KuppingerCole Report

MARKET COMPASS

By John Tolbert
July 28, 2020

Endpoint Protection, Detection, and Response

The KuppingerCole Market Compass provides an overview of the products offerings in Endpoint Protection, Detection and Response. The Endpoint Security space continues to see much innovation and some consolidation. The formerly separate products Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) are increasingly coming together in the marketplace.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Management Summary 4

2 Market Segment 7

2.1 Market Description 7

2.2 Market Direction 8

2.3 Capabilities 11

2.3.1 Common functionality 11

2.3.2 EPP Functionality 11

2.3.3 EDR Functionality 13

3 Vendors and Products 17

3.1 Vendors Covered 17

3.2 Featured Vendors 17

3.2.1 Featured for EPP capabilities: F-Secure 18

3.2.2 Featured for EPDR capabilities: Kaspersky 18

3.2.3 Featured for EPP innovation: Bitdefender 19

3.2.4 Featured for EPDR innovation: Sentinel One 20

3.2.5 Featured for EDR innovation: Sophos 21

3.2.6 Featured for XDR innovation: Palo Alto Networks 22

3.2.7 Featured for EPDR universal coverage: ESET 23

3.2.8 Featured for Threat Intelligence integration: Symantec 24

3.2.9 Featured for Threat Intelligence integration: McAfee 25

3.3 Vendors to Watch 26

4 Ratings at a Glance 29

5 Product/Service Details 33

5.1 Bitdefender 35

5.2 BlackBerry 38

5.3 Cisco 41

5.4 Cybereason 44

5.5 ESET 47

5.6 F-Secure 50
5.7 FireEye 53
5.8 Fortinet 56
5.9 Kaspersky 59
5.10 Malwarebytes 63
5.11 McAfee 66
5.12 Microsoft 69
5.13 Palo Alto Networks 72
5.14 SentinelOne 75
5.15 Sophos 78
5.16 Symantec 81
5.17 VMware 84
6 Related Research 87
Methodology 88
Content of Figures 91
Copyright 92

1 Management Summary

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

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.

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

Worms spread across unsecured networks, relying upon unpatched, compromised applications and unprotected ports.

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

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

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

Ransomware attacks are still popular and evolving. Ransomware is a form of malware that either locks users' screens or now more commonly encrypts users' data, demanding that ransom be paid for the return of control or for decryption keys. The newest forms of malware can be deployed similarly to an APT campaign, with staging of ransomware on various machines throughout an enterprise and exfiltration of data prior to ransomware detonation. Needless to say, paying the ransom only emboldens the perpetrators and perpetuates the ransomware problem. Over the last couple of years, attackers have used ransomware techniques and payloads for purely destructive purposes too – rather than asking for ransom, these destructive "wiper" malware types simply delete or zero out data.

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

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

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

Most ransomware attacks arrive as 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 come from drive-by downloads and malvertising.

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

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

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

Additionally, as part of the detection process, EDR also performs evaluation of threat intelligence information, event correlation, interactive querying, live memory analysis, and activity recording and playback. EDR helps to automatically uncover attacks and enables security teams to understand what is happening from start to finish by consolidating all relevant information into a single view.

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

Like EPP, EDR solutions can be tightly integrated with other tools in vendor suites and can interoperate with security analytics tools.

A number of different, independent testing regimes exist that vendors can participate in to demonstrate the effectiveness of their products. **AV-Comparatives, AV-Test, ICSALabs**, and **NSSLabs** run tests focusing on malware detection and prevention. They also run in-depth tests to simulate the kinds of scenarios business users encounter. KuppingerCole reviewed test results as published by these organizations for vendors examined below.

The **MITRE ATT&CK Framework** is a comprehensive look at all the various TTPs that malicious actors use to compromise systems for the purpose of data exfiltration. Many security vendors contribute to MITRE ATT&CK and many of their tools map detections to the various steps and techniques to facilitate analysis. MITRE has performed two full test scenarios simulating and attack by APT3 and APT29. These tests demonstrate the abilities of vendors' EDR products (and services from MSSPs) to detect and alert on malicious behavior. Many vendors participated in these tests, particularly the most recent one based on APT29. The **results of these simulated attacks** and the effectiveness of vendor responses are considered and noted in this Market Compass. Such tests are point-in-time measurements, not absolute determinants of efficacy and value in customer environments. It is also possible and likely that individual deficiencies that were observed in vendor products may have been remedied by now.

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

2 Market Segment

This Market Compass covers solutions that can detect and prevent malware from executing on endpoints, have built-in firewalls, perform URL filtering, application whitelisting/blacklisting, and the full gamut of typical EDR functions such as monitoring for post-execution of and compromise by malware, IoC detection, file analysis, registry analysis, alerting/reporting, attribution theory creation, and threat hunting.

2.1 Market Description

The Endpoint Security product market has been well-established for 30+ years. Anti-virus vendors arrived on the scene to deal with the earliest viruses and worms. Some of the original vendors in that space have survived and thrived from the beginning, although their products have changed significantly over the decades. Along the way, many start-ups have emerged to deliver innovative solutions, having specialized products with cutting edge technology to deter the ever-increasing and ever-changing threats in the landscape. The larger vendors have acquired some of these start-ups and incorporated their technologies into their security stacks. This is especially the case with EDR products. Many EDR solutions started out as standalone agents but have been assimilated into endpoint security suites.

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

- Detection and prevention of malware execution and subsequent compromise
- Secondary endpoint protection capabilities such as
    - Endpoint firewall
    - URL filtering
    - Application whitelisting/blacklisting
- Detection of IoCs such as
    - registry and system file changes
    - unusual use of network ports by applications
    - contact with known bad IPs and URLs
    - unusual process injections
    - modification of module load points
- Integration of threat intelligence

- Alerting and reporting mechanisms
- Query interface for threat hunting
- Console for admins, analysts, and threat hunters
- Automatic response functions
    - Process termination
    - Update detection rules based on findings
    - Delete or move files
    - Rollback to known good states

EPP and EDR solutions are not generally easy to operate, and usually require a dedicated team of (numbers depend on organization size and complexity) to make the best use of the capabilities.

2.2 Market Direction

The Endpoint Security market is rapidly changing in a few ways. The use of Machine Learning (ML) algorithms for automated malware analysis was at one time novel. Ten or more years ago, using ML for endpoint security product enhancement was a significant differentiator. However, given the exponential proliferation of malware variants, old-style signature-based anti-virus is now less than 70% effective on new malware, which makes using ML for malware identification a requirement, rather than a nice-to-have.

Secondly, as mentioned above, there has been ongoing consolidation in the security market, particularly with vendors pairing EPP and EDR products in their portfolios. The motivation for this is two-fold: endpoint security vendors seek to become the monolithic security vendor of choice for their customers, and customers want to minimize the number of agents running on endpoints as well as vendors and maintenance contracts to manage. KuppingerCole predicts that such consolidation will continue, as new products better suited at certain aspects of endpoint protection emerge, and security suite vendors desire to bundle essential functions into their client software. Moreover, we expect to see new start-ups entering the endpoint security market, as the field is still ripe for innovation to thwart constantly changing threats.

Though endpoint security by definition necessitates installing and maintaining software on endpoints, most vendors offer cloud-hosted management consoles. This can actually be a significant benefit for customers, due to the complexity of the console software, the removal of the administrative burden for consoles, and improved ability to get updates. This trend will likely continue as well.

More vendors are offering managed services for endpoint security products. These services are positioned especially for running the EDR portions of their products (Managed Detection & Response, or MDR). EDR tools are in general difficult to run. The expertise and staffing needed to extract maximum value from forensics and threat hunting activities can be out of reach for SMBs and some larger enterprises. MDR service providers can operate EDR tools, including routine analysis and threat hunting, on behalf of many clients and do it at a scale that is more affordable than each customer doing it for themselves.

Many organizations are adding Network Detection & Response (NDR) capabilities to their security portfolios. NDR tools are generally deployed as appliances or virtual appliances to monitor traffic on networks and in cloud environments to look for signs of nefarious activities. NDR can be an effective solution for environments which cannot support EPDR agents. Some vendors in the EPDR space also offer NDR solutions. We see a trend toward “XDR”, or the union of EDR and NDR technologies. Such an approach will make it easier and more cost effective for organizations to implement comprehensive security monitoring capabilities.

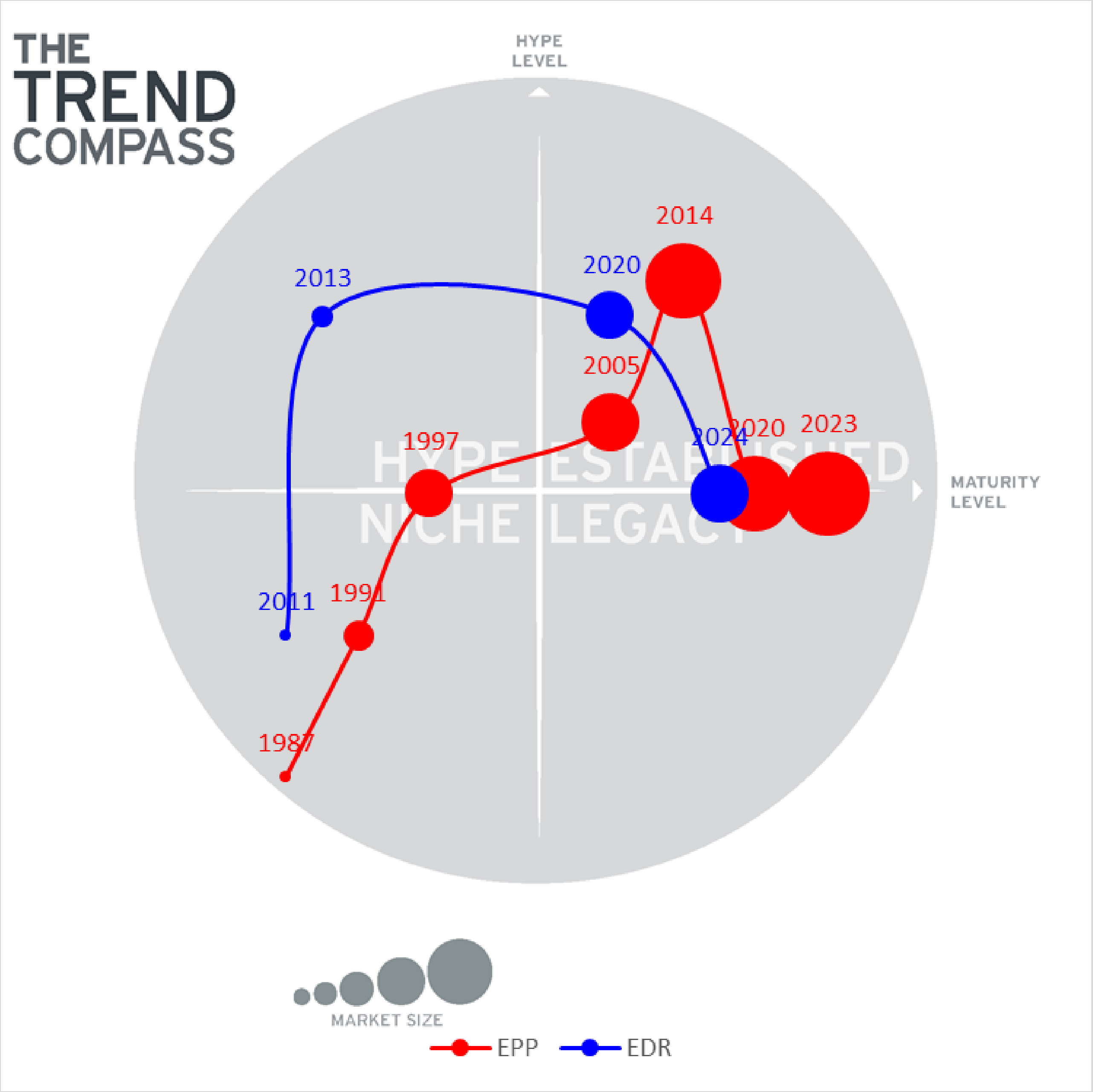


Figure 1: Trend Compass

The Trend Compass tracks the development of EPP and EDR independently. EPP began as antivirus and grew steadily in importance and effectiveness from the late 1980s through the early 2000s. Though the advent and usage of ML techniques may have led to some additional marketing buzz around EPP in the early 2010s, anti-malware technologies have never been over-hyped. Today EPP is widespread and mature, and that's a good thing, as attacks involving malware are frequent and still increasing.

EDR products came onto the scene in the early 2010s in response to sophisticated APT attacks. EDR did go through a hype phase, but the functionality was and is needed by an increasing number of organizations. EDR products are mature and will continue to be important tools in cybersecurity architectures for the foreseeable future. Moreover, EPP and EDR are fusing into EPDR, and this trend will continue for reasons detailed above.

2.3 Capabilities

The Endpoint Security market is mature, but there has been a lot of churn: emergence of new technologies and new approaches embodied by new vendors, acquisition of these capabilities, and assimilation into security stacks. Many of the features examined below may have lineage initially outside of what we used to think of anti-virus products, but they have now become common in the solutions in the endpoint security market.

2.3.1 Common functionality

The common functionality that should be provided by all solutions includes:

Use case	Description	Relevance
Autonomous agent operation	Though many endpoint protection, detection and response solutions utilize cloud-based deployment, update, and even sandboxing functionality, organizations deploying these solutions need to ensure proper, autonomous operation of agents when disconnected from corporate networks and the Internet. The effectiveness of agent’s ability to detect and prevent malware infection may vary widely between vendors depending on internet connectivity for detonation and analysis of suspect code samples.	Required
Strong authentication and access controls for administrators	Administrative access to enterprise EPDR consoles and dashboards must be secured. Best practices include support for strong or multi-factor authentication, federation, and role-based and delegated access controls.	Required

2.3.2 EPP Functionality

The Endpoint Protection feature list that will be rated in the following sections include:

Use case	Description	Relevance
Multiple detection engines: signature scanner, pre-execution heuristics, memory analysis, and sandboxing	Most endpoint security solutions contain more than one detection engine. **Signature scanning method**: researchers collect malware samples and create signatures based on the discovered malware types. Anti-virus scanners then perform pattern matching of known malware signatures against files. **Pre-execution heuristics**: code is intercepted prior to execution and agent attempts to predict what it will do. Vendors have compiled and analyzed the behavior of millions of malware types to extrapolate activity patterns that can be applied during heuristic scanning. If the scanning engine finds that the code in question seems malicious, the system is protected because the code is prevented from running in the first place. **Memory Analysis**: file-less malware infection techniques work by getting PowerShell developed code snippets into memory then piping them into an interpreter. Signature scanners will always miss file-less malware, as there is no file to scan. Thus, full endpoint protection requires the ability to analyze code in different process memory spaces and prevent them from being assembled and sent to command interpreters.**Sandboxing**: code is shunted into a special protected thread and memory space, the sandbox, to watch what it does during execution. If malicious behavior is detected, the detection engine can kill the processes and clear the memory space to prevent escape. In most cases, sandbox “detonation” takes place in the vendor’s cloud environment, meaning internet connectivity for endpoints is a requirement for the most effective protection.	Required

Use case	Description	Relevance
Crypto API library and filesystem monitoring	Agents monitor for suspicious calls to native cryptographic APIs and/or third-party libraries with large numbers of enumerated files or wildcards as arguments and stop execution of the calling process if encountered. For example, most ransomware variants perform large numbers of reads, copy-on-writes, file type changes, and file renaming in common locations. Others begin their infection by deleting the Windows Volume Shadow Copy. There are very few legitimate reasons why any program would ever delete this disk structure, so such an attempt can almost always be considered malicious and should be stopped prior to executing this kind of code.	Required
Exploit prevention	Agents proactively read-ahead in the instruction queue to look for attempts by code to employ known operating system and application exploits (CVEs) and shut down such processes before they execute; thereby preventing damage.	Required
Secondary EPP functions	Many endpoint security solutions include the ability to whitelist sanctioned applications and prevent execution of all non-essential applications; a device-level firewall to harden individual hosts by turning off listening on unnecessary ports; and the ability to block users and programs from accessing known bad URLs, domains, and IP addresses.	Recommended

2.3.3 EDR Functionality

The Endpoint Detection & Response features that will be considered include:

Use case	Description	Relevance
Near real-time evaluation of anomalous behavior	Some anomalies are innocuous and alerting on these false positives takes time away from security analysts that is better spent on other tasks. In recent years, many security tools have been enhanced with Machine Learning (ML) algorithms and techniques. ML-enhanced tools are generally trained on massive amounts of data from both normal and malicious activities to help their customers sift through telemetry from their implementations, thereby reducing false positives. Many tools also utilize unsupervised ML algorithms to recognize truly anomalous behavior for follow-up by security analysts. ML algorithms only enhance EDR evaluation when they have been sufficiently trained on multiple models to develop a baseline of normal, non-malicious activities on customer networks.	Required
Multiple, comprehensive sources for IOCs	EDR solutions look at Indicators of Compromise (IOCs), which include items such as MD5 file hashes, known bad IPs and URLs, file-to-process name mismatches, unusual network port usage by applications, unusual process injections, changes to module (DLL) load points, DLL to process/thread mapping, and registry changes (typically to make sure certain code runs after reboots). These are some examples. EDR solutions need to have multiple sources of IOC intelligence, parsed and validated quickly, with distribution to clients in near real-time to be most effective.	Required

