Critical Capabilities for Endpoint Protection Platforms

Published 31 December 2022 - ID G00752297 - 39 min read

By Chris Silva, Peter Firstbrook

Initiatives: Infrastructure Security

This report focuses on EPPs' prevention, protection and detection capabilities. It will help you assess offerings' suitability for the use cases of mature and aggressive (Type A) organizations, mainstream (Type B) organizations, and the least mature and aggressive (Type C) organizations.

Overview

Key Findings

- The top buying priorities in the endpoint protection platform (EPP) market remain ease of use, prevention, and endpoint detection and response (EDR).
- Managed services are essential for successful detection of, and response to, modern "human-driven" attacks. Fully managed services are now core offerings for most vendors.
- Cloud adoption is now mainstream, with most organizations abandoning on-premises infrastructure in favor of better operational efficiency.
- EDR capability is integral to an EPP. It is beginning to evolve into extended detection and response (XDR) with the integration of additional sources of information and orchestrated responses across multiple security tools.

Recommendations

Security and risk management leaders responsible for endpoint protection who need to evaluate incumbent solutions to ensure they keep up with the rapidly changing EPP market should:

- Assess products' fitness for the existing environment, with a focus on operating systems (OSs) and deployment requirements, rather than individual features, so as to create a manageable list of EPPs to evaluate.

- Maintain operational efficiency by testing their team's ability to maintain and continually tune their EPP with existing skills and staff. Any possibility that an internal security operations center (SOC) would need to monitor the EPP should prompt a discussion about how managed services may help share the operational burden.

- Adjust the critical capability weightings in the interactive version of this report to suit your organizational model.

Strategic Planning Assumptions

By the end of 2025, 80% of Type C organizations using endpoint detection and response (EDR) capabilities will use managed detection and response (MDR) capabilities.

By the end of 2025, more than 50% of Type B organizations will consolidate EDR into a preferred vendor portfolio of security investments for more efficient security operations.

By the end of 2026, 80% of Type A organizations will be consuming EDR as part of a multitool extended detection and response (XDR) architecture.

What You Need to Know

EPPs continue to transform from basic anti-malware protection offerings into fully fledged EDR products. This transformation and the rise of sophisticated, targeted attacks, such as human-operated ransomware, means that management, monitoring and automation are now crucial.

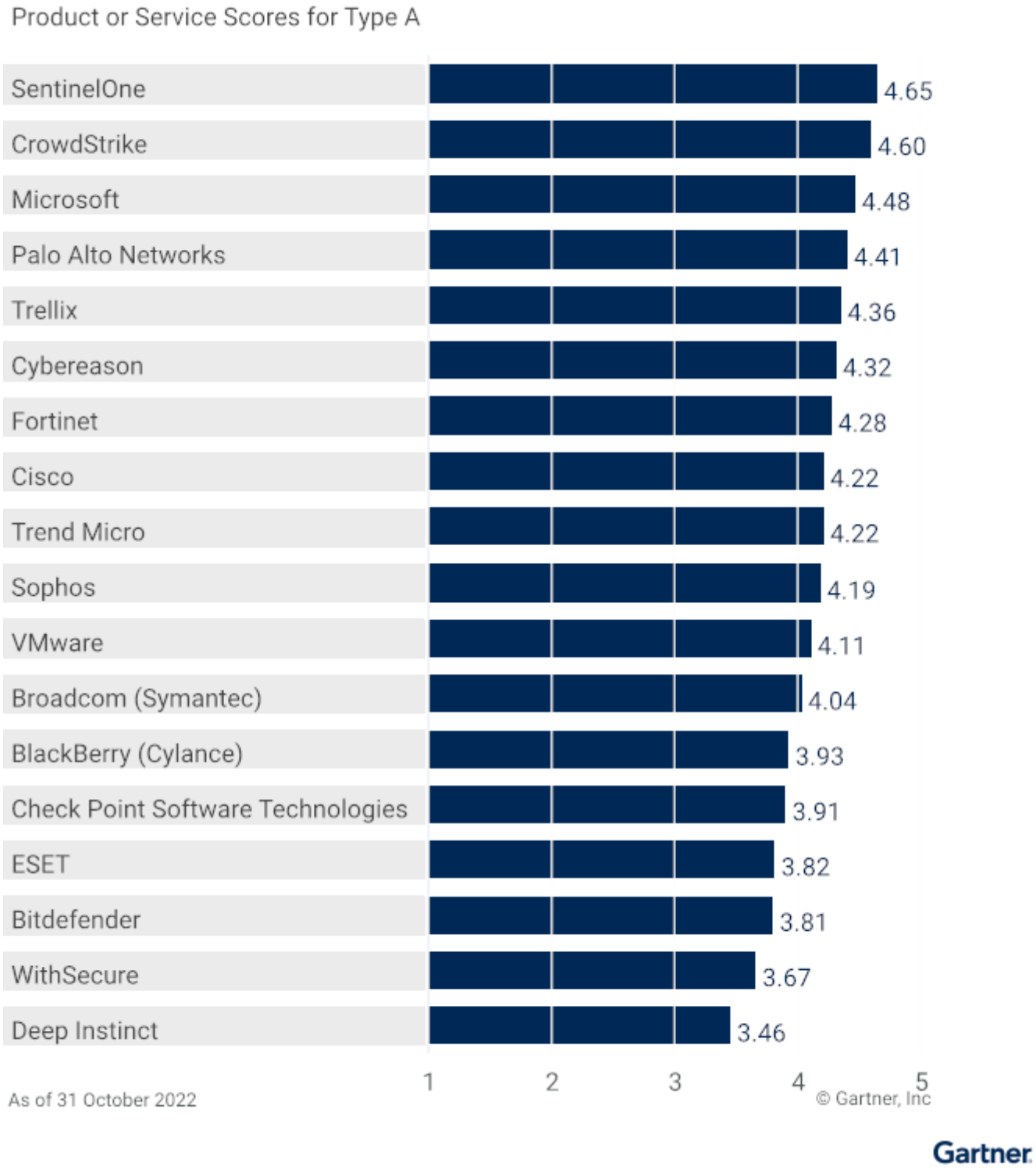
Most customer organizations have now embraced cloud-delivered EPPs, with only those in a few highly regulated industries and regions still prioritizing on-premises solutions. Vendors are also investing heavily in cloud-based, rather than on-premises, solutions, and some no longer support or develop any on-premises EPP feature enhancements. Organizations that are only now transitioning to SaaS solutions should consider the capacity to expand skills into new areas, such as detection, that on-premises, protection-focused tools lack.

