

Endpoint Protection Detection and Response

Martin Kuppinger and John Tolbert

October 9, 2024



LEADERSHIP
COMPASS
2024

This report provides an overview of the Endpoint Protection Detection & Response (EPDR) market and a compass to help you find a solution that best meets your needs. It examines solutions that provide pre-execution malware identification and prevention, endpoint firewall, system file integrity monitoring, application controls, URL filtering, compromise detection threat hunting, forensic analysis, reporting, alerting, and manual and automated response capabilities for endpoints of various types.

Contents

Executive Summary	3
Key Findings.....	6
Market Analysis	7
Delivery Models	8
Required Capabilities	8
Leadership	10
Overall Leadership	10
Product Leadership	12
Innovation Leadership	14
Market Leadership.....	16
Products and Vendors at a Glance	18
Product/Vendor evaluation.....	20
Spider graphs	20
Broadcom – Symantec Endpoint Security Complete (SESC)	21
CrowdStrike – Falcon Prevent (NGAV), Falcon Insight XDR (EDR/XDR), Falcon Device Control, and Falcon Firewall Management.....	24
ESET – ESET PROTECT	28
Fortinet – FortiEDR	31
Group-IB – EDR	34
IBM – QRadar EDR and MaaS360	37
Microsoft – Defender for Endpoint.....	40
SentinelOne – Singularity XDR Platform	43
Sophos – Intercept X Advanced	46
Trellix – Endpoint Security.....	49
Vendors to Watch	52
Absolute Software	52
AhnLab	52

Acronis	52
Bitdefender	52
BlackBerry	53
Checkpoint	53
Coro.....	53
Cybereason	53
Deep Instinct	54
G Data	54
GoSecure	54
Heimdal Security	54
Malwarebytes	55
OpenText.....	55
ThreatLocker	55
Trend Micro	55
WithSecure.....	56
Xcitium.....	56

Executive Summary

Endpoint security is a foundational element of cybersecurity architectures that is even more important today than in decades past. All end-user computers, smartphones, and tablets should have Endpoint Protection Detection & Response (EPDR) clients installed, preferably with up-to-date subscriptions. Servers and virtual machines/desktops should be protected as well. Windows platforms are still the most vulnerable, though there is an increasing amount of malware for Android. It is important to remember that Apple's iOS and Mac devices are not immune to malware, and as market share increases, particularly for Mac devices, the amount of malware for that platform has increased too.

What drives the need for EPDR? Ransomware is a top-of-mind concern for CISOs and cybersecurity professionals globally. It has unfortunately turned into a profitable business for cybercriminals. They now deliver ransomware-as-a-service with a well-defined business model with job specializations.

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 increasing in frequency. Attackers have diversified their targets. Now businesses, small and large, non-profits, and government agencies face this threat

daily. Ransomware, in the traditional sense, is a form of malware that encrypts users' data, demanding that ransom be paid for the return of control or for decryption keys. Most forms of ransomware are deployed similarly to an Advanced Persistent Threat (APT) campaign, using phishing, other social engineering, or compromised credentials to get into their victims' assets. They may then stage ransomware on various machines throughout an enterprise and exfiltrate data before ransomware detonation. In years past, some ransomware operators did not provide working decryption keys, so paying the ransom was purely a waste of money. This has changed somewhat since cybercriminal outfits have started to function like businesses: they must provide "customer" service to victims. 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 data.

Alternatively, attackers may simply infiltrate victims' assets, then copy and exfiltrate data with the threat of leaking customers' personal information or intellectual property if ransoms are not paid. The advantage for the attackers is that it does not matter if the victims have good backups, they could still leak the exfiltrated data if ransoms are not paid. In these cases, they may pose as uninvited penetration testers. This technique is becoming more popular. In any case, paying the ransom only emboldens the perpetrators and perpetuates the ransomware problem. Cyber insurance policies are commonly acquired by all kinds of organizations to offset the costs of cyber-attacks, sometimes including ransom payments. However, to qualify for cyber insurance, organizations must demonstrate that they have cybersecurity measures in place.

Backups are of course still an important part of cyber hygiene. Restoration is sometimes problematic if users or organizations have not been keeping up with backups, if restore process are not defined and have not been tested before, or if backups have been contaminated by malware. Cybercriminals have gotten adept at finding and encrypting data backed up to the cloud. Even if pristine backups are readily available, time will be lost in cleaning up the compromised computers and restoring the data. Thus, preventing ransomware infections and the compromises that lead to such events is preferred. However, no anti-malware product is 100% effective at prevention. It is still necessary to have defense in depth.

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.

Other malware types are still out there. Viruses are far more sophisticated than they were decades ago. Now, viruses are polymorphic, meaning they alter their structure to try to avoid detection upon every iteration. Worms are malicious code that spreads across unsecured networks, relying upon unpatched, compromised applications and unprotected ports. Worms are back in the news since researchers have found that AI LLMs (Large Language Models) can easily generate that type of code. Rootkits are low-level malware, usually implemented like device drivers in operating systems. Rootkits allow bad actors complete control of affected machines. Rootkits usually arrive in the form of a Trojan, software disguised as to its true intentions.

Botnets are collections of controlled devices, often compromised by rootkits, which 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.

Endpoint Protection Platforms (EPPs) are an evolution from the antivirus programs of old and even the “next generation” antivirus (NGAV) systems from a decade or more ago. Antivirus programs were generally signature-based, meaning that they could scan for known virus patterns. NGAV systems began harnessing the power of Machine Learning (ML) algorithms to detect and classify malware. ML-based detection became imperative due to the exponentially proliferating varieties of malware: with thousands and then millions of variants of malware, human analysts could not keep up. EPP systems are NGAV plus secondary features such as endpoint firewalls, URL filtering to prevent users from communicating with known bad domains, application controls to prevent malicious executables from running, and system file integrity monitoring.

Endpoint Detection & Response (EDR) solutions search for evidence and effects of malware that may have slipped past endpoint protection / antivirus 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.

The **MITRE ATT&CK Framework** is a comprehensive approach that addresses 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.

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.

EPP and EDR toolsets have converged 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.

Several independent testing regimes exist that vendors can participate in to demonstrate the effectiveness of their products. [AV-Comparatives](#) runs various extensive 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. Notes about vendors' participation in these independent testing scenarios will be included where relevant throughout chapter four.

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

Which organizations need EPDR? All of them, from small, sole proprietors to multinational corporations, non-profits, and from small city and county governments to national governments. The EPDR market is large, and it has been for decades. It will continue to grow as the number of deployed assets increase and the threats increase.

For information on our research practices, see [KuppingerCole Leadership Compass Methodology](#).

Key Findings

- The threat of ransomware in all its permutations continues to grow.
- Attacks are more frequent, and ransoms and cleanup costs are getting more expensive.
- Sometimes malware is not even involved in cyber-attacks where ransoms are demanded; this makes the detection of compromise on the endpoint more difficult but more important.
- The EDR components must be adept at finding signs of Indicators of Compromise (IoCs) even if malware is not present, generally using behavioral analysis.

- Fileless malware and “living off the land” (LotL) techniques are more commonplace today.
- Worms are making a comeback and may be precursors to additional attacks.
- Since the advent of SOAR and XDR, it is imperative that EPDR solutions have full but secure API exposure.
- Connectors for third-party solutions such as Security Information Event Management (SIEM), Security Orchestration Automation & Response (SOAR), IT Service Management (ITSM), and Cyber Threat Intelligence (CTI) sources are preferred.
- Multi-engine scanners that include a mix of old and new Machine Learning (ML) enhanced techniques are needed for comprehensive, highly performant detection.
- Application controls, in-agent endpoint firewalls, and system file integrity monitoring are essential features above and beyond malware scanning and prevention.
- Many EPDR solutions use kernel mode drivers, which grant access to low-level operating system functions. Improper use of or lack of sufficient testing of EPDR system components can lead to outages.

Market Analysis

The EPDR market has been around, even in its current amalgamated EPP plus EDR form, for quite some time. Major security vendors have offerings in this area. Although it is well-established, occasionally new players enter the market. However, full EPDR contains too large of a feature set for most startups to tackle at once. Thus, we see newer companies entering subsets such as EPP or EDR. It takes a good deal of innovation or a radical new approach to break into the endpoint security market successfully.

Since ransomware is a chief concern of nearly every organization around the world, preventing ransomware attacks, or at least quickly detecting them and mitigating damage, is the top priority for EPDR solutions. Although there has been much development by cybercriminals in terms of techniques, malware, and the business model itself, EPDR vendors have generally done a good job at keeping up with ways to thwart those attacks.

Much of the innovation in EPDR has gone toward defending against the ransomware threat. Machine Learning (ML) algorithms have been used by endpoint security vendors to enhance detection models to find malicious code for years. Unsupervised ML algorithms do not require pre-training and are often used to discover anomalies within data sets. Supervised ML algorithms are useful for classifying anomalies and malware types. Deep Learning (DL), a subset of ML, leverages artificial neural networks with multiple layers (deep neural networks) to model complex patterns in data. It has become increasingly important in endpoint protection due to its ability to automatically extract features and learn intricate patterns that traditional methods might miss. Researchers at EPDR vendors continually refine their models based on the continuous input of new malware variants. Security companies also use ML and DL to enhance detection of malicious user behavior. These technologies analyze vast amounts of data to identify patterns and anomalies associated with malicious activities. By continuously learning from new data, ML detection models can improve accuracy and adapt to new threats more quickly than traditional methods such as signature-based detection.

Since some ransomware attacks do not involve malware to get inside the victim organization, it has become important to look at other activities to see if attacks may be underway.

EPDR is a core element of security architectures for all industries and for all sizes of organizations. It will remain so for the foreseeable future. Although XDR encompasses endpoint security, it is not likely to supplant the independent XDR market.

Delivery Models

The delivery model of EPDR solutions is two-fold. There are central consoles and data stores and local components at the endpoint, delivered as agents.

Agents are required for endpoint protection. Most vendors support the current versions to one or two versions back of the most common operating systems (OSes). A few vendors have good support of even older operating systems. Agents should be available for all the device types in a given organization, in fact, determining for which OSes agents are available is a key requirement when looking for EPDR and XDR solutions. Agents are needed for Windows workstations and servers, Linux, macOS, Android, and iOS. Virtual desktops and machines also need coverage. Some EPDR and XDR solutions have “agentless” scanning options, which offer significantly less functionality when it comes to enforcing security policies.

Agents often have kernel mode drivers and elements that allow the EPDR solution access to the lowest levels, including hardware access. This is so that the EPDR tools can read and write to files and examine memory to look for malicious code. EPDR vendors must take great care to ensure that the kernel mode drivers and data structures directly used by these drivers do not cause system instability, thereby crashing and becoming a liability themselves. If faults in security software make their hosts unavailable, then the resulting situation is itself a security incident.

EPDR consoles may be able to reside on-premises, in private clouds, in IaaS, or in the vendor’s SaaS environment. Actual deployment models vary considerably between vendors.

Required Capabilities

These are the capabilities that KuppingerCole views as foundational for EPDR:

- Endpoint Protection (EPP)
 - Agents for Windows, Linux, Mac, and virtual desktops
 - Autonomous agent operation
 - Multiple malware pre-execution detection engines
 - Near real-time monitoring of anomalous behavior
 - File-less malware detection and prevention
 - Ransomware detection and prevention
 - Applied AI/ML for malware analysis and malicious activity discovery

- Sandboxing
 - Exploit prevention
- Secondary EPP Controls
 - Endpoint firewall
 - Application control
 - URL filtering
 - System file integrity monitoring
- Endpoint Detection and Response (EDR)
 - CTI standards support, integration with CTI sources
 - Ability to discover and remediate against major attack vectors
 - Threat hunting
 - Forensic investigations
 - Automated responses / playbooks
 - Interactive query and live remote memory examination
 - Activity recording and playback
 - Automated evidence collection
 - Case management
 - IoC customization
 - Automatic update of detection rules based on findings
- Enterprise Console and Common Features
 - MFA and at least role-based authorization for admins and analysts
 - API-enabled remote management and SOAR integration
 - MITRE ATT&CK® mapping in dashboards and analyst interfaces
 - Auditing, reporting & dashboards
 - Flexible, modern software architecture & deployment

The following features are considered innovative in this market:

- Mobile device client coverage
- Delegated administration
- Endpoint browser or application-level sandboxing
- Applied AI/ML for self-learning of analyst responses
- Advanced pre-execution heuristic detection models

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify 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 various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

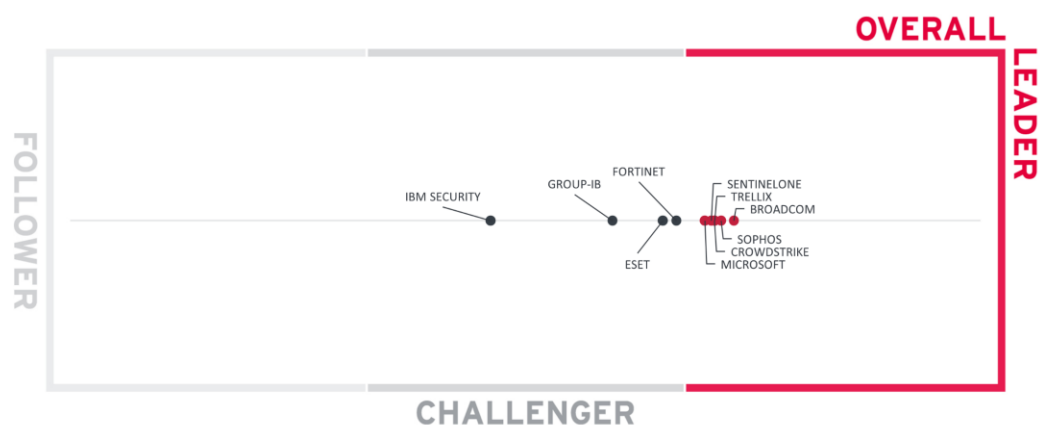


Figure 1: Overall Leadership in the EPDR market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Broadcom with its Symantec Endpoint Security Complete leads the field with, as the product name implies, a complete EPDR solution that has a large share of the market and many innovative features. It is followed by Sophos, Trellix, CrowdStrike, SentinelOne, and

Microsoft. Each has strong products, with varying degrees of innovation, and comparatively large market share.