Use case	Description	Relevance
Threat hunting and forensic investigations	Some mature organizations today proactively look for evidence that they may have been breached. EDR tools allow threat hunters to search through endpoint logs and interactively live-query machines to figure out what is running across an enterprise. EDR tools are informed by threat intelligence sources that deliver reasonably up-to-date information on Indicators of Compromise (IOCs), malicious URLs, and malware. When an actual attack has been discovered, EDR tools are also used during the forensic investigation. EDR solutions typically include management consoles to allow tracking of events and investigations across an enterprise. Moreover, many EDR solutions assist analysts in the next layer up phase of creating text reports with attribution theories and confidence levels.	Required
Automated remediation	Once attacks are discovered, depending on the circumstances, quick and automated responses may help limit damage and accelerate recovery. Examples of automated responses can be alerting security staff, terminating suspicious processes, opening tickets/cases, collecting snapshots, enabling agent-level recording for later playback and analysis, device quarantining, and even device re-imaging. Most EDR customers today opt to only use basic responses.	Required
Interactive querying	EDR consoles should support live interactive querying for various items, artifacts, and conditions to allow security analysts to have optimal situational awareness. For example, an analyst may find a certain unknown process running, and wants to determine if it is running elsewhere on the network. Other examples of items subject to query could include file presence or unusual machine-to-machine communication. Support for natural language queries is a plus.	Required
Live remote memory examination	Some EDR agents allow security analysts to conduct live memory analysis from the management console. This can be an unobtrusive way of actively looking for malicious behavior without alerting the user or malicious actor.	Recommended

Use case	Description	Relevance
Evidence collection, analysis, and recommendations	Some solutions in this space offer integration with forensic tools and threat analyst workbenches. The more sophisticated EDR solutions not only gather forensic evidence, but also analyze it and provide confidence/priority levels to events and generate attribution theories. These tools may also create recommendations for incident handling (playbooks) for specific types of events.	Recommended
Activity recording and playback	Some EDR agents allow for all relevant information to be “recorded” for later playback so that analysts can reconstruct what an attacker was doing on a machine. Examples of relevant data to capture are user logins, drivers loaded, processes launched, files accessed, registry changes, network communications log (including process to network port mapping), archive files created, files copied to removable media, etc. Recording operations can be CPU intensive, and require large volumes of log space, thus it is not something that can be on by default or left running for long periods.	Desirable

3 Vendors and Products

The vendors covered by this report provide endpoint security functionality in the areas of Endpoint Protection (analysis of code prior to or during execution to prevent compromise by malware) and Endpoint Detection and Response (analysis of system level changes to detect evidence of malware compromise).

3.1 Vendors Covered

- Bitdefender
- BlackBerry
- Carbon Black
- Cisco
- Cybereason
- ESET
- F-Secure
- FireEye
- Fortinet
- Kaspersky
- Malwarebytes
- McAfee
- Microsoft
- Palo Alto Networks
- Sentinel One
- Sophos
- Symantec

3.2 Featured Vendors

Some vendors are better positioned to meet narrow use cases, while others have stronger offerings across the range of Endpoint Protection, Detection and Response use cases. We have identified a few vendors that are notable for their unique strengths that may not be apparent in the table below. Vendors are featured for specific attributes as detailed below:

3.2.1 Featured for EPP capabilities: F-Secure

F-Secure is a first-generation antivirus company with next-generation anti-malware technology. F-Secure uses standard and cutting-edge methods to detect and prevent malware from running, including signatures, full system scanning (MFT to memory), exploit prevention, and multiple ML detection models. F-Secure is a regular participant in independent testing. In recent tests, they were one of just a few vendors who successfully blocked all malware variants, including some unknown or zero-day types of attacks.

FEATURED FOR
EPP CAPABILITIES
ENDPOINT PROTECTION, DETECTION AND RESPONSE
MARKET COMPASS 2020
KUPPINGERCOLE ANALYSTS AG, JULY 2020

Figure 2: Featured for EPP Capabilities

3.2.2 Featured for EPDR capabilities: Kaspersky

Kaspersky offers a leading-edge EPP suite. It utilizes all available technical methods to discover and prevent execution of malware as well as provide automatic responses to malicious actions, utilizing innovative ML techniques. Secondary EPP functions included: encryption, application control, firewall, malicious URL detection and vulnerability and patch management. Kaspersky provides rich EDR capabilities powered by Threat Intelligence and MITRE ATT&CK mapping, with all functions in a single agent. EPDR can be further scaled into the Extended Detection and Response (XDR) solution, combining EDR capabilities and network-level advanced threat discovery. Kaspersky's commitment to openness is demonstrated by their launching of global transparency centers as well as regular testing of their anti-malware capabilities by multiple independent testing organizations, including MITRE ATT&CK evaluation.

FEATURED FOR
EPDR CAPABILITIES
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 3: Featured for EPDR Capabilities

3.2.3 Featured for EPP innovation: Bitdefender

Bitdefender is a top of the line EPP solution, deploying all relevant pre-execution and runtime malware detection and prevention techniques. Their solution makes full use of advanced ML algorithms. Bitdefender also excels in independent testing. What sets Bitdefender apart is that they license their anti-malware engine and SDKs to other vendors, including other cybersecurity vendors. Bitdefender offers 20 different modular licensing solutions to over 150 partners. This boosts their total number of protected endpoints to over 500 million.

FEATURED FOR
EPP INNOVATION
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 4: Featured for EPP Innovation

3.2.4 Featured for EPDR innovation: Sentinel One

Sentinel One Platform has some of the most advanced EDR features, relying on state-of-the-art ML detection models. Sentinel One does not baseline devices, but rather uses continuous monitoring of good and bad behavior. It has excellent interfaces for analysts and threat hunters. The agent can perform well even autonomously, that is, without a constant connection to Sentinel One’s cloud. This gives it an advantage in environments like ICS and IoT, where devices and thus agents may not be able to do real-time queries. Sentinel One performs well in independent real-world tests. The console supports MFA and SAML federation. Lastly, Sentinel One Ranger effectively turns endpoint agents into network listeners, allowing customers to move toward XDR.

FEATURED FOR
EPDR INNVOATION
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 5: Featured for EPDR Innvoation

3.2.5 Featured for EDR innovation: Sophos

Sophos been a recognized name in EPP for decades. It has a good reputation for anti-malware, which was enhanced with the addition of Invincea a few years ago. Sophos has fairly recently added full-fledged EDR capabilities to their product offering. Their EDR tool covers all the expected functions, looking at file and registry changes, app-to-port network monitoring, etc. However, Sophos has taken a different approach to EDR and threat hunting in particular. The addition of a SQL query interface for node and cross-enterprise searches puts advanced threat hunting capabilities into the hands of system administrators. This increases the value of their solution by taking sophisticated functionality and making it accessible to IT staff rather than only highly specialized threat hunters.

FEATURED FOR
EDR INNOVATION
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 6: Featured for EDR Innovation

3.2.6 Featured for XDR innovation: Palo Alto Networks

Palo Alto, once the pioneer in Next Generation Firewall (NGFW) technology, is now the pioneer for “XDR”, or the union of EDR and network security monitoring. Palo Alto leverages their NGFW and network security technologies in conjunction with their EPP and EDR clients to provide a comprehensive and holistic look at all activities within an enterprise. The Cortex XDR product was among the first to put all telemetry into a data lake where it can be analyzed against ML detection models to find anomalous behavior, classify it, alert customers, and take actions. Palo Alto is pushing the boundaries and defining what XDR is for the market.

FEATURED FOR
XDR INNOVATION
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 7: Featured for XDR Innovation

3.2.7 Featured for EPDR universal coverage: ESET

ESET has been an avant garde anti-malware company for many years. Their products incorporate the latest approaches to discovering and preventing malware from executing, including advanced ML detection models, exploit prevention, memory analysis, and anti-stealth technologies that can eliminate hard-to-discover UEFI and MFT rootkits. ESET covers all aspects of the market, from SMBs to enterprises. They have offices around the globe and support the widest variety of languages in their products and documentation. Moreover, their products have agents for the broadest array of operating systems in use today.

FEATURED FOR
EPDR COVERAGE
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 8: Featured for EPDR Universal Coverage

3.2.8 Featured for Threat Intelligence integration: Symantec

Symantec, a global cybersecurity leader for decades, has a wide range of integrated security products, covering endpoints, applications, networks, and the cloud. One of the keys to Symantec's success in the market is their Global Intelligence Network. Symantec receives telemetry from hundreds of millions of covered endpoints and applications as well as industry partners. Like many vendors in this report, Symantec is a member of the Cyber Threat Alliance. Their high-quality threat intel powers their suite of integrated products, including Symantec Endpoint Protection which is covered in this report.

FEATURED FOR
THREAT INTEL. INTEG.
ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020

Figure 9: Featured for Threat Intelligence Integration

3.2.9 Featured for Threat Intelligence integration: McAfee

McAfee was an early pioneer in antivirus and cybersecurity products and is a charter member of the Cyber Threat Alliance. McAfee’s Global Threat Intelligence (GTI) informs not only their own cybersecurity tools, but also is available to 3rd-parties as a service. GTI provides information on certificate, file, IP, and URL reputation and website categorization. Intelligence is sourced primarily from their millions of protected nodes, and in response to over 100 billion requests to their cloud service monthly.

ENDPOINT PROTECTION, DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, JULY 2020
MARKET COMPASS 2020
FEATURED FOR THREAT INTEL. INTEG.

Figure 10: Featured for Threat Intelligence Integration

3.3 Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that have some but not all required capabilities in the EPDR market. These vendors do not fully fit into the EPDR market segment or do not meet our eligibility criteria to be considered in this evaluation. We provide short abstracts for these vendors below.

- AhnLab: was founded in 1995 and is headquartered in Seoul. They are a privately held, top cybersecurity product vendor in the APAC region, serving the consumer, SMB, and enterprise markets. AhnLab offers a range of products, including their regionally well-known anti-malware products, security assessment, EDR, network layer malware sandbox, and cloud workload protection platform (CWPP) for AWS and Azure. AhnLab offers managed security services.
- Avira: Established in 1986 in Germany. Avira has EPP but not EDR. They have solutions for API/SDK and IoT security. They also provide threat intelligence feeds and APIs for other security related applications to consume. Avira is a vendor to watch for future developments in the rapidly growing IoT security space.
- Avast: Founded in 1988 in Prague. Avast has EPP functionality, including many secondary EPP functions such as patch management, internet/email/web gateway, and content filtering. They do not have EDR. Keep an eye on Avast because they have a full range of EPP functions and may be a target for acquisition to pair with EDR.
- Checkpoint, a global cybersecurity vendor, was founded 27 years ago in Israel. They now have dual

HQs in Tel Aviv and Silicon Valley. SandBlast is their EPP and EDR combined product. They are well known for the firewall and VPN products, and also have email and web security appliances, SIEM, mobile security clients and management solutions, and Cloud Security Posture Management and Cloud Workload Protection services. CheckPoint's ThreatCloud Managed Security Service is a full featured managed service offering.

- Comodo: Founded in 1998 and headquartered in New Jersey, US. Comodo Security Solutions has EPP, endpoint firewall, HIPS, and content filtering functionality. The parent company owns Sectigo, a Certificate Authority; and DNS.com, a DNS managed service provider. Watch this vendor as they grow organically and through acquisitions to become a major security stack vendor.
- Fidelis Cybersecurity: Fidelis was founded in 2003 and is headquartered in Bethesda, MD, outside Washington, DC. They are a privately held company. They have EDR but not EPP functionality. They also offer Network Detection & Response (NDR) and Network Threat Deception products. Fidelis has a reputation for excellent high-security products. Watch Fidelis as they add product offerings and increase their market size.
- GoSecure, a late stage venture-backed company, has dual headquarters in Montreal and La Jolla, CA. They were founded in 2012. Their initial entry into the market was in EDR with the CounterTack product. In late 2019 they launched NGAV. In mid-2019 they acquired EdgeWave, for their inbox detection and response capabilities. They offer full MDR services.
- Infocyte: Headquartered in Austin, TX. Their tools and services are centered on incident response, using their EDR and threat assessment tools. Clients generally come to them when they believe an incident has occurred. Infocyte Threat Assessment can perform internal vulnerability assessments, and their agents can provide the full range of EDR functions. The solution does not contain EPP, but they partner with CheckPoint. Infocyte has found a niche in the security market in which they are doing well. We will monitor this vendor as they add capabilities and potentially become a target for acquisition.
- Tanium: Tanium was founded in 2007 in the Bay Area. They are a late stage venture-backed firm. They have products in the endpoint security and management spaces. They are focused on EDR and UEM rather than EPP. Tanium is well-known in this corner of the endpoint management and security market. Watch this vendor as they expand their market share and partner with others.
- Trend Micro is a large and venerable player in the endpoint security market, having been established in 1988 in Tokyo. Beyond EPP and EDR, Trend Micro has email and web security gateway solutions, SaaS application security, cloud migration tools, and a global threat intelligence service. They also offer IoT security and management solutions covering connected cars, smart factories, and connected consumer use cases. Trend Micro participates in independent malware detection tests regularly. Trend Micro should be evaluated for their array of security products.
- Webroot: Launched in Colorado in 1997, Webroot offers an EPP product, cloud-hosted DNS protection, endpoint data protection, and security awareness training services. Keep an eye on Webroot as they build out their security product portfolio.

- Ziften: Austin-based Ziften was founded in 2009. They are a late stage venture-backed firm focused on endpoint security. Zenith, the main EPP/EDR product, has agents for Windows, Mac, and Linux. In addition to EPP and EDR, Zenith can perform asset inventory and utilization, app inventory, vulnerability and patch monitoring, and endpoint performance monitoring and hardening. Ziften offers MDR services. Ziften provides integrations for SIEM and SOAR. Ziften is a vendor to watch as they grow and become a candidate for acquisition.

4 Ratings at a Glance

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

Product	Security	Interoperability	Usability	Deployment	Malware Protection	Threat Hunting	Automated Responses	Secondary EPP	Common Functions
Bitdefender Gravity Zone Elite, Ultra Plus	⚫	⚫	⚫	⚫	🟢	⚪	🟢	🟢	⚫
BlackBerry Protect, Blackberry Optics	⚫	⚫	⚫	⚫	⚫	⚫	⚪	⚪	⚫
Cisco AMP for Endpoints	🟢	🟢	🟢	🟢	🟢	⚫	⚫	⚪	⚫
Cybereason Defense Platform	🟢	⚫	⚫	⚫	⚫	🟢	⚫	⚫	🟢
ESET Endpoint Security	🟢	🟢	🟢	🟢	🟢	⚫	🟢	⚫	⚫
F-Secure Business Suite / Protection Service for Business	⚫	⚫	⚫	🟢	🟢	⚫	⚪	⚫	⚫
FireEye Endpoint Security	🟢	🟢	⚫	🟢	🟢	🟢	⚫	⚪	🟢
Fortinet FortiClient, FortiEDR	⚫	⚫	⚫	⚫	⚫	🟢	🟢	🟢	⚫
Kaspersky Endpoint Security for Business	🟢	🟢	🟢	🟢	🟢	🟢	⚫	🟢	⚫
Malwarebytes Endpoint Protection, Endpoint Detection & Response	⚫	🟢	🟢	🟢	🔴	🔴	🟢	🔴	⚫
McAfee MVISION	🟢	⚫	⚫	⚫	⚫	⚫	🟢	🟢	🟢
Microsoft Defender Advanced Threat Protection	🟢	🟢	⚫	🟢	🟢	⚫	⚫	🟢	🟢

Product	Security	Interoperability	Usability	Deployment	Malware Protection	Threat Hunting	Automated Responses	Secondary EPP	Common Functions
Palo Alto Networks Cortex XDR Pro	🟢	🟢	⚫	🟢	⚫	🟢	⚫	🟢	🟢
SentinelOne Singularity Platform	🟢	🟢	🟢	🟢	🟢	🟢	🟢	⚪	🟢
Sophos Intercept X	🟢	⚫	⚫	🟢	🟢	🟢	⚫	⚪	⚫
Symantec Endpoint Security Complete	🟢	🟢	🟢	🟢	🟢	🟢	⚫	🟢	🟢
VMware Carbon Black Endpoint Standard	🟢	⚫	⚫	🟢	🟢	🟢	⚪	⚪	🟢
Legend						🟠 critical	🔴 weak	⚪ neutral ⚫ positive	🟢 strong positive

5 Product/Service Details

Spider graphs

In addition to the ratings for our standard categories we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the Market Compass. For this Market Compass, we look at the following five areas:

- Common functions
  EPP and EDR products require an agent to be installed on endpoints to perform their functions. Sometimes solutions have an “agent-less” mode, but this usually involves process injection, which is temporary commandeering of OS or app processes to scan other processes or memory spaces. Ironically, this is the method by which many forms of malware take over devices. Thus, all EPDR products require agents to be installed, and it is highly important that these agents are able to function adequately when they are not able to contact the vendor’s cloud service or customer management console.
  Secondly, the ability to strongly authenticate admins to EPDR tools and dashboards is required. Vendors should provide strong MFA options. Role-based and delegated access controls are similarly advised.
- Malware protection
  EPP is about discovering which code fragments are malicious and preventing them from executing. Toward that end, multiple detection engines are needed to effectively find and stop malware before it has a chance to run: signature scanner, pre-execution heuristics, memory analysis, and sandboxing. EPDR products need to be able to monitor usage of crypto APIs and for attempts to delete the Volume Shadow Copy in Windows in order to quickly shut down ransomware.
  Malware generally exploits known vulnerabilities. Many anti-malware solutions look for code in the pipeline that is about to use known exploits (CVEs) and halts associated processes. Malware protection capabilities are assessed via independent testing. Low false positive rates as reported by independent testing also factor into the malware protection metric.
- Secondary EPP functions
  Full-featured EPP products possess endpoint firewall functions, application whitelisting and blacklisting, URL filtering, and critical file system monitoring capabilities. Some also bundle Unified Endpoint Management features such as asset tracking, patch management, vulnerability assessment and management.
- Threat hunting
  Basic EDR and threat hunting capabilities are rated in this category. This includes integration of high-quality threat intelligence sources (IOCs), near real-time detection and evaluation of threats, and

query ability for analysts and hunters. More advanced features in this area include live remote memory analysis and activity recording and playback.

