cybereason

Three Reasons Why Endpoints Cannot Remain A Security Blind Spot

After a period of stagnation, endpoint security is undergoing a renaissance with a slew of products debuting in the market. Antivirus software and its promise of constant protection is seen as unrealistic, giving rise to the more practical approach of detection and incident response at the user device. Companies are realizing the importance of endpoint security and will boost endpoint security budgets by five percent to 10 percent in 2016, according to Forrester.

However, some enterprises are still unconvinced that endpoints are the most valuable source of information for real-time detection and response. Here's how endpoint detection can benefit your businesses.

Endpoints are notorious for having major weaknesses, including inadequate protection and being used by people who are prone to falling for deceptive tactics like phishing emails.

1. Endpoint visibility increases the chances of early detection

Hackers realize targeting endpoints gives them the best chance for their attack to succeed. Endpoints are notorious for having major weaknesses, including inadequate protection and being used by people who are prone to falling for deceptive tactics like phishing emails.

Comprising an endpoint is a hacker's initial move. Continuously monitoring your endpoints can help a company detect a breach early before significant damage occurs.

2. Endpoint data can eliminate false positives

Attackers attempt to capitalize on the fact that hacking behavior can resemble normal employee activity. Hackers often use legitimate tactics to deceive security systems and avoid getting caught.

For instance, some employees may need four attempts to log in to their email account because they forget their user name and password. In other cases, though, a hacker could be behind those actions.

However, many security systems can't distinguish between legitimate and malicious actions and will issue an alert for benign activities. This leads to a rash of false positives overwhelming security analysts, who may choose to ignore some of these warnings.

In the case of the multiple failed authentication attempts, endpoint data can show if the log-in attempts were made from either an office or a remote location where a business lacks a presence, giving analysts the information they need to distinguish a harmless mistake from hacker activity.

The only way security teams can differentiate between user activity and a hacker in disguise is by looking at all surrounding activity.

3. Endpoint information reveals an entire attack

Since endpoint solutions are deployed on every machine, they allow security teams to oversee the entire IT environment. Used this way, endpoints let you to understand the connection between multiple malicious acts and respond efficiently.

For example, hackers are known to use a software-pairing technique, where they install multiple malware programs to protect and maintain control of their operation. Most malware detection tools label these as isolated events instead of a single operation, preventing security personnel from removing the entire attack and allowing hackers to continue collecting information.

Endpoint data will allow you to understand a hacker's entire campaign and get rid of it entirely.

cybereason

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.