This Critical Capabilities report evaluates vendors' offerings suitability for the organizational models of three distinct types of organization: Type A, Type B and Type C (for definitions, see Note 1).

Analysis

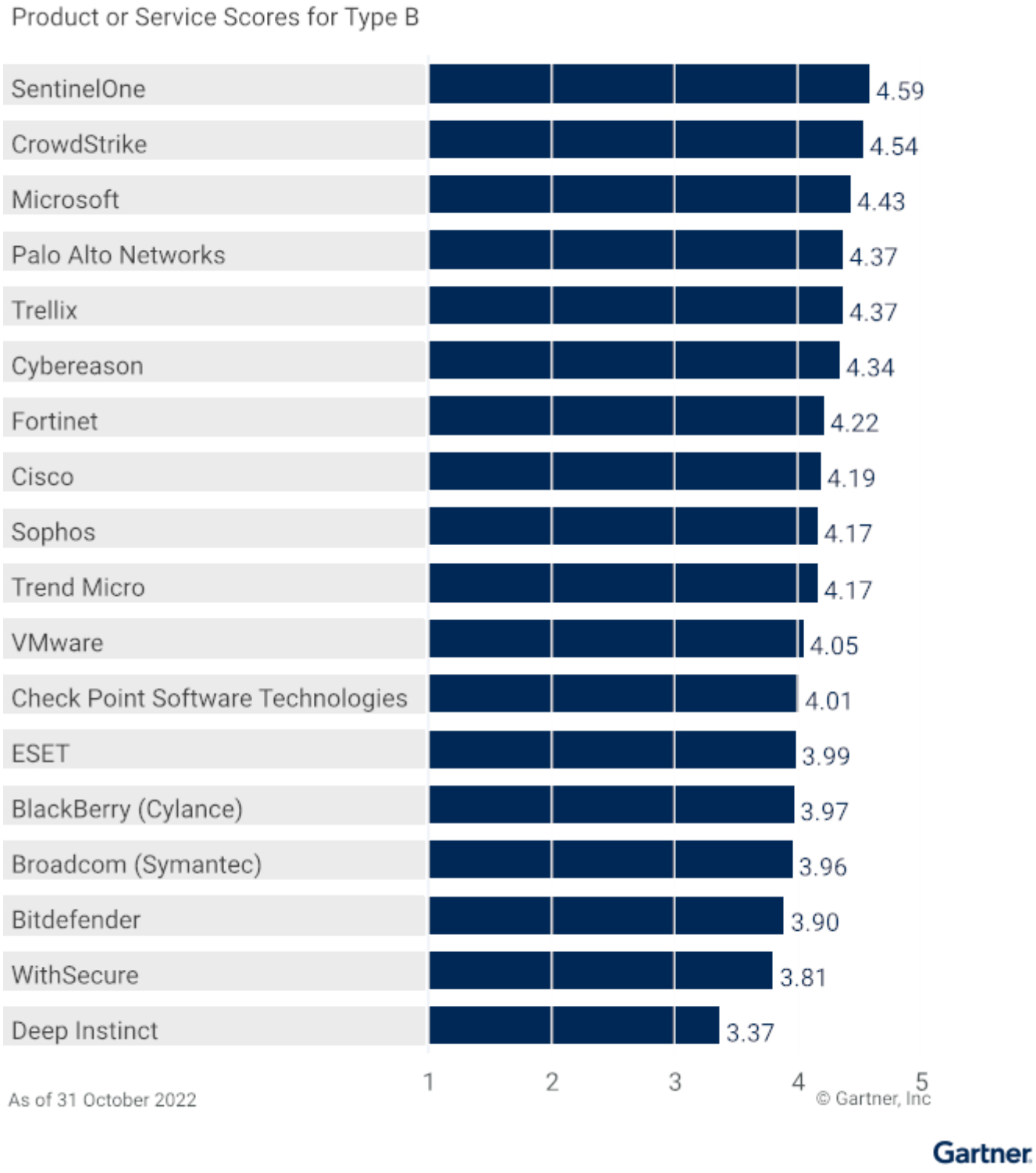
Critical Capabilities Use-Case Graphics

Vendors' Product Scores for Type A Use Case



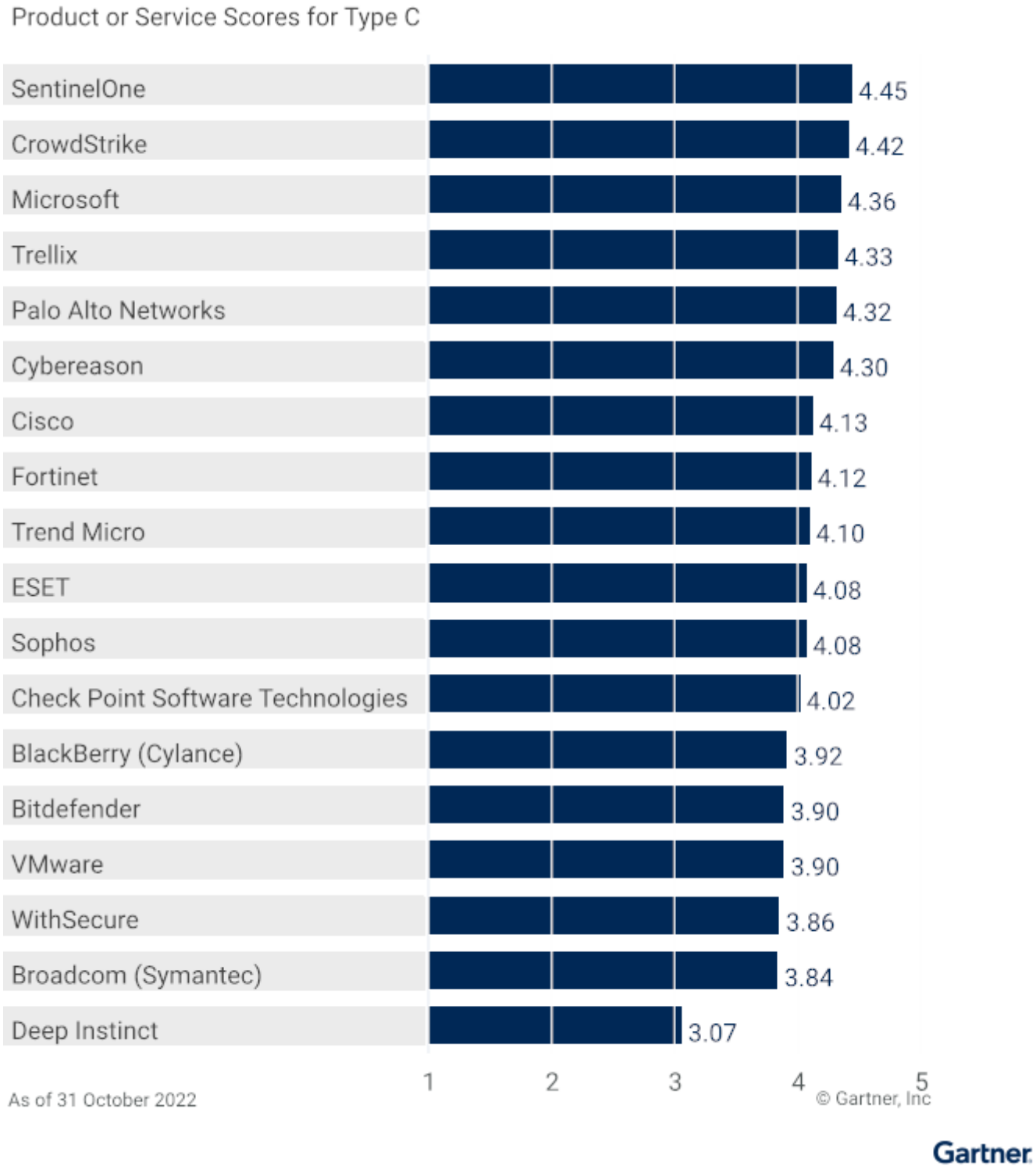
Source: Gartner (December 2022)

Vendors' Product Scores for Type B Use Case



Source: Gartner (December 2022)

Vendors' Product Scores for Type C Use Case



Source: Gartner (December 2022)

Vendors

Bitdefender

Bitdefender's GravityZone EDR offering is best suited to Type B and Type C organizations in North America and EMEA that want a single solution with effective, easy-to-use protection capabilities.

Bitdefender has a strong threat intelligence capability backed by its own lab and third-party intelligence. Bitdefender is consistently a top performer in file-based and fileless malware protection

tests. Its feature set combines endpoint management and patching, which improves visibility into existing endpoint posture compliance. These capabilities can help to improve security hygiene. Bitdefender also provides full-disk encryption, web content filtering and device control, offering complementary products to address related endpoint security functions. Bitdefender recently launched GravityZone XDR, which integrates Microsoft Office and Active Directory telemetry to contribute to detection logic and incident response.

BlackBerry (Cylance)

BlackBerry (Cylance) is suitable for Type B organizations' use cases, as well as for Type A and Type C organizations converging endpoint security, managed services, and endpoint and identity management.

BlackBerry continues to invest in and evolve its managed detection and response (MDR) services under its CylanceGuard branding. It has expanded its XDR capability through a partnership with Exabeam, a security information and event management (SIEM) vendor.

BlackBerry's unification of EPP, EDR and managed threat detection (MTD) solutions in its Unified Endpoint Security bundle offers a single platform for multiple functions with a sliding scale of managed service offerings. This combination also makes it a good option for Type B and Type C organizations looking for cloud-managed capabilities that have a low performance impact and work well offline.

Broadcom (Symantec)

Broadcom (Symantec)'s Symantec Endpoint Security Complete (SESC) is suitable for Type A and Type B organizations, especially those looking to consolidate endpoint management and security tools.

