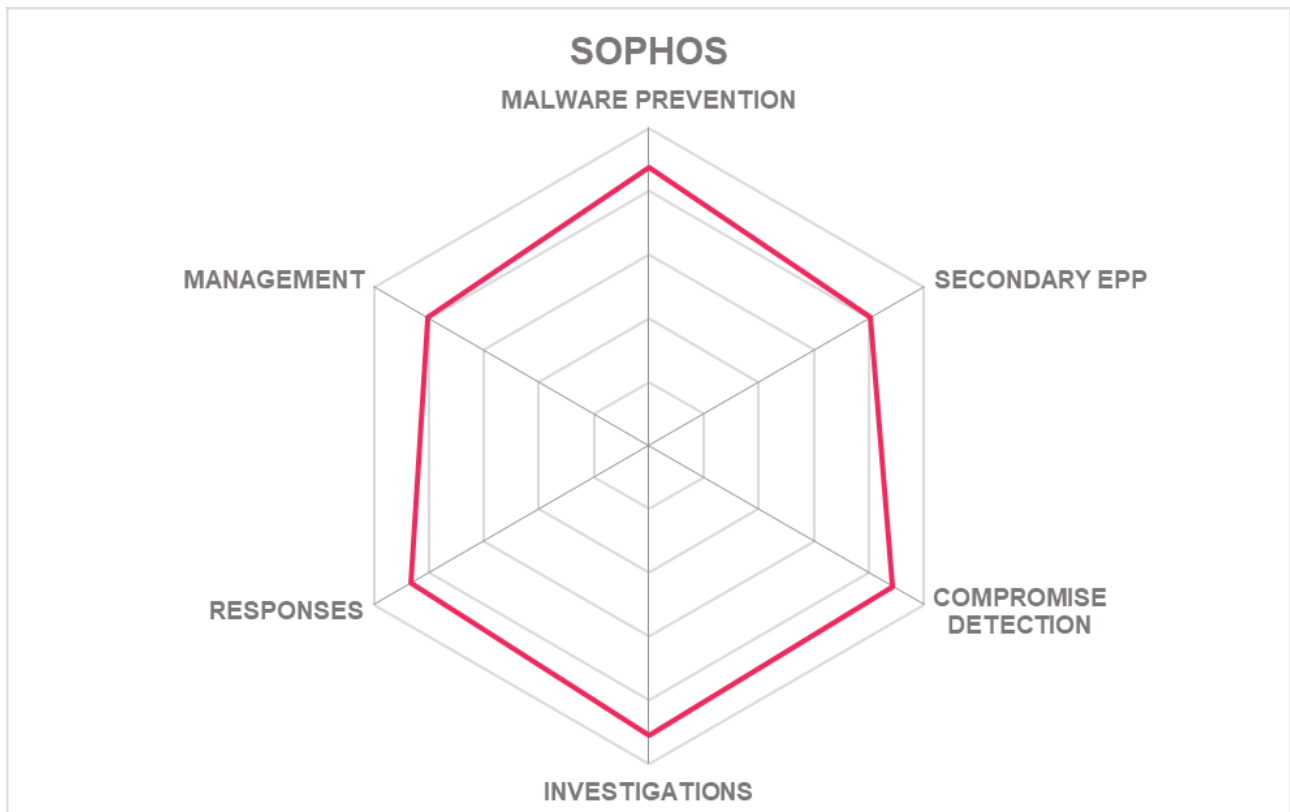
- Per-user/multiple devices licensing available as well as standard per-endpoint options
- InterceptX is evolving into a full SASE client
- Cyber Threat Alliance affiliate member
- Advanced DL detection methods utilized
- Consistently scores well in independent tests
- Innovative SQL-like query interface
- Broad range of responses permitted and automatable
- Excellent interoperability with security and IT infrastructures such as SIEM, SOAR, and ITSM

## Challenges

- Additional attribute-based app control and URL filtering enhancements could be useful
- Compatibility issues with other vendors' endpoint agents
- Does not block browser extensions
- Needs more MFA options and support for SAML federation for console access

## Leader in





## 5.9 Symantec (was acquired by Broadcom Inc.)

Symantec was founded in 1982 and was acquired by Broadcom in 2019. Symantec Endpoint Security Complete (SESC) contains protection capabilities (SEP), Mobile Threat Defense, Adaptive Protection, App Control and Isolation, Intrusion Detection and Prevention, Cloud Analytics, Threat Hunter, and Deception. Customers can deploy the management components on-premises and Symantec hosts it as a SaaS offering. Endpoint agents can be deployed on Windows, Mac OS, Linux, Android, and iOS. In addition to Endpoint Security, Symantec also has data and web security products. Licensing is per endpoint with enterprise options available. Services are provided by partners.