- Automated responses
  "R" stands for response, and EPDR products can have a variety of response options, ranging from simple alerting, to process termination, quarantining, forensic evidence collection, and even rollback to known good states.

These spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for strategic choice of product.

5.1 Bitdefender

Bitdefender is a private company, and was founded in 2001 in Bucharest, Romania. The company specializes in cybersecurity technologies for Windows PCs, Macs, iOS, Android, and virtual environments. Related products in their suite handle APT protection, IaaS and SaaS security, disk encryption, device control, application whitelisting, patch management, email system security, web security/URL filtering, network detection and response, etc.

Bitdefender excels in independent enterprise malware detection tests. Agents are available for Windows 7 – 10, Windows Server 2008R2-2019, MacOS 10.9.5 - 10.15, multiple Linux flavors, and Android and iOS mobile. Bitdefender uses a layered defense against malware: signature scanning; pre-execution file scanning using ML techniques such as neural net, binary decision tree, etc.; dynamic analysis at execution monitors process behavior; agent-integrated cloud sandboxing; rootkit prevention driver; and file-less malware detection capabilities. Bitdefender's anti-malware engine is OEM'd into products by other vendors.

EDR features are in the same agent and are activated by a license. Process, file, registry, and network activities can be examined to look for process injections, config changes, and unusual network communications. Discovered threats are tagged according to MITRE ATT&CK framework. Bitdefender performed well in the latest round of MITRE ATT&CK evaluations. Automated responses include process termination, quarantine, system rollback, and basic Root Cause Analysis (RCA). 2FA/MFA is limited to Google Authenticator. The console can send event data via syslog with in-product filtering for SIEM integration.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ○ ○
Automated Responses	● ● ● ● ●
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ○

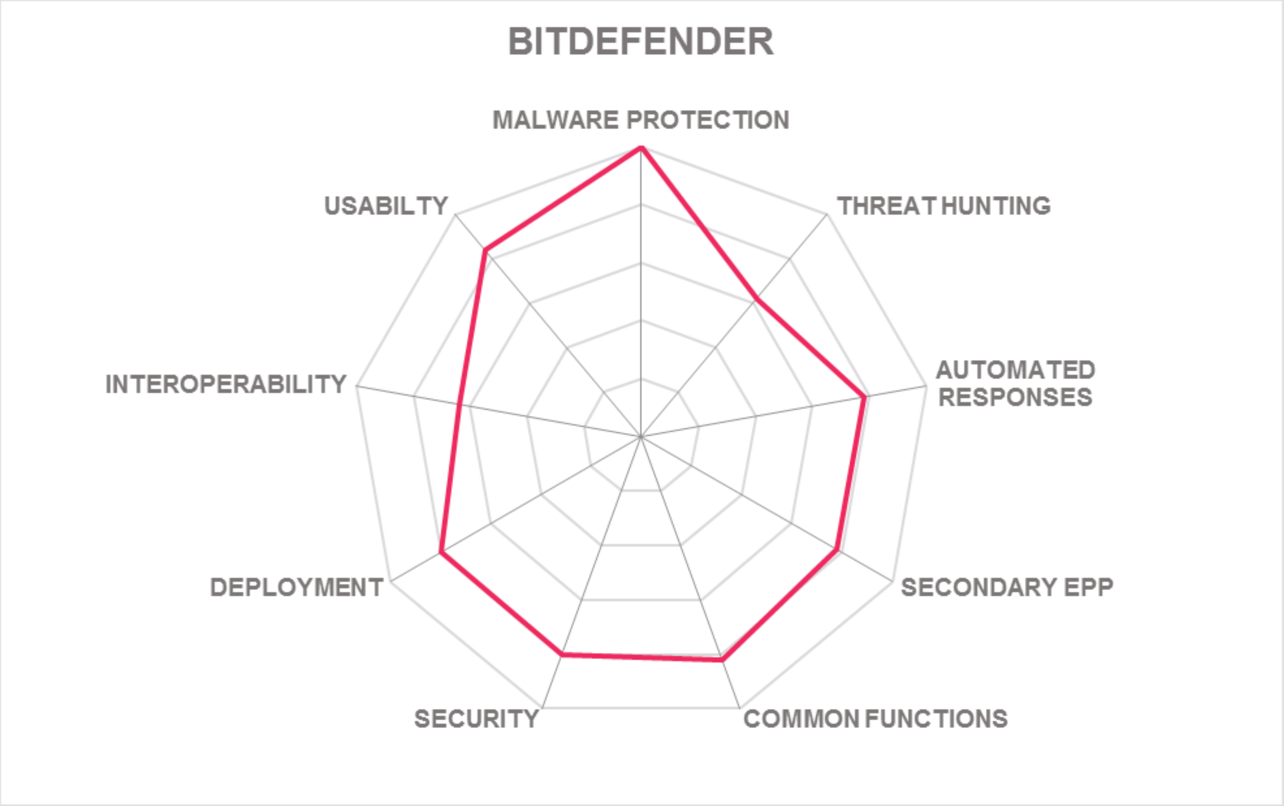
Bitdefender®

Strengths

- Excellent malware detection and prevention, OEM’d by other vendors
- Good coverage for Linux
- Includes URL filter, endpoint firewall, app control, device control, patch management, and encryption
- Full range of automated responses available

Challenges

- Needs more MFA options
- Sandbox only operates in the cloud


BITDEFENDER
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.2 BlackBerry

Following its 2019 acquisition of Cylance, an advanced AI-based cybersecurity company, BlackBerry has been transforming itself as a security vendor. It recently introduced a unified endpoint security (UES) solution that provides EPP, EDR, mobile threat defense and UBA for both mobile devices and desktop. BlackBerry plans to integrate its UES suite with BlackBerry Unified Endpoint Management as well as other vendor's UEM products. BlackBerry Guard is the company's offering for managed detection and response services.

BlackBerry Protect uses multiple advanced ML detection methods and memory analysis but not signatures, sandboxes, or heuristics. Agents are available for Windows 7 – 10, Windows Server 2003-2019, MacOS 10.9+ and Linux. BlackBerry Protect includes USB media control to prevent unauthorized data transfers and application control. It can also monitor and stop malicious scripts and PowerShell commands from executing to prevent file-less malware attacks.

BlackBerry Optics is the EDR product, and it resides in the same agent. The customer configurable Context Analysis Engine focuses on registry inspection and monitoring and examining the sources of DNS queries. Discovered threats are mapped to MITRE ATT&CK. Playbooks are supported, and automated response types include device isolation and forensic investigations. Federated authentication for admins is supported.

BlackBerry

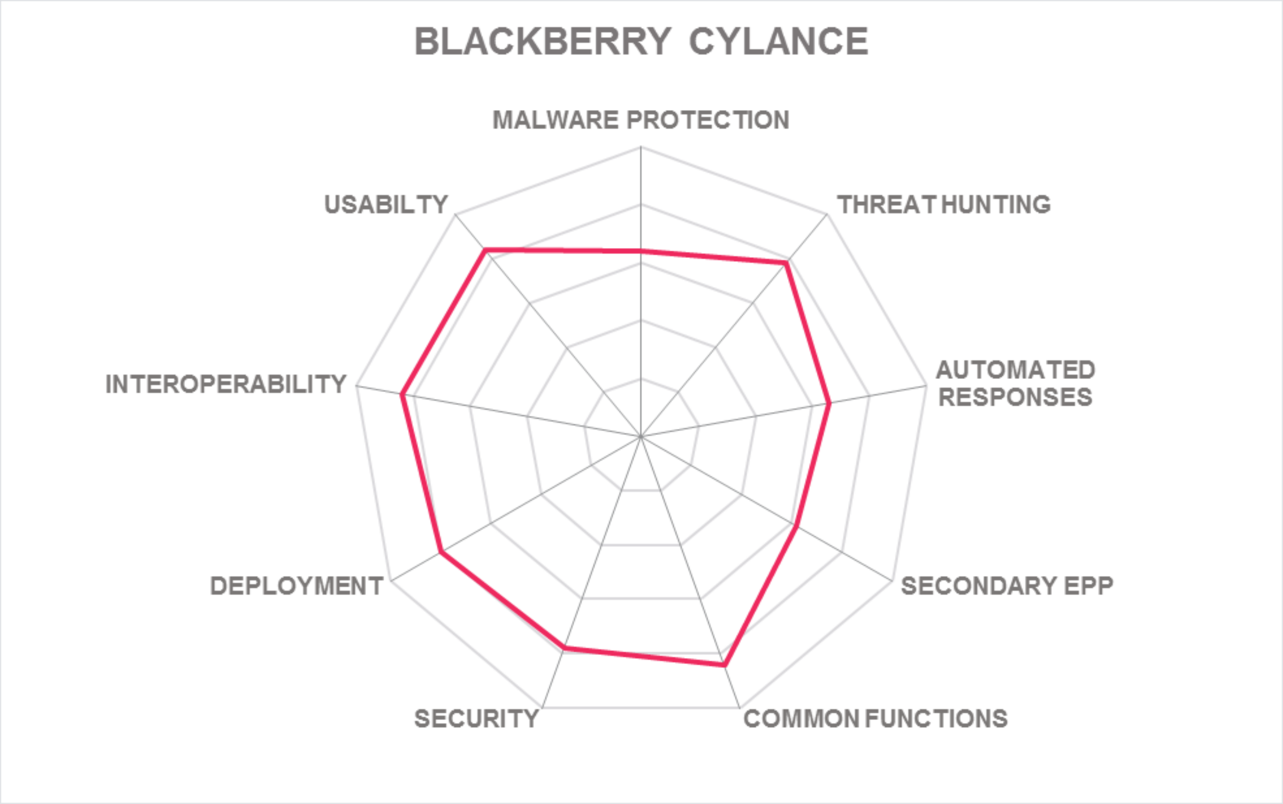
Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Malware Protection	● ● ● ● ○
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ○ ○
Secondary EPP	● ● ● ○ ○
Common Functions	● ● ● ● ○

Strengths

- Federated authentication options for admins
- Does not require constant internet connectivity to vendor cloud
- Customer configurable threat hunting options
- Single, lightweight agent that has very little impact on system performance

Challenges

- Vendor does not often participate in independent malware detection tests
- Solution emphasizes ML detection techniques to the exclusion of other effective methods
- ML detection models can be deliberately gamed into missing malware
- May require other vendor products to build a full endpoint security solution


BLACKBERRY CYLANCE
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.3 Cisco

Cisco, well-known for network devices and services, also offers many security solutions. AMP for Endpoints is their EPP and EDR combined product with built-in cross-control detection and response with Cisco SecureX. They also have NGFW, email security, web security, and Network Detection and Response (NDR) products. Cisco also has security services, including MDR and threat analytics via a global SOC-as-a-service.

Cisco has begun to participate in some independent testing. Agents are available for Windows 7 – 10, Windows Server 2008R2 - 2016, MacOS 10.12 - 10.13, RHEL 6/7, CentOS 6/7, Android 2+, and iOS 11+. Cisco employs the full gamut of techniques for pre-execution and runtime malware detection: signature-based scanning, file and app reputation, exploit prevention, sandboxing, behavioral indicators, and memory analysis. It can detect sandbox-aware malware. Its ML detection models are informed by Cisco Talos threat intelligence.

Cisco views EDR as an extension to EPP. They apply similar techniques (in the same agent) when looking for IoCs retrospectively. Talos Threat Intelligence is the source of IoCs for AMP's EDR functions. IoC types include file and registry changes and network comms patterns. Automated responses include process termination, quarantine files, and node isolation. Its built-in Cisco SecureX platform allows analysts to run automated playbooks and simplify endpoint security orchestration and automation. Cisco is a charter member of the Cyber Threat Alliance. Cisco supports CyBox, STIX, and TAXII. APIs permit interoperation with SIEM and SOAR apps such as QRadar and Splunk. Their platform has not been evaluated against MITRE ATT&CK however, Cisco is registered for Round 3 of evaluations slated for this year and have already completed its querying, IoC, and cloud-delivered malware analysis capability mapping to MITRE ATT&CK. There are limited options for admin MFA and SAML federation can be configured for admins.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ○ ○
Common Functions	● ● ● ● ○

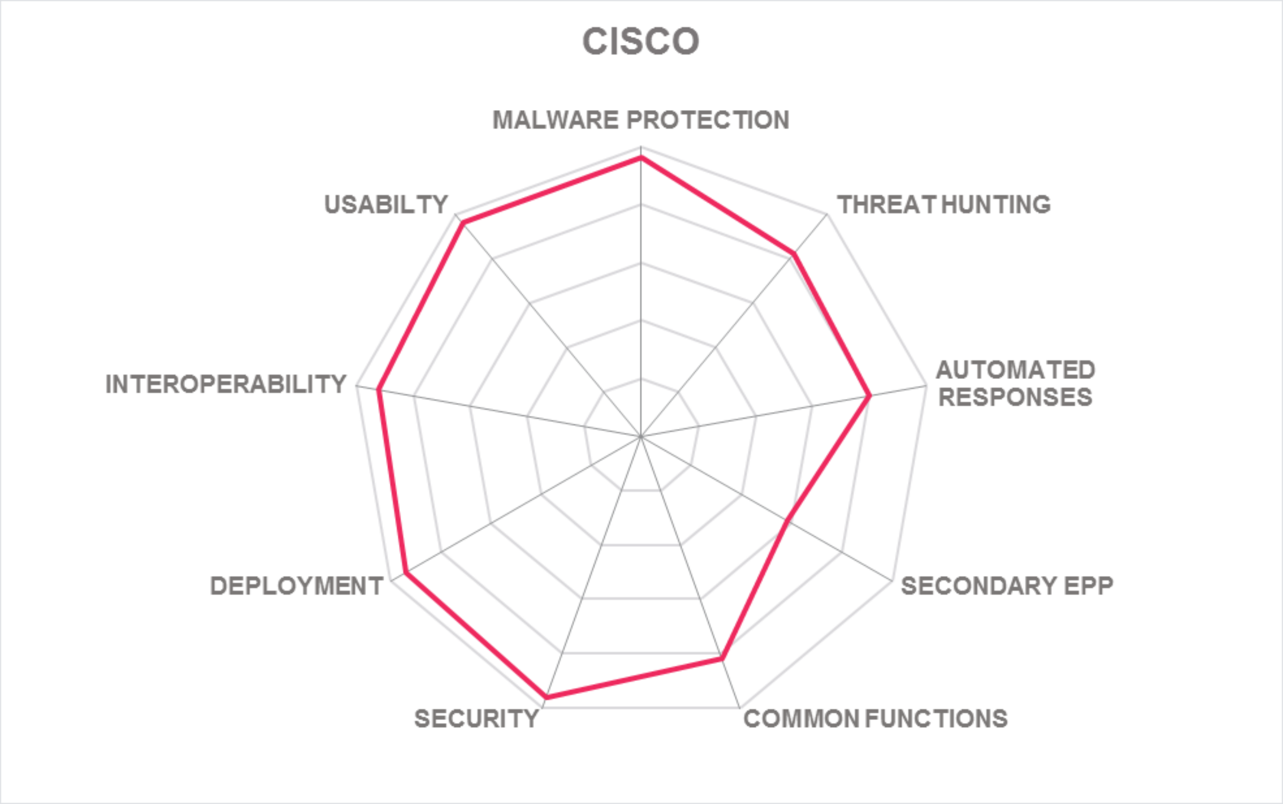
CISCO

Strengths

- Comprehensive pre-execution and runtime malware detection
- Products enhanced by Cisco Talos Threat Intel
- Detects sandbox-aware malware
- Tight integration with other Cisco and 3rd-party security tools

Challenges

- Professional services needed for playbook and IR development
- More MFA options would benefit customers


CISCO
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.4 Cybereason

Cybereason, a late stage venture backed company, was founded in 2012 and is based in Boston. Today they have a strong global presence. Cybereason started with EDR and has added EPP functionality and associated controls such as endpoint firewall, endpoint controls, hardening, and full disk encryption. Cybereason offers MDR, incident response, cybersecurity posture analysis, and threat hunting services for clients.

