Threat Defense Isn't Just About Detection: It's How You Respond

WHITE PAPER

Organizations looking for more intelligence and automation within their security defenses should include endpoint detection and response solutions to thwart new threats and protect endpoint-accessible assets.

Table of Contents

The Case for Intelligent Endpoint Security

An intelligent endpoint is one that is highly automated to detect security problems faster and more accurately, respond immediately and remediate problems fully. If done correctly, intelligent endpoints provide invaluable insights and forensics into threat behaviors.

In order to stop increasingly sophisticated threats, many security and IT organizations have focused on endpoint detection and response (EDR). Creating truly intelligent endpoints requires a comprehensive and easily managed security framework, one that automatically detects and responds to threats before they do their damage. If an intelligent endpoint is your strategic goal, then meaningful integration and flexibility are important aspects to consider in an EDR solution.

Why Does EDR Matter So Much?

Beyond stopping the sheer volume of threats, detecting and protecting against advanced threats has become essential to maintaining trusted endpoints. Endpoint security supplements centralized security measures with additional protection at the point of entry for many threats as well as effectively blocking access attempts prior to entry.

Another stark reality is that advanced threats are, by nature and design, attacking more than one endpoint at a time in order to gain access to valuable data and systems through multiple footholds. It is increasingly rare that a security breach can be contained within a single system or application, in large part because so many attacks successfully evade security point products.

TechTarget® Custom Media
A TECHTARGET WHITE PAPER

Additionally, security administrators are stretched to capacity trying to be experts on emerging threats and react in time to stop impending data breaches. Threats evolve, requiring administrators to learn and evolve, as well. Meaningful insights and automation are necessary to keep security professionals informed and moving forward.

This means the emphasis has shifted from trying to stop attacks to quickly pinpointing, identifying and shining a bright light when attacks occur. Determining which endpoints are being attacked, what data is vulnerable and how quickly it can be remediated before massive damage is done is paramount.

That's where EDR comes in. According to Gartner,[1] the EDR market is defined as solutions that have the following four primary capabilities:

1. Detect security incidents.
2. Contain the incident at the endpoint, such that network traffic or process execution can be remotely controlled.
3. Investigate security incidents.
4. Remediate endpoints to a preinfection state.

Together, these capabilities help organizations that have largely depended on manual processes address threats in a more intelligent, efficient and timely manner. By 2018, 80% of leaders' and visionaries' endpoint protection platforms will include endpoint detection and response capabilities—up from 45% in 2016.[2]

By 2018, 80% of leaders' and visionaries' endpoint protection platforms will include endpoint detection and response capabilities **— up from 45% in 2016.**

Gartner, *Market Guide for Endpoint Detection and Response Solutions*, 16 December 2015

EDR is all about speed and agility; it helps organizations reduce their windows of threat exposure from weeks or days to just minutes. The best EDR sorts through all the noise most security defenses yield, which often shows up as inordinate numbers of alerts or rising incidents of false positives.

With the cost of remediating a data breach now exceeding tens of thousands of dollars per day, the pressure has intensified to spot problems with greater reliability and speed, to correct them immediately and to protect against further endpoint incursions and data exfiltration.

At the end of the day, intelligent endpoints must be able to spot trouble, avoid it and limit the damage when threats do strike. It's one thing to say you have a problem; it's an entirely different thing to fix the problem immediately or prevent it altogether.

What to Look for in an EDR Solution

Historically, the focus of EDR solutions has been on first-level defenses—primarily detection and investigation. Obviously, those are important, but they are quickly becoming table stakes. As threats continue to increase and become more sophisticated, organizations will need to look for solutions that are proactive in preventing attacks and remediate them quickly and thoroughly if they do get through.

There are two major design attributes you should look for as part of your EDR functionality: integration based on common architecture and centralized management. Because organizations already have numerous security solutions such as antivirus, IPS, gateways and firewalls in their security infrastructure, the best approach is to have a common integrated architecture that allows those and other security solutions to work together in order to share insights and respond faster. Managing through a single pane of glass improves visibility, cuts down complexity, and prevents the gaps and overlaps of disparate solutions.

Here are some of the specific EDR capabilities and integration points you should be looking for as part of an intelligent endpoint solution:

- Access to and integration with a threat intelligence environment that supports endpoint threat detection and real-time information sharing

- Pervasive connection to a secure web gateway, which prevents the majority of both known and zero-day malware delivery wherever the endpoint travels—even off-network
- Seamless integration with traditional endpoint security (AV, HPS, Firewall, HIPS)
- Centralized management for improved visibility, monitoring and quick access to events and automated responses
- Hunting and automation capabilities that radically accelerate the ability to detect and remove advanced threats

Conclusion

No security professional wants to acknowledge that their systems can't stop all current and future advanced attacks. Unfortunately, the reality is that the speed at which threat tactics are evolving leaves most organizations in need of a serious upgrade and modernization of their endpoint defenses. Making a new breed of endpoints more resilient and intelligent is a high priority, and EDR is at the heart of that effort.

Without faster, more reliable and more efficient endpoint security, IT and security professionals will spend more time fighting fires and chasing the next new thing in advanced threats—often long after the damage has been done. EDR helps rebalance the equation in favor of integrated, collaborative, automated defenses that detect and take action rapidly to shorten the window of time new and emerging threats have to wreak havoc. It also offers greater insights into the behavior, origins and methods attackers are using so that administrators can leverage those forensic details to harden their policies and educate users.

McAfee has long been a market leader in endpoint security; its solutions are built around the key concepts of integration, automation and centralized management. The company offers a broad range of intelligent endpoint security products, including McAfee Endpoint Security 10 and McAfee Active Response. McAfee Endpoint Security 10 leverages technologies that communicate and learn from each other in real time to combat advanced threats and deliver insights with actionable threat forensics. It is also built with a framework designed with the future in mind and is extensible so that even more of your endpoint solutions can be centrally managed as your business grows.

McAfee Endpoint Security 10 features a native connection to both the cloud and on-premises McAfee Web Gateway. This helps security teams shift from the firefighting activity of constant remediation to strategic threat defense by preventing the vast majority of known and zero-day malware from reaching endpoint systems.

One of the key elements of McAfee Active Response is its ability to seamlessly integrate with antivirus, gateway and intrusion detection systems. This not only strengthens the investment organizations have already made, but it also facilitates the sharing of security intelligence based on activity at different endpoint locations and actionable insight from the company's threat intelligence exchange.

These solutions are centrally managed by McAfee ePolicy Orchestrator, a single-pane-of-glass management console. Additionally, the organization's Foundstone Services group takes incident response and endpoint protection to a new level by combining remediation with forward-thinking preventative measures.

For more information on McAfee's approach to intelligent endpoints and EDR, please go to **http://www.mcafee.com/us/products/active-response.aspx**.

DigitalEra • *Trusted Cybersecurity Advisors*

DigitalEra helps organizations of all kinds protect data, systems and people. We assess and solve complex security challenges, provide guidance on security technologies and solutions, and implement comprehensive security strategies and solutions.

4831 SW 75th Avenue | Miami, Florida 33155
786.621.8600 | www.DigitalEraGroup.com

digitalera
Trusted Cybersecurity Partners

McAfee™
Together is power.

[1] Gartner, *Market Guide for Endpoint Detection and Response Solutions*, 16 December 2015

[2] Ibid.