SESC delivers protection and EDR capabilities in a single agent and supports fully cloud-based and hybrid deployments. Recent improvements include Adaptive Protection, which provides policy-based execution restrictions for commonly attacked utility applications (such as Microsoft PowerShell). Symantec has a broad range of security tools and offers enterprise agreements that can lower the total cost of ownership and provide common management and integration opportunities. It also has a strong threat analysis capability through its labs, which produce actionable global threat intelligence to assist SOC teams.

Broadcom announced its intention to acquire VMware, which owns CarbonBlack, on 26 May 2022. At the time of evaluation, however, both Broadcom (Symantec) and VMware met the inclusion criteria for this Critical Capabilities report and continued to operate as separate entities. Gartner will provide further insight as more detail becomes available about the future roadmap for these vendors' existing portfolios.

Check Point Software Technologies

Check Point Software Technologies' highest use-case score is for Type C organizations. It is suitable for Type C organizations seeking an EPP that is simple to deploy and maintain and that offers good support for all OS and device types.

Check Point has a long history in the EPP and network security market. The recent acquisition of Avanan provided new email and cloud access security broker (CASB) security capabilities. The Check Point Harmony Endpoint provides EPP and EDR in a single agent, which is supported by a broad range of OSs. Check Point launched its Horizon XDR/MDR combined offering in September 2022. The Horizon XDR component is not evaluated in this Critical Capabilities report because it was not generally available in time.

Although the Harmony Endpoint can stand alone, it delivers most value when integrated with other Check Point products. It can integrate with Check Point Infinity to share intelligence and provide a single point of management for Check Point's endpoint, mobile, Internet of Things (IoT), network, email, data, and cloud security solutions.

Cisco

Cisco's highest scores with its Secure Endpoint product are for Type A and Type B organizations' use cases. It is suitable for Type A and B organizations that want to consolidate network and endpoint security products and improve their security operations.

Cisco SecureX, a cloud-native XDR platform, is included at no additional cost to Cisco customers. It provides XDR capabilities across multiple Cisco security products, including endpoint, network, cloud, email and identity products, and integrates with third-party log data sources. SecureX also enables rapid sharing of threat intelligence from the Cisco Talos Intelligence Group and local detections. Cisco's aspirations to deliver an integrated security operations experience are slightly ahead of its execution, so customers should anticipate continuing maturation.