Cybereason has participated in independent testing including some recent tests, in which the product excelled at malware detection. Single agent deployments are available for Windows XP SP3 – 10, Windows Server 2003 - 2019, MacOS 10.12 - 10.15, and multiple Linux flavors, Android, and iOS. Cybereason employs several approaches for malware detection via a multi-layered prevention stack: signature-based scanning, exploit protection, document protection, and process behavioral and memory analysis to stop file-less attacks. It uses crypto API and deep filesystem and volume shadow copy monitoring to deter ransomware.

Cybereason was a pioneer in standalone EDR products. Thus, the product covers all the expected IoC types, and also allows customization for threat hunts and inclusion of multiple external threat intel feeds. Cybereason follows the MITRE ATT&CK framework; mapping alerts to the ATT&CK framework and they have participated in all rounds of testing. Threat hunters can use the analyst UI and an NL query builder to investigate and hunt for threats. Cybereason consolidates all relevant information for each attack into a single view called a Malop (Malicious Operation). Malops facilitate a quick and intuitive understanding of malicious attacks. Within a Malop, you can easily see all related attack elements, including the root cause, all affected machines and users, incoming and outgoing communications and a timeline of the attack. Cybereason is focused on efficient administration, with a 1:150,000 ratio for admin to nodes. Automated and one-touch responses include process termination, quarantine files, remote shell, granular rollback of system-level changes, and node isolation. 2FA is limited to Googlew Authenticator app, but SAML and SSO via other identity providers are supported. Multiple roles can be selected for console access. The console can send event data via syslog with in-product filtering for SIEM integration.

cybereason®

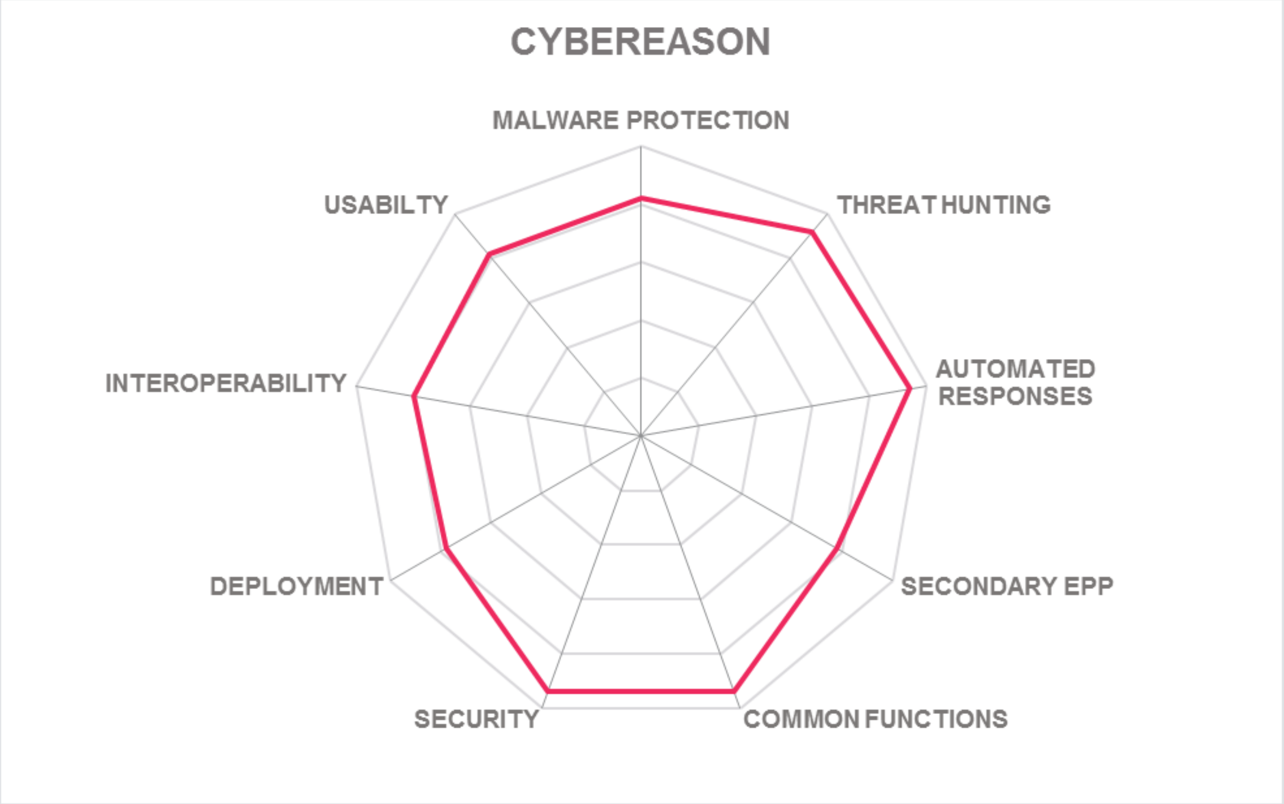
Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Malware Protection	● ● ● ● ○
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ● ○
Common Functions	● ● ● ● ●

Strengths

- Excellent threat hunting facilities
- Strong results in malware detection tests
- Secondary EPP functions include endpoint controls and disk encryption
- SAML support for admin authentication

Challenges

- Smaller market share
- Additional native MFA options would be beneficial


CYBEREASON
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.5 ESET

ESET was founded in 1987 and is headquartered in Bratislava, Slovakia. They specialize in EPP and EDR. For enterprise customers they also offer threat intelligence services. They provide endpoint security software and services to MSPs.

ESET Endpoint Security is their EPP product. Agents are available for Windows 7 – 10, Windows Server 2003-2019, MacOS 10.9 - 10.15, all major Linux variants, z/OS, VDIs, Android 4+ and iOS 9+. The ESET Augur engine uses deep learning neural nets and long-short-term memory plus additional unsupervised ML sorting algorithms. Augur analysis informs the ESET DNA Detections component, which extracts the bad "genes" of malicious and extrapolates results to allow the widest possible detection of potential malware. ESET agents have kernel-level components for self-defense. ESET Network Attack Protection, Reputation & Cache or Exploit Blocker features prevent execution of unknown threats to protect the agent(s) themselves. For example, Reputation & Cache locally hosts reputation information to enhance performance. Agents communicate with ESET Live Grid® in the cloud to get updated information on potential threats and file reputations. ESET agents use sandboxing both locally and send suspicious code to ESET's cloud sandbox for detonation and analysis. ESET leverages Windows AMSI, and provides a Script Scanner, Advanced Memory Scanner, a Ransomware Shield. ESET regularly participates in independent testing.

ESET Enterprise Inspector (EEI) is their EDR solution. It looks for a variety of different high-level activities to detect directed attacks, lateral movement by APT-type actors, address spoofing, privilege escalation, abnormal process execution and injection, abnormal DLL usage, abnormal file access, client agent tampering, registry changes, remote PowerShell script execution, remote network connections with attempts to execute code, and data exfiltration attempts. EEI supports interactive live querying and memory analysis. Automated response options are network isolation of suspect nodes, process termination, moving/deleting files, and running scripts. ESET has some 2FA options for admins. They contribute to and map to the MITRE ATT&CK framework, but have not participated in formal evaluations, although they are planning on being in round 3 in 2H2020.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ● ●
Secondary EPP	● ● ● ● ○
Common Functions	● ● ● ● ○

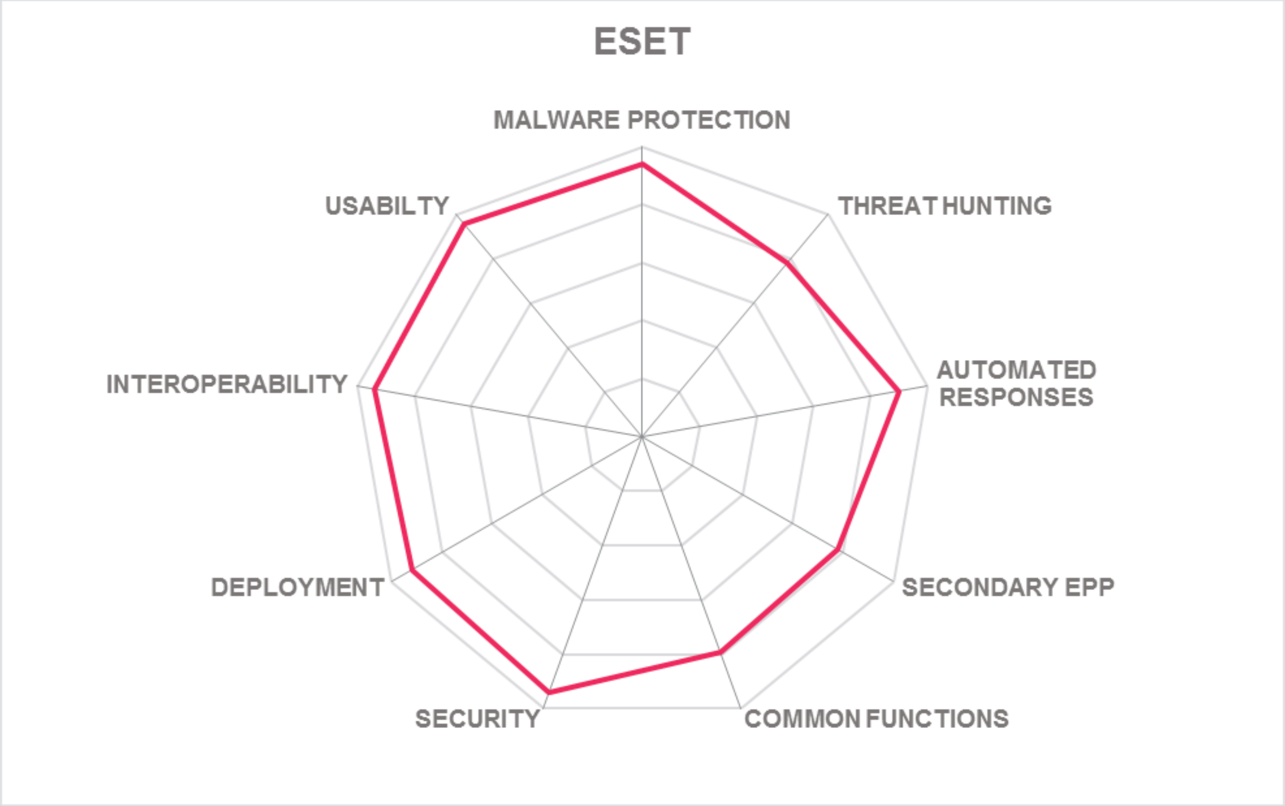
eset®

Strengths

- Broadest range of node OS support for EPP
- Complete suite of detection and protection techniques, including pre-execution static analysis and post-execution behavioral analysis, exploit blocking, botnet protection, network attack protection
- UEFI scanning ability
- Excellent implementation of multiple, advanced ML algorithms for discovering malicious activity patterns
- Support for most commonly used and requested automatic response options

Challenges

- Does not support SAML federation
- Interoperating with 3rd- party tools such as UEM may require customization


ESET
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.6 F-Secure

F-Secure was founded in 1988 in Helsinki. They are consistently rated among the highest scoring anti-malware vendors in independent tests, including at detecting zero-days. F-Secure also has EDR, vulnerability and patch management, Microsoft Office 365 and Salesforce cloud protection products. Moreover, F-Secure has MDR, threat hunting, and anti-phishing and security training services, as well as cyber security consulting services.

F-Secure has agents for Windows 7-10, Windows Server 2008R2-2019, MacOS 10.13-10.15, and many Linux variants. It employs multiple malware detection techniques: signature-based, system scanner (memory and process analysis), cloud-based sandbox, and a pre-execution heuristics scanner. The agents can detect and prevent polymorphic and Powershell-based file-less malware. Kernel mode drivers in the agent can detect and remove rootkits. The solution detects and stops malware by both signature-based scans and monitoring for common ransomware techniques such as attempts to delete the volume shadow copy. DataGuard module provides DLP-like functionality for an additional layer of ransomware protection.

Rapid Detection & Response is their EDR product. Agents are available for not only Windows but also Mac, which sets them apart in the field. Their Broad Context Detection™ uses Machine Learning (ML) techniques and pre-configured rules to detect anomalous behavior and is designed to narrow down the number of detections to a small number of meaningful incidents that may indicate that systems or data have been compromised. The specific functions that Broad Context Detection^{TM} performs are baseline determination, host profiling, detection significance analysis, and suitability score analysis. Broad Context Detection^{TM} flags indications of possible breaches by alerting admins of tactics, techniques and procedures (TTPs) used in targeted attacks, such as registry changes, process injections, apps communicating on strange ports, and the full gamut of IoCs. Some detections require deeper threat analysis and guidance by specialized cyber security experts. For these cases, the solution has a unique built-in "Elevate to F-Secure" service. It offers professional incident analysis of methods and technologies, network routes, traffic origins, and timelines of Broad Context Detection™ to provide expert advice and further response guidance whenever under attack. F-Secure participated in MITRE ATT&CK evaluations and performed very well, with one of the lowest numbers for missed detections. Automated response options are quarantining of suspect nodes and process termination. F-Secure has 2FA but does not support advanced MFA or SAML for admins.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ○ ○
Secondary EPP	● ● ● ● ○
Common Functions	● ● ● ● ○

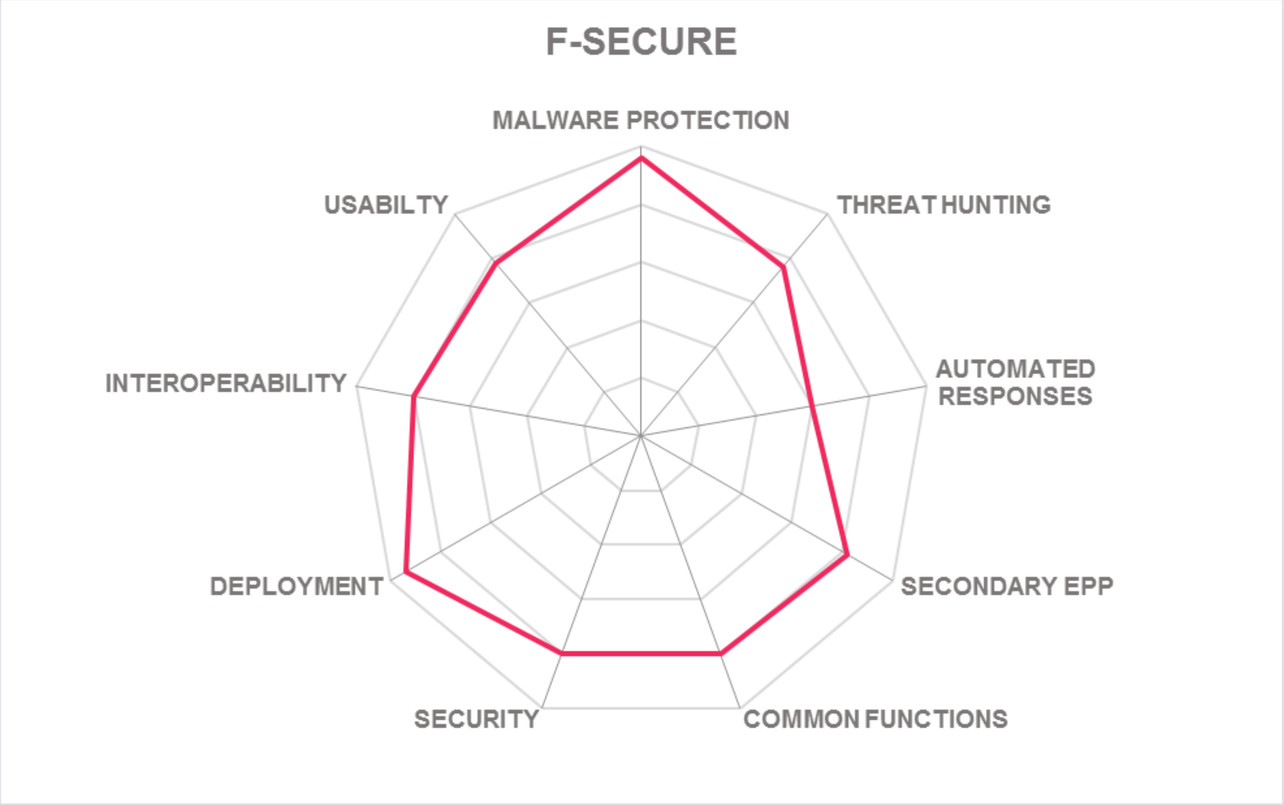
F-Secure®

Strengths

- One of the best products for detecting malware, including zero-days
- High EDR detection rate in MITRE ATT&CK evaluations
- Strong malware removal and quarantine capabilities
- Good implementation of multiple, advanced ML algorithms for discovering malicious activity patterns in Broad Context Detection™
- Excellent regional/language support
- Unique “Elevate to F-Secure” feature offers the support of F-Secure’s cyber security experts when needed

Challenges

- Attribution theories and root cause analysis EDR features on the roadmap
- Strong presence in EU, growing elsewhere


F-SECURE
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.7 FireEye

FireEye was founded in 2004 in Milpitas, CA. FireEye started out with email and web sandboxing tools, but through growth and acquisition they have added a wide range of cybersecurity products. Their cybersecurity portfolio includes cloud security, email and web security, endpoint security, network detection and response (NDR), SIEM, SOAR, User Behavioral Analysis, and Cyber Threat Intelligence (former iSIGHT and Mandiant). FireEye also offers services in these areas plus the full portfolio of Mandiant's forensic services.