SESC agents are available for Windows 7-11, Windows Server 2008+, MacOS 10.13+, and all Linux versions. SESC uses all standard methods for malware identification, including signatures, static file analysis, exploit prevention, memory and process behavioral analysis, and micro-virtualization. Detection models are ML-based. URL filtering, in-browser content scanning, and endpoint firewall functions are present. Symantec offers some of the most granular policy-based application controls in the market. SESC can monitor system files for integrity.

The dashboard shows top level incident info, and analysts can drill down to individual events, including timelines, process trees, command line arguments, etc. The query builder takes guided regexp as input. Analysts can save, edit, and share queries. It supports multiple automated remediation steps such as quarantining, denylisting, blocking, remote shell execution, and evidence collection. Symantec allows for continuous recording when triggered by suspicious events for later analysis.

Email, SMS, SNMP, Slack, and other services can be used for alerting. Coordination of responses can be achieved through built-in XDR functions or through external SOAR systems, which can be integrated via Symantec ICDx. Root cause analysis and attribution estimates are available.

Symantec can send suspicious samples its Symantec Cloud sandbox (Cynic) or CASMA.. Symantec has high quality threat intelligence and IoC sources, so all its downstream products benefit from that. CEF, REST APIs, SNMP, and syslog communications allow connectivity to SIEMs and SOAR platforms through ICDx. ITSM integration is not supported. CAC cards, Kerberos, LDAP, Microsoft Azure AD, and RADIUS are available for strong authentication. It supports SAML for federation. It can use 3rd-party PAMs to lockdown admin and service accounts. Role-based and delegated administration are supported.

Symantec services are ISO 27001 and SOC 2 Type 2 certified. Symantec is an affiliate member of the Cyber Threat Alliance, with which it shares CTI. More in-platform automation options would benefit customers that do not have SOAR solutions. Symantec has updated the admin and analyst interfaces. SESC is a complex product, but Symantec have enhanced the deployment process and management capabilities. Organizations with experienced threat hunters and security analysts will want to consider SESC for EPDR.

|                  |           |
|------------------|-----------|
| Security         | ● ● ● ● ● |
| Functionality    | ● ● ● ● ● |
| Deployment       | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability        | ● ● ● ● ○ |



