CounterTack®

What To Look For...

...In Endpoint Detection & Response Tools and Services

Organizations are quickly learning that keeping the bad guys out of an enterprise environment isn't as simple as deploying firewalls and antivirus.

As cybercriminals utilize customized malware and bypass traditional antivirus solutions, it's become necessary to take a broader and more proactive approach to protect the endpoint. This means real-time monitoring, detection and advanced threat analysis coupled with response technology.

A multitude of EDR tools on the market, accompanied by short-staffed IT teams, can create confusion for organizations making it not so simple to implement. This document will break down what IT professionals need to know about EDR technology as well as best practices when considering and implementing an EDR platform.

EDR - The Basics

Companies are now required to pay closer attention to their endpoints including the attackers' activity once in and how employees are behaving on their devices. Organizations have found that prevention-only measures won't do the trick, as they do not provide the level of context needed for addressing and managing the aftermath of an attack.

The Benefits

EDR technology offers a number of benefits including:

- More in-depth: Deeper detection and response.
- Always on: Continuous monitoring, threat hunting and remediation capabilities.
- More visibility in real-time: The ability to counter advanced attacks and gain more real-time insight into how these attacks are impacting customers.

Finding A Solution for You

Endpoint protection solutions differ substantially, ranging from the classic signature-based antivirus software, to more mature solutions with capabilities that can scale via Big Data technologies, including deep security monitoring, threat detection and incident response capabilities.

ANALYST PERSPECTIVE

Endpoint detection and response tools are an important component of modern security architectures. Existing tools support organizations trying to quickly detect, identify and react to threats on workstations and servers.

- Augusto Barros, Anton Chuvakin; Gartner, Inc. June 2016

The EDR Check List: Is Your Organization Susceptible to Endpoint Attacks?

Before you can evaluate an EDR solution, first determine the level of susceptibility and ask questions such as:

- Do your end-users have mobile or other high-risk devices that you don't have visibility into?
- Are your users using laptops and connected mobile devices outside of your network?
- Are your users able to visit websites of their choice?
- Are your employees sharing their connected systems with others, such as family members and clients?
- Is your organization in a high-risk field, such as critical infrastructure, government and government contracting, healthcare, financial services, or professional services that support those fields?

Understand the threats and evaluate previous experiences

It's critical to have a firm grasp on the types of attacks that can impact your organization.
Ask yourselves these questions:

- Are you regularly subjected to attacks? If yes,
    - Are attacks persistent?
    - Are attached difficult to remove?
- Have you already experienced a data breach and if so, how severe was it and what was taken?
- Were you able to gather the information you needed to understand the attack or breach?
- Would a breach of systems or data create a negative impact to your organization, your clients, your customers or the public?

The Challenges

Once you create a checklist and begin evaluating your organization, you may find that taking advantage of the various endpoint technologies available, and integrating them with other security offerings, can be expensive and difficult to manage. Across the board, shortages in skilled IT staff are also creating difficulties when it comes to integrating new technologies.

Outsourcing - Easing the Process of Finding Talent

Simply purchasing the latest and greatest piece of technology is not enough today. An organization needs full-time employees to manage the technology they purchased to ensure it's operating effectively and to get the most value. On the other hand, finding the talent to manage EDR and other technologies in-house can be extremely difficult as the industry is facing a shortage of skilled workers with more than a million jobs in the cybersecurity industry vacant around the world. As a remedy, businesses are turning to managed security services providers (MSSPs) to manage the technology for them.

Increased Visibility

Many organizations have minimal visibility into threat intelligence without expensive threat intel teams.
Partnering with a trusted adviser gives access to global threat intelligence that can be leveraged in proactively using EDR solutions to look for indicators of compromise in the client environment. Working with a MSSP provides both management of these capabilities and a wide set of crucial global threat intelligence.

CounterTack®

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com