DATA SHEET

Endpoint Detection & Response

Why is Endpoint Detection & Response (EDR) important?

Endpoint detection and response (EDR) should be considered a foundational technology requirement for any IT environment because of its success in reducing the business impact of attacks. EDR provides protection and mitigation capabilities across the attack lifecycle.

At the beginning of the attack lifecycle, EDR provides strong prevention capabilities to block malware from executing, exceeding legacy antivirus' capabilities. Should a threat slip through, EDR provides multiple opportunities across the attack lifecycle to detect and investigate threat activity. Should a threat actor establish a foothold in an environment, EDR provides security personnel with a rapid means of containing the attack.

Prevent

Though there are no silver bullets capable of preventing every attack, leading EDR tools' prevention capabilities are effective at stopping a variety of common attack scenarios. From a prevention standpoint, EDR tools are most effective in key phases of the attack lifecycle, where a small intrusion has the potential to turn into an enterprise-wide incident.

For example, when an attacker gains initial entry into the environment by exploiting a vulnerability and deploying backdoor malware to remotely control that system, EDR is well positioned to detect and block aspects of that process. If an attacker gains entry and attempts to escalate privileges, that activity is also a prime candidate for detection and automatic blocking by EDR. In a ransomware scenario, where the attacker has obtained the necessary privileged credentials and is poised to mass execute a ransomware encryptor, that activity too is ripe for being blocked by EDR.

In addition to EDR's direct risk reduction benefits, potentially malicious executions that are stopped reduce the number of alerts that your security team needs to triage. From a human capabilities perspective this helps analysts be more effective at their jobs.

Benefits of working with MOXFIVE

IT & Security Expertise On-Demand

With a deep understanding of both IT operations and security, MOXFIVE Technical Advisors can provide the expertise you need and help determine the most efficient and cost-effective solution.

Access to Experts at Scale

MOXFIVE maintains an ecosystem of the industry's best technology experts and service providers so we can quickly assemble the right team with the skills you need.

Streamlined Process

MOXFIVE manages the selection, implementation and procurement processes to keep projects on schedule and minimize disruption.

Resilient Outcomes

MOXFIVE identifies gaps between business, IT and security objectives to build a more resilient environment.

Detect & Investigate

EDR provides a game-changing degree of visibility across the environment, which becomes especially valuable whenever analysts need to understand what events transpired on a particular system or group of systems. Having an EDR tool in place can make the difference between a minor incident being triaged and contained within a few hours, and a major intrusion event that takes weeks to resolve amidst significant business disruption. Let's consider the example where a significant vulnerability becomes publicly disclosed. It is severe because an attacker who exploits it can take over an Internet-facing server at an administrative level of privilege.

Security teams want to understand whether there is any evidence that the vulnerability was exploited in their environments. With EDR tools installed, analysts can query several sources of potential evidence remotely, in real time, and spend an hour of review to determine whether or not such evidence exists. If the initial analysis shows that suspicious activity occurred recently analysts could then quickly query systems across the environment and gauge the potential impact in a matter of hours. They could also easily bring in additional team members to help them review data, and also leverage outside expertise or surge support if needed.

Without EDR, that process may take days as various methods are cobbled together to provide the necessary data. If there is an active attacker in the environment, these methods will not be quick enough to get ahead of the attacker. Without EDR, analysts are forced to focus on the mechanics of getting answers, rather than applying their expertise to analyzing data and acting to contain. This approach does not scale and limits the effectiveness of a scarce and valuable resource – security analysts' time.

Contain & Eradicate

Modern EDR tools provide a range of capabilities that can be used to stop attacks and remove attacker tools from systems. Having them at responders' fingertips, particularly when fighting an active attacker, simplifies and shortens the time to contain.

- Quarantine system (network isolation)
- Stop processes
- Delete registry keys and file associated with malware and attacker tools
- Run customized actions via scripts or by manual interaction with the system

www.moxfive.com
(833) 568-6695
info@moxfive.com

MOXFIVE