Market Guide for Endpoint Detection and Response Solutions

Published: 30 November 2016 **ID:** G00298289

Analyst(s): Peter Firstbrook, Neil MacDonald

Summary

Security and risk management leaders in large enterprises with dedicated security operations teams who want to know about the most effective technologies to protect endpoints and manage endpoint security must invest in EDR solutions.

Overview

Key Findings

Detection mechanisms must move up the stack to combinations of behavioral indicators that detect attacker tool techniques and procedures. EDR solutions must be capable of detecting fileless malicious activities that use memory exploits and take advantage of Windows utilities such as PowerShell.

EDR solutions require very technically knowledgeable operators to gain good insight.

Scalable data management, data mining analytics capability and detection techniques that incorporate advanced understanding of changing attacker tradecraft are critical.

Scaling the database and data mining capability is a key implementation barrier, which will lead to more cloud-based deployment options.

EDR will be a feature of endpoint protection platform (EPP) solutions for improved visibility and occasional incident response.

Recommendations

Security and risk management leaders responsible for endpoint security:

Implement EDR solutions to improve detection and response of high-severity attacker tool tactics and techniques, but be wary of EDR solutions' ability to provide real-time protection.

Mature (Level 3 and up) security operations centers (SOCs) and managed SOC service providers should invest in EDR solutions with capabilities to provide scalable data management and search, APIs for integration with other security systems, and advanced workflow capabilities.

Less mature organizations (Level 1 to 2) should invest in EDR as a feature of EPP solutions that will provide good-enough capability for occasional incident response and improved visibility into threat impact, as well as improved remediation recommendations.

Strategic Planning Assumptions

By 2018, 100% of Leaders' and Visionaries' EPPs will include EDR capabilities.

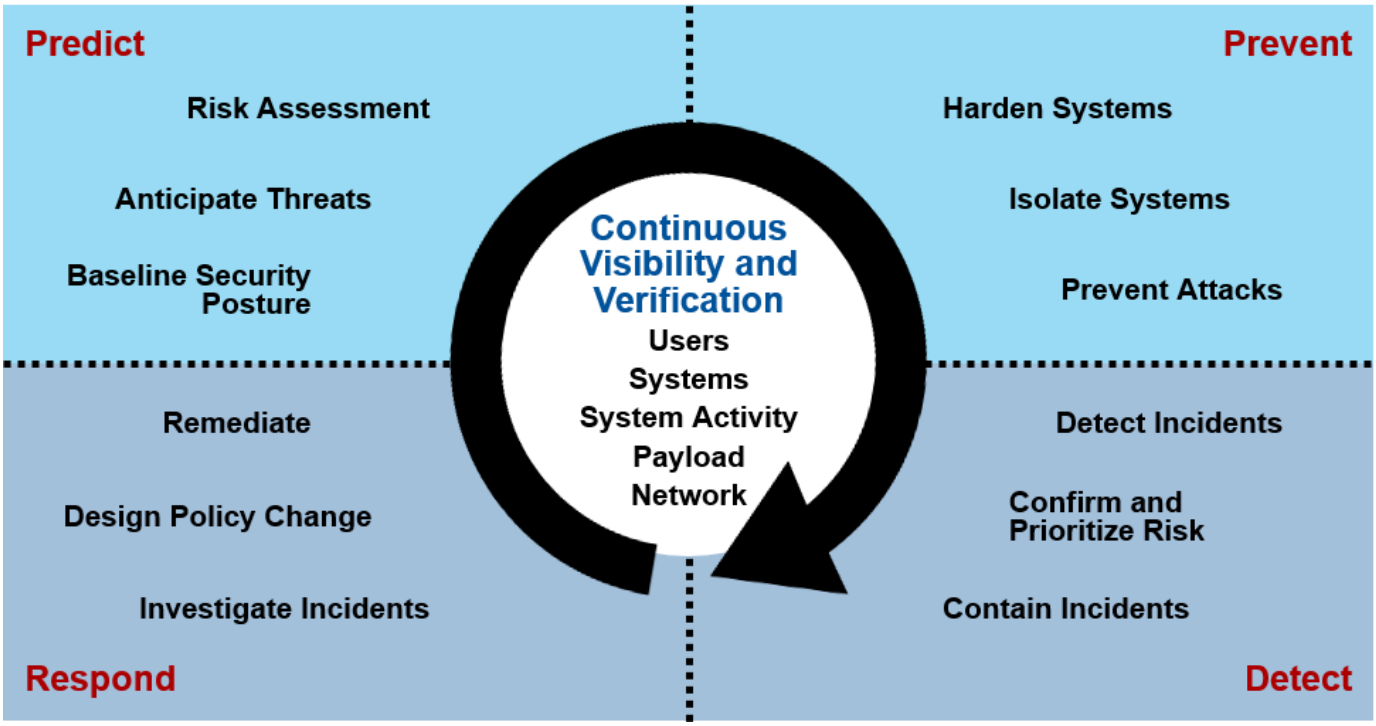
By 2020 80% of large enterprises, 25% of midsize organizations and 10% of small organizations will have invested in EDR capabilities.

