vmware Carbon Black

SMB Retailers: Three Signs It's Time to Replace Your Antivirus Solution

The threat landscape is rapidly changing with attackers innovating new tools as they leapfrog over traditional security solutions. Meanwhile, SMBs that rely on legacy antivirus (AV) solutions are experiencing attacks that were once targeted at large enterprises.

Trust in traditional AV solutions is diminishing. SMBs need more advanced, secure and reliable options, such as next-generation endpoint protection.

Here are three key signs that indicate it's time to replace your antivirus solution.

1. Your antivirus solution leaves you vulnerable to modern attacks.

- Emerging attacks are innovating quickly and devising new ways to infiltrate networks and systems. In fact, 80 percent of respondents in our recent Global Threat Report stated that attacks have become more sophisticated amid the recent health crisis.[1]
- As new attacks emerge, businesses struggle to identify the signature and provide an update, which can take weeks. This leaves you vulnerable as attackers continue to innovate using non-malware attacks.
- Legacy AV only prevents known malware, which accounts for a small portion of today's attacks.

2. Your antivirus solution doesn't provide actionable insights.

- Limited visibility is a critical barrier. How can you fix something if you can't see it?
- To identify and proactively protect against malicious activities, you need to understand them first.
- A single endpoint can detect between 10,000 to 40,000 individual events that can help identify activity that might lead to harmful attacks. Legacy AV solutions don't have the processing power to collect or analyze this data.
- You need visibility and context to know:
  - What problems exist?
  - Where are they located?
  - How important are they?
  - How can you to fix them?

3. Your antivirus solution is slowing down your endpoints.

- Constant updates and file scanning slow down user machines. And AV scans require a lot of local processing and hard disk scanning, which are burdensome to endpoints.
- Re-imaging user machines can frustrate employees and become security liabilities.
- Savvy employees might turn off their endpoint security, which can put you in non-compliance and at risk of breach.

Protect your growing business with a cost-effective solution that is easy to deploy and manage.
Visit **carbonblack.com/resources/replace-av-buyers-guide/**

References:
1. VMware. "Global Threat Report." June 2020.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Item No: 720439_SMB_Retailers_ReplaceAV_Infographic 12/20