Signs It’s Time To Review Your Endpoint Protection

One You’re still using signature-based security products

Employees regularly source work resources with smartphones, making mobile devices a primary target for phishing attacks. In fact, 80% of phishing attacks are delivered via mobile devices, and phone numbers can also be phished for the sake of what may result in expensive enterprise costs.

Two Your mobile devices are vulnerable

Legacy AV products may rely on resource-intensive systems to detect malware. These systems require a lot of resources to operate, making them vulnerable to false positives. It’s time to consider new mobile-first solutions.

Three You still perform regular system scans

Many enterprises engineer a layered security approach to secure their data. In this layered approach, the accumulation of security steps may strain system resources and negatively impact system performance. “Your PC may be a sign of this time to transition your endpoint solution.”

Four Your new PCs seem slow

Every day, your PC team spends troubleshooting your AV selection is a critical task. Your new business partners, or from strategic projects that could prove very expensive your defense. If your current solution is a time-drain on your hands, operations, it’s time to consider new options.

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

As new techniques for identifying malware have evolved, so too have the number of malware incidents reported by AV solutions. It’s time to consider new options.

Six You spend too much time managing your AV

If you cannot manage your AV from the cloud, you need to reevaluate your security strategy. It’s time to consider new solutions.

Seven You spend too much time responding to false alerts

Everyday, 450,000 new malware and potentially unwanted applications are detected.¹

Eight You see gaps in your endpoint strategy

In some cases, business critical systems are exposed to unexpected vulnerabilities. It’s time to consider new options.

Nine Your endpoint security strategy is entirely reactive

In some cases, business critical systems are exposed to unexpected vulnerabilities. It’s time to consider new options.

Ten You haven’t upgraded your OS to accommodate your AV

If your OS is not compatible with your AV solution, it may be time to consider new options.


⁶ McDunnigan, Micah “Do Firewalls & Virus Programs Slow Down the Computer?”, Houston Chronicle, 2018, smallbusiness.chron.com/firewalls-virus-programs-slow-down-computer-63186.html