FireEye has agents for Windows XP - 10, Windows Server 2003 – 2019, MacOSX 10.9+, and Debian, RHEL, OpenSUSE, Oracle, and Ubuntu Linux. AMIs are available for AWS. Support for Azure and Google Cloud will be available in July and August 2020 respectively. It has four major malware detection components: Malware Protection, an OEM'd antimalware engine, enhanced by FireEye and configurable through FireEye's console; Malware Guard, which uses ML detection models for pre-execution analysis of files; and Exploit Guard for prevention of exploits and malicious application behavior in highly targeted resources such as Microsoft Office files, browsers, Java, and Adobe Acrobat. The Realtime Indicator detection engine uses intelligence from FireEye against which it matches user and system behavior to identify threats. Both ExploitGuard Realtime Indicator Detection employ behavioral rule to identify file-less attacks. FireEye participates in a wide array of independent tests.

EDR functions are available in the same agent as EPP. FireEye's EDR product design is strongly influenced by Mandiant's leading edge forensic capabilities. The client looks for IoCs as informed by FireEye's threat intelligence. More than 100 attributes covering registry, file, process, network, and DNS lookups can be analyzed by the agent, making it one of the most extensive functional lists in the industry. Customers can select which attributes for analysis per policy and define more inclusive monitoring policies for high value assets. The threat hunting interface allows for deep hunting and analysis but is complex. Discovered events are mapped to MITRE ATT&CK. Admins and analysts can remotely perform live memory analysis, raw disk analysis, open PowerShell sessions and execute scripts. Alerting, process termination, node isolation are the primary responses, which are initiated manually in the Host Remediation module. Additional response actions are available in the separately licensed SOAR product. FireEye has participated in MITRE ATT&CK evaluations and performed very well, demonstrating the ability to automatically identify many APT techniques and showing very low numbers for missed detections.

FireEye interoperates with a long list of other security vendor tools including ArcSight, CyberArk, Demisto, McAfee, Palo Alto, Panorama, QRadar, Splunk, etc. FireEye contributes to the Cyber Threat Alliance. FireEye offers granular feature updates outside of the normal release cycle via downloadable modules, allowing customers to pick up features as soon as they are available. The console supports SAML federation; and LDAP, RADIUS, and TACACS for authentication. Role-based and delegated administration are supported.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ○ ○
Common Functions	● ● ● ● ●

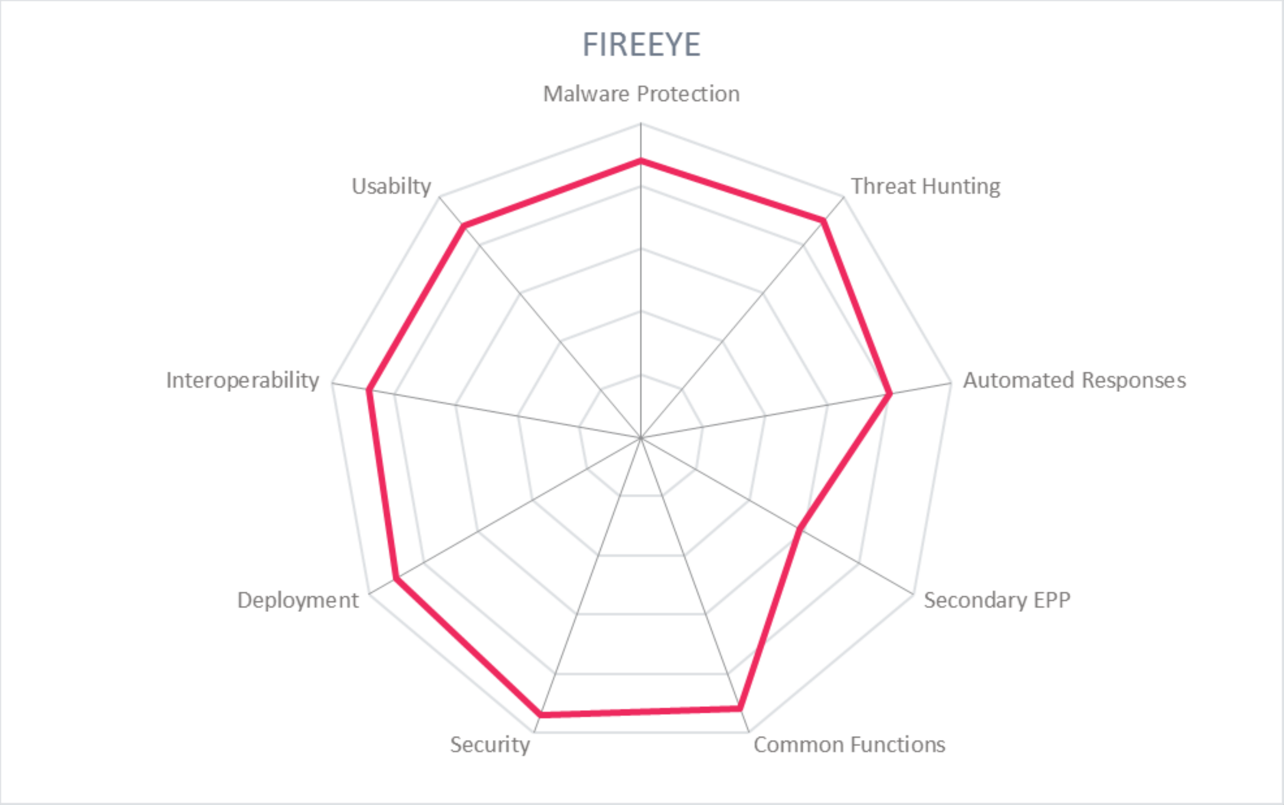
FIREEYE™

Strengths

- Highly interoperable with other security solutions, including other EPP products
- Deep EDR capabilities shaped by Mandiant forensics
- High EDR detection rate in MITRE ATT&CK evaluations
- Strong authentication and federation supported
- Products informed by excellent threat intel (FireEye/Mandiant/iSIGHT)

Challenges

- More automated response possibilities should be built into the product
- Full featured but complex EDR analyst interface
- Missing some secondary EPP functions


FIREEYE
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.8 Fortinet

Fortinet was founded in 2000 in Silicon Valley. In late 2019 they acquired EnSilo. The company produces a wide range of hardware and software security products, covering endpoints, IoT, cloud workloads, networks, and secure processing solutions. Fortinet participates in some independent testing regimes. The company offers consulting services, deployment services, and ongoing operations services.

FortiClient is the endpoint protection component of their overall Security Fabric model, which is built around the FortiGate NGFW. FortiClient can run on Windows 7-10, Windows Server 2008-2019, MacOS 10.11+, and multiple types of Linux. FortiClient uses exploit prevention, behavioral analysis, and memory analysis. Suspicious code is sent to FortiSandbox in the cloud for detonation. For secondary EPP functions, Fortinet includes asset discovery and management, patch management, vulnerability assessment and shielding, web filtering, app controls, and VPN.

FortiEDR has some advanced features that are not commonly found in other EDR products, such as the ability to take memory snapshots and to execute deep system-level changes including rollbacks. FortiEDR supports detailed and customizable playbooks, designed with an emphasis on business continuity during incidents. Their portfolio is aligned to MITRE ATT&CK, but they have not participated in evaluations. Fortinet is a charter member of the Cyber Threat Alliance. Fortinet does support some limited MFA options via LDAP and RADIUS.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Malware Protection	● ● ● ● ○
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ●
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ○

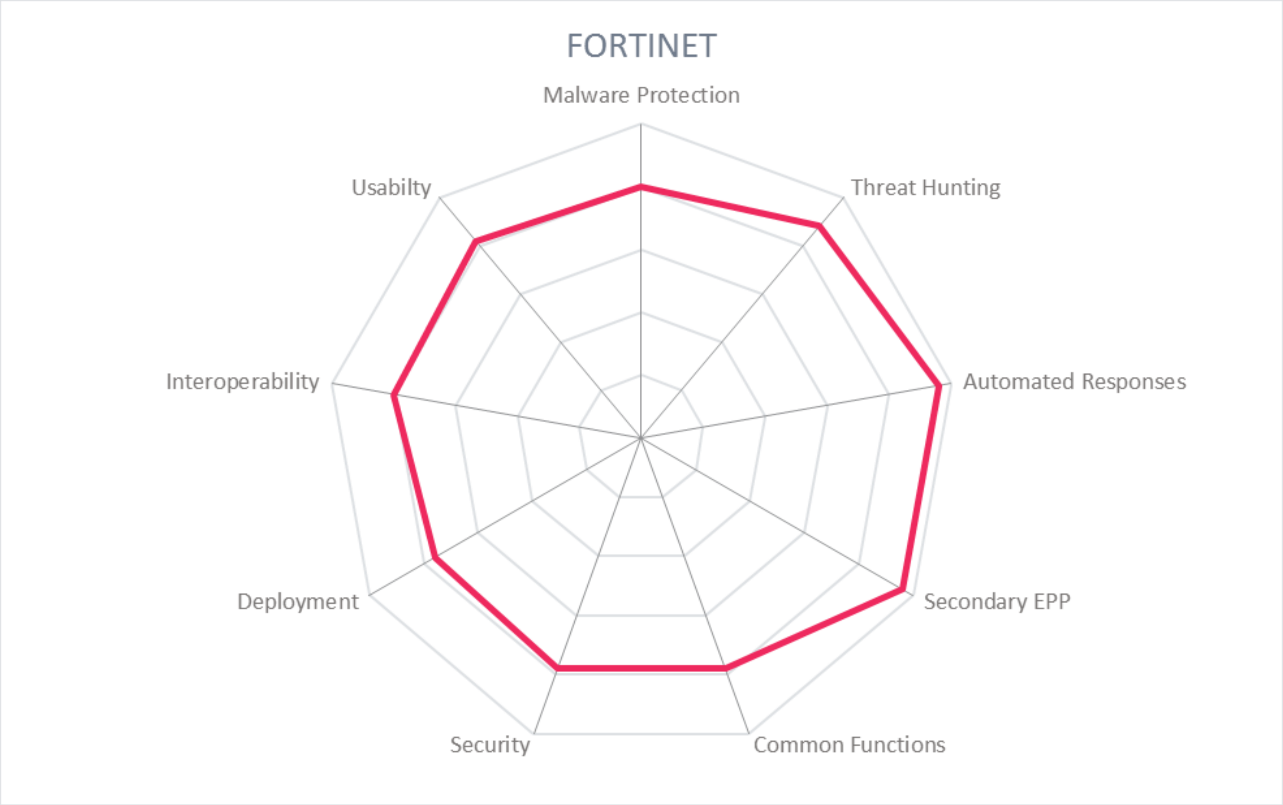
FORTINET®

Strengths

- Tightly integrated Security Fabric approach
- Advanced EDR functions
- Excellent selection of secondary EPP functions

Challenges

- More MFA options needed
- Full deployment requires multiple SKUs


FORTINET
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.9 Kaspersky

Kaspersky has been providing cybersecurity solutions for more than two decades and is best known for the EPP product. Though headquartered in Russia, Kaspersky has a global presence with transparency centers in Switzerland and Spain. In addition to Endpoint Security, Kaspersky has Network Detection and Response (NDR) and Fraud Reduction Intelligence Platform (FRIP) offerings; heir endpoint security solution, Kaspersky offers a range of cybersecurity products (cloud or on-premise), training platforms and services designed to meet the needs of customers ranging from SMBs to government agencies, global enterprises and NGOs. Their product suite covers multiple aspects of business environments: endpoint/web/mail/network/data including specialty ICS and other air-gapped networks.

Kaspersky frequently participates and does well in independent anti-malware testing regimes. Kaspersky Endpoint Security for Business (KESB) has agents for Windows 7-10, Windows Server 2008-2019, MacOS 10.9+, and a number of Linux variants. Product deployment is simple, and the KESB agent removes any other endpoint protection software during the installation. Seamless upgrades to latest product versions minimize maintenance efforts. Kaspersky's scanning engine employs multiple techniques, including signature-based scanning, pre-execution heuristics, system monitoring, real-time behavioral analysis, exploit prevention, and sandboxing. Kaspersky's sandboxing methods are the very thorough, including VM, Browser, Internet, and application emulation. Their sandbox employs anti-evasion technology, which allows it to detect sandbox-aware malware. The engine can also use micro-virtualization for the maximum separation of code from production environments. The product provides effective protection from rootkits/bootkits at the BIOS/UEFI level, and can detect and prevent polymorphism, file-less malware, and ransomware. The anti-ransomware feature is available for multiple OS platforms. The product can detect and prevent polymorphism, file-less malware, and ransomware. The anti-ransomware feature monitors for unauthorized crypto operations and attempts to delete the volume shadow copy and can automatically roll files back to a fresh state prior to malicious encryption attempts. The exploit blocking capability can also perform virtual patching in cases where devices have not been patched and may be susceptible to known vulnerabilities. It can also initiate patch updates in conjunction with configuration systems and monitor critical system files for changes.