The top Challengers are Fortinet and ESET. Group-IB and IBM Security round out the Challengers.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Broadcom
- CrowdStrike
- Microsoft
- SentinelOne
- Sophos
- Trellix

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

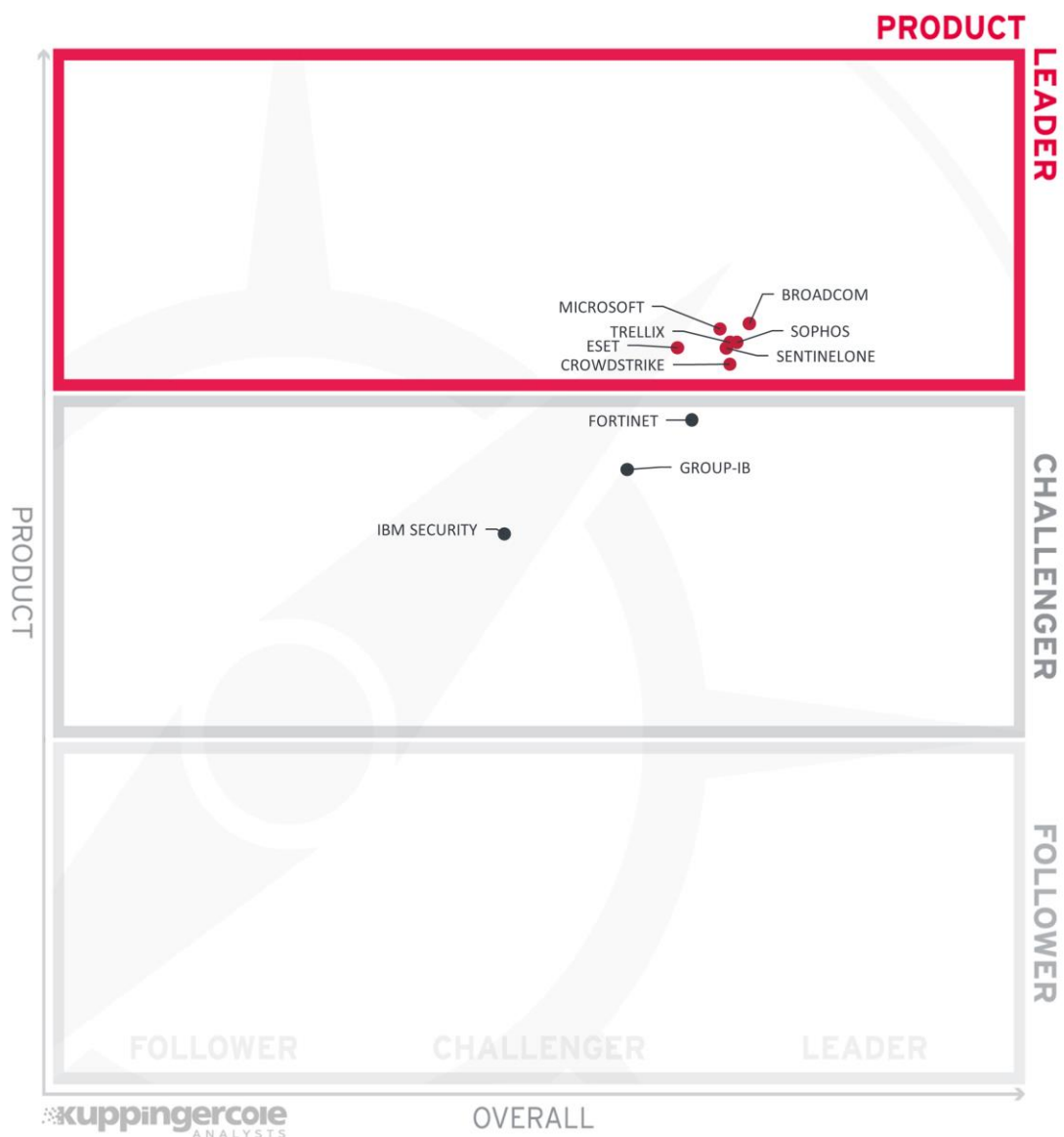


Figure 2: Product Leadership in the EPDR market

Broadcom is at the top of the Product Leadership ranking. They are followed by Microsoft, Trellix, Sophos, ESET, SentinelOne, and CrowdStrike. Each of these products is excellent and has specific strengths and challenges that will be outlined in the following chapter.

Fortinet is also a top Challenger in Product Leadership. Group-IB and IBM Security are also in the Challenger position.

There are no Followers in Product Leadership.

Product Leaders (in alphabetical order):

- Broadcom
- CrowdStrike
- ESET
- Microsoft
- SentinelOne
- Sophos
- Trellix

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.

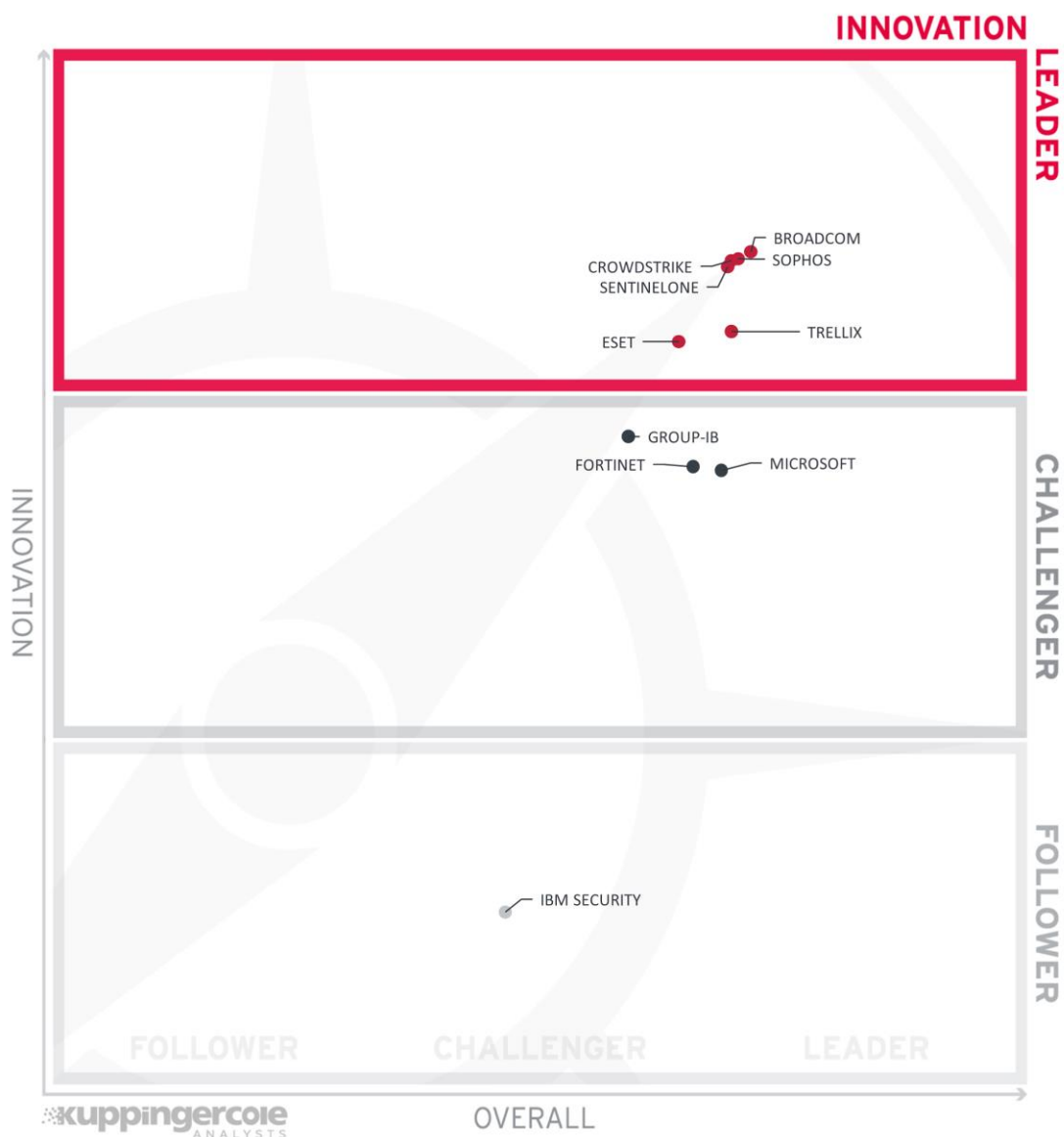


Figure 3: Innovation Leadership in the EPDR market

This view is mainly based on the evaluation of innovative features, services, and technical approaches as defined in the Required Capabilities section. The vertical axis shows the

degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests, but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

Broadcom, Sophos, CrowdStrike, SentinelOne, Trellix, and ESET are the Innovation Leaders in this edition. Innovation in EPDR is evidenced by the use of advanced ML, some use of Generative AI, deeply capable threat hunting interfaces, intuitive dashboards and reports, automatic case handling and threat intelligence correlation, and integration with other components in customers' security infrastructure.

Group-ID, Fortinet, and Microsoft are the Innovation Challengers, all quite near the threshold.

IBM Security is a Follower in Innovation, indicating there is room for improvement in some basic features as well as the need for adding leading-edge capabilities.

Innovation Leaders (in alphabetical order):

- Broadcom
- CrowdStrike
- ESET
- SentinelOne
- Sophos
- Trellix

Market Leadership

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

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

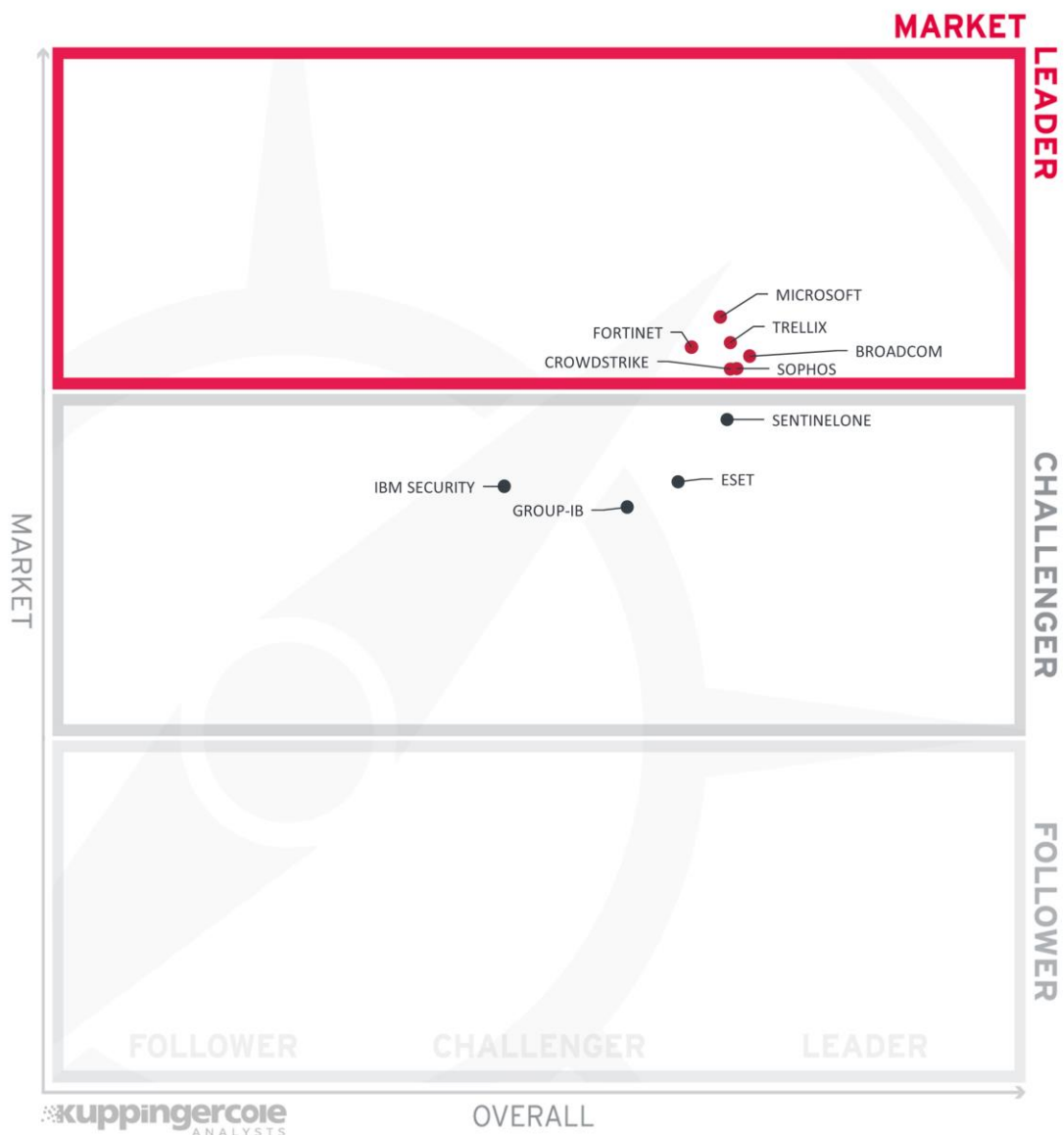


Figure 4: Market Leaders in the EPDR Market

The Market Leaders in EPDR are Microsoft, followed by Trellix, Fortinet, Broadcom, Sophos, and CrowdStrike.

SentinelOne is the top Challenger in the field. Most of the rest of the field is above center in the Challenger section, including ESET, IBM Security, and Group-IB.

There are no Followers in the EPDR market.

