SANS

A SANS Whitepaper

Passive Isn't Good Enough: Moving into Active EDR

Written by **Justin Henderson**

May 2019

Sponsored by:

SentinelOne

Introduction

Life today is full of surprises. While infections from browsing malicious sites are still a reality, modern attacks are becoming more prevalent than ever. Now, malware can infect a system using nothing but the binaries already on the system itself, and other flavors of malware—such as ransomware—can encrypt an organization's files, causing massive business disruptions. What this means is that both old and new attacks are in play. Combating this requires endpoint controls that are mature enough for advanced prevention, detection and response capabilities.

The question one may ask is: Why the focus on endpoint controls? Placing a next-generation firewall at the edge to centrally analyze traffic is a simpler control to maintain. However, the firewall and many alternative network controls lack visibility due to several factors: Encryption blinds them; they are unable to see traffic flowing through them, such as a laptop entering and exiting the network; and they don't have visibility into what is occurring on an endpoint.

Attacks against a desktop, laptop or server contain massive amounts of digital interaction that can be useful for future prevention and detection. Let's take the example of ransomware: It deals with invoking encryption tools or built-in application programming interfaces, may connect to multiple remote file shares, touches numerous files and often runs under the context of the user who ran the malware.

Given the challenges posed by modern-day attacks, organizations need to identify a holistic endpoint solution that provides modern detection and prevention capabilities. To that end, we look beyond traditional endpoint detection and response (EDR) and endpoint protection platforms (EPP) to evaluate and consider implementation of Active EDR solutions. Active EDR provides enterprise scalability with the ability to provide real-time detection, response and prevention controls without the massive labor and performance overhead common to both EDR and EPP.

To help organizations identify the appropriate modern endpoint security controls, this paper will provide:

- A better understanding of EDR and EPP controls
- Capabilities to look for in selecting an effective endpoint security solution
- Information on why endpoint controls are necessary
- How to factor in staff when considering a solutions implementation
- How to justify moving to a new endpoint solution

The State of EDR and EPP

Modern malware is sophisticated and constantly changing. Fortunately, plenty of products provide detection capabilities to keep up with the constant changes. One of the predominant solutions is endpoint detection and response. An EDR solution focuses on all the various areas of digital interaction that occur within an endpoint operating system. The analysis of networking, process creation and termination, DLL injection and more means EDR comes with substantial visibility. The goal of an EDR solution is to detect anomalous activity at scale. However, not all EDR solutions are equal. There are many vendor variations of EDR, some with major problems. As you evaluate tools, consider the following:

- Signature-based EDR solutions are more akin to traditional antivirus with better logging. They do not handle new attacker techniques or malware because their rule sets are too specific and lack behavioral context.
- Cloud-based EDR solutions often perform analysis in the cloud, resulting in delays and end users having to wait to perform tasks. This means prevention and detection capabilities are not performed in real time.
- Internally deployed EDR solutions require planning for future growth. EDR involves a massive amount of endpoint data and must be able to scale as assets are added.
- For any EDR solution, the most important consideration is how much time and staff are necessary to analyze anomalies. It is common for an organization to purchase an EDR solution only to find out it cannot maintain or use it due to staffing limitations.

For any EDR solution, the most important consideration is how much time and staff are necessary to analyze anomalies.

While advanced detection capabilities are necessary for today's environment, many organizations ignore solutions such as EDR or SIEM in favor of prevention-oriented solutions such as EPP. The mindset is that it is better to prevent an attack rather than detect it, so it is best to place more priority on prevention controls. Thus, EPP technologies focus on advancements in prevention beyond signature-based controls.

