White Paper

EDR Buyer’s Guide: Addressing Multi-stage Attacks and Operational Inefficiencies

Mind the Gap with Endpoint Detection and Response

By Doug Cahill, ESG Senior Analyst
October 2017

This ESG White Paper was commissioned by OpenText and is distributed under license from ESG.
Contents

Businesses are Augmenting Endpoint Protection with Detection and Response Tools ................................................................. 3
Cyberthreats and Proactive Use Cases Drive EDR Deployment .................................................................................................. 3
The Five Core Capabilities of an Effective EDR Solution ........................................................................................................ 5
1. An Easy-to-use, Actionable Interface ..................................................................................................................................... 5
2. Deep Contextual Visibility .................................................................................................................................................. 6
3. High-fidelity Threat Detection ........................................................................................................................................ 6
4. Automation with Targeted Remediation and Forensic Tools ............................................................................................ 7
5. Integration with Internal and External Solutions ........................................................................................................... 7
The Bigger Truth ........................................................................................................................................................................ 8
Businesses are Augmenting Endpoint Protection with Detection and Response Tools

Increasingly sophisticated cyberattacks and the operational inefficiencies of traditional endpoint security solutions are taking a toll on both cybersecurity effectiveness and business performance. At the same time, organizations are beginning to realize that traditional endpoint protection platforms (EPP) alone are no match for highly complex attacks—and that they’ll need more powerful security capabilities when prevention fails.

It’s not surprising, then, that CISOs are attempting to improve security and operational efficiencies by layering endpoint controls on top of existing solutions. Recent research from Enterprise Strategy Group (ESG) found that 41% of respondents deploy additional controls on all or most of their endpoints, while 32% take a more targeted approach by layering add-on controls on high-value endpoints only. The reason? Organizations need more advanced monitoring and analytics capabilities to gain visibility into ever-more complex and covert compromises. As a result, businesses are augmenting their endpoint security strategy of prevention with detection and response capabilities. Many are turning to endpoint detection and response (EDR) solutions to help them more quickly and efficiently detect, respond to, and recover from cyberattacks. In particular, businesses want additional controls to defend against elusive threats that often evade traditional and even next-generation antivirus solutions.

Fighting Complex Attacks

Organizations need more advanced monitoring and analytics capabilities to gain visibility into ever-more complex and covert compromises.

The pivot toward EDR is gaining momentum: The same ESG survey found that 35% of businesses currently use EDR on a limited basis and an additional 21% plan to implement EDR over the next 24 months. However, selecting the right EDR product can be a challenge. An effective solution should proficiently detect threats and enhance operational efficiency by being easy to use, providing automated capabilities, and easily integrating with other tools. To get started, this buyer’s guide identifies the key components of a comprehensive EDR solution that will address complex cybersecurity issues and operational inefficiencies—and meets your company’s unique business needs.

Cyberthreats and Proactive Use Cases Drive EDR Deployment

It’s no secret that cyberattacks are becoming more frequent and complex. Many businesses, in fact, have been hit with a barrage of disparate and damaging intrusions.

Responding to these incidents is challenging. Skilled threat actors are developing multifaceted malware and refining attack methods to evade detection for as long as possible. This delay between infection and detection enhances adversaries’ ability to gain a stealthy foothold on endpoints and move laterally across business systems and networks.

In particular, organizations are worried about fast-evolving, multi-stage, and targeted attacks, which are notoriously difficult to detect and intercept at the perimeter (see Figure 1). Security leaders are also anxious about ransomware, exploits to unpatched software, and compromises that exploit a legitimate application to execute a script as part of their attack chain. Compounding these concerns is an acute shortage of skilled cybersecurity professionals to mitigate the risks these threat types represent.

What’s more, traditional whitelists and blacklists have become less effective in stopping advanced threats. Cybercriminals are evading detection by using highly effective social-engineering tactics, new attack vectors like third-party vendors and supply-chain partners, and zero-day vulnerabilities. Identifying these threats will require a serious commitment to proactive threat hunting and improving anomaly-detection capabilities.