Market Leaders (in alphabetical order):

- Broadcom
- CrowdStrike
- Fortinet
- Microsoft
- Sophos
- Trellix

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. 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. Since some vendors may have multiple products, these are listed according to the vendor's name

Vendor	Security	Functionality	Deployment	Interoperability	Usability
Broadcom	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CrowdStrike	Positive	Strong Positive	Positive	Strong Positive	Positive
ESET	Strong Positive	Positive	Strong Positive	Positive	Positive
Fortinet	Positive	Positive	Strong Positive	Positive	Strong Positive
Group-IB	Positive	Positive	Positive	Neutral	Strong Positive
IBM	Positive	Neutral	Positive	Neutral	Positive
Microsoft	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
SentinelOne	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Sophos	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Trellix	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive

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

In Table 2, we provide 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
Broadcom	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CrowdStrike	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ESET	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Fortinet	Positive	Strong Positive	Strong Positive	Strong Positive
Group-IB	Neutral	Positive	Positive	Positive
IBM	Weak	Positive	Strong Positive	Strong Positive
Microsoft	Positive	Strong Positive	Strong Positive	Strong Positive
SentinelOne	Strong Positive	Positive	Strong Positive	Strong Positive
Sophos	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Trellix	Strong Positive	Strong Positive	Strong Positive	Strong Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we have 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 EPDR market segment, we look at the following categories:

Multi-engine agents – this is the analysis of the combinations of different techniques and technologies employed by the solution in software agents to identify malicious code and prevent it from executing and achieving its goals. The metric also considers the variety of agents available for different operating systems, with broader support leading to better scores.

Endpoint hardening – this category represents some of the additional security functions provided by EPDR suites, including URL filtering, endpoint firewall, application controls, and system file integrity monitoring.

Compromise detection – this is the 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 – this category examines how each solution's facilities for investigations and threat hunting are used, such as IoC creation, query construction and execution, memory, and file system analysis, etc.

Responses – this header represents the actions available within the solutions' management consoles, such as alerting staff, process termination, deletion or quarantine of malicious files, node isolation, registry and file system rollbacks, full endpoint restoration, etc. This category also considers the availability of and organization of playbooks for customers to utilize for responses.

Administration – this rubric is our evaluation of the management console functionality including SOC integration, dashboards, reports, and analyst/investigator interfaces.

Broadcom – Symantec Endpoint Security Complete (SESC)

Broadcom is a large, publicly listed US-based manufacturer of semiconductor products and supplier of infrastructure software solutions founded in 1961 and headquartered in San Jose, California. The bulk of Broadcom's customers are in the NA and EMEA regions. In 2018, Broadcom acquired CA Technologies, and the following year acquired Symantec's enterprise security portfolio. Symantec Enterprise Software is a division within Broadcom Software and is focused on the largest global firms, including those in highly regulated industries such as banking, telecom, and manufacturing. Symantec Endpoint Security is licensed per covered device. Enterprise licensing agreements are also available.

The enterprise console can be run on-premises from a physical or virtual appliance, on Windows Server in any IaaS, and they host it as SaaS. STIX, TAXII, and YARA are supported CTI standards. Symantec has its own sandbox (CASMA), so no third-party sandboxes are supported. Symantec provides CTI for customers, and multiple connectors for third-party sources are available. They share CTI with other service providers and are an affiliate member of the Cyber Threat Alliance. CEF, REST APIs, event streaming, and syslog communications allow connectivity to SIEMs and SOAR platforms through ICDx. ITSM integration is not supported. CAC/PIV cards, Kerberos, LDAP, Microsoft Azure AD, Okta, RSA SecurID, and Symantec VIP are available for strong authentication. It supports SAML and OIDC for federation, and it has a flexible, fine-grained internal authorization model based on customizable administrator/analyst roles. The solution supports REST APIs, with OAuth2 for its API authentication method. Communication between agents and the console uses TLS 1.3. Notably, the product does not require a root, administrator, or service account on endpoints.

SESC agents are available for Windows Vista through 11, Windows Server 2008+, macOS 13+, all Linux types, Android 14+, and iOS 17. 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.

SESC detects evidence of attacks including command and control traffic, botnet activity, port scans and reconnaissance, lateral movement, AD enumeration, DNS tunneling, data exfiltration, disabling security controls, and changes to firmware or boot configurations. It automatically assigns priority levels to event items, which can be configured by customer admins. The solution reduces false positives through extensive testing of signatures prior to release and adaptive endpoint activity recording rules. The analyst interface features a drop-down list query builder, regular expression searches, drill-down capabilities from dashboards into investigations and threat hunts, timeline view, global map, and the ability to launch playbooks.

Automated incident analysis is performed, including correlation of relevant events and assembly of incident data into cases for analysts. Custom IoCs can be created for threat hunts, and the solution facilitates the derivation of custom IoC variants based on published IoCs and behavioral analysis. The product supports live memory analysis on endpoints, remote inspection of disk structures such as the MFT (Master File Table), and activity recording/playback for forensic analysis. Analysts can save, edit, and share queries. It

supports multiple automated remediation steps such as quarantining, denylisting, blocking, remote shell execution, and evidence collection.

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 theories can be generated.

Symantec services are ISO 27001 and SSAE SOC 2 Type 2 certified. Broadcom has not participated in AV-Comparatives evaluations in several years, but they did participate in MITRE's Engenuity Enterprise in 2023. More in-platform automation options would benefit customers who do not have SOAR solutions. SESC is a complex product, but Symantec have enhanced the deployment process and management capabilities. Setup and incident handling support are part of the standard package. Symantec is a leader due to the extensive feature list. Organizations with experienced threat hunters and security analysts should consider SESC for EPDR.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 3: Broadcom's rating

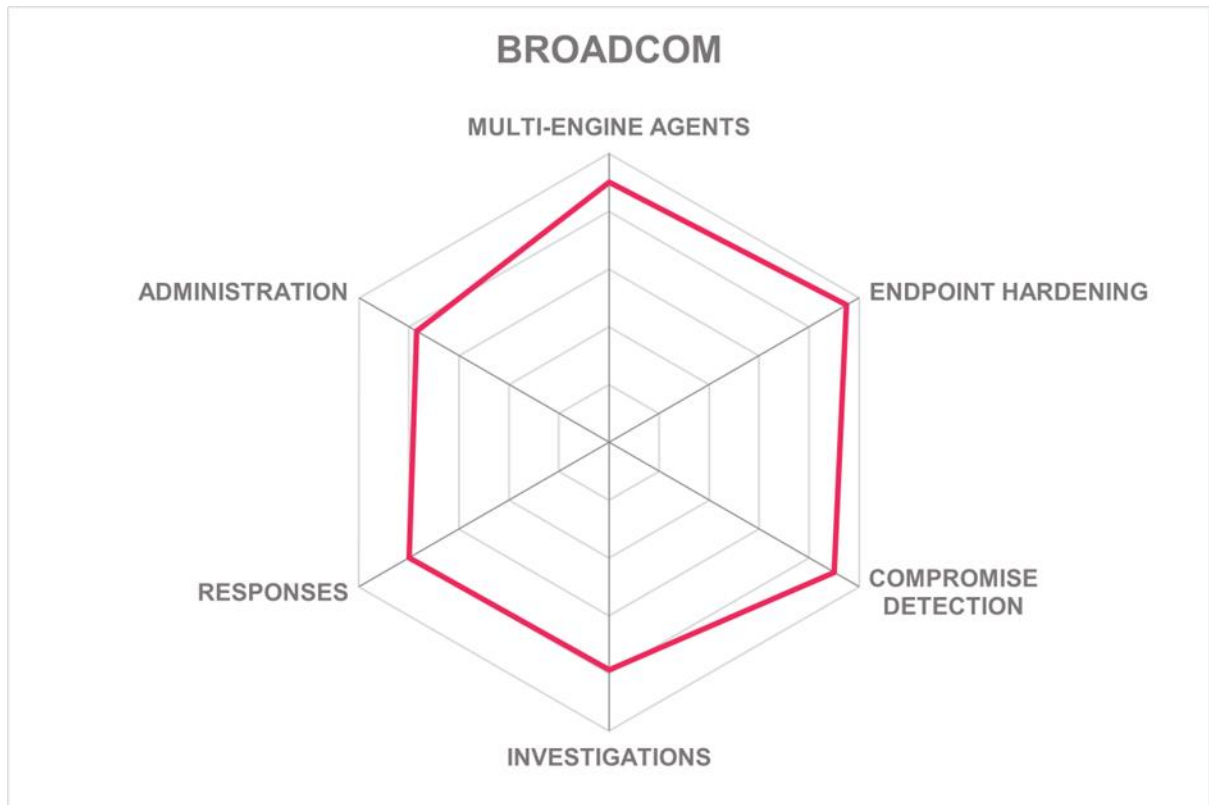
Strengths

- Leverages all major malware identification techniques and has advanced ML detection models
- Includes fine-grained application controls, endpoint firewall, and system file integrity monitoring
- Wide range of choices for strong authentication to the enterprise console
- Most typical response actions are supported
- Setup and incident handling assistance are provided
- Aids with root cause analysis and attribution theory generation
- Affiliate member of Cyber Threat Alliance

Challenges

- Does not have out-of-the-box integrations for ITSM
- Default data retention periods should be longer
- Support for additional languages would be useful
- Playbooks cannot currently be edited

Leader in



CrowdStrike – Falcon Prevent (NGAV), Falcon Insight XDR (EDR/XDR), Falcon Device Control, and Falcon Firewall Management

CrowdStrike was founded in 2011 and is headquartered in the Bay Area. They offer EPDR, XDR, ITDR, and multiple cloud security solutions. They are a large public company with customers around the world. CrowdStrike is a cloud-native solution. Licensing costs are per node and based on the length of data retention required by each customer. Falcon Prevent (EPP), Falcon Insight XDR (EDR/XDR), Falcon Device Control, and Falcon Firewall Management are the components considered here for EPDR.

The management console is hosted in CrowdStrike's own and public IaaS data centers in the US and EU. Certified US GovCloud on AWS instances are available for those who need that. Full support for CTI standards is given, including STIX, TAXII, YARA, MISP, Sigma, Snort, and Zeek. Customers can augment the provided CTI with VirusTotal, RiskIQ, DomainTools, OPSWAT, and Sixgill integrations. CrowdStrike has its own sandbox but can easily integrate with third-party sandboxes via APIs if desired. It supports CEF, REST APIs, and syslog for event streaming, thus it can interoperate with any standards-based SIEM and SOAR. Customers can build connections from Falcon to their ITSMs as necessary via REST. Webhooks are also supported for sending near real-time messages to third-party apps.

Dashboards and reports can be customized. The dashboards have a MITRE ATT&CK heatmap. Admins can create and modify roles to suit the delegated management requirements of complex organizations. Time-based One-Time Passwords (TOTP) such as Duo are currently supported for MFA. FIDO support is planned for later in 2024. Customers can also configure MFA through federation to their own IAM or IDaaS services. CrowdStrike implementations do not depend on root or service accounts on endpoints.

Falcon agents are available for Windows 7/10/11, Windows Server 2008+, all major Linux variants, macOS 13/14, and recent Android and iOS versions. Additional support for legacy OS such as Windows XP/Vista/8 and Server 2003 is planned for late 2024. All browsers are supported; files and code in browsers are scanned and can be blocked or allow-listed. CrowdStrike is compatible with other AV or full EPDR agents, although it is recommended that only one EPDR agent be configured in active blocking/prevention mode.

For malware prevention, CrowdStrike uses ML- and DL-based detection models for heuristics, static file analysis, memory analysis, runtime behavioral analysis, sandboxing, and exploit identification. It omits older signature-based techniques. Falcon watches for Indicators of Attack (IoA), such as attempts to delete backups, accessing the Windows Volume Shadow Copy, mass calls of encryption routines, etc. to deter ransomware. Running at the kernel level enables Falcon to detect trojans and rootkits. It looks for IoAs such as process hollowing, process migration, DLL sideloading, PowerShell execution, registry changes, and privilege escalation to shut down file-less and other malware. CrowdStrike integrates with the Microsoft Anti-Malware Scanning Interface (AMSI) to have better visibility into Office Macros to prevent malicious ones from running. Since Falcon emphasizes runtime behavioral analysis, it can detect malware written in uncommon programming languages. Falcon also scans the BIOS for compromise persistence techniques.

CrowdStrike states that the agents can function autonomously and just as effectively when they cannot connect to the CrowdStrike cloud. Falcon does not do category-based URL filtering. It does provide its own host-based firewall, coarse-grained reputation-based application control facility, and system file integrity monitoring.

Falcon EDR watches for post-infection IoAs, such as C2 activity, lateral movement, DNS tunneling, AD enumeration, attempts to disable security controls, botnet communications, etc. Falcon sensor integrates with Falcon Data Protection to get detailed information about the movement of sensitive data like intellectual property, which helps discover staging and exfiltration techniques. The analyst interface allows for multiple query types, including regular expression searches and the “Investigate with Charlotte AI” feature. Charlotte AI allows analysts to input information about IoAs, then it automatically correlates all related events and uses its internal LLM (Large Language Model) to generate incident summaries. Furthermore, it supports live remote memory analysis, remote inspection of disk-level structures such as the MFT, and records up to one hundred telemetry types for later playback in forensic investigations.

Falcon can send alerts via email, Microsoft Teams, and Slack. Other channels can be configured with Webhooks. Automated responses are facilitated through playbooks in Falcon Fusion SOAR, which is included at no additional cost. Examples of playbook types include Jira or ServiceNow ticket creation, evidence collection, dispatching suspicious files to sandbox for analysis, adding an account to identity protection watchlist, and more. Playbooks can be edited in a no-code manner using a visual flowchart designer. Currently, it does not recommend specific playbooks for incidents, but they are integrating Charlotte AI with Falcon Fusion, and that is expected to happen within the next year. Granular actions permitted within responses include all the expected options, such as process termination, host isolation, blocking IPs, preventing/rolling back registry changes, and full rollback to a last known good state. Falcon can also generate root cause analyses and provide attribution theories.