For example, EPP solutions often include capabilities such as threat intelligence, sandboxing and behavior analytics using various applied data science. Oddly enough, the same techniques can be found in EDR platforms, but the use case is different. EPP uses the data to identify and block activity that is highly anomalous. EDR can block activity but tends to place more emphasis on reporting activity that is anomalous based on different severity levels. As with EDR, there are many vendor variations of EPP. The following are some areas to be cautious of when choosing an EPP solution:

- Some EPP solutions still focus heavily on signature-based controls. Threat intelligence, while important, still leans toward signature-based identification.
- Other EPP solutions are rebranded traditional technologies like antivirus, host-based intrusion prevention and application whitelisting combined together.
- Not all EPP products have the same capabilities. Some have little to no support for detecting modern attacks. For example:
    - **Memory resident attacks—**Some EPP products cannot analyze memory or have the capability turned off by default.
    - **Live-off-the-land attacks—**Operating systems have tools such as PowerShell available, and malware can use the built-in tool. Some EPP products ignore existing operating system binaries and capabilities.
- Many EPP solutions tout advanced prevention capabilities yet do not support key monitoring integrations such as integrating with Microsoft's Antimalware Scan Interface. In this case, vendors are either reinventing the wheel or likely missing visibility into certain attack methodologies.
- Prevention ultimately fails. Detection is critical, and a response is vital.

To be clear, traditional defenses like antivirus are completely insufficient today. EDR and EPP are better equipped to deal with modern attacks, but both have key flaws. Instead, a combination of the two, with emphasis on better handling large-scale data, is necessary. Gartner correctly states in "The Evolution of Endpoint Protection" that a convergence of EDR and EPP is necessary and a natural progression.[1] Vendors are now in a race to successfully converge EDR and EPP solutions into a single effective product, resulting in multiple in-between product states and variations.

[1] "The Evolution of Endpoint Protection," www.gartner.com/imagesrv/media-products/pdf/symantec/symantec-1-4SNI36O.pdf?es_p=6816496

Detection at Scale

Detection is one of the most important capabilities an organization can have. EDR solutions attempt to provide detection capabilities by analyzing data and generating anomalies. With all the endpoint visibility tools and analytics available, these anomalies often identify incidents and malware. But is the implementation of an EDR solution enough to generate tons of meaningful anomaly detection? Take a moment and think about these next statements. EDR solutions commonly generate so many alerts that organizations do not have enough staff to analyze each anomaly. If an anomaly detects an attack but no one has time to review it, respond to it and remove the threat, we would argue that the organization has only the potential for detection. Not good enough!

Active EDR solutions focus on detection that enables a response. Instead of identifying a bunch of anomalies that lack context and require massive labor investments, an Active EDR solution focuses on providing effective and actionable detection capabilities. Detection with Active EDR delivers:

- Real-time endpoint analytics
- Anomalies with context
- A story on what happens within the endpoint
- Actionable data ready for human consumption

To achieve the above points, EDR must evolve into Active EDR. This evolution requires changing focus and how we think of endpoint security. Pushing endpoint data to a cloud solution or even an internal centralized system to apply data analytics means a delay in detection, which can result in a lack of data due to network issues. Instead, analytics need to be completed in real time. With Active EDR, the endpoint is now the active asset potentially running malicious code. The same endpoint has full visibility and can apply data analytics locally. The analytics can and should include applied data science, such as machine learning and artificial intelligence, to automatically identify features that indicate normal versus potentially malicious or unauthorized. While data science is often thought of as requiring massive computing power and supervised learning through large data sets, the truth is that there are many methods of applying data science in real time with minimal performance overhead.

To simplify an understanding of what local data analytics is doing, consider the Windows process **`svchost.exe`**. Under normal conditions, the **`svchost.exe`** process has the following traits:

- It is always created from the parent process of **`services.exe`**.
- Multiple instances of **`svchost.exe`** run concurrently.
- Each instance comes from the binary at **`%SystemRoot%\system32\svchost.exe`**.