## Strengths

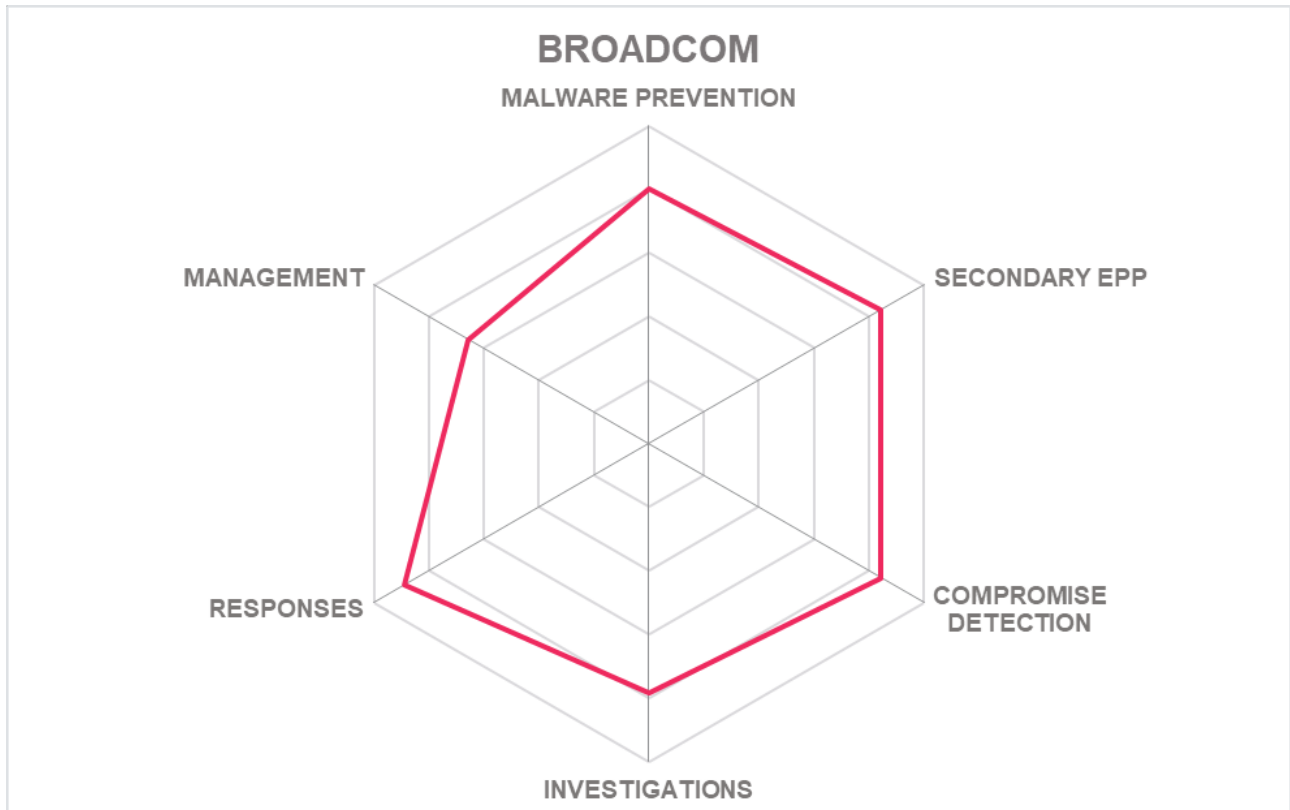
- All available malware identification methods used
- Fine-grained application controls
- Deception features built-in
- Multiple MFA methods supported
- Cyber Threat Alliance affiliate member
- XDR integrated into the package at no additional cost

## Challenges

- No connectors for ITSM systems
- Advanced automation requires SOAR, which is configurable via REST API

## Leader in





## 5.10 WithSecure

WithSecure, formerly F-Secure Business, was founded in 1988, and is one of the first companies formed specifically to help customers prevent malware. They are headquartered in Helsinki. WithSecure's entire product portfolio is based on endpoint (EPDR and vulnerability management) and cloud collaboration security for Microsoft 365 and Salesforce. The WithSecure Business Suite Policy Manager can run on-premises, but WithSecure Elements Security Center is hosted by them as SaaS. WithSecure Countercept is their MDR service offering, and they also have incident response, cloud security posture management, attack surface management and security consulting services. Licensing is per endpoint and usage-based pricing is available.

WithSecure has agents for Windows 7+, Windows Server 2008+, all Linux types, Mac, iOS, and Android. WithSecure can block browsers from accessing known malicious URLs. Elements has no known incompatibilities with other security agents. The agent is most effective if connected to WithSecure's cloud. All malware prevention techniques are employed except micro-virtualization. Their DeepGuard technology uses process monitoring, exploit prevention, and file reputation analysis, and DataGuard adds an extra layer of detection and ransomware protection to user data folders. WithSecure uses an array of unsupervised and supervised ML detection models. Elements includes policy-based URL filtering, which can be applied to groups and by location. The agent also manages an endpoint firewall and has granular app controls, which can include browser extensions. WithSecure does not monitor system files or firmware for integrity but does protect user data.

The dashboard provides views of EPP, EDR, Vulnerability Management, and Microsoft O365 mailbox coverage, addressing detections and prioritizing remediation. Analysts can drill down into events from the timeline view of the dashboard and run queries with regular expressions. Broad Context Detection? is their automated ML-based detection engine and threat hunter. WithSecure alerts customers when they find events that need to be investigated. Auto-generated cases are packaged with relevant threat intelligence. If customers need help with an investigation, they can "Elevate to WithSecure", getting feedback from their experts within a 2-hour SLA. Analysts can conduct cross-enterprise searches with WithSecure-curated IoCs and forensic evidence gathering processes are automated. Remote memory analysis is available. Suspicious code is captured and sent to WithSecure's Cloud for evaluation. WithSecure provides root cause and attribute theory assessments.