CrowdStrike has obtained an impressive list of certifications, including ISO 27001, SSAE SOC 2 Type 2, CSA Star Level 1 and 2, US FedRAMP, NSA-CIRA, UK G-Cloud, TISAX, and more. CrowdStrike Falcon Pro achieved AV-Comparatives LSASS Credential Dumping certification in mid-2024 and blocked 100% of attacks in their Real World Business Security Test in the spring of 2024 and blocked 99.8% of attacks in their Mac Security Test. CrowdStrike participated in MITRE Engenuity Enterprise 2023 and was able to directly detect all 143 specific techniques used by the simulated attacker. Initial setup support is included, and incident handling support is available for additional charges. CrowdStrike offers managed detection and response with Falcon Complete. CrowdStrike has excellent language support.

On July 19, 2024, CrowdStrike released a routine content configuration update, intended to enhance threat detection, that inadvertently and unexpectedly caused software disruptions on certain devices running Windows. During these disruptions, the Falcon cloud platform remained fully operational, and customer data and systems were not compromised by a threat actor. This incident has negatively affected their ratings in this edition of the report, since it indicated insufficient quality assurance and a lack of resiliency in deploying updates

prior to the incident. However, CrowdStrike worked quickly to resolve it and the company was transparent and timely in its communications about the root cause and measures to avoid similar outages in the future. Due to their lessons learned and go-forward improvement plans, any organization looking for a modern, AI-powered endpoint security solution should still have CrowdStrike Falcon near the top of their list for RFPs.

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive



Table 3: CrowdStrike's rating

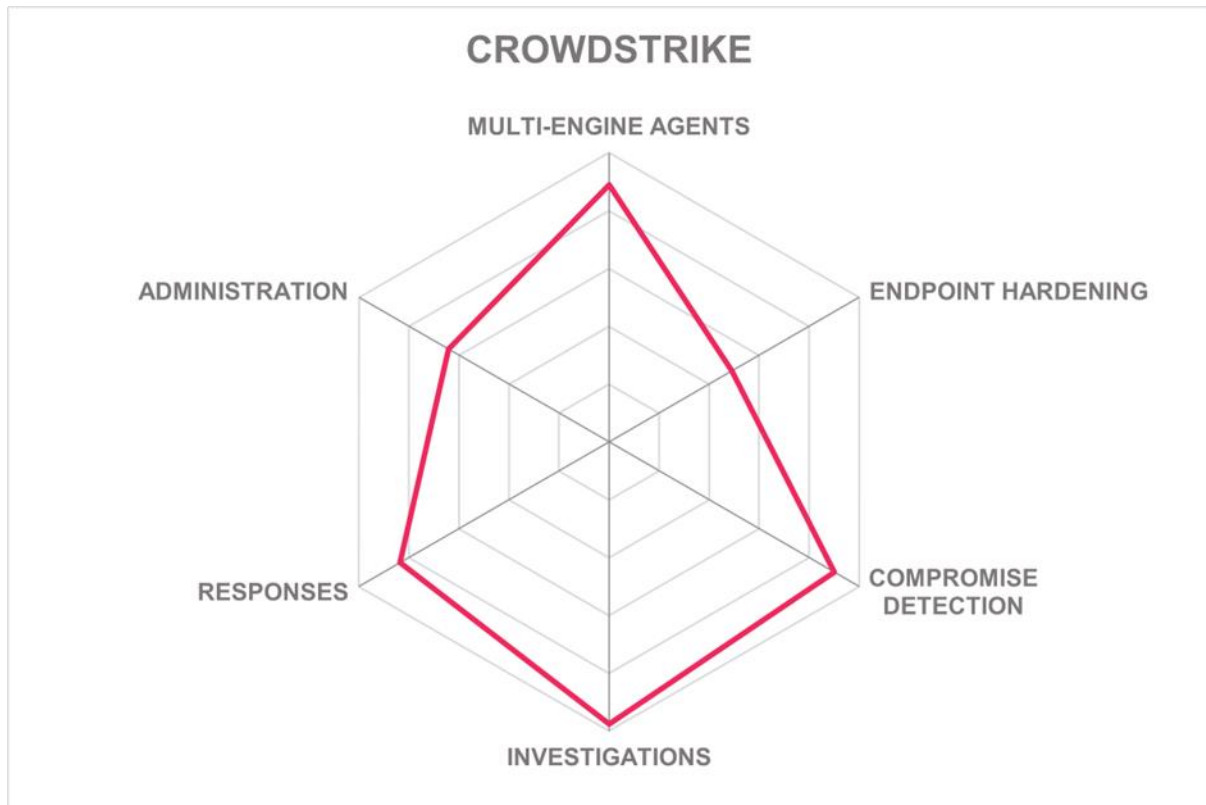
Strengths

- One of the first cloud-native EPDR solutions; compatible with other AVs or EPDR solutions
- Broad support for CTI standards; multiple third-party CTI sources integrated into the analyst interface
- Runtime behavioral analysis to find Indicators of Attack
- Excellent highly customizable dashboards and reports
- Integration with Falcon Data Protection provides details on sensitive data movement
- LLM-powered Charlotte AI facilitates investigations and analysis
- Provides full range of automatic responses, including full node rollback
- Many security certifications and excellent results in multiple AV-Comparatives independent tests

Challenges

- Very short default data retention period of 7 days; more can be purchased
- Needs more MFA options, and FIDO support is planned
- TLS 1.3 for agent communications is in work
- Does not do category-based URL filtering
- Limited app controls
- Does not yet recommend playbooks, but that is on the roadmap
- Routine content configuration update unexpectedly caused outages on devices running Falcon on Windows on July 19, 2024, but the problematic update was promptly pulled back and root cause analysis was published outlining process improvements and mitigation steps to prevent this incident from recurring

Leader in



ESET – ESET PROTECT

ESET, a privately held company headquartered in Bratislava, Slovakia, 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. ESET was an early adopter of ML algorithms for detection models. 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 node-based licensing and is moving to a subscription model.

ESET's enterprise console offers flexible hosting options, supporting both on-premises deployments and cloud-based environments. It supports integration with various IaaS providers like Amazon AWS, Microsoft Azure, Google Cloud Platform, Oracle Cloud, and IBM Cloud. The console can be run on Windows and most Linux variants. Additionally, the console is available as a SaaS solution provided by the vendor, hosted in their own facilities and a major IaaS provider with data center locations in the EU, NA, and Japan. The solution adheres to multiple CTI standards and formats, including STIX, TAXII, and YARA. For threat intelligence, ESET products use their own high-quality threat intelligence and connectors are available for many third-party sources. ESET PROTECT supports CEF, REST API, and syslog for SIEM connections. APIs require SAML or key exchange for authentication. ESET Connect Cloud Gateway enables integration with ITSM and SOAR systems. ESET features customizable dashboards and fine-grained authorization capabilities. It supports MFA through various methods, including SMS OTP, Google Authenticator, their own mobile app, YubiKeys, Android fingerprint biometrics, iOS Face ID, and iOS Touch ID. SAML and OIDC enable identity federation. Communication between the agent and the console employs TLS 1.3. The product does require root accounts for operation.

ESET security products are available for Windows 7-11, Windows Server 2008+, all Linux types, macOS and Android. It works with all major browsers, and ESET Web Access Protection prevents downloads of malicious content. It has very granular URL filtering, and customers can create their own allow/deny lists. There are no known incompatibilities with other security software. ESET PROTECT uses multiple malware detection techniques including signatures, static analysis, sandboxing, behavioral analysis, memory analysis, and exploit prevention. It can detect all types of malware attacks such as ransomware, botnets, file-less malware, like rootkits, RATS, and trojans. It can detect and prevent attacks and persistence at the lowest level with their UEFI scanner. ESET can auto-quarantine malicious code and does not require constant internet connectivity for optimum detection, making it a good choice for offline or air-gapped deployments. Their solution uses a full range of unsupervised and supervised ML and DL detection models, which are updated as frequently as needed. ESET PROTECT includes an endpoint firewall that can prevent node-level DDoS and botnet participation, and basic application controls to prevent users from running unsanctioned software. ESET Inspect monitors and prevents rogue system file changes.

ESET Inspect looks for all the post-compromise IoCs including C2 traffic, reconnaissance, lateral movement, AD enumeration, changes to boot-up configs, and data exfiltration attempts. Alerts are prioritized by severity and context and delivered via email or SNMP. Behavioral analysis is used to reduce false positives. Events are automatically correlated,

and relevant threat intel is applied. The analyst interface starts with the customizable dashboards with timeline views, from which analysts can drill down into investigations. Customers can create and modify IoCs for threat hunting. Live remote memory analysis is not supported, but full activity recording can be enabled.

Playbooks are rudimentary and can only be edited as XML files. Response actions include most common options including terminating processes, isolating hosts, quarantining files, stopping file changes; however, registry change and full node rollback are not possible. It can generate root cause analyses and attribution theories on the source of attacks.

ESET participated in MITRE Engenuity Enterprise 2023 as well as in the 2021 and 2022 rounds. In the H1 2024 Real-World Protection test by AV-Comparatives, ESET PROTECT blocked 99.6% of attacks, in the Q1 SE Labs Enterprise Endpoint Security test, ESET achieved 100% Protection and Legitimate Software Accuracy, and in two most recent 2024 tests by AV-TEST, ESET achieved a perfect score in each category: Protection 6/6; Performance 6/6; Usability 6/6. ESET has obtained ISO 27001 certification but has not yet gotten SSAE SOC 2 Type 2 for their SaaS solution. ESET has the broadest possible language support. They offer initial setup and incident analysis services as part of the standard package.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive



Table 3: ESET's rating

Strengths:

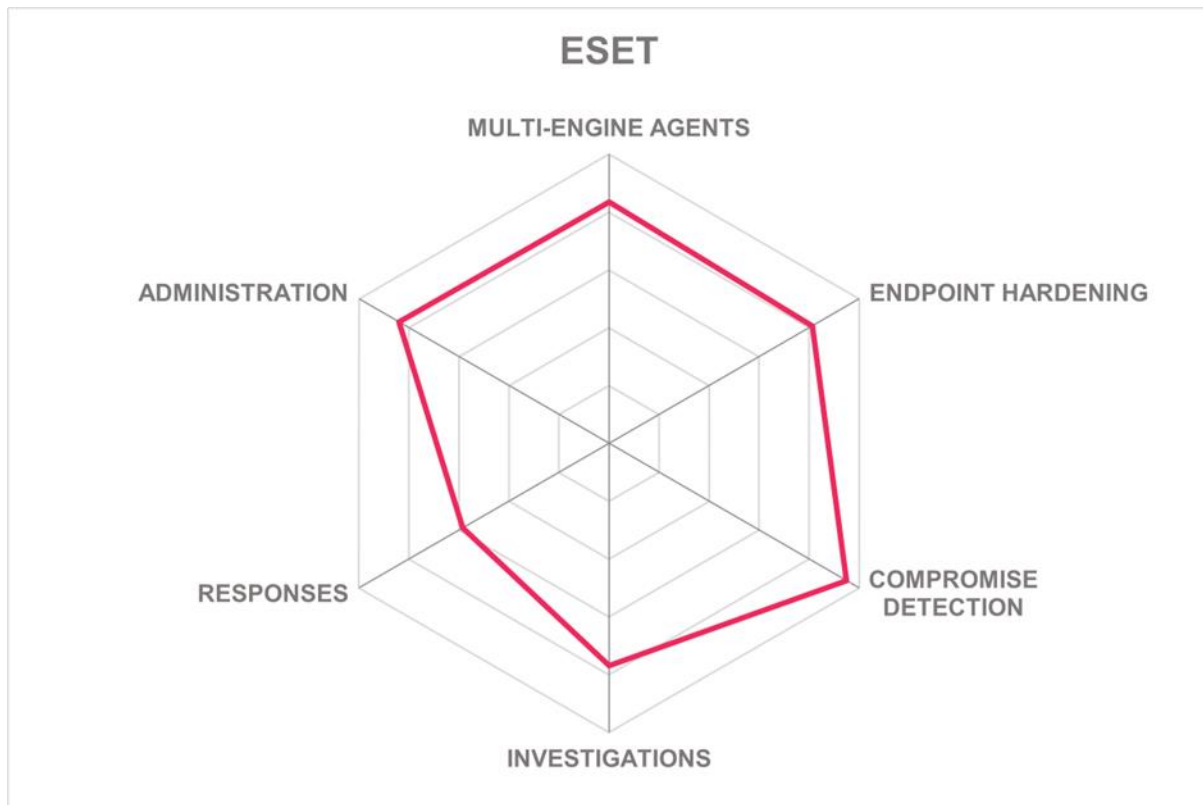
- Broad support for languages and geographies
- Low-level UEFI scanner prevents sophisticated malware from persisting
- Leverages all malware detection engine types except micro-virtualization
- Includes app controls, URL filtering/web access protection, endpoint firewall, and system file integrity monitoring
- Setup and incident analysis support is provided as part of the standard package
- FIDO authentication to console is available via ESET Secure Authentication Cloud
- Root cause analysis and attack attribution theory generation

Challenges:

- Does not support regular expressions
- App controls implementation could be more granular

- Playbooks can only be edited in XML format; solution does not recommend playbooks based on incident context
- Needs modern alerting channels such as Slack and Microsoft Teams
- Cannot roll back registry changes or nodes to last known good state

Leader in



Fortinet – FortiEDR

Fortinet was founded in 2000 and is headquartered in Sunnyvale, CA. They offer a broad spectrum of cybersecurity products and services, covering almost every functional area, including Operational Technology (OT). Fortinet is global and publicly traded. FortiEDR is their offering in this space. Licensing costs are calculated based on numbers of protected endpoints each year.

The management console is a virtual machine that can be hosted on-premises or in the cloud, and Fortinet offers it as SaaS. FortiEDR supports STIX, TAXII, and YARA rules for intel sharing. They have participated in MITRE evaluations. Fortinet products use their own dedicated sandbox and threat intel sources. Fortinet shares CTI with the Cyber Threat Alliance, of which they are a founding member. FortiEDR can stream event data via CEF/REST/syslog and connectors are available for FortiSOAR, IBM QRadar (PAN Cortex), and Splunk for SIEM/SOAR. FortiEDR provides standard reports and customers can create new reports. Dashboards are widget-based and customer configurable. Fine-grained authorization for discrete roles is possible within the management interface. Strong/MFA access to the console can be required; Fortinet supports mobile push notifications and users can authenticate through their mobile app. Customers can also set up identity federation to leverage their own strong/MFA methods. REST APIs and Webhooks enable connections to other security tools; API authentication is limited to key exchange. It supports TLS 1.3 for agent communications. Accounts for agents are required, and it can work with PAM systems, though none are explicitly tested.

