

10

Signs It's Time To Review Your Endpoint Protection

The ongoing trend of successful cyber 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 security is primed for action or ready for retirement.

BlackBerry

Intelligent Security. Everywhere.

ONE

You're still using signature-based security products

In the past, new malware could be individually detected, catalogued, and blocked by security companies. Malicious files were identified by their [unique file hash](#), a.k.a. signature, and restricted from running by signature-based security solutions. Modern threat actors release about 1,200 new malware variants per day. The sheer number of unique threats being generated today greatly reduces the effectiveness of a signature-based security approach.

Employees regularly access work resources with smartphones, making mobile devices a primary target for phishing attacks. Up to 83% of phishing attacks occur in text messages or in other mobile apps. Mobile devices are also prime candidates for data leakage, which may result in regulatory violations and fines.

TWO

Your mobile devices are vulnerable

THREE

You still perform regular system 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.

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.

FOUR

Your new PCs seem slow

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.

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.

SIX

You spend too much time managing your AV

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.

Your endpoint strategy covers legacy devices but does not adequately support mobile, IoT, and embedded systems. Your current solution has limited or no capability to scale to new and emerging technologies, leaving you vulnerable to future innovations.

EIGHT

You see gaps in your endpoint strategy

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.

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.

TEN

You have to upgrade your OS to accommodate your AV

BlackBerry

Intelligent Security. Everywhere.

If any one of the above describes the state of your current endpoint security strategy, it may be time for a new approach. The BlackBerry Spark® Unified Endpoint Security Suite provides complete security, threat prevention, and safeguards against sophisticated threats with advanced AI. It provides a Zero Trust solution with coverage across a full spectrum of devices, ownership models, networks, apps and users. For more information, visit us at <http://www.blackberry.com/>.

¹ Malware Statistics For 2020 And What To Expect, PixelPrivacy, 2020, <https://pixelprivacy.com/vpn/guides/guide-malware-statistics-and-facts/>

² Raphael, JR, "8 mobile security threats you should take seriously in 2020", CSO, 25 Feb 2020, <https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html?page=2>

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