1 Source: ESG Research, The Evolution of Endpoint Security Controls and Suites, July 2017. All ESG research charts and data presented in this buyer’s guide has been taken from this survey unless otherwise noted.
In terms of the risk level to your organization’s endpoints, how concerned are you with each of the following threat types? (Percent of respondents, N=385)

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Not concerned</th>
<th>Concerned</th>
<th>One of our top concerns</th>
<th>Our top concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted penetration attacks</td>
<td>7%</td>
<td>29%</td>
<td>37%</td>
<td>11%</td>
</tr>
<tr>
<td>Multi-stage attacks which may exploit a legitimate application to execute a script as part of its attack chain</td>
<td>8%</td>
<td>28%</td>
<td>39%</td>
<td>10%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>7%</td>
<td>27%</td>
<td>40%</td>
<td>9%</td>
</tr>
<tr>
<td>Exploits that take advantage of vulnerabilities in legitimate, but unpatched software</td>
<td>6%</td>
<td>29%</td>
<td>39%</td>
<td>8%</td>
</tr>
<tr>
<td>Targeted malicious software</td>
<td>5%</td>
<td>27%</td>
<td>43%</td>
<td>7%</td>
</tr>
<tr>
<td>Commodity/mass malicious software</td>
<td>6%</td>
<td>30%</td>
<td>42%</td>
<td>6%</td>
</tr>
<tr>
<td>File-less attacks including scripts and weaponized content that take advantage of a legitimate application</td>
<td>5%</td>
<td>34%</td>
<td>38%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Some organizations deploy EDR only after they (or a business in their industry) experience a breach, often as a means to mitigate their cybersecurity risk exposure or improve detection competencies. But businesses are also implementing EDR to enable proactive use cases (see Figure 2). These can include the need to:

- Facilitate response capabilities by reducing dwell time of malware (the period between infection and detection)
- Accelerate detection through threat hunting (the proactive search of threats previously undetected based on latent indicators of compromise)
- Improve visibility into the entire threat lifecycle by better understanding specific attack-chain behaviors and hardening defenses by adjusting security policies and controls

When assessing the requirements of an EDR solution, businesses should identify current operational inefficiencies that the product can help address. Top concerns are an abundance of manual processes, inefficient endpoint security workflows, and security tools that cannot be integrated with other systems. Above all, though, organizations want a solution that can address the runaway number of threat alerts, many of which are found to be false. Whether real or erroneous, these threat alerts require intensive monitoring and triage that can chip away at resources.

How Threats Evade Detection
Cybercriminals are evading detection by using highly effective social-engineering tactics, new attack vectors, and zero-day vulnerabilities.
And then there’s the continuing shortage of skilled cybersecurity workers. It will be all but impossible to realize the full value of endpoint security without the right people. Yet finding qualified cybersecurity workers represents a huge challenge; it’s a cross-industry issue that shows little sign of abating.

Nonetheless, getting EDR right is critical. After all, a cybercriminal has to be correct only once to infiltrate a network. A security team must be right 100% of the time—or risk compromise. To be sure, no security team can be unfailingly correct, but an effective EDR solution can help improve the odds of early detection, response, and remediation.

**Figure 2. Primary Reason for Deploying or Planning to Deploy an EDR Solution**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>We need to monitor for anomalous end-user and entity behavior that could be indicative of an insider threat putting our data assets at risk of loss</td>
<td>8%</td>
</tr>
<tr>
<td>We are doing more around security analytics and believe that an endpoint forensics solution will complement and supplement this work</td>
<td>10%</td>
</tr>
<tr>
<td>My organization suffered a security breach in the past, so we are adding an endpoint security detection and response solution to mitigate the risk of another breach</td>
<td>10%</td>
</tr>
<tr>
<td>One or several organizations in my industry have suffered a security breach, so we decided to add an endpoint detection and response solution to proactively mitigate our own risk</td>
<td>11%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution can help us improve the time and effectiveness related to incident response measures</td>
<td>16%</td>
</tr>
<tr>
<td>We require visibility into the entire threat lifecycle to understand specific attack chain behaviors to respond to incidents and to harden our defenses</td>
<td>15%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution can help us improve the time it takes for incident detection by engaging in threat hunting</td>
<td>15%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution complements our existing endpoint protection platform (EPP) suite</td>
<td>14%</td>
</tr>
<tr>
<td>One or several organizations in my industry have suffered a security breach, so we decided to add an endpoint detection and response solution to proactively mitigate our own risk</td>
<td>11%</td>
</tr>
<tr>
<td>We are doing more around security analytics and believe that an endpoint forensics solution will complement and supplement this work</td>
<td>10%</td>
</tr>
<tr>
<td>My organization suffered a security breach in the past, so we are adding an endpoint security detection and response solution to mitigate the risk of another breach</td>
<td>10%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution can help us improve the time and effectiveness related to incident response measures</td>
<td>16%</td>
</tr>
<tr>
<td>We require visibility into the entire threat lifecycle to understand specific attack chain behaviors to respond to incidents and to harden our defenses</td>
<td>15%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution can help us improve the time it takes for incident detection by engaging in threat hunting</td>
<td>15%</td>
</tr>
<tr>
<td>We believe that an endpoint detection and response solution complements our existing endpoint protection platform (EPP) suite</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: Enterprise Strategy Group, 2017

