10 Signs It's Time To Review Your Endpoint Protection

Cyber attacks are increasing in frequency, sophistication, and effectiveness! The ongoing trend of successful attacks demonstrates that cybersecurity practices are not keeping pace with modern threats. Is your organization well-defended, or living on borrowed time?

Here are ten signs to help you determine whether your endpoint protection is primed for action or ready for retirement.

BlackBerry CYLANCE

ONE
You're still using signature-based security products

In the past, new malware could be individually detected, cataloged, and blocked by security companies. Malicious files were identified by their unique file hash, aka "signature," and restricted from running by signature-based security solutions. Today, threat actors release over nine million new malware variants per month[2]. The sheer number of unique threats being generated today greatly reduces the effectiveness of a signature-based security approach.

TWO
You accept ransomware as inevitable

Many businesses are improving their backup processes and implementing rollback solutions in the hopes of mitigating the effects of a ransomware attack. While maintaining a robust backup policy is a good idea, accepting the inevitable success of ransomware is not. Instead, consider a more proactive security solution that prevents ransomware from being successful.

THREE
You still perform regular systems scans

Legacy AV solutions rely on resource-intensive system scans to discover malware. These scans may be scheduled, on-demand, or occur after signature updates. Regardless of when they occur, their negative impact on system performance is undeniable . If your security solution still requires system scans, it may be time for an upgrade.

Today, threat actors release over nine million new malware variants per month.

FOUR
Your new PCs seem slow

Many enterprises implement a layered security model where solutions to new threats are built on top of existing ones. Over time, the accumulation of security layers puts a strain on system resources and negatively impacts system performance . Slow PCs may be one sign that it is time to reevaluate your endpoint solution.

FIVE
You still use an on-premises server for AV management

If you cannot manage your AV from the cloud, it's probably time to update. Remember, many AV solutions may require constant Internet connectivity in order to be effective. Make sure your AV works regardless of users being online or off.

SIX
You spend too much time managing your AV

Every minute your IT team spends managing your AV solution is a minute taken from core business productivity, or from strategic projects that could proactively shore up your defenses. If your current solution is a time-drain on your tech specialists, it's time to consider new options.

SEVEN
You spend too much time responding to false alerts

As new techniques for identifying malware have evolved, so too have the number of false positives reported by new detection methods. If behavior-based identification, sandboxing, host-based intrusion prevention, and URL/reputation filtering are wasting too much of your time with spurious alerts, it is time for a change.

EIGHT
You are looking at EDR

Does your endpoint protection platform (EPP) consume too many resources and deliver layer after layer of inconsistent results? Are you considering replacing your EPP with an endpoint detection and response (EDR) solution? Now is the perfect time to evaluate your options.

NINE
Your endpoint security strategy is entirely reactive

Does your endpoint strategy largely rely on response actions that occur after a successful breach? If your current endpoint solution cannot detect zero-day malware or offer proactive tactics designed to prevent breaches, it is time to consider alternative solutions.

TEN
You have to upgrade your OS to accommodate your AV

In some cases, business-critical systems are locked to a particular operating system for technical reasons and are unable to upgrade. Selecting a security solution that runs on numerous systems, both old and new, could save your organization money while simplifying your security stack.

BlackBerry CYLANCE

If any one of the above describes the state of your current endpoint security strategy, it may be time for a new approach. BlackBerry Cylance uses highly-trained artificial intelligence to detect, prevent, and investigate threats before they can execute.

For more information, visit us at **cylance.com**

[1] 2018 State of Endpoint Security Risk Report, Ponemon Institute, 2018, www.barkly.com/ponemon-2018-endpoint-security-risk

[2] AV Test New Malware, AV Test, 2018, www.av-test.org/en/statistics/malware/

[3] McDunnigan, Micah "Do Firewalls & Virus Programs Slow Down the Computer?", Houston Chronicle, 2018, smallbusiness.chron.com/firewalls-virus-programs-slow-down-computer-63186.html

[4] Korolov, Maria "The dark side of layered security", CSO, 13 Nov 2015, www.csoonline.com/article/3004856/data-protection/the-dark-side-of-layered-security.html

2018113-0006