ANTIVIRUS VS. EDR:

WHAT'S THE DIFFERENCE?

The dangers of malware extend far beyond a common computer virus. Malware can be used to steal personal information, pirate software, and damage valuable hardware. Plus, it has the potential to create worms that spread quickly online – infecting multiple devices in a short amount of time.

In fact, there are more than 450,000 types of malware reported every day.

Cyber criminals often use malware in large-scale attacks like ransomware. Luckily, there are two ways of detecting and intercepting malware before it spreads. These two methods, which we'll explore in this white paper, are antivirus (AV) and endpoint detection and response (EDR). Let's look into what sets each apart and how you can incorporate them into your practice's cybersecurity management strategy.

What is antivirus?

Antivirus, also known as antivirus software, is designed to detect and remove malware from devices. It scans the system for malicious code, identifies any threats, and removes them before any damage can be done. For example, antivirus software can monitor incoming files, emails, and web downloads for signs of malware. It also scans websites to ensure they are safe to enter without the risk of a virus or other malicious code.

What is EDR?

EDR takes a more proactive approach to protect network endpoints from malware. EDR solutions monitor the behavior of all applications on an endpoint or network device to detect suspicious or anomalous activity that could signal an attack occurring. They also include response capabilities such as automated containment, remediation, investigation, and rollback options in the event of a security breach.

For example, EDR can recognize when an application is exhibiting behavior that could indicate a malicious attack. can then respond to this threat by isolating the application or device from the network and running scans or isolation protocols to prevent further infection

EDR systems are typically integrated with existing security solutions such as antivirus, firewalls, and intrusion prevention systems for added protection.

Finally, EDR solutions can also be used to detect malicious activity that antivirus software may miss. These solutions are often cloud-based and offer advanced analytics and machine learning capabilities to improve detection accuracy.

How do both methods support cybersecurity defense?

Both antivirus and EDR are essential for protecting your network from threats. While antivirus software provides a reactive approach to defense, EDR offers a proactive solution that can identify malicious behavior before it becomes an issue.

Using the two methods together will help ensure that any potential threats are identified quickly and addressed appropriately.

For example, let's say an employee opens a malicious email attachment that contains malware. The antivirus software will detect the threat, remove it, and alert IT staff of the issue.

At the same time, EDR will recognize any suspicious activity associated with the threat, such as trying to access restricted data or opening certain files.

It can then isolate the application or device from the network and provide additional security measures to ensure no further damage is done.

How can EDR and antivirus work together?

EDR and antivirus software can work together to provide more comprehensive protection for your network. By combining the two solutions, organizations gain better visibility into their networks and the ability to detect and respond to threats quickly.

Particularly, antivirus software should be a front-of-the-line defense against malware attacks.

EDR should be used to augment existing security tools and provide an additional layer of protection.

For example, if antivirus software detects a malicious file like spyware, EDR can be used to determine the extent of the attack and feed diagnostic behavior analysis to IT and cybersecurity teams.

This approach can prevent spyware from analyzing user keystrokes to steal personal and financial information.

EDR vs. antivirus: The final verdict

When it comes to antivirus vs EDR, there is no clear verdict on which is the superior cybersecurity measure.

Antivirus software and EDR are two important tools to protect organizations from malicious attacks. By using these solutions together, companies can identify suspicious behavior quickly and respond with containment measures before any damage is done.

The combination of the two provides an effective defense against known threats while still being able to detect and analyze new ones as soon as they appear.

However, it's important to keep in mind that no security solution is foolproof, and it's essential to invest in comprehensive security measures such as next-generation firewalls and MFA's.

HTI's ProCare Business provides both antivirus and AI-powered monitoring, a security operations center, complete response remediation, and enterprise-grade EDR technologies to protect dental practices from the ever-evolving ransomware threats. **For more information on ProCare Business or how to build a secure cybersecurity defense, call a specialist at (877) 222-1508 #5.**