Cisco has strong global operations, training opportunities, and support and services. Enterprise licensing opportunities can provide attractive pricing for organizations looking to optimize spending.

CrowdStrike

CrowdStrike scores consistently well for all use cases, which indicates appropriateness for all three types of organizations. It scores especially well for the Type A use case, where buyers focus on feature completeness.

Additions to CrowdStrike's Falcon Platform in 2021 and 2022 have focused on zero trust identity analytics; enrichment of file integrity monitoring functions; expansion of managed services offerings; and improvements to modules for device control, firewall management, vulnerability management and patching.

CrowdStrike has also recently established the CrowdXDR Alliance, which offers deep, out-of-the-box integrations with participating partners' products, and a community edition of Humio for a broader

range of security vendors to use. CrowdStrike's clients are predominantly in North America and EMEA. Its products suit all three use cases, with managed service options to suit all organizations. The fully managed Falcon Complete product suits organizations that do not have their own security operations teams.

Cybereason

Cybereason scores consistently well for the Type A, Type B and Type C use cases. It is suitable for a broad range of organizations of different types, sizes and levels of maturity.

Cybereason's EDR capability collects a broad stream of endpoint telemetry and preprocesses it locally to detect cross-device malware operations. Cybereason offers broad platform coverage in its tool, with integrations to third-party tools for richer threat intelligence. Cybereason extends its visibility into other platforms addressed by its tool (such as mobile platforms) and can enhance it using threat intelligence generated by its managed services activities. Type C organizations will benefit from multiple managed service offerings, ranging from monitoring and triage to full response, reporting, and proactive hunting.

Additionally, the integration of Cybereason's platform with Google Cloud's SIEM and security orchestration, automation and response (SOAR) products will attract some buyers, as will Cybereason's investments in infrastructure and operations to address government customers.

Deep Instinct

Deep Instinct scores fairly consistently across all three use cases. It is appropriate for buyers seeking a solution with strong prevention capabilities but without advanced detection capabilities.

Deep Instinct focuses on providing effective prevention against unknown malware and fileless attacks. It takes a deep-learning approach that reduces the need for feature engineering and model updates by humans. It does not rely on cloud-based threat intelligence for signature databases or known indicators of compromise (IOCs), which enables its agent to work effectively offline or in bandwidth-constrained environments with minimal updates (one or two per year). Deep Instinct offers a $3 million ransomware warranty underwritten by Munich Re, as well as a less-than-0.1% false-positive-rate guarantee.

Deep Instinct is suitable for all organizations looking for effective and efficient prevention capabilities. However, Type A and Type B organizations that choose Deep Instinct should consider deploying its capabilities alongside a stronger EDR solution.

ESET

ESET's highest scores with its EDR product are for the Type B and Type C use cases. It is appropriate for organizations seeking endpoint protection and detection capabilities and container support.

ESET rates well for protection functionality. Its OS support across Windows, Linux and container workloads receives a solid score. So too does its geographic support, although ESET supports fewer regions for its managed services than leading vendors.

ESET is a good choice for Type C organizations looking for solid protection with a set of core detection capabilities that receive in-region support from managed services.

Fortinet

Fortinet's highest scores are for the Type A and Type B use cases, but it is suitable for all organizations, particularly those seeking XDR-integrated network and endpoint security.

The FortiClient agent now acts as more of a general fabric platform extension, with multiple integrations and a centralized management and reporting platform. FortiXDR combines endpoint and IoT security, network access, zero trust network access, and application and cloud security capabilities in one solution.

Fortinet has added connectors to third-party data sources. These additions offer broad visibility across a number of endpoints and security tools and make Fortinet ideal for complex Type A organizations and the managed security service providers (MSSPs) that support them. Fortinet has a global reach, with products suited to organizations in all industry sectors and of varying maturity, especially midsize organizations seeking an integrated XDR security platform that have already invested in Fortinet technology.

Microsoft

Microsoft scores consistently well for the Type A, B and C use cases. Microsoft Defender for Endpoint is suitable for all organization types in all regions.

In September 2021, Microsoft increased the range of protections included in its Defender for Endpoint Plan 1 and Enterprise E3 license bundles. Microsoft has also introduced the Defender for Business option for businesses with up to 300 seats, which enhances its appeal to Type C organizations.

Microsoft Defender for Endpoint is available in two main options: Plan 1 offers a comprehensive EPP solution; Plan 2 adds EDR facilities, advanced threat hunting, vulnerability management and access to the Microsoft Security Experts support facility. Both plans provide coverage of Apple Mac, Linux and Windows systems, plus Android and iOS mobile devices. Defender for Endpoint can also be licensed individually via a stand-alone option for customers who do not want a bundled plan.

Palo Alto Networks

Palo Alto Networks' highest score is for the Type A use case. It is especially suitable for Type A organizations that are consolidating network and endpoint security products with strong XDR security operations capability.

The tuning and management of Palo Alto Networks' console have been identified by buyers as pain points, but the vendor's Unit 42 MDR can help buyers offload operational overhead.

The Cortex XDR platform provides detection across endpoint and network domains, along with response actions capable of spanning both domains. A mix of in-house and third-party integrations underpin this vendor's XDR offering. Cortex XDR is suited to teams with experience of managing and tuning EDR offerings for their environment.

SentinelOne

SentinelOne scores highly for all three use cases. It has a comprehensive set of bundles and add-ons for varied needs and environments. It also has its own managed services and many third-party support options through a host of MSSPs.

In May 2022, SentinelOne acquired Attivo Networks, thus adding identity threat detection and response (ITDR) and deception capabilities to an already comprehensive XDR platform.

SentinelOne's main markets are North America and EMEA, but it also has a major presence in the Middle East. The vendor has continued to invest in, and see growth in the uptake of, its MDR offering, which is appropriate for companies of all sizes and types.

Sophos

Sophos' highest score is for the Type B use case. It is also suitable for Type A and Type C organizations seeking strong capabilities in cloud and server environments.

Sophos has broadened its platform's support for Linux endpoints with the acquisition of Capsule8, thus creating an XDR platform. Third party integrations, including with the Microsoft Security Graph API, help extend visibility into cloud hosting environments. Sophos has launched a fixed-cost risk and vulnerability assessment tool aimed at customers across segments.