Kaspersky EDR (KEDR) enables threat discovery with range of detection engines including their sandbox. It applies retrospective analysis with fast access to the collected data and proactive threat hunting powered by their Threat Intelligence Portal and 3rd-party sources. KEDR monitors for the full expected list of IoC types, including process, port, registry, and network activities. KEDR comes with hundreds of built-in rules to look for Indicators of Attack (IoAs), such as illegitimate use of PowerShell which is common in file-less attacks, as well as attempts to clear event logs. Customer admins can make additional entries using OpenIOC and YARA. Analysts can query across all nodes using a natural language interface and perform live memory analysis remotely. KEDR can perform recording and playback. It can execute automatic evidence collection and initial analysis aligned to MITRE ATT&CK complete with confidence levels and attribution theories. KEDR can be built into Kaspersky Anti Targeted Attack (KATA) Platform for extended detection and response (XDR) capabilities to secure multiple potential threat entry-points at both the network and endpoint levels. Automated responses options include evidence collection and rollback. Other response options require customer analysts to initiate pre-configured actions, such as node isolation, quarantining files, and process termination. KESB and KEDR support MFA using Google Authenticator, Microsoft Authenticator, and SMS OTP.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ○

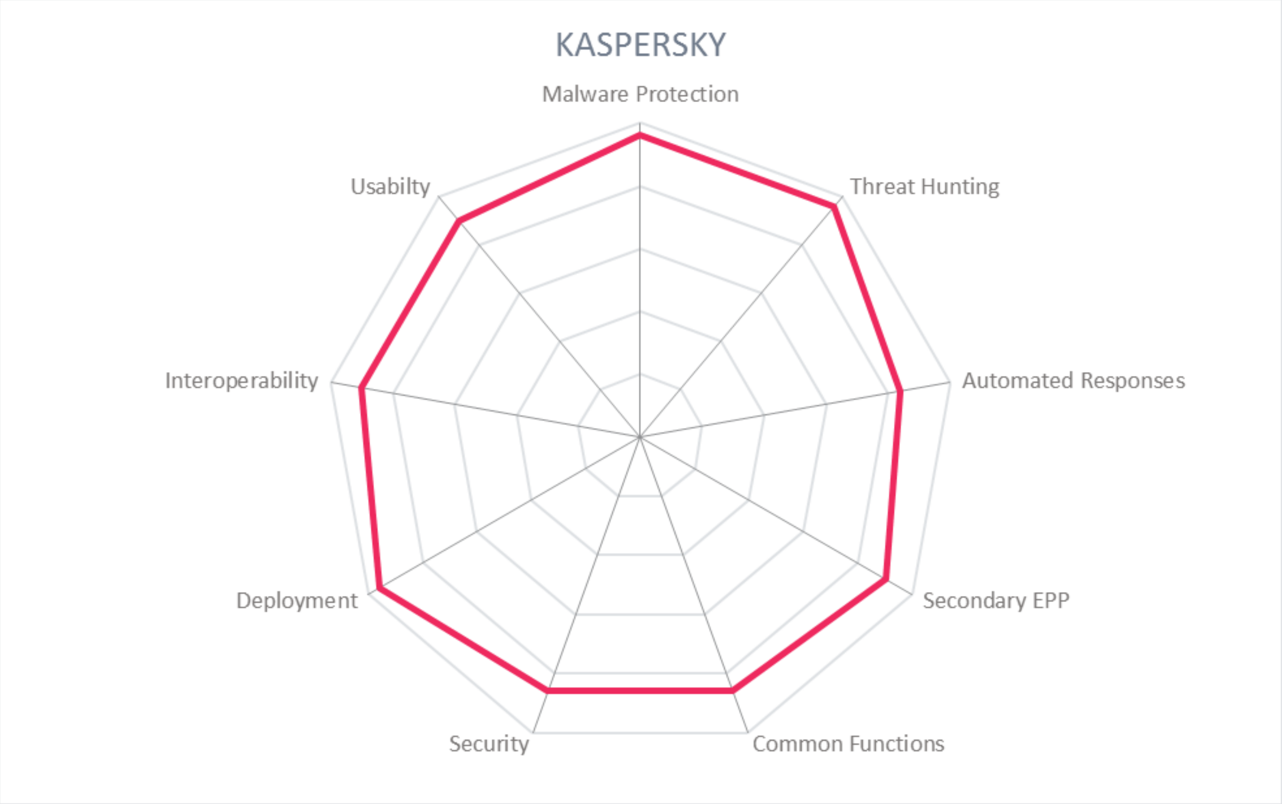
kaspersky

Strengths

- Excellent malware detection and prevention across multiple platforms
- Commitment to openness with Global Transparency Centers and full participation in independent testing
- Excellent implementation of advanced ML detection models
- Integrated patching and virtual patching protect older OSes

Challenges

- Needs SAML federation for admins
- Additional EDR automation options would be beneficial


KASPERSKY
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.10 Malwarebytes

Malwarebytes was founded in 2008 and is headquartered in Silicon Valley. They are a mid-stage venture-backed company best known for their consumer anti-virus and malware removal tools, but have been pushing into the SMB market and larger enterprises by expanding and enhancing their products with centralized management capabilities and additional features. Malwarebytes is focused on endpoint security, having added EDR and more recently MDR and IR services.

Malwarebytes has agents for Windows XP – 10, Windows Server 2008 - 2019, and MacOS 10.10+, and Linux (RHEL 7/8, CentOS 7/8, Debian 8/9, Ubuntu 16/18, and Amazon Linux 2). Their agents can co-exist with other vendors' endpoint security agents. Malwarebytes uses a variety of malware discovery techniques, including signature-based scanning, exploit prevention, memory analysis, process and file system monitoring. For example, monitoring the use of PowerShell to prevent file-less attacks; and monitoring the use of crypto APIs and attempts to delete the volume shadow copy to foil ransomware attacks. Malwarebytes has a cloud-based sandbox that supports a wide variety of environment emulations, so suspicious files are sent there for analysis, which also means internet connectivity is needed for optimal operation. The only secondary EPP function Malwarebytes supports is URL filtering.

Malwarebytes EDR product is relatively new and contains basic functionality. It doesn't ingest 3rd-party threat intelligence. It only scans for limited number of IoC types and does not allow customer admins to write their own IoC profiles or IoA rules. All telemetry is sent to the Malwarebytes cloud, but data storage is limited to a very short 2 days. Analysts can search through events on all nodes and do live memory analysis via the Flight Recorder Search feature. It does not generate root cause analysis estimates or attribution theories. Automated responses include process termination, file quarantine, script execution, node and network segment isolation, and even rollback to good state (within 72-hour range). Some limited reporting features are available. Malwarebytes was evaluated in the lastest MITRE ATT&CK, but had a high number of missed detections. Malwarebytes supports relevant standards for interoperability with other security tools. The admin console allows for 2FA and SAML federated authentication, and there are three levels of admin roles.

Security	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Malware Protection	● ● ○ ○ ○
Threat Hunting	● ● ○ ○ ○
Automated Responses	● ● ● ● ●
Secondary EPP	● ● ○ ○ ○
Common Functions	● ● ● ● ○

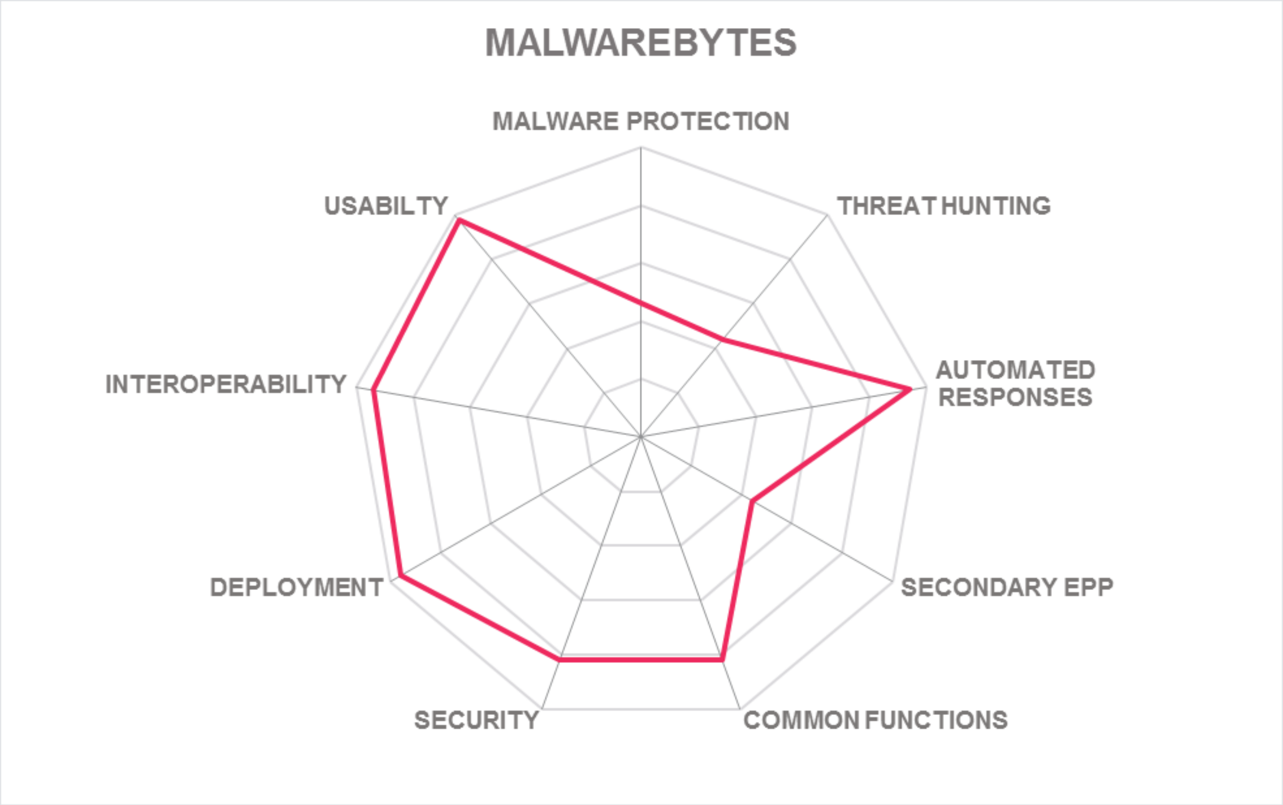
Malwarebytes

Strengths

- Easy to deploy and operate
- Excels at malware removal
- Interoperability and compatibility with other tools

Challenges

- Limited scope of detection for EDR functions
- Few secondary EPP functions
- Missing advanced features for threat hunting


MALWAREBYTES
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.11 McAfee

Silicon Valley based McAfee was an early pioneer in the anti-virus business. McAfee was founded in 1987, acquired by Intel in 2011, then spun off from Intel in early 2017. McAfee makes a full set of related products, such as DLP, Threat Intelligence, SIEM, network and email scanners, etc. Endpoints can be managed from either on-premises or cloud-based consoles. McAfee offers MDR services.

McAfee supports Windows 7 – 10, Windows Server 2008 – 2019, MacOS 10.9+, and various forms of Linux (different versions of agents are required). McAfee's detection and prevention engine uses signature-based scanning, pre-execution heuristics, system monitoring, runtime behavioral analysis, and both local and cloud-based ML detection. Dynamic application control (DAC), the local sandbox function, isolates untrusted apps and processes for analysis. The product can detect and prevent polymorphism, file-less malware, and ransomware. It is implemented at the kernel level to detect and remove rootkits. The "Advanced Threat Protection" module provides the anti-ransomware functions, is now enabled by default upon installation. It uses both major categories of techniques to identify potential ransomware: crypto API/library monitoring and filesystem monitoring. Enhanced remediation can restore files even when encrypted by ransomware. Secondary functions include URL filtering, endpoint firewall, and app control.

McAfee's EDR is backed by their excellent Global Threat Intelligence platform, which provides rich IoC information. The agent monitors processes, files, registry entries, and maps application to network communication, utilizing ML detection methods to discover anomalous traffic, and then triage and classify suspicious events. It has the ability to do recording and playback. Threat hunting and forensic analysis is available in the GUI, which integrates well with other McAfee products and leverages AI Guided Investigations. ePO (ePolicy Orchestrator) allows for automatic execution of scripts, process termination, file quarantine, evidence collection and initial analysis including mapping to MITRE ATT&CK, remote command shell operations, and complete rollbacks. McAfee participated in MITRE ATT&CK evaluations but had a high number of missed detections.

McAfee console can be integrated with Microsoft Active Directory for administrative user authentication and authorization. McAfee has also partnered with SecureAuth for additional strong and multi-factor authentication options.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Malware Protection	● ● ● ● ○
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ● ●
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ●

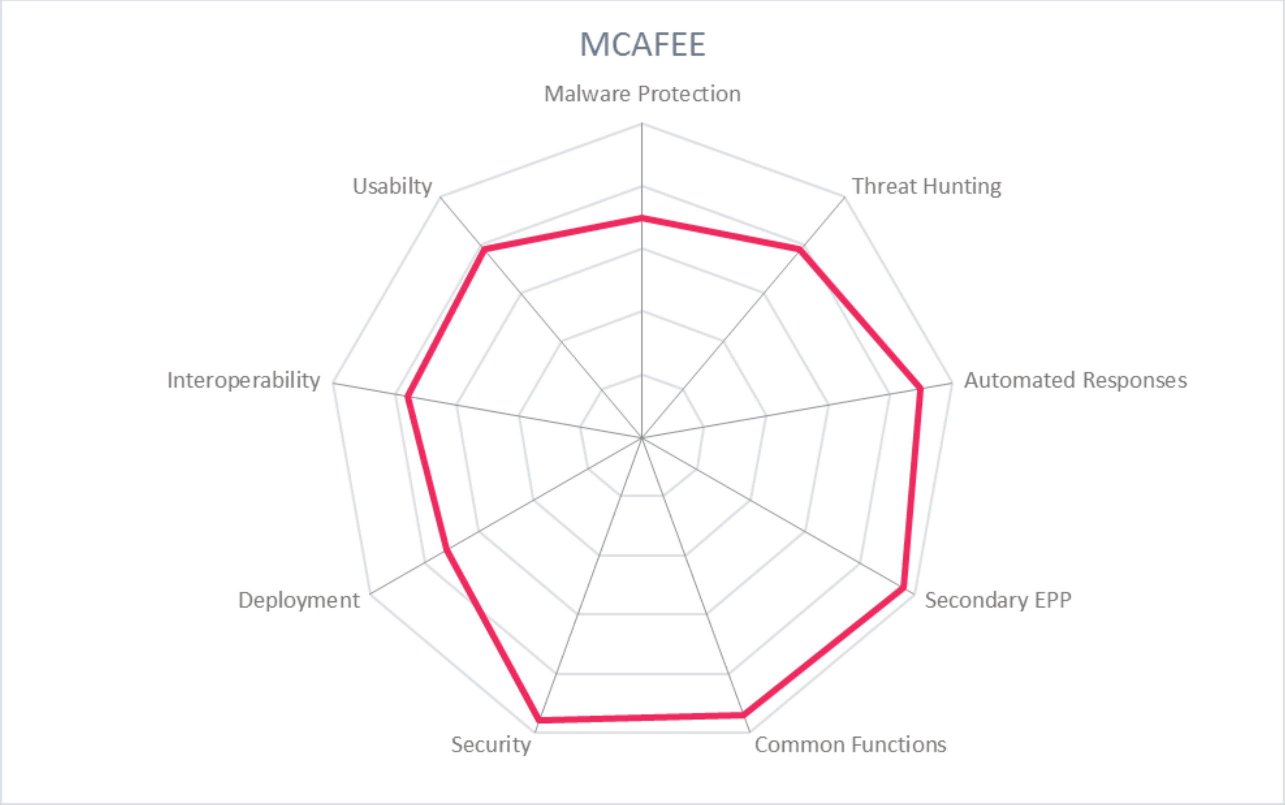
McAfee™ Together is power.

Strengths

- Leading cyber threat research publisher; Integration with McAfee Global Threat intelligence
- Intuitive console for threat hunting and forensic investigates
- 2FA/MFA to console via Windows AD or SecureAuth integration

Challenges

- May remove similar endpoint security tools
- Difficult to uninstall from Mac
- Does not use micro-virtualization for quarantining suspicious processes


MCAFEE
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.12 Microsoft

Redmond-based Microsoft began offering Defender as an anti-spyware program more than a decade ago. Defender ATP has evolved considerably since then, becoming a full endpoint security solution working in conjunction with other security functions within the Windows operating system. Defender ATP runs on Windows 7-10, Windows Server 2008R2-2019, and also has agents for Mac 10.13-10.15 and many Linux variants.

Defender ATP uses multiple detection methods, including signature-based scanning, pre-execution heuristics, runtime memory analysis, exploit prevention, local and cloud-based sandboxing. The sandbox can emulate the filesystem, full OS, browser, and applications. Windows 10 itself now provides virtualization-based security and can create separate virtual environments for applications and system processes. Microsoft has moved from content to behavior analysis; thus Defender ATP can detect and stop illegal cross-process injection techniques which are often used by file-less malware types. Unified Extensible Firmware Interface (UEFI) Secure Boot and Early Launch Anti-Malware (ELAM) technology helps prevent rootkits and kernel-level malware from loading. Defender ATP on Windows 10 along with the Edge browser are far more effective at detecting and containing malware than previous versions. MDATP has a full range of secondary EPP functions, including endpoint firewall, web filtering, threat and vulnerability management, device control, and controlled folder access. Defender ATP is compatible with many 3rd-party EPP solutions and can run in passive mode.

Defender ATP also has strong EDR capabilities, starting with a dashboard showing events, vulnerable devices, users at risk, automated investigation results, and possible actions. Defender ATP on Windows of course has access to all machine and OS level attributes to look for IoCs. Response actions available in the console include initiate automatic investigation, collect evidence, run antivirus, live remote shell, restrict app execution, isolate machine, and escalate to Microsoft threat experts. Some actions need to be manually triggered but customer admins can create triggers and customize detection models. Live Response feature supports real-time remote memory dump and analysis and examination of MFTs. Threat hunters can use Kusto Query Language (KQL) which is similar to SQL and supports regular expressions. Microsoft just launched an automated block mode, which is available for Windows 10 and Windows Server 2019. The EDR console presents a machine and event timeline view. Microsoft participated in MITRE ATT&CK evaluations and performed very well, with one of the lowest numbers for missed detections.