FortiEDR has agents for Windows 7+, Windows Server 2008+, macOS 10+, most Linux OSes, Android 10+ and iOS 15+. Agentless options are present as well. FortiEDR works with all major browsers and scans content and prevents drive-by downloads. FortiEDR has been tested for compatibility with many other endpoint security solutions. It uses signatures, pre-execution code/file analysis and sandboxing, runtime behavioral analysis, memory analysis, and exploit identification and prevention. The solution emphasizes advanced behavioral analysis to find and stop macro malware, file-less malware, rootkits/trojans, and other malware. Fortinet's patented ransomware protection writes to copies of files rather than the files themselves so that it can compare and determine if unwanted encryption has taken place. Fortinet states that the agents operate offline as effectively as when connected. FortiEDR uses ML and DL for malware analysis and pushes new detection models to clients quarterly. FortiEDR has robust URL filtering and its own endpoint firewall. It has application controls apart from OS controls, and it performs system file integrity monitoring.

FortiEDR looks for most attack types with a few exceptions. Analysts and managers can drill down into details directly from the dashboard. The analyst interface features drop-down list query building and regular expression searches. It has timeline, geographic, and network map views. FortiEDR assembles cases for analysts to work on and sends alerts over Slack, SMTP, or SNMP. It begins automated event analysis, inserts fresh CTI, and correlates events from multiple nodes. SOC analysts can query interactively across all managed nodes and can do live remote memory analysis. FortiEDR records process, network, and file activity for later forensic investigations.

FortiEDR playbooks are focused on notifications, investigation, and remediation. FortiEDR can automatically terminate processes, isolate endpoints, block communications by IP, prevent and rollback registry changes, prevent mass encryption and volume shadow copy deletion. It does not offer full automated rollback, however.

Fortinet has obtained multiple security certifications including ISO 27001, HIPAA, CSA STAR, SSAE SOC 2 Type 2, TISAX, and US DoDIN. They offer initial setup services, 24/7 technical support, and fully managed services are available for additional expense. The solution has excellent language support. Several critical vulnerabilities have been discovered in FortiOS and related products this year, but the company has issued patches. FortiEDR is a well-rounded EPDR solution that can work well with other security tools as well as function as part of a tightly integrated full security stack solution. Any organization looking for EPDR should consider Fortinet, and those which have OT environments should strongly consider their solutions given the completeness of the offering in that space.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive



Table 3: Fortinet's rating

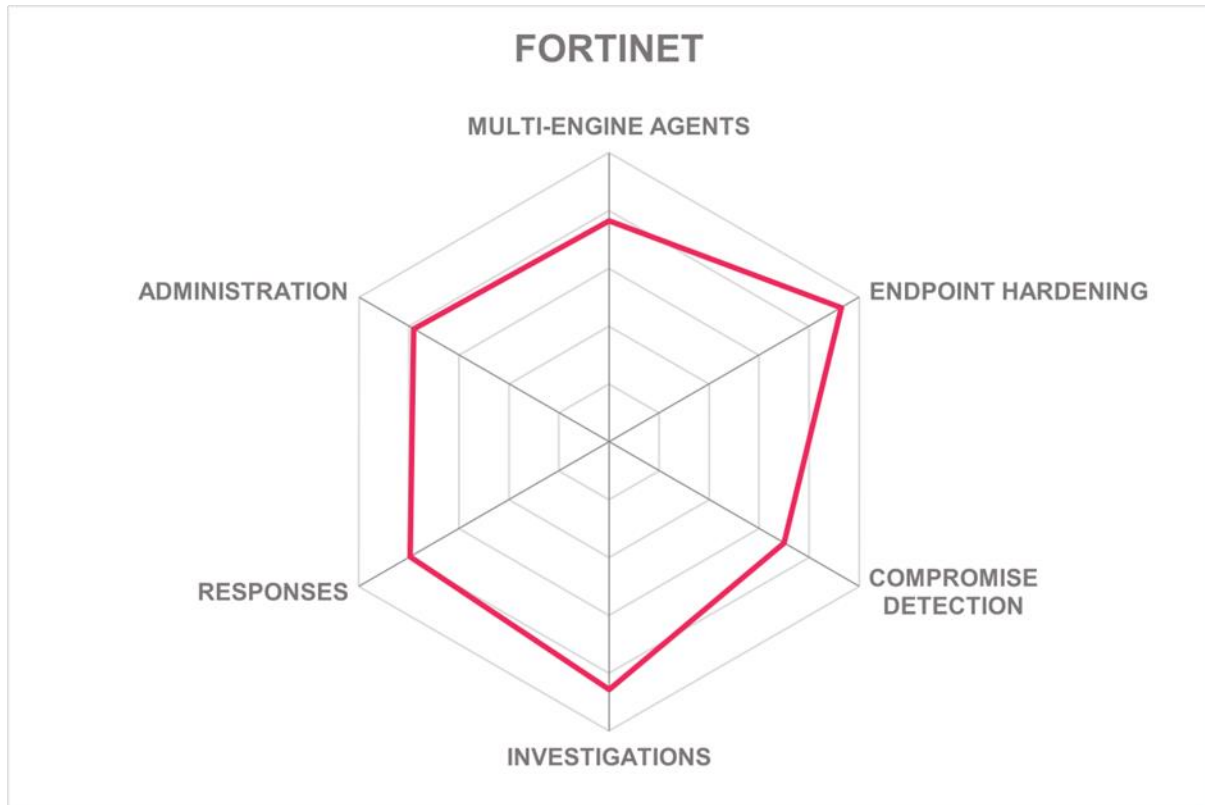
Strengths

- Founding member of Cyber Threat Alliance
- Excellent operating system agent support
- Works with all browsers to prevent drive-by downloads
- Includes system file integrity monitoring, and distinct endpoint firewall and app control functions
- Good interface for doing investigations and threat hunts
- Playbooks address most common issues

Challenges

- Limited OOTB MFA methods, although federation is supported
- Needs better API authentication method support
- Does not look for firmware level changes
- Does not support fully automated rollback to last known good state
- Playbook editing could be more user-friendly

Leader in



Group-IB – EDR

Privately held Group-IB was founded in 2003 and has its global headquarters in Singapore. Beyond Managed XDR, Group-IB offers Fraud Protection, threat intelligence services, attack surface management (ASM), and business email protection and anti-piracy products. They also have DFIR services, cyber defense and SOC consulting, audit, and red-teaming services. Most of their customers are in the EMEA and APAC regions. The enterprise console can run on-prem on an appliance (including for air-gapped environments), in partner's clouds, and they host it as SaaS from their own facilities. There are no IaaS hosting options for the console. Product costs are determined by the number of servers and user devices.

Group-IB supports Sigma, Suricata, YARA, and ZEEK for intel sharing. It has not participated in MITRE or AV-Comparatives evaluations because they do not position the product as EPP or NGAV. Group-IB does not provide connectors for third-party sandboxes or other CTI sources, since it has its own. Syslog is supported, but there are no out-of-the-box connectors for SIEM or ITSM. It can integrate with Palo Alto XSOAR. REST APIs are present and could facilitate connections with third-party solutions. Their APIs use basic authentication, key exchange, or can require SAML or OIDC for authentication. Agent to console communications use TLS 1.2/1.3. Group-IB EDR does need root accounts on endpoints.

Agents are available for Windows 7+, Windows Server 2008+, most Linux types, and macOS 10.15+. Browser scanning capabilities are comprehensive, scanning in-browser content, scripts, and files before download or execution. The solution is compatible with other vendors' endpoint security solutions. Group-IB's XDR employs multiple scanning techniques, such as signatures, static file and code analysis, pre-execution sandboxing, runtime behavioral analysis, memory analysis, and exploit identification. It effectively detects various attack types, including ransomware, RATs, botnets, file-less malware, macro-delivered malware. The solution auto-quarantines suspicious files and can operate autonomously without constant internet connectivity, although connectivity enhances its capabilities. Both unsupervised and supervised ML models, along with proprietary deep learning algorithms, are used for detection and classification, with models updated daily. URL filtering is achieved via integration with their ICAP and NTA products. Endpoint firewall capabilities are absent, but application control modes such as audit, allowlist, denylist, and user prompts are supported. System file integrity monitoring can be configured through writing detection rules.

Group-IB's XDR solution detects signs of compromise, including command and control traffic, botnet activity, port scans, lateral movement, AD enumeration, DNS tunnelling, data exfiltration, and the attempted disabling of security controls. The solution automatically assigns priority levels to event items based on severity. The analyst interface includes several features, including drop-down list query builders, regular expression searches, drilldowns from dashboards into investigations, timeline views, global maps, and automatic context-specific threat intelligence insertion into open cases. Automatic analysis features include the correlation of relevant events and assembling of incident data into cases for analysts. Custom IoCs can be created for threat hunts, and the solution facilitates the

derivation of custom IoC variants based on published IoCs and behavioral analysis. It supports live memory analysis on endpoints and remote inspection of disk structures such as the MFT. Additionally, the product provides activity recording and playback for forensic analysis.

Group-IB's XDR solution does not adhere to the playbook model for responses. However, it does support alerting via email and SNMP and can integrate other alerting methods via REST API. Rather than playbooks, Group-IB provides some remediation scripts which can be augmented by customers as needed. These scripts allow actions such as quarantining files, terminating processes or network sessions, isolating hosts, block communications, disabling user accounts, and rolling back registry and file changes.

Group-IB has attained ISO 27001 but not SSAE SOC 2 Type 2 certification. The solution is missing certain elements of EPDR functionality but seems strong in investigative capabilities. Group-IB provides assistance to customers for deployment and for incident handling if needed.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Strong Positive



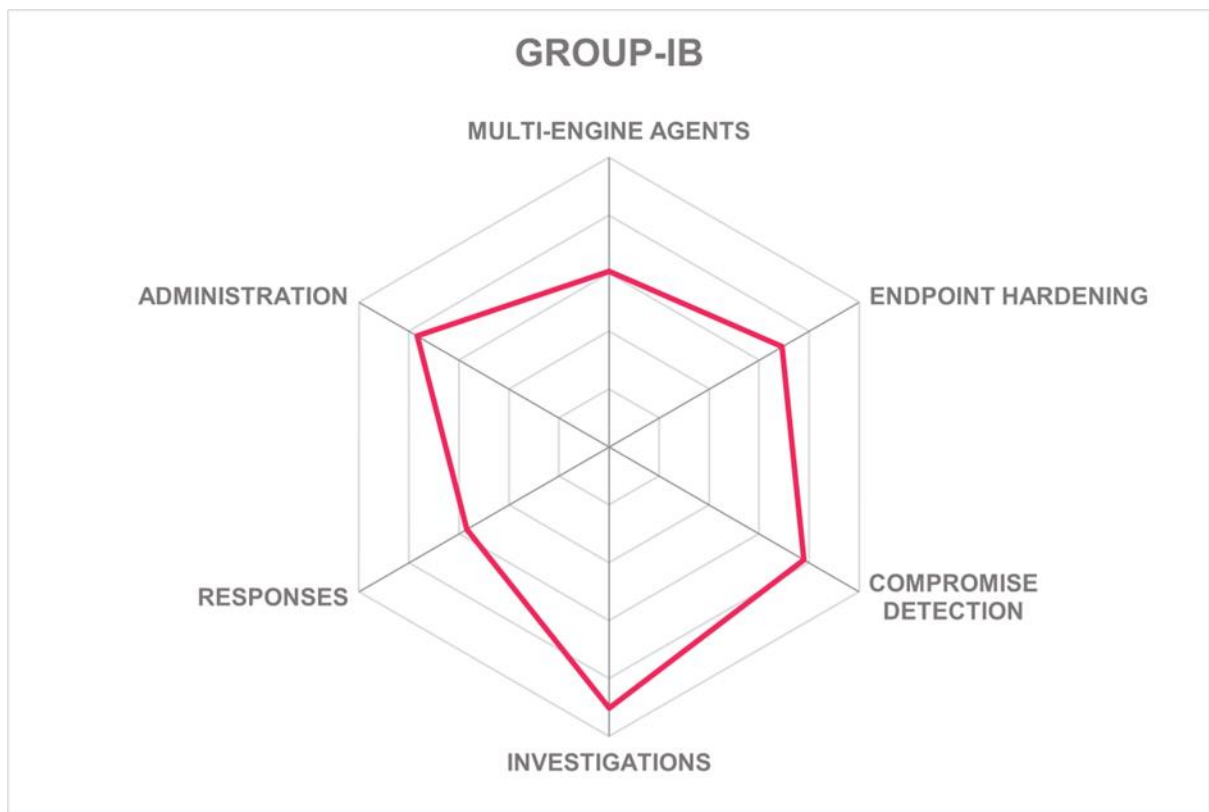
Table 3: Group-IB's rating

Strengths

- Daily ML-enhanced detection model updates
- Wide set of own models in use and continuous additions to models for new threats
- Granular application controls
- Agents for most common operating systems
- Setup and incident handling support are provided
- Good experience in threat hunting and ability for providing additional services

Challenges

- Has not participated in independent tests
- No agents for mobile devices
- Short default data retention period for cloud-hosted data
- No connectors for ITSM or third-party CTI
- Lacks an endpoint firewall



IBM – QRadar EDR and MaaS360

IBM, founded in 1911, is a large, publicly traded, global technology and consulting company headquartered in New York. IBM offers a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and information security. IBM Security has solutions for endpoint, network, identity management, and fraud prevention. The QRadar EDR and MaaS360 product consoles can be run on-premises on Linux, Windows, or virtual appliances; in all major IaaS; and they host it as SaaS. IBM offers two pricing models: predictable enterprise pricing (based on the size of the customer environment) and usage-based pricing (combination of metrics about users, managed endpoints, appliances, etc.).