Email and SIEM integration are the means for alerting analysts to events. Many response actions are possible, such as process termination, network session termination, host isolation, etc., but playbooks can only be managed by WithSecure. Response actions must generally be taken manually, although some can be configured to trigger automatically for customers without 24/7 SOC's.

STIX/TAXII and YARA formats are not utilized by Elements. WithSecure relies exclusively on their own threat intelligence and sandbox services. Syslog support enables SIEM connectivity. Interoperability with ITSM and SOAR are possible via REST APIs, no pre-packaged integrations are available. WithSecure does work with Google Workspace, Microsoft Intune, Miradore, MobileIron, and VMware for MDM. Admin roles

are hard-coded and cannot be edited. Customers can use Duo Mobile and Google Authenticator for MFA.

WithSecure is ISO 27001 certified. WithSecure lacks support for some relevant communication standards, and connectors are not available for other key parts of customer security architectures. Customers can build API level integrations with such tools if needed. WithSecure Elements consistently performs well in independent malware detection tests. Their emphasis on cloud-delivered services backed up by WithSecure support personnel make the solution appealing for organizations without 24/7 SOC's or without experienced analysts who need solid anti-malware capabilities with managed EDR services.



|                  |   |   |   |   |   |
|------------------|---|---|---|---|---|
| Security         | ● | ● | ● | ● | ○ |
| Functionality    | ● | ● | ● | ● | ○ |
| Deployment       | ● | ● | ● | ● | ○ |
| Interoperability | ● | ● | ● | ○ | ○ |
| Usability        | ● | ● | ● | ● | ○ |

