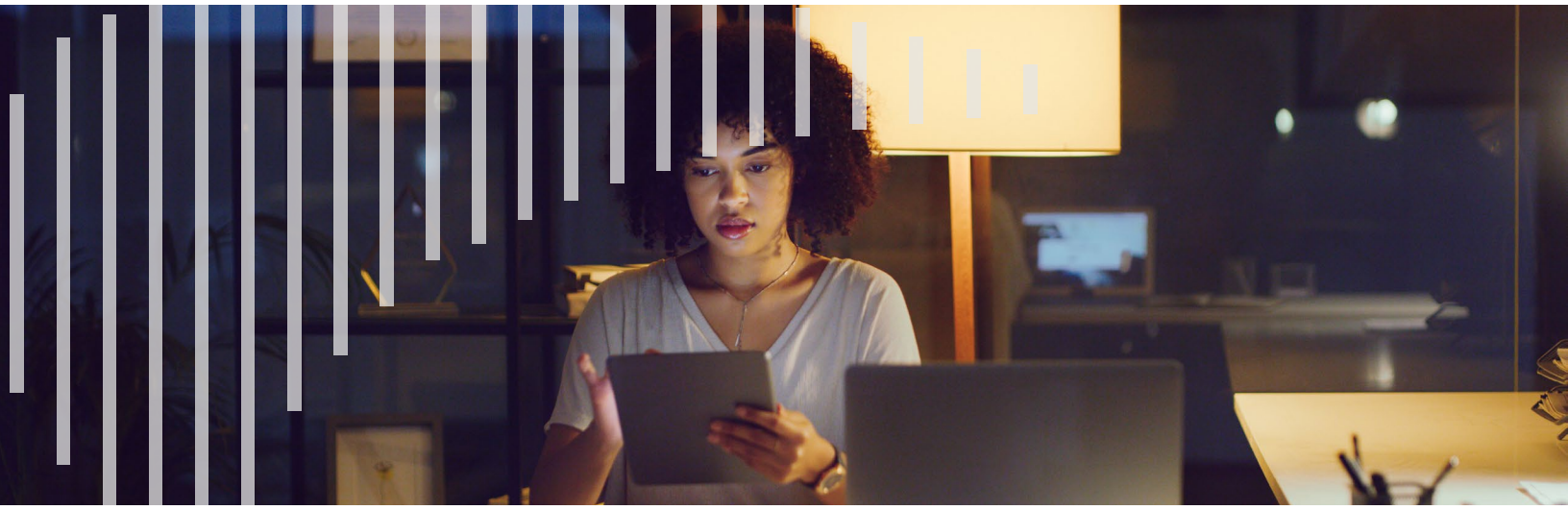

EXECUTIVE BRIEF

What Administrators Need to Look for When Buying an Endpoint Security Solution

A fresh perspective on the challenges of endpoint protection

Abstract

Administrators struggle with the challenges of endpoint security products. This brief examines several of these persistent challenges, including:

- Security maintenance and enforcement
- Encrypted and advanced threats
- Managing alerts and remediation
- Policy creation and maintenance
- Visibility into tenant health
- Unpatched vulnerabilities
- Hunting for threats across devices

The management and security of endpoints is critical in today's evolving cybercrime environment especially when they are away from the office. End users continually connect in and out of the network with their endpoint devices. At the same time, these endpoints are the battleground for today's threat landscape. Encrypted threats are increasingly reaching endpoints unchecked, ransomware is on the rise and credential theft silently persists. The ever-growing threat of ransomware and other malicious malware-based attacks has proven that client protection solutions cannot be measured on endpoint compliance alone.

These challenges are exacerbated when one must manage multiple tenants, either within a single organization or for multiple customers. This often requires different policies and configurations based on user group, device and location.

The challenges of endpoint protection

Endpoint security products have been on the market for years, but administrators struggle with:

- Keeping security products up to date
- Enforcing policies and Web compliance
- Threat hunting
- Getting reports and managing access
- Detecting threats coming through encrypted channels
- Understanding alerts and remediation steps
- Managing licenses
- Stopping advanced threats like ransomware
- Not knowing where critical vulnerabilities lie
- Knowing tenant health and maintaining global policies

Keeping security products up to date

Administrators need to ensure managed endpoints are running the correct version of the installed security software components as mandated by compliance policy.

To thwart emerging attacks, network security administrators need managed endpoints to continually evaluate security posture and report back with status updates on an ongoing basis.

Some administrators need to stop east-west traffic across their data centers, which can often account for a majority of the traffic across their switches. They need the option to quarantine a device locally in case it falls out of compliance or becomes infected. In these cases, the firewall must block access to the internet and block that device from the LAN, thus restricting the network paths to the same quarantine locations the firewall is enforcing.