IBM Security's enterprise console can be hosted both on-premises and in the cloud. Supported operating systems for hosting include CentOS, Debian, RHEL, SUSE, Ubuntu, and Windows. The console can also be run from a virtual appliance. Their SaaS is hosted in data centers across five continents. IBM Security supports only YARA formats for third-party CTI. Connectors are available for many third-party sandboxes and CTI services. The solution provides connectors for many SIEM and SOAR platforms. Supported methods for console authentication include SMS OTP, mobile push notifications, many authenticator apps and most major hardware token authenticators. Supported API types are SOAP, REST, JSON-RPC, XML-RPC, and webhooks, with REST API authentication methods including JWT, OAuth2, SAML, and key exchange. Communication between agents and the console utilizes TLS 1.3. No root account is required on endpoints for agent operation.

IBM has agents for Windows 7+, Windows Server 2008+, most common Linux distributions, macOS 13+, Android 7+, and iOS 5+. It scans content in browsers prior to downloading or execution. The scanning techniques employed include signature-based detection, static file and code analysis, and runtime behavioral analysis. It can detect and prevent various malware attacks such as ransomware, RATs, backdoors, trojans, botnets, file-less malware, macro malware, and spyware. Suspicious files are automatically quarantined, and the solution operates autonomously without requiring constant internet connectivity, although internet access is necessary for updating signatures. IBM Security QRadar Suite utilizes both supervised and unsupervised ML algorithms for detection, which are present in the agent itself. Basic endpoint firewall features are available. Application controls support audit/monitoring, allowlisting, and denylisting, although the implementation is somewhat rudimentary. System file integrity monitoring is not offered.

IBM Security QRadar Suite's EDR capabilities include detection of various post-infection attack activities such as command and control traffic, botnet activity, port scans, reconnaissance, lateral movement, and disabling security controls. There are several important kinds of TTPs that it does not look for, however. The solution automatically assigns priority levels to events, which can be configured by customer admins, and employs multiple methods to reduce false positives, such as an AI assistant that learns from the analysts' feedback. The analyst interface features a drop-down list query builder, and drill-down functionality from dashboards into investigations and threat hunts. The interface also includes a global map, automatic insertion, and update of context-specific threat intelligence

in open cases, annotation, and manual alerting capabilities. Automated incident analysis is supported, including correlation of relevant events and assembly of incident data into cases for analysts, with capabilities such as one-click node isolation and auto collection of forensic data from the endpoint. Custom IoC creation for threat hunts is not supported. The solution does not support live memory analysis or remote inspection of disk structures such as the MFT, and it lacks recording features for forensic examinations.

IBM Security QRadar Suite does not use the playbook model for automated responses and alerting is limited to email. The response actions available include terminating processes, isolating hosts to communicate only with the enterprise console, quarantining files, rolling back registry changes, preventing user data encryption, and collecting and preserving forensic information. A few other common response actions, such as terminating network connections, preventing registry changes, removal of malicious registry changes, preventing the termination of security processes, and preventing deletion of the volume shadow copy are not present. The solution generates root cause analyses for incidents with confidence levels, including correlation of relevant events and impact scoring, but does not attribute incidents to specific threat actors.

IBM has not participated in AV-Comparatives testing, but did participate in MITRE Engenuity 2023. IBM is ISO 27001 and SSAE SOC 2 Type 2 certified. Setup support is included, but incident handling requires a separate IBM X-Force Response Services contract. Although this solution set lacks several key sets of functionalities, it could be of interest to organizations with other IBM Security solutions.

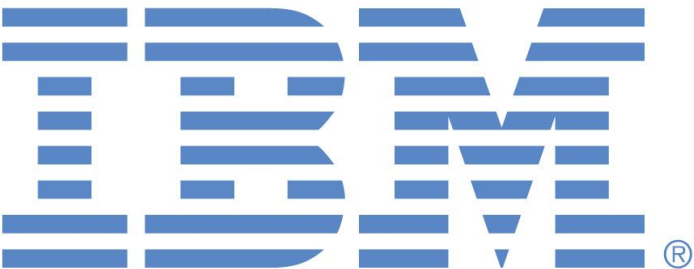
Security	Positive	
Functionality	Neutral	
Deployment	Positive	
Interoperability	Neutral	
Usability	Positive	

Table 3: IBM's rating

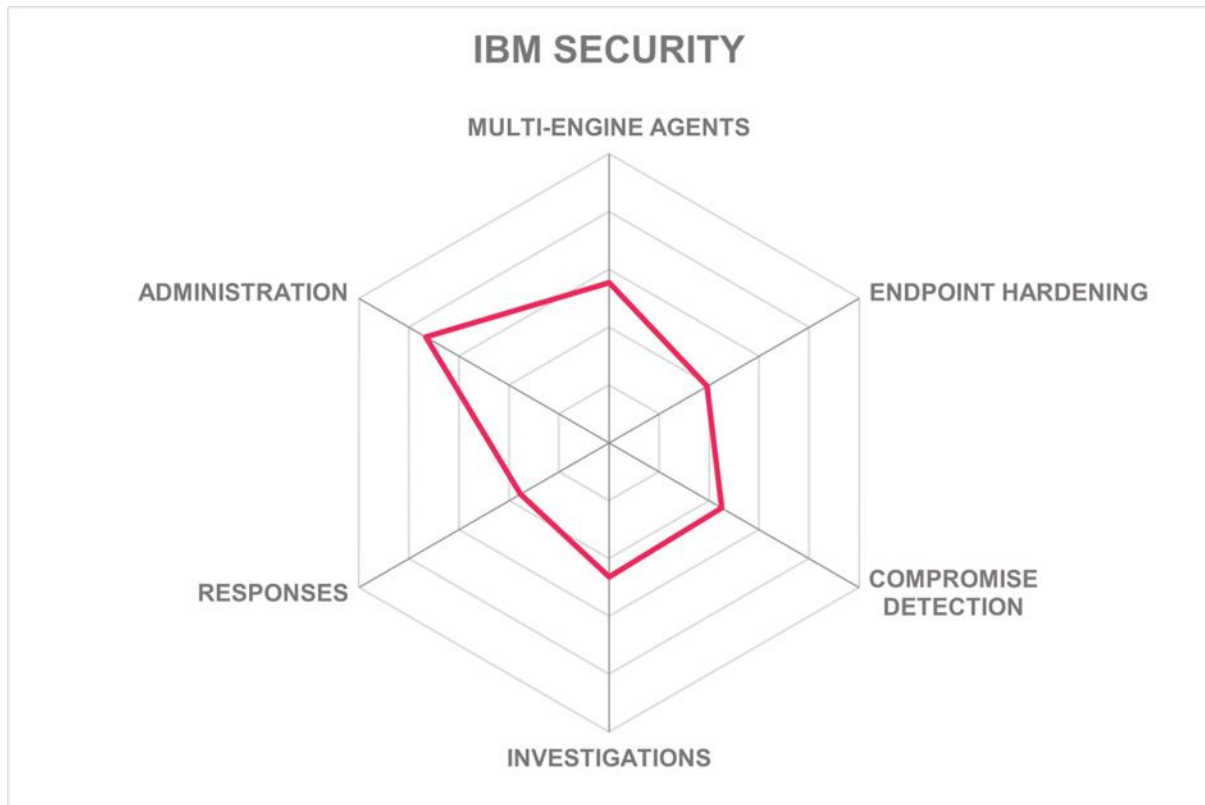
Strengths

- Excellent support for languages
- Wide range of strong authentication methods to the console are present
- Many integrations for SIEM, SOAR, and ITSM systems

Challenges

- Malware scanning engine does not employ the full range of techniques
- Does not do URL filtering or support allow/deny lists
- Limited threat hunting features; does not support regular expression searches
- Missing some basic response capabilities

- No playbooks



Microsoft – Defender for Endpoint

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, becoming Defender for Endpoint. The console is hosted by Microsoft in Azure. Licensing is per user, with multiple tiers of service.

Defender agents are available for Windows 8-11, Windows Server 2012+, all major Linux types, macOS, Android, and iOS. In-browser content scanning is most effective in Microsoft Edge, although Chrome, Mozilla, and Safari are now covered. If running another EPP tool on Linux or Windows, Microsoft recommends switching Defender Antivirus to passive mode. The EDR components can function side-by-side with other EDR tools. Optimal detections require internet connectivity to their sandbox. Defender uses a full array of detection techniques, including signatures, static file and memory analysis, and micro-virtualization. Starting with Windows 10, Exploit Prevention includes Arbitrary Code Guard, Controlled Folders Access, and Attack Surface Reduction Rules, 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 (SmartScreen) which can prevent user bypasses. Windows Defender System Guard can be enabled to protect device firmware. 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 managed by the Windows kernel but only for that OS.

Microsoft Defender for Endpoint looks 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 regular expressions (RegExp) searches are permitted for investigations and threat hunting. Advanced threat hunting and investigations leverage Kusto Query Language. Remote disk/memory analysis and activity recording/playback are possible within the analyst interface. Data exfiltration prevention requires Microsoft Purview DLP, which is sold separately.

Email, SMS, Slack, Microsoft Teams, 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 (available through separately licensed Intune). Playbooks run from Microsoft Sentinel and are somewhat limited, but they do cover most remediation use cases. Playbooks can be customized using the Logic App, which may incur additional charges. User Contain is a newer feature that can prevent even admin users from executing malware, including ransomware.

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 or Entra can be used for granular authorization.

As a leading cloud hosting provider, Microsoft is ISO 27001/27018 and SOC 2 Type 2 certified. The Microsoft Azure hosting environment is a CSA Trusted Cloud Provider. Microsoft was able to detect all 143 techniques used in the MITRE Engenuity 2023 simulated attack. They regularly participate in AV-Comparatives tests and have collected several awards recently, including the Real-World Test and Performance tests. Microsoft offers incident response services through as needed and active retainer arrangements. 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	Strong Positive
-----------------	-----------------

Functionality	Strong Positive
----------------------	-----------------

Deployment	Strong Positive
-------------------	-----------------

Interoperability	Positive
-------------------------	----------

Usability	Strong Positive
------------------	-----------------



Microsoft

Table 3: Microsoft's rating

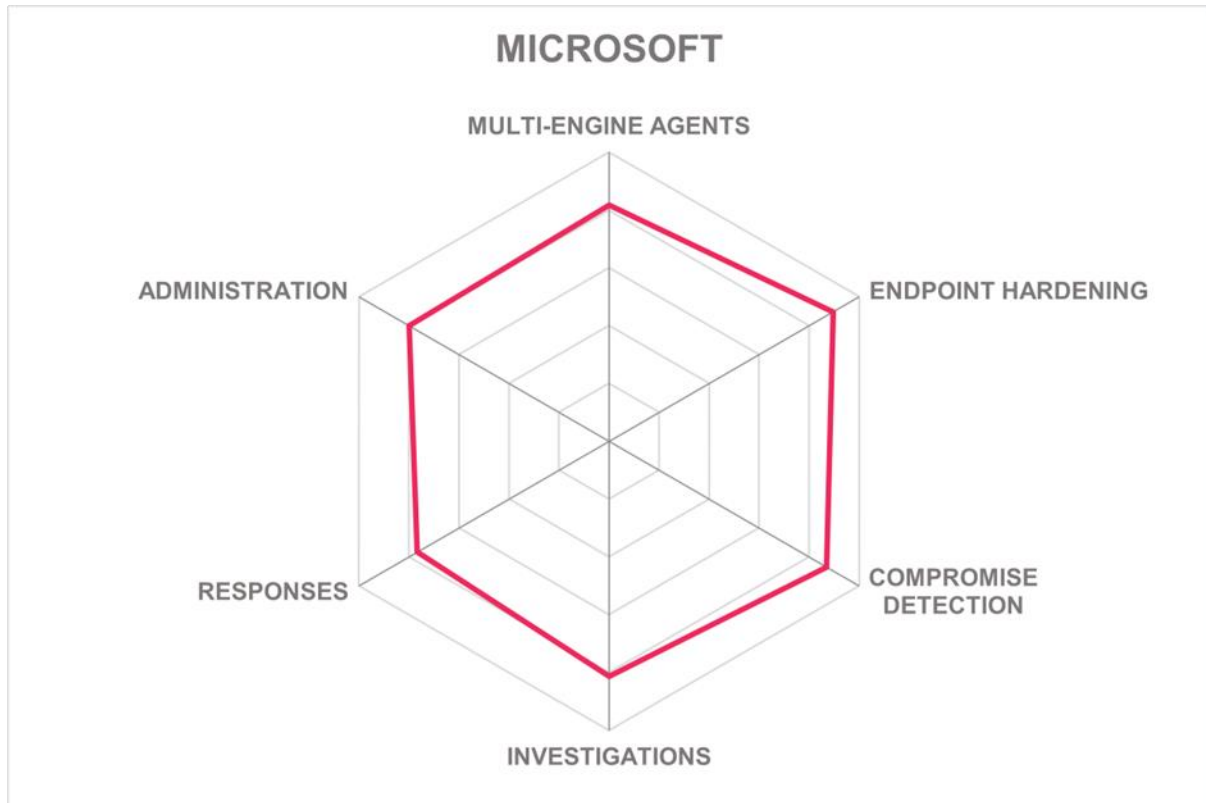
Strengths

- Regular participant and award recipient in independent effectiveness tests
- 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
- Most common response actions supported for Windows machines
- Many relevant security certifications

Challenges

- System file integrity monitoring is not available for non-Windows OSes; response actions are limited for Mac and Linux
- In-browser scanning is most effective in Microsoft Edge, not available for Safari
- Advanced threat hunting requires knowledge of Kusto Query Language
- Data exfiltration prevention requires Microsoft Purview DLP (add-on)
- Playbook customization requires Logic App (add-on)
- Blocking certain file types from download and full node rollback requires Intune
- Support for pre-Windows 10 versions not available

Leader in



SentinelOne – Singularity XDR Platform

SentinelOne was founded in 2013 and is headquartered in Mountain View, CA. SentinelOne had their IPO in 2021. Their products and services are focused on endpoint and cloud security and advanced SIEM and XDR capabilities powered by full-stack data ingestion and AI-enhanced analytics. SentinelOne is active globally, but most customers are in North America. Customers can run the console on-premises via virtual appliances, in IaaS, and SentinelOne hosts it as SaaS in multi-tenant / multi-site architecture in their own data centers and public IaaS across four continents. SentinelOne's MDR, Digital Forensics, and Incident Response (IR) services utilize this platform, and they have MSSP partners who use it as well. Subscription costs are calculated per endpoint and per workload node for cloud.