Market Definition

This document was revised on 19 December 2016. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The EDR market is defined as solutions that record endpoint-system-level behaviors and events (for example user, file, process, registry, memory and network events; see Note 1), and store this information either locally on the endpoint or in a centralized database. Databases of known IOCs and behavior analytics techniques are then used to continually search the data to identify early identification of breaches (including insider threats), and to rapidly respond to those attacks. These tools also help with rapid investigation into the scope of attacks, and provide response capability (see Figure 1).

Figure 1. Adaptive Security Architecture



Source: Gartner (November 2016)

EDR solutions must provide the following four primary capabilities:

1. **Detect security incidents.** Typically, this occurs by self-detection via monitoring of endpoint and application behavior violations, or by validating internally or externally discovered IOCs. Ideally, the solutions will prioritize the detected incidents for the security analyst based on confidence, severity and risk in order to prioritize the response activities.
2. **Contain the incident at the endpoint.** This ensures that network traffic or process execution can be remotely controlled, while quarantining the system from the rest of the enterprise network.
3. **Investigate security incidents.** The investigate function must include a historical timeline of all primary endpoint events across all monitored endpoints to determine both the technical changes that occurred (such as file, registry, network, driver and execution

activities) and the business effect (i.e., loss of customer data, transaction fraud).

4. **Remediate endpoints to a preinfection state.** Ideally, solutions will remove malicious files, roll back and repair other changes. At a minimum, solutions must create remediation instructions for other groups to implement with their own toolsets.

Not all vendors are mature in all four capabilities at this stage of the market, and we have used as broad inclusion criteria as is practical for this guide.

In essence, this market delivers capabilities that map directly into capabilities in the bottom half of Gartner's Adaptive Security Architecture (see Figure 1 and "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"), and some that bleed into the Predict and Prevent quadrants.

Market Direction

We estimate that there are roughly 40 million EDR seats licensed as of year-end 2016 across 30 vendors. By way of comparison, there are roughly 400 million endpoint protection seats licensed by the EPP Magic Quadrant participants. As a result, we estimate that the market is roughly only 10% penetrated so far.

Average prices for EDR licenses for a 1,000-seat organization are between $5 and $25 per seat per year. As such, a rough estimate would peg the market run rate at approximately $498 million at year-end 2016. A group of 10 leaders is dominating the market with 75% market share. These providers are growing at roughly two times year over year. However, it is difficult to envision EDR as a mainstream market product due to the operator skill requirement. As such, growth of dedicated EDR solutions will falter, likely by 2019, as more EDR functionality becomes a lower-cost feature of endpoint protection tools.

The rapid growth of EDR solutions is primarily a result of CIO and executive-level concerns about increasing public disclosures of data loss that result from advanced and targeted attacks that have bypassed traditional preventative controls and persist undetected for extended periods of time. EDR tools do not typically replace other tools. New budget allocations for EDR are common.

Buyers tend to be more mature (Level 3-plus; see "ITScore for Information Security") security organizations that are struggling with alert resolutions and incident response, and looking to improve SOC productivity. Lean-forward security industries such as finance, telecom, high tech, pharma, government, military/defense and critical infrastructure are the most common industries where EDR is deployed.

