THREATLOCKER

Why Threat Detection Isn't Enough to Protect Your Organization

One of the biggest challenges IT Professionals face today is establishing the right security foundation for their organization.

As the cybersecurity landscape becomes more diverse and sophisticated, IT leaders are searching for the most efficient solutions to combat cyber threats.

It's easy to get caught up in buzz words like "Next-Gen" or "Real-Time" which are commonly over-hyped.

"Next-Generation Antivirus" has gained momentum as of late; however, it is only a small piece of an effective security strategy.

Here's Why.

Antivirus is commonly described as signature-based, artificial intelligence (A.I.), or behavior-based; however, none of these approaches will solve your endpoint protection challenges on their own.

New malware is evolving at an alarming rate that even machine-learning cannot recognize. If a threat is detected in an environment, there is a high chance that an attack is being carried out or has already occurred. In fact, nearly 1 million malware variants are released weekly and zero-day exploits occur almost every week. By 2021, Cybersecurity Ventures predicts that cyber criminals will launch new exploits daily.

A zero-day exploit is a major threat because it is unknown until it is too late. Instead of taking a reactive approach, you should implement a security solution that will protect your organization from widespread damage.

While it is critical to detect threats, organizations must understand that these solutions are not enough to protect your data from malicious attacks. By relying on threat detection alone, many attacks - old and new - are missed if you're not specifically searching for them.

Ultimately, without the proper controls in place, antivirus software can be ineffective. If your endpoint security solutions are evaded, a cybercriminal can compromise and exploit your most valuable assets. It only takes one cyber attack to devastate your organization's finances, productivity, and reputation.

In order to be proactive, you must broaden your cybersecurity approach to protect your data from unknown malware and address all phases of the threat lifecycle. By doing so, you significantly limit the damage that could be done if you are hit with ransomware or other malicious threats.

It's time to implement a logical solution to stop viruses and malware from affecting your organization. By combining Ringfencing with Application Whitelisting, you effectively stop attacks that live-off-the-land.

The Cybersecurity Paradigm is Shifting, Join ThreatLocker at the Cutting Edge

For more information about ThreatLocker, please visit ThreatLocker.com