The Sophos Adaptive Cybersecurity Ecosystem (ACE) platform includes both endpoint security and network security facilities, as well as the security operations tools needed to integrate and manage it in a SOC.

Sophos' clients are mainly large organizations with their own staff. However, organizations without security operations staff can achieve scalable detection via fully managed service options.

Trellix

Trellix is a new company formed around the combined products of McAfee Enterprise and FireEye. Its highest scores are for the Type B and Type C use cases.

Trellix has engaged in an extensive marketing campaign to increase awareness of its brand and its "Living Security" message. Existing customers of its Mandiant-delivered managed services will continue to be able to use Mandiant services, while additional MSSPs are onboarded. Ease of use

differs across the two EDR options — Trellix EDR (formerly FireEye Helix) and Trellix ENS (formerly McAfee MVISION) — which enable it to target mature and less experienced SOC teams, respectively.

Trellix's clients are mostly in North America and EMEA. Its existing FireEye and McAfee Enterprise products are extensively used by organizations that still require an on-premises management option together with support for a broad range of modern and legacy platforms. Trellix's new cloud services will appeal to all types of organizations that are able to connect their systems to the internet.

Trend Micro

Trend Micro's scores indicate suitability for the Type A and Type C use cases. Trend Micro is also suitable for Type B organizations looking to consolidate multiple security products into a single-vendor platform to improve security operations.

Few of Trend Micro's current customers use its managed services. Its EDR tends to appeal more to organizations that have sufficient internal staff to support its operation. Trend Micro has consolidated and extended its endpoint security solutions under its new Vision One brand; the unification of management consoles is important to buyers looking for an EPP, given the trend for tool consolidation.

Trend Micro's Vision One platform offers deep integration with the vendor's own tools and a selection of third-party tools, as part of an XDR strategy. It is appropriate for organizations with an existing Trend Micro investment that require rich support for legacy platforms and EDR for operational technology assets. Trend Micro has a global presence.

VMware

VMware's highest scores are for the Type A and Type B use cases. It is a suitable choice for organizations with growing virtualized and cloud workload environments.

Integrations between Carbon Black and VMware's endpoint management tools help enable VMware to provide an XDR platform that correlates threat intelligence and coordinates responses via its Contexa offering. VMware also has strong cloud workload protection capabilities, including tools for microsegmentation and cloud configuration management. Additionally, VMware has launched a direct MDR offering.

Broadcom has announced an intention to acquire the outstanding shares of VMware, but, at the time of evaluation, both Broadcom (Symantec) and VMware met the inclusion criteria for this Critical Capabilities report and continued to operate separately. Gartner will provide further insight as more detail becomes available about the future roadmap for these vendors' existing portfolios.

WithSecure

WithSecure's highest score is for the Type C use case, but it has similar scores for the Type A and Type B use cases. WithSecure is a new company that was formed in June 2022 when F-Secure's

corporate security business was demerged from F-Secure's consumer operations and rebranded. Increased automation and risk analysis capabilities make it slightly more suitable for organizations with more mature XDR seeking to automate actions.

WithSecure's Elements Endpoint Protection for Computers offers a narrower set of management features than other offerings evaluated in this Critical Capabilities report, but it performed well in third-party tests. Usage-based pricing is available. WithSecure offers MDR services globally, including a new service option designed for European customers, with region-specific compliance accreditations for data handling. WithSecure is appropriate for Type C organizations seeking a SaaS-only, easy-to-manage EPP that is well-integrated with other products in the WithSecure portfolio.

Context

Endpoint protection technology has evolved. Prevention technology alone is insufficient because achieving 100% prevention is not feasible. The ability to detect and rapidly respond to novel threats is crucial for success. Traditional vendors are maturing their EDR and cloud management capabilities to rival new, more narrowly focused vendors. At the same time, those new vendors have improved their offerings' protection capabilities, enabling them to replace legacy EPPs more easily. As this transformation happens, the number of "add-ons," such as for data loss prevention or file encryption, is declining, as vendors focus more on core protection, detection and response capabilities. Multiple security products are being integrated at the management level to provide better visibility and response across the breadth of security tools.

The need to scale deployments across more endpoint types and platforms presents a unique challenge for organizations, given the dearth of qualified security operations staff. This challenge continues to create immense interest and follow-through investment in EDR as a managed service, especially by the Type B and C organizations that comprise the bulk of current, active buyers.

As detection activities become more important and grow in volume, an increasing number of organizations will require outside help to scale their endpoint protection. Gartner has strengthened its Strategic Planning Assumption focused on MDR uptake, based on the continued interest in managed services. Publicly traded vendors have identified MDR as a growth area, and Gartner has observed it comprising the majority of some vendors' new business and renewals in 2022. Many EDR vendors' managed EDR services enable security operations teams to share some or all of the detection and threat hunting load, but limit services to their own products, while broader managed services partners build MDR into broader service offerings. Whether using managed services to offload a portion of the response and remediation work or relying on them to ensure 24/7 coverage of the EDR console and its detections, organizations ranging from midsize enterprises to large multinationals are using managed services to augment their endpoint security tools.

There is also growth in the number of different types of data and signals that endpoint-focused tools can ingest and interpret to identify threats earlier in their execution. Vendors' pursuit of XDR architecture focuses on building more and richer integrations with security tools in order to generate

valuable telemetry about users, apps and endpoints. Integrations within some vendors' endpoint security portfolios have driven rapid building of XDR architectures. Pragmatically, large and diverse organizations will require a multivendor XDR approach, due to the diversity of their existing toolsets. Focused vendors lacking broad, multidomain product sets will seek to improve the reach of detection through acquisitions to add functionality and through partnerships and product-to-product integrations across tools, such as event imports from a network detection and response or identity protection tool.

Three-quarters of the respondents to the 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey reported that they will have an active vendor consolidation strategy in one to three years' time, up from 80% in 2020. The integrations, product enhancements and partnerships required to drive integration across endpoint tools (for example, to integrate SIEM data sources with EDR for analysis) are evaluated as part of Gartner's assessment of vendors' responsiveness to the demand for integrated, XDR-ready security tools.

