paloalto NETWORKS

CORTEX BY PALO ALTO NETWORKS

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 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. Today, attackers can bypass antivirus with inexpensive, automated tools that produce countless unique, unknown attacks. Ultimately, traditional antivirus is proving inadequate to protect systems against breaches.

To effectively combat security breaches, organizations must protect themselves from known and unknown cyberthreats as well as the failures of traditional antivirus. This means they must focus on prevention—the only effective, scalable, and sustainable way to reduce the frequency and impact of cyber breaches. So, what must endpoint security do to effectively, comprehensively protect systems, users, and endpoints? The following sections discuss the 10 requirements.

1. Preemptively Block Known and Unknown Threats

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

2. Have No Negative Impact on User Productivity

Advanced endpoint security must enable end users to conduct daily business as well as 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 through encounters with new and unique attacks, including from third-party intelligence service providers and public intelligence-sharing constructs, must enable endpoint agents to instantly block known malware, identify and block unknown malware, and stop both from infecting endpoints. Threat data must also be gathered from the network, clouds, and endpoints within the organization. Machine learning and 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 create a large attack surface that traditional antivirus fails to protect. An organization's security infrastructure should be able to prevent exploitation of all third-party and proprietary applications. It should also be able to return security verdicts quickly in order to expedite approvals as new applications are introduced into the environment.

5. Keep Security out of the Way of User Productivity

Breach prevention must never jeopardize user productivity, so security products should not burden computational resources. Any security, including endpoint protection, must be lightweight enough to require only minimal system resources, or it will invariably degrade the 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 end-of-life. Therefore, a complete endpoint security solution must support unpatchable systems by preventing software exploits, 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 in a given jurisdiction to implement antivirus to secure their endpoints. To proactively protect endpoints while meeting these requirements, endpoint security vendors that replace existing antivirus solutions should be able to provide third-party validation of their compliance capabilities to help customers achieve or maintain compliance.

9. Provide Independent Verification as an Antivirus Replacement

Any security product intended to replace legacy antivirus should have had its performance reviewed and validated by an independent third party. Independent reviews offer an essential examination of an antivirus replacement's capabilities, beyond the baseline an organization may be looking for.

10. Be Recognized by 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. The Cortex XDR™ agent by Palo Alto Networks provides everything you need to safeguard your endpoints. It combines industry-best AI and behavior-based protection to block advanced malware, exploits, and fileless attacks. As part of the Palo Alto Networks suite of next-generation security products, Cortex XDR integrates with WildFire® malware prevention service to automatically block threats on the endpoint no matter where they originate. To learn more about how the Cortex XDR agent can effectively replace antivirus, read the Cortex XDR Endpoint Protection Solution Guide.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com