Endpoint Detection and Response Solutions - What One Needs to Know

Robust cybersecurity measures like endpoint detection and response solutions protect a company's information from bad actors trying to steal sensitive data.

Endpoint Detection & Response

LONG BEACH, CA, UNITED STATES, October 3, 2022 /EINPresswire.com/ -- Investing in cybersecurity for a business ensures end-to-end protection against malware, viruses, data breaches, and ransomware. With endpoint security explained, one can better understand this modern approach to digital security and choose the right security features for a business.

What is Endpoint Detection and Response?

Endpoint detection and response (EDR) is a next-generation security service concerned with monitoring a company's endpoints (devices like desktops, laptops, mobile phones, and tablets) for malicious activity. EDR protects against threats by combining endpoint data analytics and rule-based automated response.

EDR relies on artificial intelligence (AI) and machine learning (ML) to quickly detect, investigate, contain, and eradicate cybersecurity threats and other abnormal behavior. While it is impossible to prevent every security breach, EDR ensures awareness of all anomalous endpoint behavior and offers better protection than traditional security tools like antivirus software and firewalls.

EDR gives a company a direct lens into its security environment, invaluable in a climate that prioritizes information security. Companies can use EDR to:

- Uncover stealthy attackers automatically
- Integrate with cyber threat intelligence
- Proactively defend by threat hunting
- Enable quick and decisive remediation
- Provide real-time and historical visibility

- Speed up investigations

6 Reasons to Include EDR in a Security Strategy

1. Prevention by itself cannot ensure 100% protection
Despite preventive measures, most cyber attackers generally find a way to penetrate defenses, leaving an organization in the dark. Without EDR to identify them, attackers can linger and navigate inside a network.

2. Attackers remain inside the network and come back
When an attacker enters a network unnoticed, they can stay in the environment for weeks and create back doors that allow them to return anytime. Without EDR, a company may not learn about the breach until a third party, like law enforcement, intervenes.

3. Gives visibility to monitor endpoints
Without EDR, it can take months to discover and remediate a breach. The visibility offered by EDR allows for a full understanding of attacks when they occur so that a business can strategize preventative measures for future breaches.

4. Access to actionable intelligence
Unlike many traditional security methods, EDR allows organizations to record relevant security information, store it, and access it immediately when needed.

5. Data is only part of the solution
Collecting data is futile if the business cannot take advantage of it. EDR makes it easy for companies to analyze and capitalize on accumulated data.

6. Remediation can be costly and protracted
Without actionable intelligence from EDR, organizations can waste valuable time figuring out what action to take. Sometimes, the only recourse is to reimage machines, which tends to degrade productivity and disrupt operations.

EDR 4 Stages of Protection

EDR happens in four stages, each offering a different level of protection. These levels are as follows:

Stage 1. No EDR exists: a business is open to threats and relies on existing defense technologies.
Stage 2. Limited EDR: An IT team may recognize a suspicious event but lack the training and expertise to deal with the breach effectively.
Stage 3. Smart EDR: The IT team uses intelligent EDR to automatically detect events in real-time, analyze them, and perform custom searches.

Stage 4. MDR (managed detection and response): The highest level of security, enabling companies to proactively look for anomalous behavior without passively waiting for detections.

What are the Differences Between EDR and EPP?

EDR and EPP (endpoint protection program) are security response solutions that can detect and mitigate cybersecurity threats. While EDR provides the operational tools and increased visibility that allow security teams to react to a cyberattack, EPP helps prevent security threats before they reach the endpoint.

For this reason, many security experts recommend combining EDR and EPP for optimal endpoint protection, and some vendors even combine the two into a single system.

Is Endpoint Detection and Response Enough?

Although an essential network security tool, EDR has its limitations. Though EDR's environmental analysis uses artificial intelligence, security professionals must still investigate and act on the alerts generated by EDR tools.

Additionally, companies with small IT teams may find it challenging to respond to EDR alerts quickly and may end up swamped with data and notifications.

EDR also does not offer insights when event logs are blocked, which can occasionally take devices offline inadvertently.

What is a SIEM Tool?

The technology used in threat detection, compliance, mitigation, and security incident management is called security information and event management (SIEM) tools.

Using SIEM tools, a security team can pull information from firewalls, endpoint detection, cloud applications, and network appliances for a more holistic security picture. SIEM tools also work collaboratively, providing a centralized dashboard that makes security investigations more efficient.

Many security experts believe SIEM tools go further than EDR, leading to better data and more efficient and effective security responses.

What is Managed Detection and Response?

Managed detection and response (MDR) builds on EDR for an extra high level of security. This approach lets a business proactively search for suspicious behavior in the cyber landscape. Typically, MDR includes a round-the-clock security operations center (SOC) that monitors the

environment in real-time, including technology, processes, and people within an organization.

MDR may use the following modalities to detect and deter threats actively:

- Security Incident Event Monitoring (SIEM)
- Endpoint Threat Detection and Response (EDR)
- User and Entity Behavior Analysis (UEBA)
- Digital Forensics Analysis

A business needs MDR if they have multiple endpoints and retain sensitive data. They might also need MDR if they cannot manage EDR in-house with the current IT infrastructure or want to increase their cybersecurity protections. Most businesses can benefit from MDR, especially private businesses that deal with sensitive financial or medical data and do not have robust cybersecurity in-house.

Do You Need MDR and EDR?

While one or the other can be used, combining MDR and EDR provides comprehensive cyber protection. MDR uses EDR to protect against viruses, while EDR needs MDR due to its real-time, in-person threat-detection monitoring.

Businesses should seek cybersecurity services to assess, manage, and respond to digital threats.

Craig Ima
Windes
+1 562-304-1329
cima@windes.com
Visit us on social media:
Facebook
Twitter
LinkedIn