The enterprise console supports 2FA/MFA for administrators, including Smart Cards, mobile apps, SMS OTP, etc., via Active Directory. Fine-grained access controls and delegated administration models are also possible. The console can integrate with a variety of SIEM tools.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ○
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ●

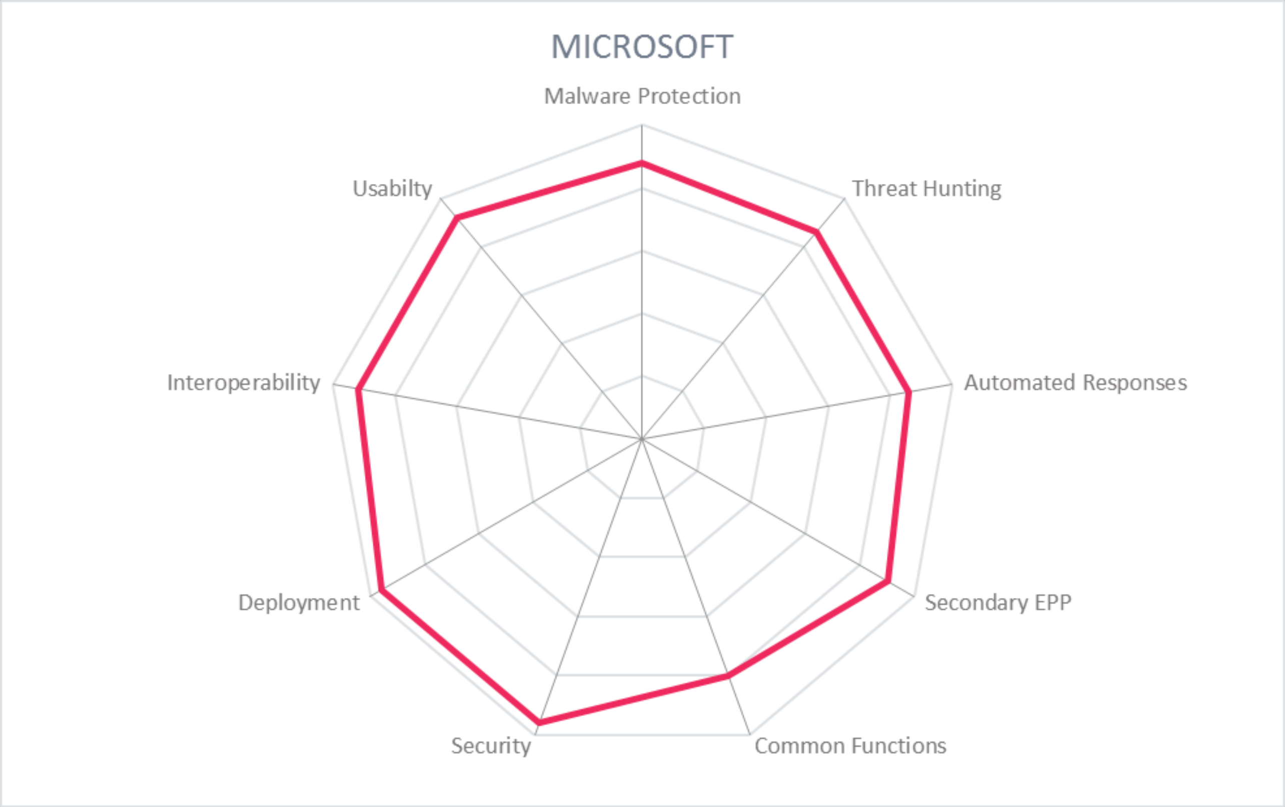
Microsoft

Strengths

- EPP & EDR built into the OS
- Compatible with 3rd-party tools
- Easily managed in Microsoft utilities
- Excellent admin MFA options
- Good selection of response actions
- SQL-like query interface for threat hunting supports RegExp
- High EDR detection rate in MITRE ATT&CK evaluations
- Informed by Microsoft’s expert Threat Intelligence program
- Cooperation with 3rd-party threat intel sources

Challenges

- Mac and Linux versions are somewhat less capable
- Anti-malware functions are most effective on Windows 10
- Automated block mode only works on latest OS versions


MICROSOFT
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.13 Palo Alto Networks

Palo Alto Networks was founded in 2005 in Santa Clara, CA. It has become a leading network security vendor. First known for their Next Generation Firewall, Palo Alto has developed many other cybersecurity products, including solutions for endpoint, cloud, and SOAR (formerly Demisto).

Palo Alto’s EPP solution was originally called Traps, but is now combined with Cortex XDR, their detection and response product, into a single agent with a single admin GUI. They have agents for Windows 7 – 10, Windows Server 2008 – 2019, MacOS 10.13 – 10.15, Android, and Debian/RHEL/SUSE/Ubuntu Linux. Palo Alto utilizes multiple methods for malware prevention, including ML-enhanced static file analysis, behavioral analysis, exploit prevention, anti-evasion sandboxing, and bare-metal analysis for sandbox resistant malware. Palo Alto deploys decoy files as part of its broad ransomware detection and prevention strategy: when attempts are made to encrypt decoy files, the offending process is shut down. Palo Alto’s endpoint agent relies on WildFire, their high-quality cloud-based cyber threat intelligence service. Disk encryption, endpoint firewall, app control, USB device control, system file integrity monitoring, and vulnerability assessment/management comprise the long list of secondary EPP functions provided. Recent independent testing has been limited to NSS Labs, but they have plans to work with other independent testers in the future.

Cortex XDR monitors endpoint filesystems, applications, network activities, registry, and processes. Telemetry from agents is sent to Cortex Data Lake in the cloud for analysis. Information can also be collected from Palo Alto cloud solutions (Prisma), which provide coverage for AWS, Azure, and Google Cloud. When suspicious events are detected, agents alert the console and can take a variety of actions such as quarantine or delete files, terminate processes, restrict device communications, retrieve files for forensic investigations, execute Python scripts, and interact with other security tools via APIs, such as SOAR. Palo Alto runs Cortex XDR console as SaaS for clients and has received SOC 2 Type II Plus certification. Palo Alto participated in MITRE ATT&CK evaluations and performed very well, with one of the lowest numbers for missed detections.

Palo Alto is a charter member of Cyber Threat Alliance. All functions are exposed via APIs and all console actions are scriptable. Cortex XDR supports fine-grained authorization for admin. Palo Alto supports a large number of strong authentication options including biometrics and smart cards, as well as SAML for federation.

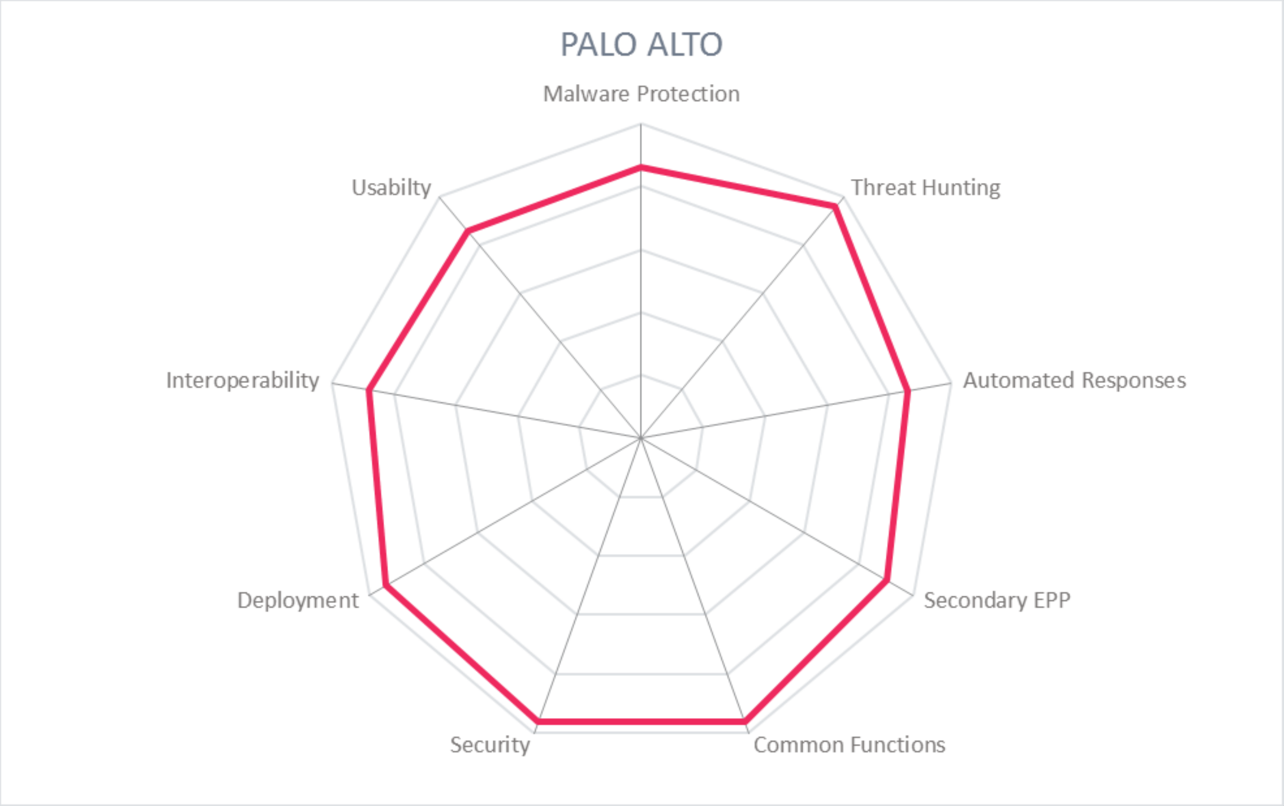
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ○
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ●

Strengths

- Support for cloud workloads
- Excellent product security with strong MFA options
- Next generation “XDR” architecture
- High-quality built-in threat intel
- Excellent detection rate in MITRE ATT&CK evaluations

Challenges

- Complex deployment and licensing models
- Few recent independent malware tests
- No application control functions


PALO ALTO
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.14 SentinelOne

Sentinel One, founded in 2013, is an endpoint security vendor headquartered in Mountain View, CA. The company is a privately held, late stage “unicorn” with a valuation over $1.1B. The company’s strategic vision is an integrated endpoint security platform to replace multiple types of endpoint and network security tools with a single solution to prevent, detect, analyze and respond to cyberthreats across all enterprise IT assets, on-premises and in the cloud.

Sentinel One has agents for Windows, including legacy versions of Windows, MacOS, and most Linux variants. Sentinel One uses advanced ML techniques for static file analysis instead of signatures. The agent monitors all processes and associated memory spaces by direct injection via asynchronous procedure calls into all running processes. This approach allows Sentinel One to detect and stop many forms of malware, including file-less and polymorphic malware. The solution does not use sandboxing for runtime evaluation or micro-virtualization for investigative isolation. The kernel mode agent can detect and block rootkits. To protect against ransomware, Sentinel One looks for typical ransomware methods such as large numbers of crypto calls, reads/copy-on-writes, mass file extension changes and attempts to delete volume shadow copies. Sentinel One offers a warranty in the highly unlikely event that a protected Windows endpoint should be compromised by ransomware.

Sentinel One’s patented Storyline technology assigns unique but consistent identifiers to each recorded event. This allows analysts to reconstruct the original sequence of events and relationships between the affected processes and artifacts. A full attack storyline can be visualized, helping the forensic experts to trace to its root cause and determine the necessary mitigation actions. The platform provides a full-featured search engine to enable proactive threat hunting. Using the Storyline ID of any file, network activity, or an indicator of compromise, analysts can look for specific potential threats or set up triggers to get notified about future detections. A full range of response actions are possible, including node isolation, process termination, all the way to roll back to pre-infection state. Sentinel One participated in MITRE ATT&CK evaluations and performed very well, with the lowest numbers for missed detections.

Sentinel One supports CEF for communication with SIEMs. The platform can receive threat intelligence in STIX and OpenIOC formats. Singularity Platform supports a number of integrations with 3rd-party security tools. Currently, over 15 integrations are offered for vendors like Splunk, Okta, or Tanium, in addition to a general SIEM connector. The console allows role-based administration, as well as 2FA for administrators with Duo Security or Google Authenticator. Sentinel One Ranger turns endpoint agents into NDR sensors, allowing adjacent endpoints to map and monitor networks, such as IoT networks. This is a move toward “XDR”, or the fusion of EDR and NDR.

SentinelOne™

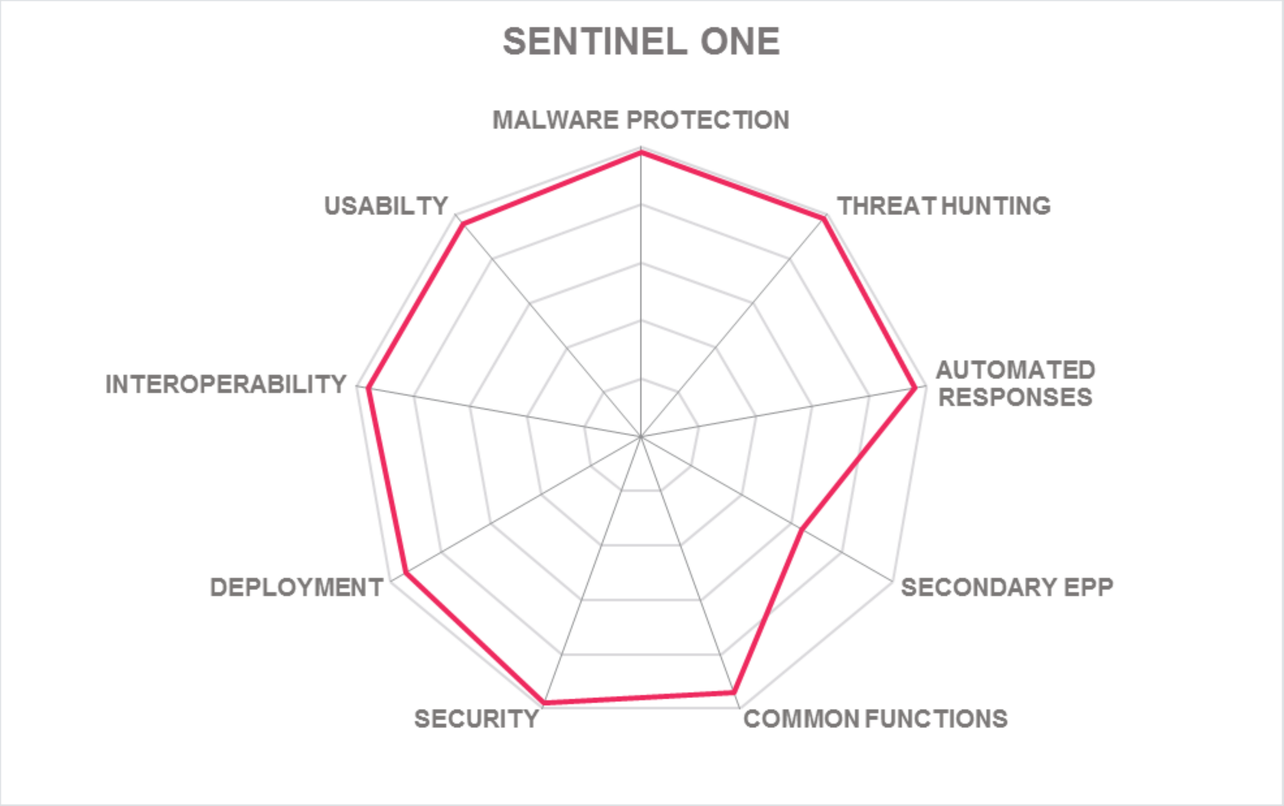
Security	●	●	●	●	●
Interoperability	●	●	●	●	●
Usability	●	●	●	●	●
Deployment	●	●	●	●	●
Malware Protection	●	●	●	●	●
Threat Hunting	●	●	●	●	●
Automated Responses	●	●	●	●	●
Secondary EPP	●	●	●	○	○
Common Functions	●	●	●	●	●

Strengths

- Fully integrated security platform with a single universal endpoint agent
- Support for Windows, Mac and Linux platforms, virtualized devices, cloud workloads and IoT devices
- Fully autonomous endpoint protection using multiple ML detection engines
- Ransomware warranty for Windows users
- MFA and SAML for admin users
- Best performance in MITRE ATT&CK round 2 evaluations

Challenges

- Does not have some secondary EPP functions, such as app control
- Does not use sandbox or micro-virtualization


SENTINEL ONE
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.15 Sophos

UK-headquartered Sophos was founded in 1985 and was acquired by Thoma Bravo in 2019. Sophos is centered squarely in the cybersecurity market, with a strong focus on the endpoint. Sophos also offers solutions for encryption, Unified Threat Management, cloud security, firewalls, and email and web gateways. Sophos regularly participates in multiple independent malware testing regimes. The company offers managed threat detection services.

InterceptX has agents for Windows 7 – 10, Windows Server 2008R2+, MacOS 10.12+, Android, and iOS. InterceptX uses advanced ML and Deep Learning detection models, behavioral analysis components to stop unknown ransomware (CryptoGuard) and destructive disk and boot-record attacks (WipeGuard), exploit prevention, and memory analysis that can detect file-less malware. InterceptX core functionality includes strong malware removal capabilities and forensic root cause analysis. Sophos regularly participates in independent tests for detecting malware, and consistently scores very well.