Malware likes to hide in plain sight. Therefore, malware may create a **`svchost.exe`** binary that breaks some of the normal conditions. If an analyst knows and understands the normal use of **`svchost.exe`**, then he or she can identify the anomaly. The example of **`svchost.exe`** is an easy use case because it is a documented Windows binary. But what about all the undocumented binaries? With local data analytics, an Active EDR platform can automatically identify anomalies based on learned behaviors. The difference between EDR and Active EDR is that Active EDR not only finds these kinds of anomalies but also automates the analysis of the anomaly.

The result for Active EDR is an anomaly that has been pre-analyzed and tells a complete story. So, instead of generating an anomaly that notes **`svchost.exe`** is running under an unusual parent process, an Active EDR solution analyzes surrounding data, including information on the parent process, the user account involved, related network connections, DNS cache information and anything else related to the anomaly, to determine whether the anomaly is malicious.

The difference between EDR and Active EDR is that Active EDR not only finds these kinds of anomalies but also automates the analysis of the anomaly.

Consider the following sequence of events:

- An end user receives an email with a malicious Microsoft Word document.
- The end user opens the Word document.
- Microsoft Word launches a macro that invokes PowerShell.
- PowerShell then makes an external connection to an attacker-controlled server.
- The malware uses the connection for command-and-control activities.

With traditional EDR, an anomaly would show that Microsoft Word is involved with an unusual macro call to PowerShell. The anomaly sits in a queue waiting for an analyst to see it and investigate why Microsoft Word made a call to PowerShell.

With Active EDR, the results are significantly different. This time, the anomaly contains associated information, such as where the PowerShell code made network connections (including the IP address and domain name), where the document originated, and the email used to access the initial attachment. From an analysis comparison, the Active EDR anomaly provides context and a full story from which analysts can make appropriate responses.

Consider how much time these two anomalies would take to analyze. The first one only tells an analyst that Microsoft Word launched PowerShell. A skilled analyst would take this and begin trying to answer basic questions. Is this malicious? Did PowerShell make any network connections? Where did this document come from? In this author’s experience, the investigation of these questions would take an analyst between 15 and 60 minutes.

The Active EDR anomaly provides analysis as part of the anomaly. Again based on this author's experience, the investigation for the Active EDR anomaly would take between five and 15 minutes. Figure 1 shows a best- and worst-case scenario time comparison for investigating the PowerShell from Microsoft Word anomalies between EDR and Active EDR.

Now take this timing and multiply it by the number of anomalies generated in a day. The number of anomalies varies from a few a day to as many as hundreds or thousands. Figure 2 shows the impact of investigating 50 to 200 anomalies.

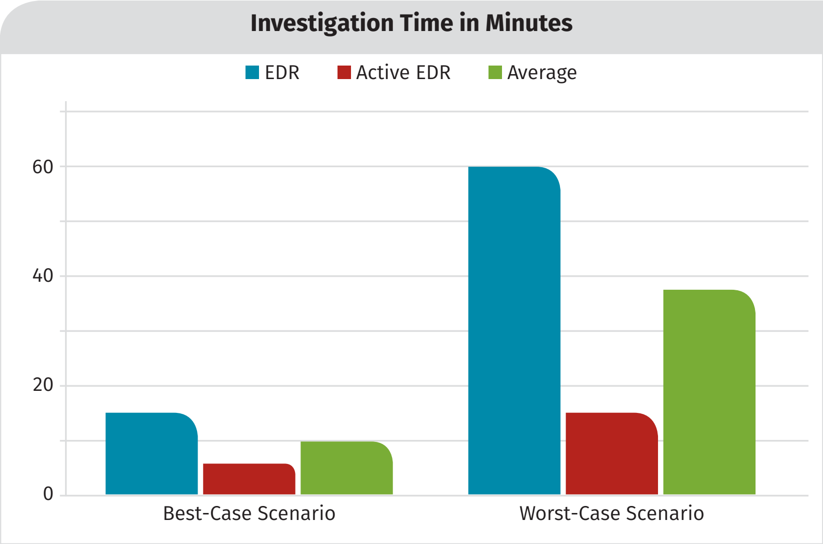

Figure 1. Investigation Time of EDR Compared with Active EDR

For 50 anomalies a day, EDR would require between 13 to 50 hours to investigate. In labor, this would be two to six full-time analysts. Under Active EDR, this changes to between four and 13 hours to investigate, or one to two full-time analysts.