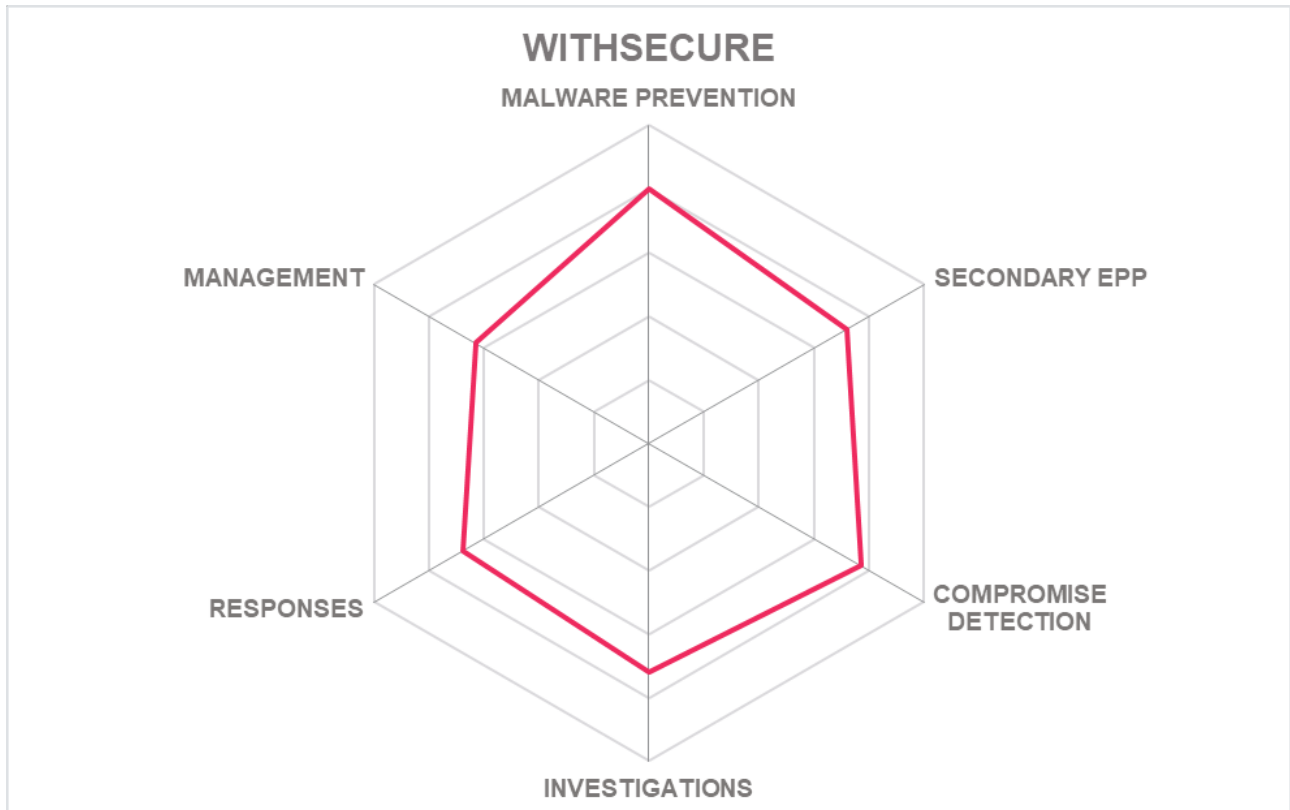


## Strengths

- “Elevate to WithSecure” support and services built into console
- Compatible with other endpoint agents
- Policy-based URL filtering
- Granular app controls allow blocking of browser extensions
- Bundled application reputation service
- Integrated vulnerability assessment and management available (at extra cost)
- Broad Context Detection? for automated EDR
- Multi-tenancy for managed service providers

## Challenges

- System file integrity monitoring is not present, although DataGuard protects user data directories
- Does not support STIX/TAXII or YARA formats
- Third-party sandbox and CTI sources not supported
- Enhanced RBAC and additional MFA / federation options would be useful
- Manual threat hunting can be difficult
- Limited rollback options



## 6 Vendors to Watch

### 6.1 AhnLab

AhnLab was founded in 1995 and is headquartered in Seoul. They are a privately held, top cybersecurity product vendor in the APAC region, serving the consumer, SMB, and enterprise markets.

**Why worth watching:** AhnLab offers a range of products, including their regionally well-known anti-malware products, security assessment, EDR, network layer malware sandbox, and cloud workload protection platform (CWPP) for AWS and Azure. AhnLab offers managed security services.

### 6.2 Checkpoint

Checkpoint, a global cybersecurity vendor, was founded 27 years ago in Israel. They now have dual HQs in Tel Aviv and Silicon Valley. Harmony Endpoint is their combined EPDR and VPN product. They are well known for the firewall products, and also have email and web security appliances, SIEM, mobile security clients and management solutions, and Cloud Security Posture Management and Cloud Workload Protection services. CheckPoint's ThreatCloud Managed Security Service is a full featured managed service offering.

**Why worth watching:** Checkpoint has a unified security suite encompassing endpoint, network, and cloud solutions. They participate in independent tests for endpoint security tools. Checkpoint's CloudGuard Security product and appliances placed as Overall, Product, Market, and Innovation Leaders in the [Leadership Compass for Network Detection & Response](#).

### 6.3 Deep Instinct

Deep Instinct, founded in 2015, is a late-stage venture-backed company headquartered in New York, with offices in Tel Aviv, Tokyo, and Reading (UK). Deep Instinct specializes in using Deep Learning detection models to discover and thwart malware.

**Why worth watching:** Deep Instinct has recently announced a partnership with EDR and endpoint security tool vendor Tanium.

## 6.4 GoSecure

GoSecure, a late-stage venture-backed company, has dual headquarters in Montreal and La Jolla, CA. They were founded in 2012. Their initial entry into the market was in EDR with the CounterTack product. In late 2019 they launched NGAV. They offer full MDR services.

**Why worth watching:** In mid-2019 they acquired EdgeWave, for their inbox detection and response capabilities. In late 2021, GoSecure acquired Covail to further build out managed detection and security services.

## 6.5 Heimdal Security

Heimdal Security was founded in 2014. They are headquartered in Copenhagen and have offices around the EU, and in Dubai and Texas. In addition to EPDR, they offer Privileged Access Management (PAM), vulnerability and patch management, email security solutions, and related services.

**Why worth watching:** Heimdal takes a Zero Trust approach to preventing malware, facilitated by integration with their PAM services.

## 6.6 Infocyte

Infocyte was founded in 2014 and is headquartered in Austin, TX. Their tools and services are centered on incident response, using their EDR and threat assessment tools. Clients generally come to them when they believe an incident has occurred. Infocyte Threat Assessment can perform internal vulnerability assessments, and their agents can provide the full range of EDR functions. The solution does not contain EPP, but they partner with Checkpoint.