Additionally, to ensure the integrity of data, security administrators need to ensure all data between the unified client and the centralized management console cannot be tampered with while in transit.

Enforcing policies and Web compliance

If the endpoints are in an out-of-policy state, administrators need to be able prevent the endpoint device from using UTM services to pass traffic through the firewall. End users also have an important role to play in endpoint security. They do their jobs on corporate laptops and other endpoints. Users need to know immediately if any malicious software or behavior is detected, so they can take action or file a ticket if needed.

With people working away from the office, enforcing your organization's Web usage policies can be accomplished with a web or content filter embedded within your security solution. It is vital to also block access to known malicious sites, and some find it important to block productivity-wasting web locations as well as adult material. If users are pulling video data through on-premise servers via VPN, throttling bandwidth on data-intensive websites should also be considered.

Threat hunting

Threats today no longer want to infiltrate or encrypt a single device within your organization. The SonicWall 2021 Annual Threat Report stated the number one intrusion method used by malware in the previous year was Directory Traversal, which was present in nearly a third of attacks. With polymorphic strains on the rise as well, a single attack can spread across multiple devices and operating systems.

Getting reports and managing access

In some cases, administrators may manage multiple firewalls, but their users are configured in a single pool. They need to be able to obtain single sign-on (SSO) from any firewall admin or security management consoles to manage client policies. At the same time, compliance regulations often dictate that all admin roles adhere to the principle of least privilege, so the unified client management should have sufficient role-based access control for privileged access. For example, this may be limited to two roles, one which has read/write access and one which has read-only access.

Threats coming through encrypted channels

With more web applications being secured through encrypted channels like HTTPS, and 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, without the mass deployment of trusted SSL/TLS certificates to all endpoints, this is not easily enforced without user experience and security challenges. This requires an underlying mechanism to distribute and manage certificates and how browsers trust them.

Understanding alerts and remediation steps

End users are typically less aware of security risks than security professionals, and as such, they would require their endpoint protection platform to alert them to the changing risk profile as they travel with their laptop between different locations, and advise them on how to stay safe.

To quickly remediate any company policy compliance issues, it can be beneficial for both end users and IT for end users to have access to self-help information. If a user's device falls out of policy and that user is quarantined, users also need guidance on actions required to get back in compliance.

License management

Administrators need to ensure any purchased endpoint security software is automatically updated to their management interface so they can keep endpoints licensed correctly. For instance, all license information related to a customer should be centrally monitored and stored. In the event of a new license purchase, a signal should be sent to the unified client centralized management to alert and commence the entitlement of software.

Some administrators need to periodically run compliance reports against all deployed third-party licenses to pay their partners.

Stopping advanced threats like ransomware

Traditional approaches can sometimes leave gaps in meeting administrative requirements. The long-embattled signature-based approach of traditional antivirus technologies has failed against the pace at which new malware is developed and evasion techniques are refined – bringing forth the need for a different approach to endpoint protection. This must not only deliver advanced threat detection engines but also support a layered defense strategy on endpoints, including integration with a sandboxing environment.

A major limitation in existing point solutions today (known as enforced AV clients) is that the development is specific to a

certain third party, and has been built into that third party's offerings. Administrators need a more open model, allowing for a relatively quick deployment of additional security modules if the business or industry demands it.

Not knowing where critical vulnerabilities lie

With the large growth in business applications, the threat of application vulnerabilities has grown exponentially. In 2019 alone, over 9.0+ critical CVSS scores were given to vulnerabilities causing headaches for IT administration and resulting in breaches. Organizations need a way to identify the number and classification of vulnerabilities so they can create a plan to either patch or uninstall risky applications.

Knowing tenant health and maintaining global policies

Many large organizations are tasked with managing a large number of endpoints; endpoint security across several regions, user groups or device types; or both. Their success in doing so is based on how quickly they can create a new tenant and whether they have a global dashboard that provides visibility into tenant health. Administrators in these situations need to quickly amend a global policy that feeds tenants and groups. MSSPs and MSPs also require the freedom to build custom policies for tenants that are not affected by changes in the global policy. The management function should give them high-level statistics on infections and vulnerabilities without the need to drill down on each tenant.

Conclusion

Because of the increased use of endpoints as a cyberattack vector, security professionals need to take steps to protect endpoint devices. Furthermore, with the proliferation of telecommuting, there is a dire need to deliver consistent protection for any client, anywhere.

Security administrators need to evaluate endpoint solutions with real-world requirements in mind.

Learn more. Read our solution brief, "Fitting endpoint security to your organization," or visit www.sonicwall.com/capture-client.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL

ExecBrief-WhatAdminNeed-US-COG-5323