EDR can be less deterministic than signature- and hash-based protection methods, and, as attackers are getting more sophisticated, early detection of IoCs requires active monitoring and detection. Given the pursuit of XDR and the inherent need to integrate tools and coordinate responses across domains, managed services partners may be helpful for maturing an EPP/EDR deployment. The breadth and depth of these partners' services vary. They range from active monitoring and alerting of just the EDR tool by the tool's vendor to fully managed detection and response across multiple tools, usually by partners and MSSPs.

The efficiency gains derived from unifying Android, iOS, macOS, Linux and Windows operational tools is driving demand for cross-platform feature parity in relation to endpoint security tools, most notably EPPs. Demand for support for server platforms and protection of cloud workloads in a single tool is increasing.

The three use cases in this analysis focus on organizational attributes, as follows:

- **The Type A use case** represents the requirements of organizations with the most aggressive adoption profile for EPP tools These organizations often have larger-than-average budgets and staffing resources. This is the smallest group of buyers.
- **The Type B use case** represents the requirements of organizations that want to stay up-to-date and proactive in terms of endpoint security tools, practices and techniques, but have less appetite for risk in terms of new technology. This is the largest group of buyers.
- **The Type C use case** represents the requirements of organizations that prioritize endpoint security technology investment when driven by operational necessity, that are cost-sensitive and that often focus on a subset of protective features. This is the second-largest group of buyers.

Product/Service Class Definition

An endpoint protection platform (EPP) protects against existing and emerging threats and exploits, typically via installation of an agent on an endpoint. An EPP must primarily protect against malware and both file-based and fileless exploits. An EPP must also identify and prevent threats using behavioral analysis of device activity. It must enforce allow-listing of known applications and provide facilities to investigate and remediate incidents when exploits evade protective controls.

The EPP market has adapted to more advanced threats and stealthier attackers. We now find that:

- Organizations place a premium on preventing unknown and non-file-based attacks.
- Machine learning and cloud-based look-up capabilities are sought as alternatives to local signature-based identification.
- Ease of use, low resource utilization and reduced maintenance are expected.
- Anti-tamper mechanisms are considered essential.

The principal developments in the EPP market are:

- Cloud-native EDR and XDR solutions that are easier to deploy and manage.
- Advances in behavior-based detection and analytics, which enable identification of zero-day threats.
- Automated response and containment facilities.
- Flexible managed service options to augment in-house resources.

Vendors are also consolidating multiple capabilities into single XDR platforms to widen their appeal and extend security protection to IT operations disciplines through:

- Firewall management, device control, threat and vulnerability management.
- Patching, application control and storage encryption.
- The ability to report on internet, network and application activity in order to derive additional indications of potentially malicious activity.

Critical Capabilities Definition

Ease of Use

This capability refers to the ease of use of the administration console, based on Gartner Peer Insights reviews and reference account scores.

Ease-of-use ratings reflect Gartner Peer Insights data for overall product capabilities, ease of deployment, ease of integration using standard APIs and tools, and quality and availability of end-user training. The impact of a solution — in terms of memory footprint, for example — is also considered.

Management

Cloud-based management of EPPs is the preferred method as it reduces the maintenance overhead of managing on-premises servers.

Flexibility of deployment models, regional support for storing data, and the ability to support disconnected or restricted devices are also valued. Where on-premises solutions are available, easy migration to cloud management is critical.

Management capabilities are rated based on the availability and range of cloud management options. Adoption and migration rates (where appropriate) to cloud management are also considered. Extra credit is given for supporting regional and restricted verticals (such as the government sector). Credit is also given for supporting partner-delivered management.

Prevention

This critical capability concerns the quality and accuracy of an EPP's preventive anti-malware technology.

Vendors must provide a combination of preexecution prevention and postexecution detection. They must also provide effective blocking or remediation of threats, and send alerts to a central console for a combination of automated and manual response options. The rating for this capability also reflects a product's participation and relative performance in public tests that test both before and after execution.

EDR Functionality

This critical capability concerns the recording of system-level behaviors and the use of these records to detect suspicious events, investigate and block malicious activity, and remediate affected systems.

The rating reflects a solution's ability to provide advanced EDR functionality, including:

- Monitoring of system-level behavior
- Retention periods for alerts and telemetry
- Response and remediation, including automated response playbooks
- Detection of security incidents
- Investigation of security incidents

- Threat hunting

EPP Suite

An EPP suite is an extended portfolio of security tools used to augment anti-malware defenses across an organization.

These tools may have capabilities such as local firewall/native firewall configuration management, device control for securing removable media, application control, secure remote access, vulnerability and patch management, and data loss prevention. These tools may include network-level tools, such as email encryption tools, secure web gateways and sandboxes for detonation of potentially malicious items. Integration of these tools by a common management infrastructure and incident response and reporting portal is desirable.

Managed Services

This critical capability concerns a provider's ability to deliver a range of managed security solutions to support clients.

Typical enterprises struggle to deploy and maintain security tools, and they find the advanced administration requirement of EDR tools particularly difficult. Solution providers are given credit for incident response capabilities that range from light incident support to full MDR and on-site incident response. The rating reflects the breadth of services, their location and scale, as well as provision for partners and service providers to add management services on top of those offered directly.

Geographic Support

This critical capability concerns a vendor's ability to support global customers.

Vendors offer local and regional support offices, 24/7 support in each client region, and other local resources to assist with the deployment and operation of their solutions. Credit is also given for language support for both endpoint and management console.

OS Support

This critical capability refers to a vendor's ability to protect a broad range of operating systems and environments.

Some vendors focus solely on Microsoft Windows endpoints. Solutions that also support macOS and Linux, with features nearly on a par with those delivered for Windows clients, most notably for advanced prevention and the activity- and event-monitoring aspects of EDR, receive extra credit. Support for mobile OSs such as iOS and Android is also evaluated. Additionally, solutions that provide specific functions for cloud, virtual and container-based workloads are given extra credit.

Use Cases

Type A

Type A organizations, also known as “lean forward” organizations, adopt new technologies very early in the adoption cycle.