**Why worth watching:** Infocyte was acquired by Datto in January 2022. Datto has a variety of backup, remote management, and business continuity solutions for both cloud and on-premises environments, serving the needs of clients ranging from small business to enterprise. Infocyte will add endpoint security capabilities to the Datto portfolio.

## 6.7 Malwarebytes

Malwarebytes was founded in 2008 and is headquartered in Silicon Valley. They are a mid-stage venture-

backed company originally known for their consumer anti-virus and malware removal tools and have been pushing into the SMB market and larger enterprises by expanding and enhancing their products with centralized management capabilities and additional features. Malwarebytes is focused on endpoint security, with both EPP and EDR as well as MDR services and Incident Response (IR) services.

**Why worth watching:** Malwarebytes is adding functionality and expanding into the MDR market. KuppingerCole will continue to monitor and report on Malwarebytes.

## 6.8 Tanium

Tanium was founded in 2007 and is headquartered in Kirkland, WA. They are a late-stage venture-backed firm. They have products in the endpoint security and management spaces. They are focused on EDR and UEM rather than EPP. Tanium is well-known in this corner of the endpoint management and security market.

**Why worth watching:** Tanium is well-regarded in the EDR space and has recently announced a partnership with Deep Instinct for advanced malware detection.

## 6.9 Trellix

Trellix is a new brand formed from the acquisitions and reorganizations of FireEye and McAfee enterprise security products by Symphony Technology Group. Trellix launched in January 2022 with assets from both progenitors, including endpoint and network security components.

**Why worth watching:** Trellix may be a new brand but has a combined security heritage and extensive existing customer base. Moreover, Trellix is positioning itself as an XDR vendor. We will monitor and include Trellix in future KuppingerCole reports.

## 6.10 Trend Micro

Trend Micro is a venerable player in the endpoint security market, having been established in 1988 in Tokyo. Beyond EPP and EDR, Trend Micro has email and web security gateway solutions, SaaS application security, cloud migration tools, and a global threat intelligence service. They also offer IoT security and management solutions covering connected cars, smart factories, and connected consumer use cases. Trend Micro participates in independent malware detection tests regularly.

**Why worth watching:** Trend Micro is one of the larger vendors in the endpoint security market. They

participate in independent tests regularly. They did not respond to our request for information for this report.

## 6.11 Webroot

Launched in Colorado in 1997, Webroot offers an EPP product, cloud-hosted DNS protection, endpoint data protection, cyber threat intelligence, and security awareness training services.

**Why worth watching:** Webroot was acquired by Carbonite, a cloud-based backup company in 2019. Webroot's CTI services are widely used across the security industry.

## 7 Related Research

[Market Compass Endpoint Protection Detection & Response](#)

[Buyer's Compass Endpoint Protection](#)

[Buyer's Compass Endpoint Detection & Response](#)

[Leadership Compass Endpoint Security: Anti-Malware](#)

[Leadership Compass Unified Endpoint Management](#)

[Executive View ESET Endpoint Security](#)

[Executive View Nucleon Security Smart Endpoint](#)

## Methodology

### About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

### Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:



- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

## Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- \*\*Security
- Functionality
- Deployment
- Interoperability
- Usability\*\*

**Security** is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

**Functionality** is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

**Deployment** is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

**Interoperability** refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

**Usability** is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

## Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

**Innovativeness** is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

**Market position** measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

**Financial strength** even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

**Ecosystem** is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

## Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

### Strong positive

Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

### Positive

Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

### Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

#### **Weak**

Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

#### **Critical**

Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

### **Inclusion and exclusion of vendors**

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

## Content of Figures

Figure 1: The Overall Leaders in Endpoint Protection, Detection, and Response

Figure 2: The Product Leaders in Endpoint Protection, Detection, and Response

Figure 3: The Innovation Leaders in Endpoint Protection, Detection, and Response

Figure 4: The Market Leaders in Endpoint Protection, Detection, and Response

Figure 5: The Market/Product Matrix for Endpoint Protection, Detection, and Response

Figure 6: The Product/Innovation Matrix for Endpoint Protection, Detection, and Response

Figure 7: The Innovation/Market Matrix for Endpoint Protection, Detection, and Response

## Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

**KuppingerCole Analysts** support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact [clients@kuppingercole.com](mailto:clients@kuppingercole.com).