E-BOOK

TOP 8 PITFALLS OF ENDPOINT SECURITY
Introduction

The management and security of endpoints is critical in today’s business climate. With end users logging on and off the network using devices with unpatched vulnerabilities, and with encrypted threats reaching endpoints unchecked, devices must be secured for the safety of both the endpoints themselves and the network as a whole. As ransomware and credential theft become increasingly more pervasive, endpoints have become the battleground of today’s threat landscape.

Despite a wealth of solutions on the market today, administrators still struggle with the visibility and management of their security posture. Additionally, they are challenged by having to provide consistent assurance of client security, along with actionable, easy-to-use intelligence and reporting. Here are some of the pitfalls you might encounter as you formulate your endpoint protection strategy.
Security Solutions That are Out of Date

Administrators need to ensure managed endpoints are running the correct version of the installed security software components, as mandated by compliance policy. This issue is exacerbated when dealing with traditional antivirus solutions that rely on an updated signature database to defend against the latest threats. Advanced Endpoint Protection (AEP) solutions that work by examining system behavior (heuristics) perform better against these attacks and can also block malicious scripts such as seen in fileless attacks.

“91% of Commercial Applications Contain Outdated or Abandoned Open Source Components”

Source: Synopsis 2020 Open Source Security and Risk Analysis (OSSRA) Report
Enforcing Policies and Web Compliance

Administrators struggle to mitigate the risks that come with people using their devices on third-party networks at home, in coffee shops, at hotels or in airports. At the same time, they face challenges when it comes to enforcing the company's web usage policy away from the office. Outside the workplace, people are more likely to hit malicious web properties and tend to visit productivity-wasting websites. And if your users are pulling all their data through your data center via VPN, bandwidth-intense content such as video may need to be throttled. Throughout the early days of the pandemic, network administrators complained that their networks were being inundated by TikTok, YouTube, Netflix and other traffic from streaming services — and this problem will continue to grow as picture quality improves and people increasingly rely on these apps for entertainment.

“30 to 40 percent of employee Internet activity is non-work-related”

Source: IDC Research
Getting Reports and Managing Access

In some cases, administrators may manage multiple tenants through firewalls, but their users are configured in a single pool. This makes obtaining a single sign-on (SSO) from a firewall admin or security management consoles a challenge when trying to manage client policies. At the same time, compliance regulations often dictate that all admin roles adhere to the principle of least privilege, so a unified client management suite that can't manage role-based access controls will cause numerous headaches. For example, someone may be limited to two roles, one which has read/write access and one which is read-only access.

Threats Coming Through Encrypted Channels

With more web applications being secured through encrypted channels like HTTPS, and with malware also resorting to encryption to bypass network-based inspection, it has become imperative to enable Deep Packet Inspection of SSL/TLS traffic (DPI-SSL). However, this is not easily enforced without the mass deployment of trusted SSL/TLS certificates to all endpoints to avoid user experience and security challenges.
Understanding Alerts and Remediation Steps

End users are typically less aware of security risks than security professionals — and as such, they don’t understand the alerts on most endpoint security clients. In addition, most clients don’t include self-help information, which results in users either ignoring the issue or filing tickets with IT. For example, if a user’s device falls out of policy and that user is quarantined, that user won’t know what is required to get back in compliance.

License Management

One issue on the backend of endpoint security software is that administrators, particularly when it comes to MSSPs, can’t ensure their software is licensed correctly. If license information related to customers isn’t centrally monitored and stored, it could cause outages and gaps in security. Additionally, administrators may struggle to run compliance reports against all deployed third-party licenses to pay their partners.
Stopping Advanced Threats Such As Ransomware

Traditional endpoint security approaches can sometimes leave gaps in meeting administrative requirements. The long-embattled signature-based approach of traditional antivirus technologies has failed to keep pace with the development of new malware and malware evasion techniques. Many legacy solutions fail to deliver advanced threat detection and also lack support for a layered defense strategy on endpoints, including integration with a sandboxing environment.

“By the end of Q3 2020, ransomware was up 40% over the same time period in 2019.”

Source: SonicWall Q3 Threat Data
Not Knowing Where Critical Vulnerabilities Lie

With the large growth in business applications, the threat of application vulnerabilities has increased exponentially, causing headaches for IT administration and resulting in breaches. Many organizations still don't have a way to identify the number and classification of vulnerabilities, which makes it difficult to create a plan for either patching or uninstalling risky applications.

“In 2019 alone, CNAs assigned 9.0+ critical CVSS scores to over 16 thousand vulnerabilities.”

Source: NIST National Vulnerability Database
Conclusion

While the number of potential pitfalls may make formulating an endpoint protection plan seem impossibly complex, there are plenty of resources available to simplify the process. To help identify the best fit for your organization, read our executive brief, “What Administrators Need to Look for When Buying an Endpoint Security Solution.”