Type A organizations represent the smallest group of buyers. They have the budgeting and staffing resources to configure and implement new technologies and solutions rapidly within their environment. They tend to focus on best-of-breed solutions that address their business, technology and security needs, and they have the capacity to integrate, develop or build custom components as required. They see the use of technology as a competitive differentiator. Their tolerance for risk is high. Their approach to technological change is to run projects in parallel, with multiple teams working on technology and business changes simultaneously. With regard to EPPs, these organizations focus on best-of-breed prevention, detection and response capabilities. They rarely require managed service capabilities.

Type B

Type B organizations aim to stay relatively up-to-date in terms of technology. They try to avoid getting too far ahead of, or falling too far behind, the competition.

Type B organizations represent the largest group of buyers. They typically experience budgeting and staffing resource constraints and, as a result, focus on overall value by weighing the risks of the early use of new technology against the benefits. Their focus is on technology deployments that improve their productivity, product quality, customer service and security. Type B organizations typically wait for a technology to become mainstream before considering implementation. They tend to be moderate in their approach, frequently using benchmarks within their industry to justify their investments in technology. Type B organizations balance innovation with reasonable caution when selecting new solutions. In terms of EPPs, these organizations focus on using a blend of prevention, detection and response capabilities, complemented by managed services where needed.

Type C

Type C organizations typically view technology as an expense, or an operational necessity, and use it to reduce costs.

Type C organizations represent the second-largest group of buyers. They have severe budgetary and staffing resource constraints and, as a result, prefer to deploy and use integrated solutions with the managed service add-ons that can best complement their minimal staff. These organizations wait for technologies to become stable and for the costs of acquisition and operation to reach the lowest quartile before committing to purchase. In terms of EPPs, these organizations focus on prevention, rather than on integrated detection and response capabilities but, if they take on detection, they prefer solutions that offer a complement of managed services.

Vendors Added and Dropped

Added

- Deep Instinct
- Palo Alto Networks
- Trellix

Dropped

- FireEye (see Trellix)
- F-Secure (replaced by WithSecure)
- McAfee (see Trellix)
- Panda Security

Inclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses, by default, an upper limit of 20 vendors to support the identification of the most relevant providers in a market. The inclusion criteria represent the specific attributes that Gartner analysts believe are necessary for inclusion in this research.

To qualify for inclusion, vendors need to meet the following criteria at the commencement of the initial research and survey process (as of 8 January 2021).

Core Inclusion Criteria

To be included in this Critical Capabilities report, each vendor had to satisfy at least 12 of the following criteria using only its own nominated solution(s):

- The solution protects against known and unknown malware without relying on daily agent/definition updates.
- There is a facility to detect malicious activity based on the behavior of a process.
- The solution stores IOCs\IOAs in a central location for retrospective analysis for at least 30 days and allows subsequent forwarding to other long-term retention storage where required by the client.
- The capability to detect and block script-based attacks, “living off the land” attacks and other exploits that do not introduce new executable processes to the endpoint.
- The solution removes malware automatically, once it is detected (that is, it deletes or quarantines files, kills processes and automatically removes artifacts).

- The solution enables false positives to be suppressed or ignored from the management console without excluding all protection techniques (for example, it must be able to suppress file detection but still monitor behavior).
- The primary EPP console uses a cloud-based, SaaS-style, multitenant infrastructure that is operated, managed and maintained by the vendor.
- Reporting and management console views display a full process tree to identify how processes were spawned, for actionable root cause analysis.
- Threat hunting is provided, including the facility to search for an IoC/IoA (such as a file hash, source or destination IP address or registry key) across multiple endpoints from the management console.
- The solution identifies changes made by malware and provides recommended remediation steps or a rollback facility.
- There is an option to integrate threat intelligence and reputation services into the solution.
- The solution protects against common application vulnerabilities and memory exploit techniques (such as process injection and dynamic-link library sideloading).
- The solution continues to protect and collect suspicious event data when the managed endpoint device is outside the corporate network or offline.
- The solution performs scheduled static, on-demand malware detection scans of folders, drives or devices such as USB drives.
- The solution can detect misuse of identity and tokens, and lateral movement associated with this misuse.

Optional Inclusion Criteria

To be included in this Magic Quadrant, vendors also had to satisfy at least four of the following criteria:

- The solution implements named vulnerability shielding (also known as virtual patching) for known vulnerabilities in the OS of the protected endpoint device and for non-OS applications.
- Provision of risk-based vulnerability reporting and prioritization of remediation actions.
- The solution implements configurable default-deny allow/block listing (of applications, for example), with trusted sources of change.

- The ability to provide protection, detection and response capabilities for cloud workloads, including serverless workloads.
- The endpoint agent has identity and/or endpoint-based deception capabilities (lures) designed to expose attackers and track their activity.
- The vendor offers managed alerting and monitoring services that alert customers to suspicious activity and provide guided remediation advice (managed detect and respond services, for example).
- The vendor offers remote managed deployment, configuration services, and detection and removal of threats on behalf of the client.
- The solution supports advanced queries across multiple endpoints and combines multiple events into a single incident.
- The solution includes playbooks and guided analysis and remediation, based on intelligence gathered by the vendor (for example, “the next steps needed to contain this threat are XYZ”).
- Reporting capability for attribution information and potential motivations behind attacks, including mapping of events and alerts to MITRE ATT&CK tactics, techniques and procedures (TTPs).
- The vendor provides a hybrid solution with capabilities comparable to its cloud-managed principal capability for air-gapped or non-internet-facing systems.
- Integration of alerts and workflows from other security solutions, including those of third parties.
- The ability to correlate and enrich weak events or alerts, from multiple sources or sensors, into strong detections.
- The solution can coordinate responses across multiple security products (for example, It can initiate a change in configuration, detection, blocking or removal using two-way API integration with other tools).
- The ability to show the overall security posture of the managed estate and give insights into exposure to the latest threats.

Exclusion Criteria

- If a vendor did not satisfy at least 12 of the core inclusion criteria, and four optional capabilities overall, it did not qualify for inclusion in this Critical Capabilities report.
- A vendor could be excluded if the majority of detection events did not come from its own detection agent and the techniques used were not designed, owned and maintained by the vendor itself. However, vendors were permitted to augment their solution(s) with an OEM engine, provided the

OEM or third-party agent/sensor was not the primary means of detection. Vendors also had to provide their EPP independently of any other solution or service.

