

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

Introduction

The management and security of endpoints is critical in today's evolving cybercrime environment. 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. However, the ever-growing threat of ransomware and other malicious malware-based attacks has proven that client protection solutions cannot be measured based only on endpoint compliance.

Furthermore, these challenges are only 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 compliance
- Getting reports
- Threats coming through encrypted channels
- Understanding alerts and remediation steps
- License management
- Stopping advanced threats like ransomware
- Creating and updating policies across the globe
- Understanding the health of each tenant
- Not knowing where critical vulnerabilities lie

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 evaluate the security posture, and report back their status on a continual 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 as well as block that device from the LAN, thus restricting the network paths to the same quarantine locations the firewall is enforcing.

All administrators for large and small companies need visibility into the application vulnerabilities present on protected endpoints. Knowing the scale of a critical vulnerability will help the organization develop a plan to patch these applications to better avoid a breach.

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

Enforcing policies and compliance

If the endpoints are in an out-of-policy state, administrators need to be able to 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.

For administrators of enterprises with multiple tenants and MSSPs, administrators need to be able to spin up policies for new tenants and amend existing policies for when a new threat is detected, or a new web property is hogging bandwidth or impacting productivity for example.

Getting reports

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 that 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 is read-only access.

They also need to have a global snapshot into the health of their tenants within a global view. They want to see the health

of each tenant. This could be judged by the number of infections, vulnerabilities present, the version of endpoint security installed or which devices are online and operating as well. They may also want to see what and who is raising the most alerts for web content.

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, this is not easily enforced without the mass deployment of trusted SSL/TLS certificates to all endpoints to avoid 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 risk 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.

For instance, an alert could be generated from a unified client or third-party software, or provide a redirect to an external source, such as a web page.

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.

On a periodic schedule, some administrators need to 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 are developed and their evasion techniques – bringing forth the need for a different approach to client 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 addition of additional security modules if the business or industry demands it.

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, mobility and BYOD, 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.

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING,

BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

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.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com