We anticipate that established incumbent EPP vendors will continue to build or buy into this market; however, a few of the emerging EDR vendors will continue to provide best-of-breed solutions for the mature SOC organization. At the same time, a few of the EDR vendors with an emphasis on protection will challenge the incumbent EPP vendors and gain a reasonable market share in the EPP market.

Market Analysis

The EDR market is one that has emerged to satisfy the need to respond to advanced attacks that evade detection by incumbent EPP solutions. The most notable improvement over current EPP solutions is the introduction of improved visibility into endpoint events, more sensitive threat

detection and improved incident response capabilities.

Innovative Improvements

Improvements in EDR solutions in 2016 focused on the following features:

- Increasing use of protection rules to block the execution of threats rather than report on them
- Integrated sandbox (on box, on-premises management server or cloud) for manual or automatic inspection of portable executable (PE) files for analysis
- Detection of in-memory attacks that exploit common utilities and do not drop malware
- Admin account monitoring to detect privileged account take-over attacks
- User interface enhancements to improve ease of use, role-based access control, role-based dashboard customization and workflow enhancements
- Improved hunting dashboard and hunting automation for more advanced SOCs
- API improvements to enable streaming data to different detection engines or to incorporate multiple IOC feeds
- Integration with other enterprise security tools, particularly security information and event management
- Expanded Linux and Mac support, including more in-depth event collection capability
- The addition of machine-learning-algorithm-based file detection capabilities
- Expansion of machine learning for malicious activity detection

Emerging Capability

Given the immaturity of the market, it is not surprising that prospects and customers still have a long laundry list of potential improvements that the industry needs to deliver. In addition, most enterprise SOCs simply do not have enough skilled staff to deal with the volume of events generated by EDR solutions. As a result, the following features are often high on that list:

- Continuous improvements in detection capabilities.
- Higher levels of automation to reduce the workload on already overtaxed incident responders, and to reduce the time between detection and response.
- Better guided investigations to help improve Tier 1 support resolution. For example, helping identify next steps, precorrelating multiple alerts into an incident, exposing attack stage information and providing hyperlinked pivoting capability to assess the extent of the attack.
- Risk-based prioritization of high-assurance events to quickly focus the SOC analyst on the events that represent the most risk to the organization.
- Improved scalability and performance to reduce the network and endpoint impact, and to scale the back-end database.
- Root cause analysis with recommended action plans and proactive configuration and security state assessments to reduce the attack surface and thus the infection rate.

Long-Term Trends

EDR market leaders will continue to focus on less deterministic detection indicators that need some level of manual oversight. Automated IOC detection is common, but less effective because attackers can rapidly change file hashes, IP domains, registry keys and other typical IOCs. It is harder for attackers to change their tradecraft. Attackers need to perform actions such as encrypt files, exfiltrate data, move laterally, compromise admin accounts and so on. These high-level behaviors are harder to change and thus more durable indicators of malicious actions.

Detecting behaviors is complicated and not highly accurate; as such, smart security operations staff will continue to be in demand and in short supply. Most organizations will not be able to hire, train and retain these operators. As a result, interest in managed SOC services is growing (see "Market Guide for Managed Detection and Response Services"). Demand for EDR as a managed service is increasing. Most EDR vendors will partner with managed security service providers (MSSPs) to offer this, and several EDR vendors will offer their own augmentation services, like CrowdStrike's Falcon Overwatch and FireEye's FireEye as a Service.

We anticipate that EDR vendors will begin to integrate deception techniques. Deception solutions provide highly deterministic alerts that can easily integrate into other detection methods (see "Competitive Landscape: Distributed Deception Platforms, 2016" and "Applying Deception Technologies and Techniques to Improve Threat Detection and Response").