SentinelOne has agents for Windows XP to Windows 11, Windows Server 2003 to Server 2022, macOS, 15 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 leverages most malware identification methods except sandboxing and micro-virtualization. SentinelOne uses advanced ML and DL detection models with that logic running 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, but customers can configure reputation sources if needed. Application control is available for all agents and Kubernetes workloads. System file integrity monitoring is on by default and can be extended to watch any file types via Storyline™ Active Response (STAR).

SentinelOne Storyline automatically monitors for all attack types, correlates events, and opens cases with relevant threat intel for analysts. A full attack storyline can be visualized immediately in alignment with MITRE ATT&CK, showing timelines and process tree views, but not map 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.

Customer admins are alerted in console, via email, Slack, and SNMP. 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 or the S1 query language (S1QL).

SentinelOne pulls in multiple CTI sources and can send code samples to external sandboxes for dynamic analysis if desired. STIX/TAXII, OpenIOC, and YARA formats are understood. CEF, REST APIs, and syslog enable interoperability with most SIEMs and SOAR platforms. Connectors for ServiceNow Incident Response and several other third-party

services are available on the marketplace. RBAC is definable within the console. Authy, Duo, Google, Microsoft Authenticator apps are accepted for console authentication, and SAML is supported for federation.

SentinelOne is SOC 2 Type 2 certified and is US FedRAMP authorized (moderate). US FedRAMP GovCloud High certification is in work. SentinelOne has regularly participated in SE Labs and VB100 labs testing. They take part in MITRE Engenuity evaluations. SentinelOne offers advanced incident response services for additional charges. Though URL filtering is available for iOS, Android, and ChromeOS, slight improvements to URL filtering / application controls for other OSes would be helpful. 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.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 3: SentinelOne's rating

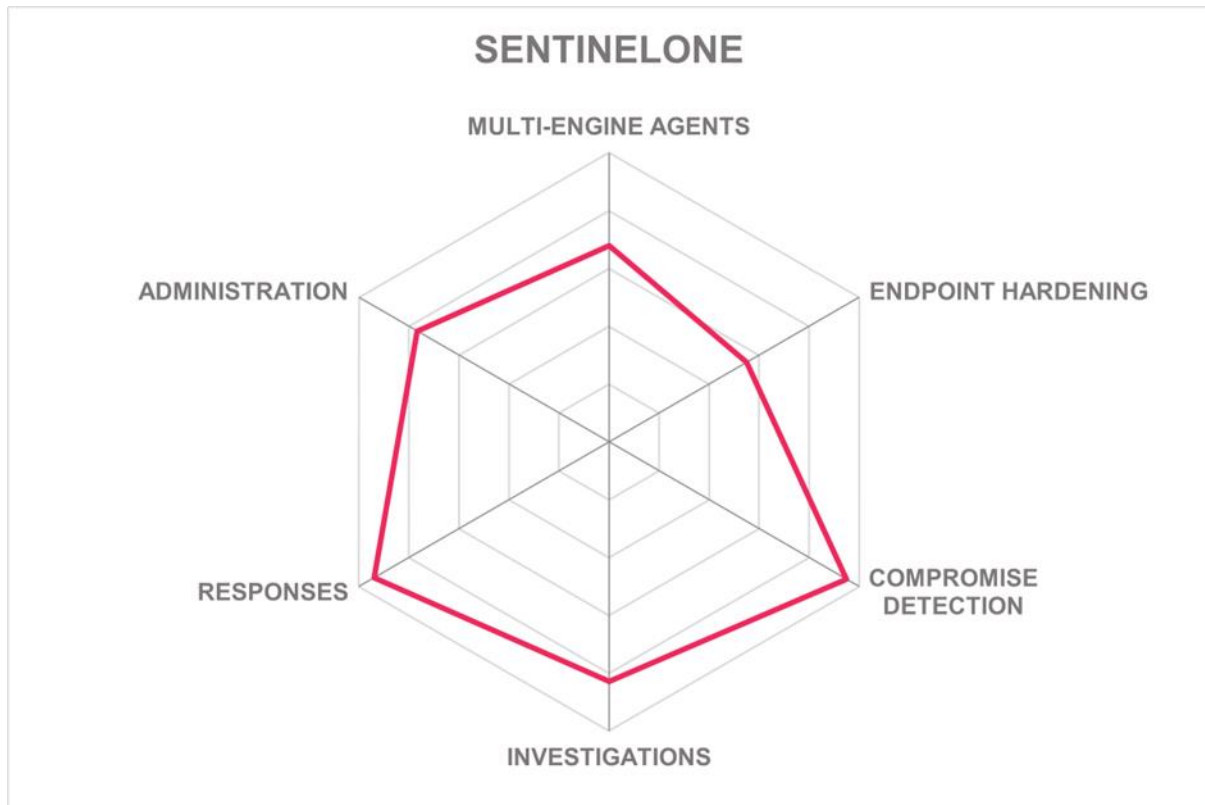
Strengths

- Agents for a comprehensive list of operating systems, including out-of-support Windows versions
- Autonomous agents effectively protect offline nodes
- Excellent analyst interface makes investigations and incident response easier
- Automated, proactive threat hunting via Singularity STAR
- Ships with many playbooks, and customers can create their own
- Singularity is part of their full IR platform
- SOC 2 Type 2 and FedRAMP-Moderate certifications, with FedRAMP-High in progress

Challenges

- URL filtering by allow/deny list only, no reputation service provided
- Playbook editing could be easier
- App control features should be more granular

Leader in



Sophos – Intercept X Advanced

Sophos was founded in 1985 in the UK. The company was acquired by Thoma Bravo in 2020. Sophos is a pure play cybersecurity solution, with a strong focus on the endpoint with their Intercept X Advanced product. Sophos also offers solutions for encryption, network security, Zero Trust Network Access, cloud workload protection and security posture management, firewalls, and email and web security gateways. Sophos hosts the management console as SaaS across five continents. They operate globally, but more than half of their customers are in the EMEA region. Sophos offers fully managed detection and response services. Per-user with multiple devices or per-device licensing options are available.

Sophos has Intercept X agents for Windows 7+, macOS 13+, all popular Linux variants, Android 7+, and iOS 16+. Agents can scan content in all major browsers prior to downloading. Sophos provides a deployment option such that it can be installed alongside other vendors' endpoint security software if customers choose to run it that way. 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 and DL detection models in the agents so as not to have their effectiveness constrained by internet connectivity. URL filtering can be applied by user/group policy and content categories, and specific file types can be blocked from download. Basic endpoint firewall capabilities are present in the EPDR product but are more feature-rich in the XDR product. Application controls are comparatively granular but do not permit browser extension exclusions. System file integrity monitoring is built-in and can be extended as needed for other files and directories.

Sophos' dashboard and analyst interface provides the standard features, including map and process views, 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. Many SQL style queries ship with the product, and more are added regularly. Intercept X 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 managed by Sophos' services. Root cause and attribution theories are generated for incidents.

STIX/TAXII and the YARA rule format are supported. Third-party sandboxes are not utilized since they have their own. They are an affiliate member of the Cyber Threat Alliance. REST APIs enable connections to any SIEM, most SOAR platforms, and multiple ITSM products. A limited number of MFA options are present, including Authy, Google, and Microsoft Authenticators. FIDO passkey acceptance is on the roadmap. SAML and OIDC are supported for federation.

Sophos has obtained ISO 27001 and SOC 2 Type 2 certification, as well as PCI-DSS and US HIPAA certification. Sophos took part in the 2023 MITRE Engenuity evaluation and was able to detect almost all the techniques in the simulated attack. Sophos also actively participates in endpoint protection tests including SE Labs and AV-Test and is also included in AV-Comparatives vendor evaluations. Initial setup services are included, and incident response can be added on. Enhancements to a few secondary EPP functions and MFA are needed. The analyst interface is their primary differentiator: its design allows knowledgeable sys admins to become more effective at forensic investigations and threat hunting. Sophos Intercept X is a feature-rich solution that should be on the shortlist for any organization considering upgrading their EPDR.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

SOPHOS

Table 3: Sophos's rating

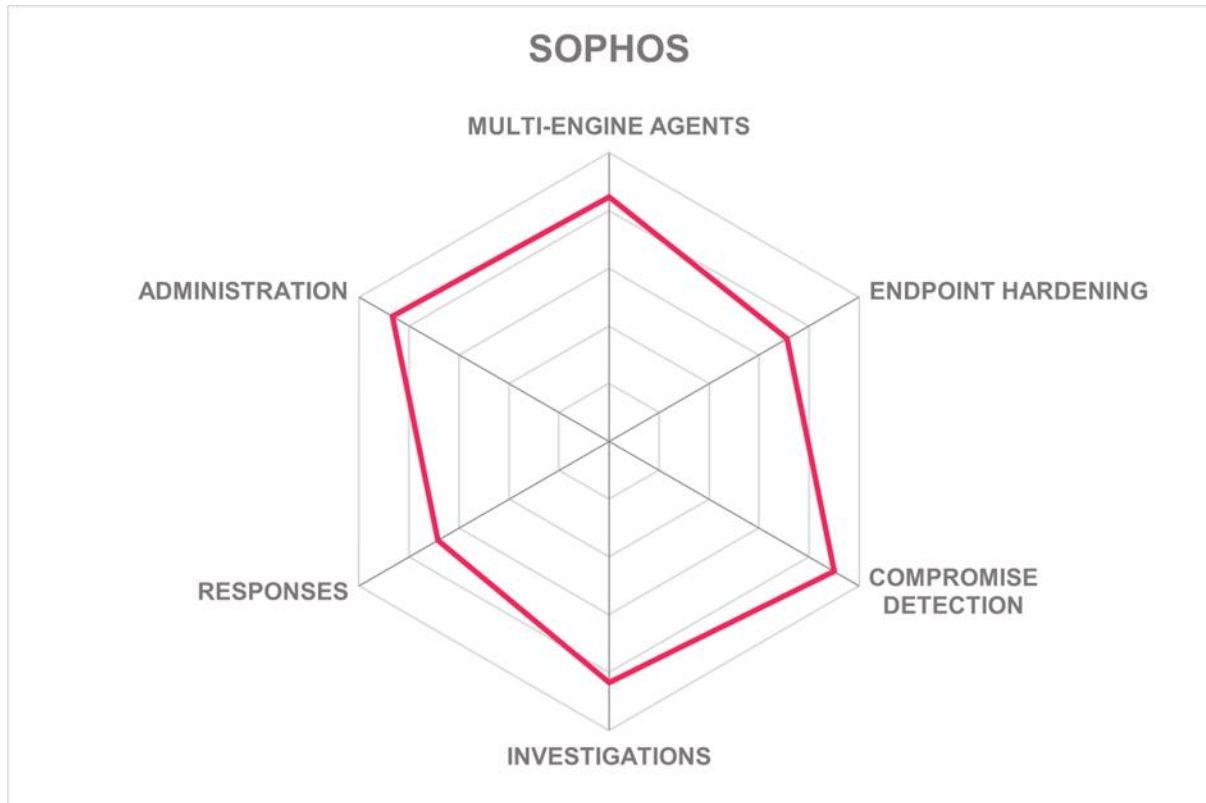
Strengths

- Per-user/multiple devices licensing available as well as standard per-endpoint options
- Cyber Threat Alliance affiliate member
- Advanced ML and DL detection methods utilized
- Innovative SQL-like query interface
- Broad range of responses available
- 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
- Does not block browser extensions
- Additional MFA options would be useful, and FIDO passkeys are on the roadmap

Leader in



Trellix – Endpoint Security

Trellix was established in January 2022 as a spin-off from the merger of McAfee Enterprise and FireEye. This strategic union combined the strengths and expertise of both progenitor companies to create a comprehensive cybersecurity platform vendor. Trellix focuses on delivering advanced threat detection, response, and resilience solutions. Major products in its portfolio beyond EPDR include NDR, XDR, email security, data security, and cloud security solutions. The enterprise console can be run on-premises on Windows or common Linux OSes, in customer-maintained IaaS, and Trellix hosts it as SaaS across multiple IaaS providers on four continents. EPDR services are priced in a subscription model based on numbers of endpoints.

Trellix's products support STIX/TAXII and OpenIOC formats. In addition to their own high-quality threat intel, their solutions can connect with multiple third-party CTI sources and other sandboxes. Dedicated connectors for multiple SIEM and SOAR solutions are available, and Trellix supports syslog and REST API integration with key exchange or OAuth2 authentication. There are no connectors for ITSM. OTP, FIDO U2F and 2.0 authenticators, and RSA SecurID and YubiKeys are accepted for console authentication. Role-based authorization is present, and custom roles can be created. Agent to console communications use TLS 1.3. Root accounts are not required on endpoints.

Agents are available for Windows 8+, Windows Server 2008R2+, macOS 10.14+, all major Linux flavors, and offers coverage on Android, iOS, and Chrome OS via OEM arrangements. Agents can scan in-browser content to prevent download and execution of malicious code and files. Trellix Endpoint Security has been tested with other security software solutions, and while there are no major incompatibilities, it may be necessary to configure the products in case of conflicts. Trellix incorporates multiple scanning engines which use most major techniques including signatures, static file analysis, behavioral analysis, memory analysis, sandboxing, and exploit prevention.

