10 REQUIREMENTS FOR SECURING ENDPOINTS

For decades, traditional antivirus has been the de facto solution to protecting endpoints. Antivirus checks all the boxes for regulatory, governance and compliance audits, but it provides organizations with minimal real security benefits. Although antivirus solutions protect nearly every endpoint and server in the world, security breaches continue at an alarming rate. This is largely because traditional antivirus is a signature-based security tool that focuses on detecting and responding to known threats after they have already entered a network. Experienced attackers can bypass antivirus with inexpensive, automated online tools that produce countless unique, unknown attacks. Ultimately, traditional antivirus is proving inadequate for protecting systems against security breaches.

To prevent security breaches, organizations must protect themselves from known and unknown cyberthreats, as well as the failures of traditional antivirus solutions. This means they must focus on prevention. Prevention is the only effective, scalable and sustainable way of reducing the frequency and impact of cyber breaches. So, what should endpoint security do to be able to effectively and comprehensively protect systems, users and endpoints? The sections below discuss the ten requirements.

1. **Pre-emptively block known and unknown threats**

   To prevent security breaches, a shift must occur – from detecting and responding to incidents after they have already occurred to preventing security breaches from occurring in the first place. Endpoints must be protected from known, unknown and zero-day threats delivered through malware and exploits whether a machine is online or offline, on-premise or off, connected to the organization's network or not. A key step in accomplishing this is to incorporate local and cloud-based threat analysis to detect and prevent unknown and evasive threats.

2. **Have no negative impact on user productivity**

   An advanced endpoint security product must enable end users to conduct daily business and use mobile- and cloud-based technologies without fear of unknown cyberthreats. Users should be able to focus on their responsibilities rather than worry about security patches and updates. They must be confident that they are protected from inadvertently running malware or exploits that may compromise their systems.

3. **Turn threat intelligence into prevention automatically**

   Threat intelligence gained elsewhere through encounters with new and unique attacks, such as third-party intelligence service providers and public threat intelligence-sharing constructs, must enable endpoint agents to instantly prevent known malware, identify and block unknown malware, and stop both from infecting endpoints. Threat data must also be gathered from within the organization – from the network, cloud and endpoint. Automation must be used to correlate the data, identify indicators of compromise, create protections and push them out across the organization.

4. **Protect all applications**

   Applications are at the core of any organization's ability to function effectively. Unfortunately, security flaws or bugs in applications give threat actors a large attack surface that traditional antivirus fails to protect. An organization's security infrastructure should be able to provide full protection against exploits for all applications, including third-party and proprietary applications. It should also be able to expedite the approval process for new applications as they are introduced into the environment by returning quick security verdicts.

5. **Don't let security get in the way of user productivity**

   Security products should not burden such resources as RAM, CPU or disk storage. Prevention of security breaches must never jeopardize user productivity. Endpoint protection, and for that matter any security, must be lightweight enough not to require significant system resources, or it will invariably degrade user experience and productivity.

6. **Keep legacy systems secure**

   Organizations may not always deploy available system updates and security patches immediately, either because doing so would interfere with, diminish or eliminate critical operational capabilities, or because patches may not be available for legacy systems and software that have reached their end-of-life. A complete endpoint security solution must support unpatchable systems by preventing the exploitation of software vulnerabilities, known or unknown, regardless of the availability or application of security patches.

7. **Be enterprise-ready**

   Any security solution intended to replace antivirus should be scalable, flexible and manageable enough for deployment in an enterprise environment. Endpoint security should support and integrate with the way an enterprise deploys its computing resources, scale to as many endpoints as needed, and support deployments that cover geographically dispersed environments. It must also be flexible in its ability to provide ample protection while still supporting business needs and not overly restricting the business. This flexibility is critical as the needs of one part

of the organization may be entirely different from those of another. Additionally, the solution must be able to be easily managed by the same group that manages security in other parts of the organization. It must be designed with enterprise management in mind, without adding operational burden.

8 **Provide independent verification for industry compliance requirements**

Regulatory compliance often requires organizations that fall within a given jurisdiction to implement antivirus to secure their endpoints. To proactively protect endpoints while meeting compliance requirements, endpoint security vendors that replace existing antivirus solutions should be able to provide third-party validation to help customers achieve or maintain compliance.

9 **Provide independent verification as an antivirus replacement**

Any security product intended to replace legacy antivirus should ideally have had its performance reviewed and validated by an independent third-party. The availability of independent reviews offers an essential check beyond what an organization looking for an antivirus replacement is capable of conducting.

10 **Receive recognition from a top-tier industry analyst and/or research firm**

Any organization looking to move away from traditional antivirus should ensure the replacement is recognized as a key player in the endpoint security space by a respected analyst or research firm. This will ensure the solution and its vendor meet a standard set of viability requirements as an endpoint security provider.

With today's widespread use of unknown malware and vulnerability exploits in targeted attacks, it is more essential than ever to protect endpoints proactively. Palo Alto Networks® Traps™ advanced endpoint protection replaces legacy antivirus with multi-method prevention, blocking known and unknown threats before they can compromise an endpoint. As part of Palo Alto Networks Next-Generation Security Platform, Traps integrates with WildFire® cloud-based threat analysis service to convert threat intelligence from the global community into malware prevention, automatically blocking threats on the endpoint no matter where they originate. Visit the Traps page to learn more about what an effective endpoint security solution must do to prevent security breaches and how Traps can effectively replace antivirus.