**The Five Core Capabilities of an Effective EDR Solution**

An effective EDR solution should incorporate multiple technological capabilities. The specific requirements will vary by individual business needs and your organization’s cybersecurity risk posture. To help you prioritize, we’ve whittled down the must-have features to five core capabilities.

1. **An Easy-to-use, Actionable Interface**

A well-designed user interface should offer much more than a pleasing color palette and a clean format. A well-designed interface can help broaden use of the solution, enable analysts to better manage alerts, and improve workflows.

Above all, the user interface must be intuitive and straightforward. The most powerful functionality in the world will have minimal impact if cybersecurity and IT staff don’t understand how to use the tool. An easy-to-use interface, on the other hand, will allow a broader range of employees—including less-experienced security analysts and incident responders—to quickly identify and prioritize the most critical alerts.

A key component of an effective interface is an intuitive dashboard that precisely labels the impact and risk potential of identified compromises. Dashboards should present metrics and clearly defined threat scores with tools.
Dashboards Can Prompt Action

Dashboards should display metrics and clearly defined threat scores alongside actionable tools that prompt security staff to take fast, informed actions. Dashboards also should prominently display the status of incident-response efforts and active investigations.

A well-designed interface should also include integrated workflows to help streamline detection, investigation, response, and remediation. Seamless workflows are especially important to combat and contain damaging multi-stage attacks. Finally, workflows enable less-experienced tier-one and tier-two SOC analysts to triage and investigate routine alerts, allowing senior staff to tackle the most urgent threats.

An effective user interface will also allow security analysts to more quickly identify “patient zero,” or the endpoint that was the point of infection for the introduction of malware or a file-less attack. Doing so can help analysts determine what vulnerability was exploited, the attack vectors and methods used, and whether other systems have been compromised.

2. Deep Contextual Visibility

Advanced data analytics solutions promise new ways to model for, detect, and ultimately predict cybersecurity intrusions. Consequently, many businesses are rushing to implement a new breed of tools that ingest and analyze massive data sets from enterprise-wide endpoints, systems, and sensor-based devices.

To deliver endpoint data for analysis and empower the use cases discussed above, endpoints will need broad telemetric capabilities. A modern EDR solution should be able to gather endpoint telemetry that communicates activities such as:

- Process activities, including parent-child relationships, user context, and location.
- Windows registry settings and changes.
- Memory usage that indicates file-less malware or other questionable activity.
- Network reputation analysis of IP and DNS activity to understand the connectivity of endpoints.

3. High-fidelity Threat Detection

The complexity and clandestine techniques of today’s targeted and multi-stage cyberthreats make accurate threat detection an essential cybersecurity defense. Additionally, EDR tools should reduce the signal-to-noise ratio so that incident alerts are more accurate and actionable. Adding contextual information also helps prioritize responses and eliminate false positives.

Fast and accurate threat detection won’t happen without an up-to-the-minute library of actionable threat intelligence drawn from a range of reliable sources. These can include a company’s proprietary threat database, the EDR vendor’s threat intelligence, third-party threat-intel feeds, and information sourced from managed service providers.

At the core of threat detection is the ability to flag anomalous system and user activities in near-real time. For example, an effective EDR solution should incorporate prebuilt policies to identify anomalous activity associated with the following Windows processes:

Reducing False Positives with Alerts

EDR tools must reduce the signal-to-noise ratio so that incident alerts are accurate and actionable, and contain contextual information.
Detecting anomalies associated with these processes can help businesses gain deeper visibility into a possible attack chain and provide contextual information on suspicious behavior. However, doing so won’t be possible without leveraging the power of threat intelligence, including threat scores based on analysis of potentially malicious files and IP addresses. These threat scores can help security teams quickly triage alerts so the most critical threats are addressed immediately.

A threat score that exceeds a predetermined threshold should automatically trigger alerts and initiate file-reputation analysis to determine if the activity has introduced known malicious code. For example, if a suspicious process is making outbound connection requests, the EDR tool should assess reputation against IP addresses and domains.