As the EDR market matures, we anticipate feature improvements will focus on increasing capabilities around the adaptive security architecture to provide more holistic and integrated security capabilities, such as:

- Community intelligence sharing portals and global comparative trending data that can improve "predict" capabilities.
- Integration with other corporate detection and monitoring components to enhance alert context. For example, integration with data loss prevention and cloud access security brokers to provide threat context and prioritize alerts, and integration with packet capture to initiate selective capture or bring packet capture (PCAP) content into the investigation window.
- Instrumentation of OS and chip-level protection capabilities, such as Microsoft EMET and Windows Defender ATP, and Intel Control-Flow Enforcement Technology.
- Proactive security state assessments will provide configuration information to spot security problems before they become a breach.
- Hardening techniques such as application execution policy will become more common to prevent malware execution. Execution policy will provide execution restriction to limit process access to OS service (i.e., no autoexecute from USB; no external network access, proxy or restrictions to OS services) to prevent malware from gaining a foothold.

Interest in EDR is expanding beyond organizations with mature security SOCs into more mainstream security teams. However, most of this interest will probably be satisfied by EDR solutions that are increasingly being integrated into EPP solutions. EDR is already a feature in many leading EPP solutions. However EPP vendors tend to focus on detection methods that are deterministic, such as IOC confirmation, and can be automated, while more advanced SOCs are looking for detection and hunting tools to help find more advanced adversaries.

Critical Capabilities

Infrastructure

Most solutions consist of an endpoint agent data collector with a centralized data repository and a management server (either cloud-based or on-premises) that provides for a central data repository, a management interface and detection engines. Most are also supported by a cloud-based source of IOC and information on attack patterns. Many include the capability to ingest third-party threat feeds. Some solutions also offer network agents to detect suspicious network traffic patterns.

All solutions support Windows-based endpoints and Windows servers. Support for OS X, Linux and Android are less common, but most solution providers have these OSs in beta or on their roadmaps. Detection capabilities will vary based on the platform. The number of endpoints supported by a single management server ranges from 10,000 to 400,000.

Architectural Considerations

Since, at their core, EDR solutions are based on monitoring and visibility of a large number of endpoint behaviors and state changes, the most significant architectural consideration is where the data is stored — distributed or centrally — and when stored centrally, whether this is kept on-premises or in a cloud-based service.

Distributed storage of endpoint logs on the endpoints themselves makes it easier to scale. However, in a global organization, typically a large number of endpoints will be powered down and nonresponsive to queries at any given time. Moreover, local storage of intrusion evidence is more susceptible to attacker manipulation. Centralizing the storage of endpoint log data is more responsive and enables more aggressive and continuous data mining, but also requires building a big data repository.

Centralizing the data store in a vendor-managed cloud instance service provides ease of implementation and scalability issues, and enables the EDR provider to provide cross-enterprise correlation of events. However, cloud-based storage of EDR data introduces data privacy and potential regulatory issues as the data is moved off-premises.

We anticipate that cloud-based centralized storage will be the desired architecture for the majority of buyers. While there are some holdout industries and geographies that prefer on-premises deployments, the majority of customers are becoming much more accepting of cloud.

Detection

The most critical EDR capability is the ability to detect sophisticated hidden threats, ideally without requiring the use of externally fed IOCs. The ideal EDR system should be capable of self-detection using its own built-in detection techniques, analytics and behavioral indicators. The range of detection techniques will be also be affected by the type of data gathered. Three realms of data are most valuable: user, endpoint and network events. This data also needs to be put into context with global threat intelligence (that is, attribution and trends). Generally speaking, more information and more context is better than less, assuming it can scale across infrastructure and information management.

The best technique is to deploy a funnel approach to detection that moves from low-cost, but highly deterministic, techniques toward less deterministic techniques aimed at spotting unknown attacks.

Most solutions deploy one or more of the following detection approaches.

IOCs and object reputation information provide a low-cost approach, but represent a very high volume of information to inspect. IOC information has a very short useful life because it is the easiest part of the attack chain for adversaries to automatically change rapidly.

Inspecting portable executable files is the second most common technique. File census data (i.e., first seen, first run, certificates and virus total score) should be used to surface suspect files for further analysis. Not all solutions inspect all file types; ensure that prospect solutions inspect interpreted scripts, such as Java, PowerShell, Perl and Office documents. File inspection can be accomplished in multiple ways:

Signatures — Direct hashes of known files, stored in a local cache database or cloud database, are the standard of antivirus vendors. To be effective, signature databases should contain both good and bad files. This is a low-overhead detection method, but its limitations are well-known.