Sophos InterceptX Advanced contains EDR but it is not available as a separate product. LiveDiscover within InterceptX allows IT admins and security analysts to perform live queries against endpoint data repositories using SQL. This novel approach makes it easier for SMBs without dedicated threat hunters to perform useful threat hunts. Similarly, LiveResponse allows security teams to execute actions remotely using a CLI. Remediations available include process termination, remote reboot, script execution, evidence collection, and remote installation/uninstallation of software. Intercept X Advanced is designed to replicate the tasks normally performed by human analysts to enable organizations to tap into threat analysis expertise based on ML and threat intelligence from SophosLabs. Sophos has not participated in MITRE ATT&CK evaluations but is included in the next round in 2H2020.

Sophos is an affiliate member of Cyber Threat Alliance. The product has good internal security, and admins can be required to use Google Authenticator or Sophos Authenticator for 2FA.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ○ ○
Common Functions	● ● ● ● ○

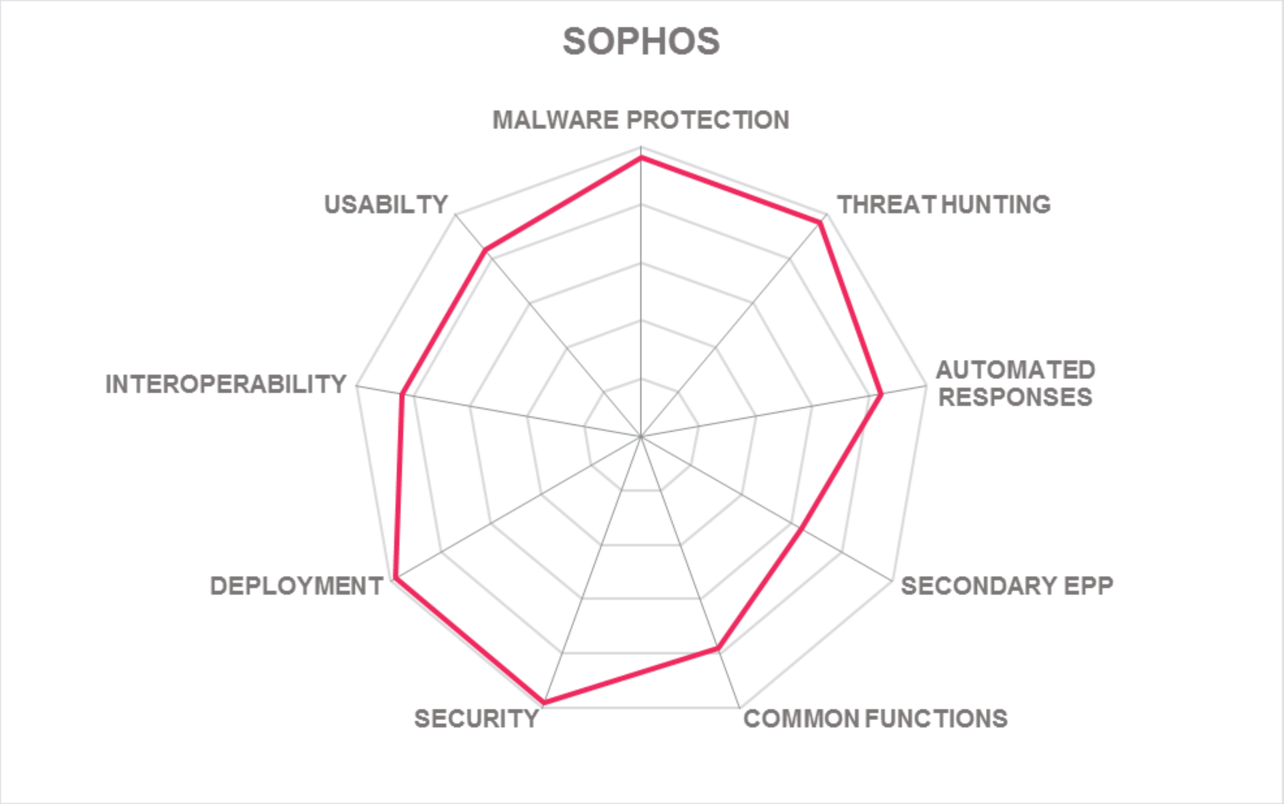
SOPHOS

Strengths

- DL-based malware detection with consistently strong results in independent product testing
- Focus on detecting and blocking exploit tools and techniques
- Anti-ransomware capability based on behavioral analysis
- LiveDiscover SQL query interface simplifies threat hunting
- Integrated EDR capabilities and Managed Threat Management services available

Challenges

- Limited secondary EPP functions
- Additional MFA options would be beneficial


SOPHOS
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.16 Symantec

Mountain View-based Symantec provides a comprehensive set of security tools. Symantec was recently acquired by Broadcom, which is maintaining the Symantec brand. Symantec Endpoint Security Complete (SESC) comes in several editions, and includes Symantec Endpoint Protection (SEP) product, which covers all versions of Windows, Mac OS, Red Hat and Suse Linux, IaaS environments, and VDIs. Symantec has a wide range of security products for enterprise through SMB markets, including Active Directory defense, application controls, CASB, etc., and they offer MDR services.

Symantec utilizes several methods to detect, prevent, and remove malware: pre-execution scanning using ML detection models, sandbox/environment emulator, and micro-virtualization. Symantec can detect polymorphism via ML detection models and uses behavior analysis to thwart file-less malware. Rootkits and botnet infections can be detected by Early Launch Anti-Malware (ELAM) system, a kernel driver component that performs static analysis, behavioral analysis, and monitoring for C2 activity. Static analysis, exploit prevention, and file system monitoring are used to detect and stop ransomware. SEP is tightly integrated with Symantec forensic tools for more efficient investigations.

Symantec Endpoint Security Complete includes EDR, and it is housed in the same agent and cloud console. Symantec has high quality threat intelligence and IoC sources, so all its downstream products benefit from that. Symantec EDR allows for continuous recording for later analysis. Their EDR contains all the features one would expect in a mature product, including looking for registry changes, process injections, lateral movement, app-to-network activity analysis, etc. Threat hunters will find a lot of functionality and automation available for their tasks. It also supports some automated responses and remediation such as quarantining, blacklisting, blocking, remote shell and evidence collection. It includes expert analysis of critical EDR incidents generated by Machine Learning. It is aligned with MITRE ATT&CK, and Symantec has performed well in MITRE ATT&CK evaluations.

CAC cards, Kerberos, LDAP, Microsoft Azure AD, and RADIUS are available for strong authentication. It supports SAML for federation. It can use 3rd-party PAMs to lockdown admin or service accounts. Role-based and delegated administration are supported. Symantec has a unique Data Access Control feature which a master admin to define which categories of data within the solution are visible to lower-level admins.

Symantec

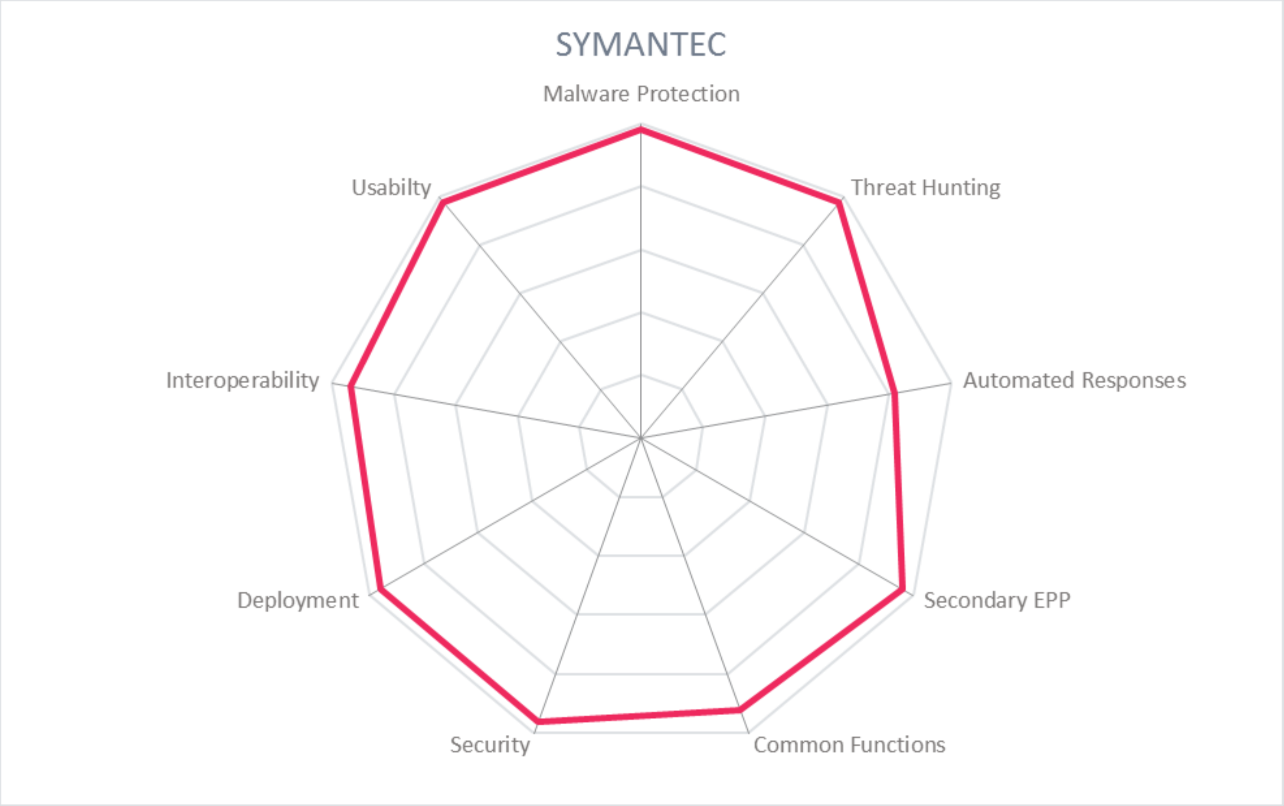
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ● ○
Secondary EPP	● ● ● ● ●
Common Functions	● ● ● ● ●

Strengths

- Full array of malware detection techniques, including sandboxing and micro-virtualization
- Consistently good results in independent tests
- High detection rate in MITRE ATT&CK evaluation
- Large global customer and support base
- Agents for many types of endpoints
- Excellent built-in threat intelligence service and IoC sources

Challenges

- Comprehensive but complex product
- Multiple management consoles
- More advanced automated response options needed


SYMANTEC
Malware Protection
Threat Hunting
Automated Responses
Secondary EPP
Common Functions
Security
Deployment
Interoperability
Usabilty

5.17 VMware

In 2019, Carbon Black was acquired by VMware. VMware Carbon Black has a strong emphasis on cloud-based EPP and EDR, and the ability to protect virtualized environments. VMware Carbon Black also offers MDR.

Endpoint Standard employs both pre-execution and runtime malware prevention. Before execution, it performs signature-based scanning, YARA rules evaluation, and file/process reputation analysis. Runtime protection is based on ongoing behavioral analysis of all running processes against historical patterns. It constantly risk-scores all activities and can terminate processes if suspicious. It can detect and prevent polymorphic, JIT, and file-less malware. New or unknown applications can be quarantined automatically until they become trusted. Agents are available for Windows XP – 10, MacOS 10.12 – 10.15, Red Hat Enterprise Linux, Oracle Linux, CentOS, and ESX. Azure, AWS, and GCP are supported as well.

EDR functionality is bundled in the EPP agent. Agents are managed from the cloud. Though their cloud service is multi-tenant, VMware Carbon Black allows customers to create and manage their own encryption keys. It has advanced threat hunting features, alert verification, automated evidence collection, and forensic analysis. Enterprise EDR also allows automated responses such as host isolation and VM suspension/termination.

vmware®

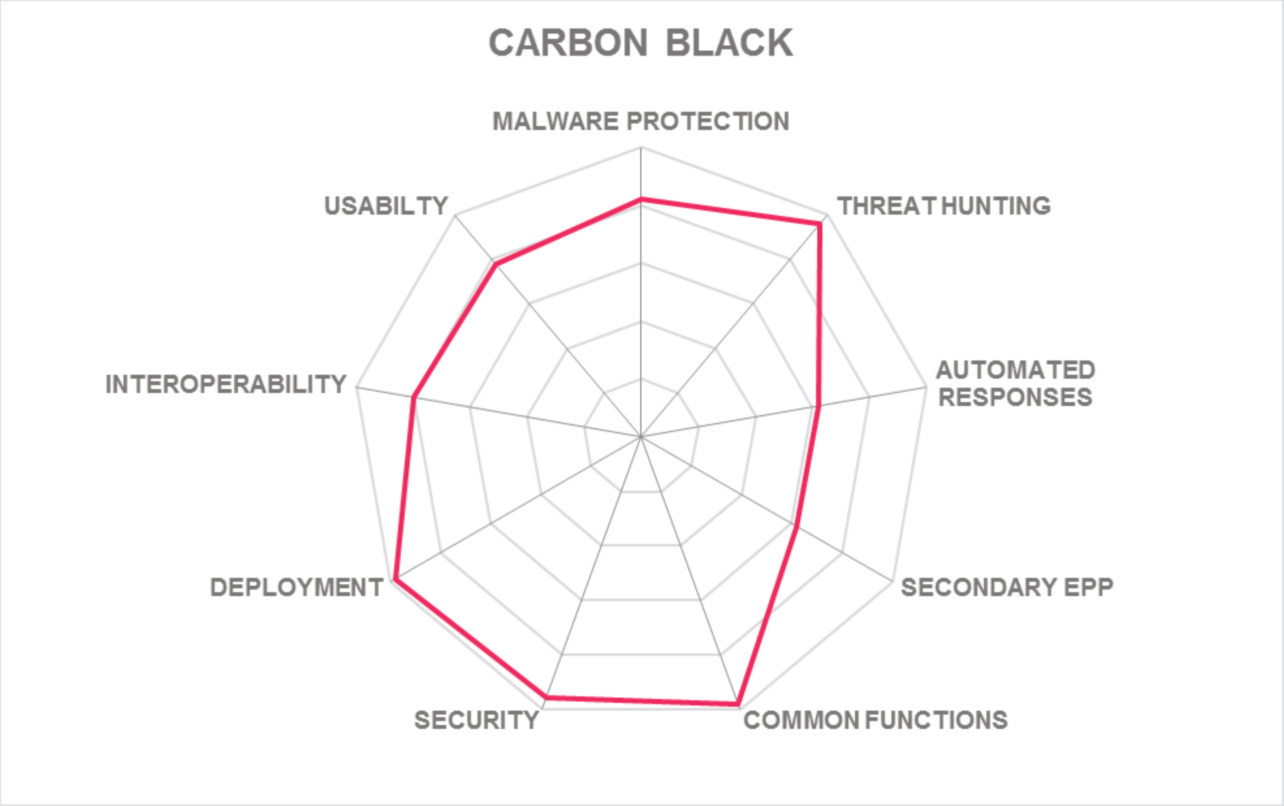
Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Malware Protection	● ● ● ● ●
Threat Hunting	● ● ● ● ●
Automated Responses	● ● ● ○ ○
Secondary EPP	● ● ● ○ ○
Common Functions	● ● ● ● ●

Strengths

- Some 2FA options for administrators
- Interoperable with many other agent-based security tools
- Advanced behavioral analysis techniques
- Auto-quarantine of untrusted apps

Challenges

- Cloud-based console only, which may be limiting for some customers
- More automated response options needed


CARBON BLACK
MALWARE PROTECTION
THREAT HUNTING
AUTOMATED RESPONSES
SECONDARY EPP
COMMON FUNCTIONS
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

6 Related Research

Leadership Compass 80126 Network Detection and Response (NDR)
Leadership Compass 71172 Endpoint Security: Anti-Malware Solutions
Leadership Brief 80187 Do I Need Endpoint Detection & Response (EDR)
Leadership Brief 80186 The Differences Between EPP and EDR
Advisory Note 80110 Buyer's Compass Endpoint Protection
Advisory Note 80213 Buyer's Compass Endpoint Detection & Response (EDR)

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based only on the information provided within this report.

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Ease of Delivery
- Interoperability
- Usability

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

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

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

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

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

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

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

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are

- **Strong positive**
  Outstanding support for the subject area, e.g. product functionality, or security etc.)
- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren’t met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Figure 1: Trend Compass

Figure 2: Featured for EPP Capabilities

Figure 3: Featured for EPDR Capabilities

Figure 4: Featured for EPP Innovation

Figure 5: Featured for EPDR Innvoation

Figure 6: Featured for EDR Innovation

Figure 7: Featured for XDR Innovation

Figure 8: Featured for EPDR Universal Coverage

Figure 9: Featured for Threat Intelligence Integration

Figure 10: Featured for Threat Intelligence Integration

Copyright

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

For further information, please contact clients@kuppingercole.com.