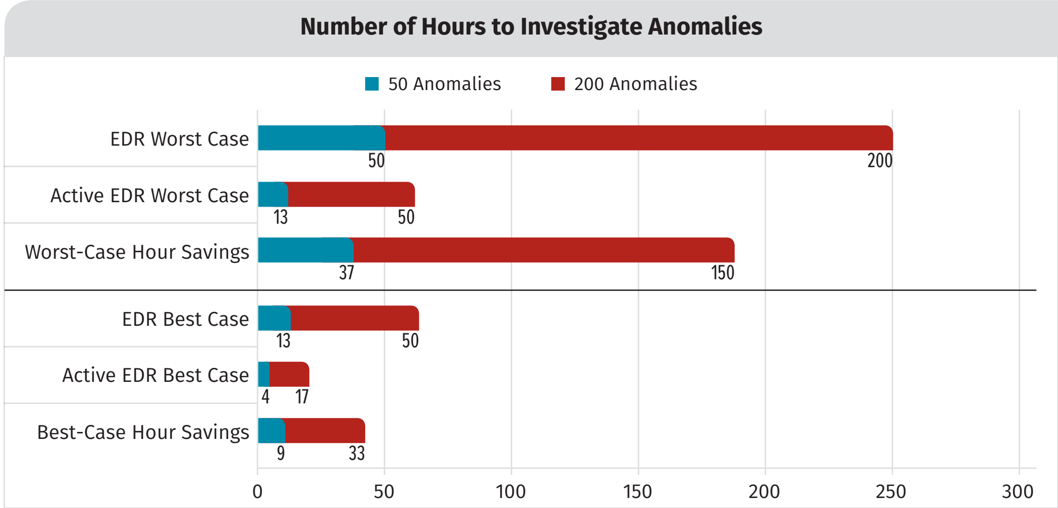

Figure 2. Comparison Time of 50 to 200 Anomalies

Based on these numbers, a major benefit of Active EDR is that it provides enough context that analysts can keep up with the anomalies it generates. In truth, the above analysis doesn't provide the whole picture. Under Active EDR, the context and story would be used for both presenting actionable data and eliminating false positives. The end result is that Active EDR not only makes it quicker to analyze anomalies, but also reduces the number of anomalies to analyze. This translates into Active EDR providing true detection capabilities.

TAKEAWAY

When investigating traditional EDR, it is important to calculate how much staff time the solution requires. Failure to do so results in a detection capability that does not provide detection. Active EDR reduces the staff time required, eliminates false positives and reduces the number of anomalies the staff needs to investigate. It truly does provide detection at all levels.

Detection Meets Prevention

Active EDR provides scalable, actionable detection against modern threats, and organizations can benefit greatly from it. However, that's not the only advantage Active EDR provides. Active EDR also offers sophisticated prevention capabilities even beyond EPP or prevention-based EDR solutions. The difference again lies with the scope of the analysis. Commonly EPP and EDR solutions do the following:

- Perform file-based analysis of malware
- Scan memory against known bad signatures or reputation-based scores
- Send binaries or commands to a cloud system or centralized server for analysis
- Use multiple solutions, such as antivirus, host-based intrusion prevention and application whitelisting, and then combine logic centrally

Prevention technologies that do not perform behavior analytics will fail to prevent unauthorized activity due to being too black and white. Simple allow or block rules are insufficient when data governance and access dictate flexibility. To add behavior analytics, products often stream endpoint data to a cloud solution. Organizations are told the cloud is bigger and better, but that is not always the case. Endpoint solutions generate enormous amounts of data. Streaming data for hundreds, thousands or more endpoints takes time and a good chunk of network bandwidth. Moreover, sending data to a centralized system results in poor performance or downtime for end users. With many solutions, either a system allows unknown code to launch and potentially cause an infection or an end user must wait for central analysis to complete.