As noted, a profusion of false-positive incident alerts can overwhelm security teams. That’s why it’s essential that endpoint security solutions help reduce false positives by scanning and collecting artifacts from endpoints as well as third-party tools like security information and event management (SIEM), network, and intrusion-detection systems. An EDR solution should also allow cybersecurity and IT staff to trigger endpoint scans based on customized policy rules. If any alerts are tied to an endpoint, an EDR solution can quickly assess its accuracy by taking a snapshot of endpoint telemetry.

4. Automation with Targeted Remediation and Forensic Tools

Detection of endpoint compromises is just one piece of the puzzle. Equally important is the need to quickly respond to threats using targeted remediation and recovery capabilities.

The rash of ransomware incidents over the past year highlights the ability to repair drives without time-consuming reimaging as a critical capability. Other essential remediation capabilities include automatically updating security policies on endpoints and quarantining infected machines to prevent lateral spread of infections.

Here again, it’s important that targeted remediation include automated forensic capabilities, which can empower staff to acquire, triage, and investigate evidence in endpoints across a range of operating systems. Analysts should be able to perform remediation tasks—like killing a process, deleting a file, and resetting or deleting a registry key—without having to reimage drives.

Also keep in mind that EDR solutions should be able to collect threat forensics in ways that allow analysts to investigate incidents using reverse engineering and sandboxing. Forensic data can also help security teams return systems to a pre-remediation state if a mistake is made as well as collect evidence for legal purposes.

5. Integration with Internal and External Solutions

Increasingly, businesses want to maximize their endpoint security investments by integrating solutions with existing security tools, often as a part of a larger cybersecurity initiative. At the same time, organizations want to eliminate multiple solutions that incompletely address endpoint security needs. The end goal is fewer security solutions that meet all endpoint security requirements.
Internally, there’s a lot of value to be gained from tying EDR solutions to existing security tools like SIEMs and network security controls. Doing so can enable businesses to amalgamate and index systems and log data—including data from connected sensor-based endpoints—that is generated and stored across the digital ecosystem. Once centralized, EDR telemetry can help security analysts correlate data to sharpen contextual visibility into attacks that span endpoints and networks.

To facilitate integration, EDR solutions should incorporate both out-of-the-box capabilities as well as a rich set of APIs for customized connections to external services. The use of APIs for integration offers a particularly seamless way for businesses to efficiently gather and analyze data, identify critical alerts, and take targeted action.

Businesses can also employ APIs to connect to advanced third-party services like data analytics, artificial intelligence (AI), and cognitive machine learning. Analytics and AI technologies can help deliver comprehensive, actionable information after a breach, while machine learning can identify vulnerabilities before an intrusion with tactics like unknown threat detection and anomalous user behavior to help predict compromises. What’s more, APIs enable seamless integration to orchestrate incident response and streamline workflows, which can deliver valuable operational efficiencies.

Some organizations are going beyond integration of point tools. Increasingly, forward-thinking companies are implementing a security operations and analytics platform architecture (SOAPA) to serve as a hub for integration of security technologies. In fact, an ESG survey found that 21% of respondents said building a SOAPA by integrating an assortment of disparate security point tools is a top priority. The reason? Deployment of innovative and highly intelligent security analytics technologies can help boost operational efficiencies and lighten the workload of security staff.

The Bigger Truth

The proliferation of cyberthreats and expansion of operational inefficiencies have made a contemporary EDR solution a critical component of any cybersecurity program. To be successful, an EDR implementation will demand a carefully crafted strategy that matches an organization’s specific operating and risk environments with comprehensive endpoint security capabilities.

When researching EDR tools, you should focus on five key requirements:

- An intuitive, easy-to-use interface
- Deep contextual visibility enabled by advanced telemetry
- High-fidelity threat-detection capabilities
- Targeted remediation and forensic tools
- Integration with internal and external solutions

It’s also important to plan for adequate staffing resources and cybersecurity expertise to manage the EDR solution. That will be a tall order for many, given the current cybersecurity talent squeeze. When carefully calibrated and correctly


© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.
implemented, an EDR solution can make you more proactive about security, help you thwart even the most elusive cyberthreats, including multi-stage and targeted attacks, and help you address a multitude of operational inefficiencies.

The right solution can also help you advance your cybersecurity defenses as you plan for the next evolution of threats. Implementing more advanced telemetric capabilities and other technologies that support a broader data analytics initiative can give you a head start on leveraging next-generation technologies and preparing for the ever-more complex threats that are certain to surface.