- If a vendor had not participated in independent, well-known, public tests of accuracy and effectiveness — such as those of AV-TEST, AV-Comparatives, MITRE, MRG Effitas and SE Labs — within the 12 months prior to 30 June 2021, it was considered for evaluation only if it was a current participant in the VirusTotal public interface. (Participation in other public tests was considered if they were equivalent to those listed above.)

- A vendor had to have more than 7 million enterprise active seats using its EPP as their sole EPP, as of 28 January 2022. Of these, more than 500,000 had to be active installations with accounts larger than 500 seats. The proportion of enterprise customers in a single region outside North America could not exceed 60% of the total number.

- Due to a pause in coverage of all Russian vendors by Gartner, there may be Russian vendors that meet the inclusion criteria described but were not evaluated. These vendors are not included in this research.

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities ↓	*Type A* ↓	*Type B* ↓	*Type C* ↓
Ease of Use	10%	15%	10%
Management	20%	20%	20%
Prevention	20%	20%	20%
EDR Functionality	30%	15%	5%
EPP Suite	5%	5%	5%
Managed Services	10%	20%	30%
Geographic Support	0%	0%	5%

Critical Capabilities	Type A	Type B	Type C
OS Support	5%	5%	5%
As of 31 October 2022			

Source: Gartner (December 2022)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	Bitdefender	BlackBerry (Cylance)	Broadcom (Symantec)	Check Point Software Technologies
Ease of Use	4.4	4.5	4.6	4.5
Management	3.9	3.9	3.8	3.9
Prevention	4.4	3.7	4.4	4.1
EDR Functionality	3.2	3.9	4.1	3.5
EPP Suite	3.3	3.5	3.8	3.8

Critical Capabilities	Bitdefender	BlackBerry (Cylance)	Broadcom (Symantec)	Check Point Software Technologies
Managed Services	3.5	4.0	3.0	4.0
Geographic Support	3.7	3.2	4.5	3.8
OS Support	4.7	4.3	4.4	4.3
As of 31 October 2022				

Source: Gartner (December 2022)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

Use Cases	Bitdefender	BlackBerry (Cylance)	Broadcom (Symantec)	Check Point Software Technologies	C
Type A	3.81	3.93	4.04	3.91	
Type B	3.90	3.97	3.96	4.01	
Type C	3.90	3.92	3.84	4.02	
As of 31 October 2022					

Source: Gartner (December 2022)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Acronym Key and Glossary Terms

AI	artificial intelligence (especially when used to identify and alert on unknown threats)
EDR	endpoint detection and response (for the postinfection stages of an attack or exploit)
EPP	endpoint protection platform (provides prevention of malware and exploits)
MDR	managed detection and response (capabilities focused on quickly detecting, investigating and actively mitigating incidents)
ML	machine learning (used, for example, where agents use mathematical determination of threats)
MSSP	managed security service provider
SIEM	security information and event management (gathers and analyzes device logs)
SOAR	security orchestration, analytics and reporting (joins solutions with workflow)
SOC	security operations center (or the team that works in it)
XDR	extended detection and response (a unified system combining telemetry sources and integrating multiple tools into a single console usually with automation and AI-powered analytics for faster and more accurate detection and response)

Evidence

Gartner's Critical Capabilities team used data from the following sources:

- More than 3,000 client inquiries since January 2022.
- More than 4,500 Peer Insights reviews on gartner.com.
- Vendors' answers to a survey containing over 500 questions about product and service capabilities and enhancements through 4Q22, as well as 30-minute demonstrations by each vendor.

- The 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey.

2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey

This survey was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, the expected or realized benefits of consolidation, and how those that are consolidating are prioritizing their consolidation efforts. Another key aim of this survey was to collect objective data on XDR and secure access service edge (SASE) for consolidation of megatrend analysis.

The survey was conducted online during March and April 2022, with 418 respondents from North America (the U.S. and Canada; n = 277), Asia/Pacific (Australia and Singapore; n = 37) and EMEA (France, Germany and the U.K.; n = 104). Each respondent represented an organization with $50 million or more in 2021 enterprisewide annual revenue. Industries covered included manufacturing, communications and media, IT, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences.

Respondents were screened for job title, company size, job responsibilities (which included those of information security/cybersecurity and IT roles), and primary involvement in information security.

Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.

Note 1: Definitions of Type A, Type B and Type C Organizations

Type A Organizations

Type A organizations, also known as “lean forward” organizations, adopt new technologies very early in the adoption cycle.

Type A organizations are the smallest group of organizations. They have the budgeting and staffing resources to configure and implement new technologies and solutions rapidly within their environments.

These organizations tend to focus on best-of-breed solutions that address their business, technology and security needs and that have the capacity to integrate, develop or build custom-made components as required. They see the use of technology as a competitive differentiator. Their tolerance for risk is high and their approach to technological change is to run projects in parallel, with multiple teams working on technology and business changes simultaneously. With regard to EPPs, these organizations focus on best-of-breed prevention, detection and response, and rarely require managed security service (MSS)/MDR capabilities.

Type B Organizations

Type B organizations aim to stay relatively current in terms of technology without getting too far ahead or behind their competitors.

Type B organizations are the largest group of organizations. They typically experience budgeting and staffing resource constraints and, as a result, focus on overall value by weighing the risks and benefits of early use of new technology. Their focus is on technology deployments that improve their productivity, product quality, customer service and security.

Type B organizations typically wait for technologies to become mainstream before considering implementation. They tend to be moderate in their approach, frequently using benchmarks within their industry to justify their investments in technology.

Type B organizations balance innovation with reasonable caution when selecting solutions. In terms of EPPs, these organizations focus on a blended approach involving prevention, detection and response capabilities that can be complemented with managed services where needed.

Type C Organizations

Type C organizations typically view technology as an expense or an operational necessity, and use it as a means to reduce costs.

Type C organizations are the second-largest group. They experience severe budgeting and staffing resource constraints and, as a result, prefer simply to deploy and use integrated solutions with the managed service add-ons that can best complement their minimal staff.

These organizations wait for technologies to become stable and for acquisition and operation costs to reach the lowest quartile before committing to purchase. In terms of EPPs, these organizations focus on prevention, rather than on integrated detection and response capabilities and solutions that offer managed services.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering

products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.