With Active EDR, the same data analytics that generates story-driven anomalies also prevents unauthorized activity. By applying analytics directly on the endpoint, prevention controls gain the following benefits:

- Real-time blocking
- Advanced decision-making via artificial intelligence
- Context behind why something is blocked
- Response capabilities beyond a single endpoint

Consider the previous attack scenario involving Microsoft Word and PowerShell. If the same attack scenario were attempted under an Active EDR solution, it is likely that Active EDR would prevent the attempt to launch PowerShell code from Microsoft Word. The decision to block PowerShell would include whether it was because of the type of code PowerShell attempted to run or because Microsoft Word should not be launching PowerShell based on analysis of the day-to-day use of the computer. Also, additional context, such as where the Microsoft Word document came from and the user's context, would be included in the block event. Based on that analysis and context, Active EDR would successfully block the malicious code and notify the organization with full details on why the code was blocked and the story of what happened.

TAKEAWAY

In the case of prevention controls, Active EDR's behavior analytics increases the prevention capabilities and provides the context behind why something is blocked. The labor savings and accuracy of context-driven controls result in organizations spending less time tuning a prevention control as well as less time investigating a blocked event. This translates to better prevention capabilities, greater context and a storyline on why a potential threat is stopped.

Conclusion

Endpoints have the largest digital footprint and capability for detecting and preventing unauthorized use. As discussed throughout this paper, a combination of both detection and prevention is necessary to win in today's world. EPP provides solid prevention capabilities but suffers from weaknesses such as analyzing memory-resident malware. EDR focuses so much on identifying potential incidents that the anomalies it generates are too difficult to keep up with and analyze.

Endpoint products such as EDR and EPP are no longer pure detection or prevention technologies. Instead, they are blending prevention and detection together. Organizations need to consider how well they blend and perform the analyses.

Furthermore, organizations require an endpoint solution that scales, is easy to maintain and provides a comprehensive analysis for detection and advanced prevention capabilities. Active EDR is not a product; it is a solution that offers a combination of EDR and EPP solutions with an emphasis on fixing their current weaknesses.

Knowing this, organizations should perform a self-assessment of their approach to endpoint security and look for Active EDR solutions that fit their environment. A few questions worth asking are:

- Are existing EDR or EPP controls consuming too much time to maintain?
- Will they fail to scale as the organization grows?
- Are red team penetration assessments able to bypass prevention or detection capabilities?
- Is advanced malware a threat the organization is concerned about?
- Is having an alert or anomaly without context an ongoing issue?

If the answer is yes to any of these questions, it may be time to look at alternative controls that include Active EDR. Active EDR is the evolution of EDR and EPP solutions and addresses each of these concerns and more. It is a modern technology that provides real-time threat hunting combined with automated analysis and reports. And it can provide organizations with a scalable, more comprehensive prevention and detection technology.

TAKEAWAY

Active EDR helps organizations focus on lowering risk. By providing context and a story on why something has occurred, organizations can spend a fraction of the time it typically takes to review or investigate their endpoints.

About the Author

Justin Henderson is a certified SANS instructor who authored the SEC555 (SIEM with Tactical Analytics) course and co-authored SEC455 (SIEM Design and Implementation) and SEC530 (Defensible Security Architecture). He is a member of the SANS Cyber Guardian Blue Team who is passionate about making defense fun and engaging. Justin specializes in threat hunting via SIEM, network security monitoring and ad hoc scripting.

Sponsor

SANS would like to thank this paper's sponsor:

SentinelOne™