Algorithms — Trained machine learning detection methods are gaining in popularity. These solutions do not require the maintenance of a signatures database and are more accurate at detecting variants of known bad files. However, they are potentially subject to gaming the algorithm, and often cause high false positive detections.

Emulated — Some solutions inspect the file code in real time looking for partial matches to known bad code snippets. It is harder for attackers to change the entire code.

Sandboxed — Files are executed in a virtual environment and detected using behavioral detection methods.

Behavioral detection methods offer the highest flexibility and are often hard for attackers to hide with automation. A series of behaviors characterize the tradecraft of the attack type, which is harder to change. Behavioral indicators can be high-level or lower in the stack — for example, at the user process or network level (e.g., late night admin account login using nonstandard LAN/application traffic to a new external address), application level (e.g., Word doc spawn "cmd.exe," starts PowerShell with downloaded pastebin code), or process level (e.g., process injection, DLL hijack). Behavioral indictors are often late in the kill chain and, in some cases, may be too late if the attackers can gain control and tamper with protection and detection techniques.

Most detection techniques are still focused on past attack patterns involving malware. Future attacks and current advanced attacks will exploit higher in the stack, including the human layer. PowerShell and Windows utilities exploits are becoming more common. Full in-memory exploits that do not require file-based persistence methods are likely. We also anticipate attacks against common privileged applications, such as system management tools. Detection methods will also have to address stolen credential attacks. Deception solutions can provide high-fidelity early detection of hackers who are already inside the network. TrapX Security, illusive networks, Seculert (Javelin) and Attivo Networks are examples of vendors offering solutions that provide early warnings of lateral attacks, but have not yet built out extensive investigation or remediation capability. RSA, The Security Division of EMC; and Damballa are additional examples of vendors that focus on detection techniques, using network traffic interception to detect exfiltration and command-and-control traffic, indicating clients are already infected.

Ideally, any detection solution will use a combination of these detection techniques to improve accuracy. Each detection engine should inform the next and will increase the accuracy of the final outcome.

The biggest problem for any buyer of EDR techniques is determining the depth and accuracy of detection techniques. There are no standardized public tests of detection capability yet. Vendors have excellent marketing departments capable of spinning even the simplest techniques into invincible ones. However, most organizations will benefit from any improvements in detection beyond traditional EPP approaches. While "known bad" IOC-type approaches can significantly improve current detection rates, algorithmic and decoy detection techniques have significant promise to provide progressively improving long-term value as these techniques mature.

Investigation

The capability to enable a security analyst to investigate suspicious events to determine both the technical- and business-level impact is the most important consideration after detection. Almost all solutions in this market are useful for SOC first responders acting to resolve an alert generated by the EDR tool itself or connected sensors. However, not all are well-suited for "threat hunting," where SOC analysts do not have an alert, but are simply hunting for anomalous activity or historic IOC events. Hunting requires the recording of all state changes, not just those that are deemed malicious, and an investigative interface that allows for easy search and pivoting. The ideal solution will surface all of the relevant information of a detected incident and put that information in context for the SOC analysis — no small task. Doing this in a way that makes it understandable and actionable by the SOC analysis is difficult and likely will require the use of visualization to reduce the sheer amount of data to be presented into something actionable.

Leading solutions will provide the following features;

- Fast rea-time (or near-real-time) natural language query tools (similar to Google) that can get rapid answers to questions about IOC-type objects against the centralized data store, or optionally against live systems.
- Risk-prioritized views based on confidence of the incident and severity of the incident based on the business value of the assets affected.
- Click-down attack chain visualization tools that allow investigators to easily pivot on interesting data elements or drill down for more information.
- Automatable fetching of suspect files or memory and disk dumps, although not all EDR tools support real-time forensics retrieval of endpoint state and artifacts.
- Automatic integrated analysis of suspect processes/files in a cloud or on-premises sandbox with clearly visible metadata combined with global information (that is, categorization, author, prevalence and providence). Not all EDR solutions provide a sandbox, and most have integration with popular third-party solutions.
- Severity and confidence indicators on threat alerts.
- Graphing relationship interface to visualize the connectivity of seemingly disparate IOCs.