For ransomware prevention, Trellix looks for attempts to delete the Volume Shadow Copy and other characteristic behaviors. It automatically quarantines suspicious files. Optimal detection requires internet connectivity for sandboxing. The Trellix Web Control module can perform URL filtering to prevent users from downloading malicious content. Trellix DLP (sold separately) can also prevent the transfer of files in data exfiltration attempts. Trellix offers application controls that work in audit, allowlist, denylist, and user prompt modes. Trellix ePolicy Orchestrator (ePO) allows customer admins to create allow/deny lists with a wide array of attributes. It also provides a robust endpoint firewall with traffic filtering, intrusion prevention, DoS protection, and detailed logging. System file integrity monitoring is included and is managed via ePO.

The EDR components of the solution look for typical IoCs, and it can create IoCs based on observed behavior in customer environments. Trellix uses built-in threat intelligence and behavioral analysis algorithms to evaluate and prioritize events based on their severity. The analyst interface shows detection timeline and graph views, and contextual info is aligned with MITRE ATT&CK. Their solution uses AI-powered investigation guides to ask and answer questions from customers' forensic teams. Trellix shows recommended actions per

event, which can be launched automatically or from a single click in the interface. It can perform most of the expected response actions, such as terminating processes, isolating nodes, and blocking connections to bad IPs/URLs. Some advanced responses such as changes to downstream firewall policies to block IPs and URLs require additional configuration from security staff. Registry rollback is possible, but full node rollback is not. Live remote memory analysis can be performed. Examination of low-level structures like disk MFTs and firmware protection is not supported. Trellix provides root cause analysis assistance and attacker attribution within the dashboard.

Trellix has obtained Business Security and Mac Security awards in AV-Comparatives tests for the last 3 years. They also participated in MITRE Engenuity evaluations in 2023. Trellix's products and services are ISO 27001, SOC 2 Type 2, and US FedRAMP Moderate certified. US FedRAMP GovCloud High certification is in process. Trellix offers advanced incident analysis support for customers for additional cost. Support for mobile OSes would make the solution more appealing. Trellix is a popular EPDR choice for enterprises worldwide because of its feature set.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive



Table 3: Trellix's rating

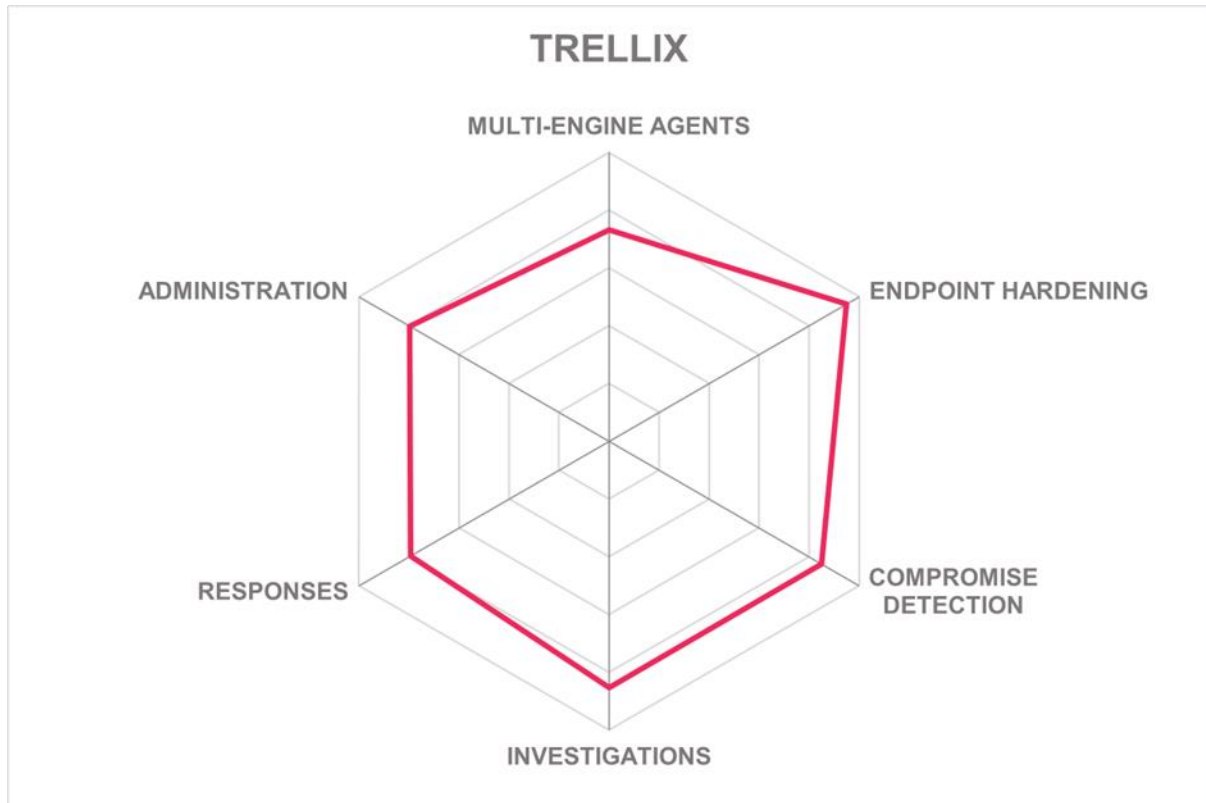
Strengths

- Consistently good results in independent tests of effectiveness
- Multiple MFA options for the enterprise console
- Advanced endpoint firewall, system file integrity monitoring, and app controls are built-in
- Can use external CTI sources and sandboxes if desired
- Many relevant security certifications, and US FedRAMP GovCloud High is in work

Challenges

- No agents for Android or iOS
- Optimal detection requires internet connectivity
- Some limitations in automated response capabilities
- More connectors for third-party security solutions would be useful
- No out-of-the-box integrations with ITSM

Leader in



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

Absolute Software

Absolute Software is not an EPDR vendor along the definition we are using for this Leadership Compass but provides additional functions that are complementary to EPDR solutions such as ransomware preparedness analysis, device health checks, and device recovery.

Why worth watching: Absolute Software's solution can support customers in providing additional layers of protection and supporting fast, remote recovery, thus strengthening the resilience of organizations against cyberattacks and other outages, such as after malfunctioning updates.

AhnLab

AhnLab Endpoint Plus extends the EPP platform by adding a range of additional capabilities, including EDR, Privacy Management, Security Assessment, and Sandboxing. AhnLab also has a focus on OT (Operational Technology) use cases.

Why worth watching: EPDR solution building on a proven anti-malware solution and adding a wide range of features plus broad support for various device types. Can also integrate with additional services such as the XDR solutions by AhnLab.

Acronis

Acronis launched in 2003. They are headquartered in Switzerland. They have offices in forty countries. They are a successful late-stage startup focused on selling to MSSPs. Their Cyber Protection Platform includes backup and recovery, asset discovery, endpoint security management, email security, cloud workload protection, data leakage prevention (DLP), vulnerability and patch management, secure remote access, and secure file sharing. Their endpoint security solution encompasses elements of EPP and EDR.

Why worth watching: Acronis has some leading-edge blockchain-based backup notarization. It uses a microservice-based architecture and is highly scalable. The inclusion of DLP with data discovery and classification add capabilities not found in other endpoint security solutions. KuppingerCole looks forward to doing a full evaluation of Acronis's products in the next edition of this report.

Bitdefender

Bitdefender was founded in 2001 and is headquartered in Bucharest, Romania. GravityZone is the name of their solution suite, which encompasses EPDR as well as XDR, CSPM, container security, patch management, email security, and whole disk encryption. Their endpoint security solutions perform well in independent tests.

Why worth watching: With a good reputation in cybersecurity, Bitdefender's malware scanning engines are OEM'd into many other products.

BlackBerry

BlackBerry Cybersecurity includes the CylanceENDPOINT as an EPDR solution. This product came in via the Cylance acquisition. It is part of the broader cybersecurity offering of BlackBerry and integrates with their other solutions. BlackBerry promises an exceptionally strong protection rate and provides GenAI backed bots supporting the users in the configuration and analysis.

Why worth watching: Proven Endpoint Security solution and part of a broader portfolio of cybersecurity solutions as well as Endpoint Management technology.

Checkpoint

Check Point's Endpoint Security, Harmony, offers anti-malware, firewall, and threat prevention technologies in a single solution. It leverages advanced threat intelligence and behavior analysis to detect, and block known and zero-day threats across devices. Additionally, the product includes encryption, VPN, and secure remote access features to safeguard data in transit and at rest, ensuring robust security for both on-premises and remote users.

Why worth watching: Check Point Harmony integrates Zero Trust Network Access (ZTNA), and industry-leading threat intelligence enables organizations to safeguard against advanced threats while providing secure, frictionless access for remote and hybrid workers.

Coro

Coro specializes in cybersecurity solutions for SMEs, including endpoint protection solutions covering EDR, EPP, and other capabilities. The solutions can be deployed by the customer or backed by the MDR team of Coro. Coro provides a solid set of capabilities with the promise of simple deployment and operations.

Why worth watching: One of the few vendors in the market that specializes in lean solutions for the SME market segment, but also complements these by MDR services.

Cybereason

Cybereason is a Boston-based, late-stage, high-valuation startup that was founded in 2012. It is focused on endpoint security and has been an early proponent for eXtended Detection &

Response (XDR). In addition to full EPDR and XDR functionality, Cybereason offers threat intelligence, MDR, and incident response services.

Why worth watching: Cybereason has agents for almost every operating system, including older, out-of-support Windows versions. Their product uses most major malware detection techniques, including advanced ML algorithms. Their solution uses the MalOp concept for threat hunting and provides a good interface for conducting investigations.

Deep Instinct

Deep Instinct provides an endpoint security solution that focuses on the prevention aspect, to ensure that no ransomware attacks succeed. They claim to have an advantage due to utilizing a deep learning framework for cybersecurity that increases their ability in stopping ransomware and other malware.

Why worth watching: Innovative vendor with a comprehensive EPP offering that is an alternative to other vendors' solutions.

G Data

G Data is a German provider of anti-malware and endpoint security solutions. Their endpoint protection business solution provides endpoint security, mobile device management, and firewall capabilities. The solution is considered as an EPP solution, not a full and comprehensive EPDR solution.

Why worth watching: Proven anti-malware and EPP solution that is specifically interesting for SMEs that are looking for an entry-level solution to protect endpoints.

GoSecure

GoSecure focuses primarily on MDR and XDR solutions, covering a broad set of capabilities. They also provide what they call NGAV (Next Generation Anti-Virus) that combines traditional signature-based analytics with advanced approaches for identifying malware. GoSecure also delivers a Secure Email Gateway (SEG).

Why worth watching: GoSecure delivers endpoint security capabilities in the context of their managed services and XDR capabilities, thus being able to provide enterprise-grade solutions covering a wide range of use cases.

Heimdal Security

Heimdal Security is a vendor headquartered in Denmark and providing a comprehensive suite of security solutions, specifically targeted at SMEs and mid-market companies. They also deliver EPDR capabilities as part of their portfolio, which integrates with other security capabilities that are provided by the Heimdal platform.

Why worth watching: European vendor with a comprehensive portfolio of cybersecurity solutions including EPDR, ransomware encryption protection, and other endpoint-focused security capabilities.

Malwarebytes

Malwarebytes is a provider of endpoint security solutions including EPP and EDR for both consumers and enterprises. The solution also includes support for incident response management and specific protection solutions for servers. Vulnerability and patch management is also supported.

Why worth watching: Established provider of endpoint security solutions with a broad product portfolio for both enterprise and consumers. Focused on SMEs.

OpenText

In 2019, OpenText acquired Carbonite and Webroot to add to its portfolio of security products. Webroot covers Windows 7+, Windows Servers 2003+, macOS 11+, VM platforms, and all major browsers. Webroot Business Endpoint Protection has integrations with forty other security tools.

Why worth watching: With these products, OpenText focuses on SMBs and MSSPs. OpenText claims a small footprint with low performance impact. It is a cloud-hosted and managed solution.

ThreatLocker

ThreatLocker is a late-stage startup based in Orlando, FL. The company was founded in 2017. They are most active in North America but also have operations in the EU and APAC regions. ThreatLocker has agents for Windows 7-11, Windows Server 2008+, macOS 13+, and some Linux distros. It has basic anti-malware capabilities but very granular application control features, which it uses to protect customers against malicious app behavior.

Why worth watching: ThreatLocker's Ringfencing™ technology restricts app interactions and limiting their execution scope, effectively acting as a containment mechanism. This additional layer of security ensures that applications operate within predefined boundaries, preventing them from performing unauthorized or potentially harmful actions.

Trend Micro

Trend Micro is a well-established player in the endpoint security market, having been founded in 1988 in Tokyo. Beyond EPDR, 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.

WithSecure

WithSecure is a Finish provider of cybersecurity solutions and part of former F-Secure. They provide a broad portfolio of cybersecurity solutions including a platform delivering EPP and EDR capabilities. The platform is integrated with the broader portfolio of WithSecure, spanning areas such as XDR as well.

Why worth watching: European provider of cybersecurity including EPDR with long experience in the market. Delivers EPDR as part of a comprehensive cybersecurity platform.

Xcitium

Xcitium provides a comprehensive EPDR platform named Enterprise Platform for advanced endpoint protection. They claim to have achieved a rate of zero infections across eighty-five million endpoints. They also claim to have a low footprint in terms of both of required memory and CPU consumptions as well as the support of outdated operating systems such as Microsoft Windows XP.

Why worth watching: Strong platform with a significant number of protected endpoints. Low footprint and support for legacy systems makes them a candidate for protecting OT environments.

Related Research

[Leadership Compass: Managed Detection and Response](#)

[Leadership Compass: EPDR 2022](#)

[Leadership Compass: Unified Endpoint Management](#)

[Leadership Compass: SASE Integration Suites](#)

[Leadership Brief: The Differences Between EPP and EDR](#)

[Leadership Brief: Do I Need Endpoint Detection & Response?](#)

Copyright

©2024 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 in-depth analysis, positions presented in this document will be subject to refinement or even major changes. KuppingerCole refuses 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 does 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 making 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.