Investigation tools should also provide for an alert management workflow that enables incidents to be assigned, transferred, annotated and resolved easily.

Containment and Remediation

Contextual actions should be available in the administration interface to contain a suspected incident while it is being investigated. The most common option is simply to quarantine a suspected infected endpoint from the rest of the network and isolate its communications to only

internal systems or, ideally, only the EDR management console while it is under investigation. Other initial containment options typically include process network isolation and process kill/block. Ideally, solutions will provide a way to classify endpoints such that critical systems are not taken offline. Interaction with end users may also be necessary, thus full directory information with user contact details can be helpful. Leading solutions will eventually provide an IM-type communications window with the end user.

While most enterprise organizations reimage machines for all but the most simplistic threats, this approach is expensive and disruptive. Leading EDR solutions should have enough detailed event history information to outline repair actions that will roll back the recorded malicious activity. Leading solutions present operators with a detailed remediation task list and the ability to make changes to the endpoints. Larger organizations will likely have rigid change control policies and separation of duties between operations and the security teams. As such, EDR tools should be able to transfer the repair tasks list to other operations tools. Remediation is the least mature function in the current crop of EDR tools and most focus on simply containing the threat. To prevent other systems from being affected by the same attack, ideally the EDR solution would provide simple hash-based application control that can be used to block any further execution of the file until a signature can be obtained from the EPP provider.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

- Carbon Black
- Check Point Software Technologies
- Cisco
- CounterTack
- CrowdStrike
- Cyberbit
- Cybereason
- Cynet
- Digital Guardian
- Endgame
- F-Secure
- Fidelis
- FireEye
- Guidance
- WatchGuard (Hexis Cyber Solutions' HawkEye G)
- Infocyte
- Invincea

LightCyber

McAfee, an Intel company

Nehemiah Security (Triumfant)

Nuix

Outlier Security

Panda Security

Red Canary

RSA

SecureWorks

SentinelOne

Symantec

Tanium

Trend Micro

Tripwire

Verint

Ziften

(For more information, see "Comparison of Endpoint Detection and Response Technologies and Solutions.")

Market Recommendations

The EDR market is clearly in the Gold Rush days, with a large number of smaller vendors and nearing the Peak of Inflated Expectations, and not all vendors will survive into the mainstream market. However, deploying any EDR is likely better than doing nothing, given the poor state of signature-based protection, and some startup vendors can provide very intimate support and services. It is more important that security and risk management leaders focus on the fit within their organizations. Buyers with experienced SOC staff and mature security programs should focus on vendors with the best investigation and detection capabilities that focus on attacker tradecraft. Those that are less mature should consider the ability to prevent incidents in the first place, and consider investigation and response to be secondary considerations. Managed services should be considered by those organizations that do not have staff or those looking for staff augmentation.

Evidence

This research is based on survey data, interviews and demos of EDR solutions, with more than 900 Gartner client interactions on EDR since the publication of the last EDR Market Guide.

Note 1
Recorded Events

File (e.g., create, rename, delete, write, read, path, file attributes, file size, creation and modification date, versions, file hash, certificates)

Scripts and command parameters (e.g., CMD and PowerShell usage)

Registry (e.g., create, read, overwrite, delete, erase, rename)

Network (e.g., IP address port protocol, DSN query bytes)

Process/thread (create terminate, inject, parent-child relationships)

DLL/COM (load inject)

Windows user accounts (login, logout, username, domain logon time, domain, password age, privilege)

Mutex (open, create)

Autorun changes

Scheduled tasks

Machine information (machine name, OS version, platform architecture, time zone)

System mount points (drive letter, device name, volume name, media type)

Configuration changes (e.g., UAC disabled, antivirus disabled, firewall disabled, automatic updates disabled)

Site Index (http://www.gartner.com/technology/site-index.jsp)

IT Glossary (http://www.gartner.com/it-glossary/)

Contact Gartner (http://www.gartner.com/technology/contact/contact_gartner.jsp)