SONICWALL

SOLUTION BRIEF: BEST PRACTICES FOR GLOBAL ENDPOINT SECURITY OPERATIONS FOR MSSPS AND DISTRIBUTED ENTERPRISES

Concerns, considerations and guidelines for a multi-tenant environment

Abstract

Distributed enterprises and managed security service providers must address a host of complex issues in today's cybersecurity environment. This brief explores the significant challenges they face in protecting distributed networks at the endpoint. It examines best-practice steps for evaluating risk, presents real-world use cases, and outlines recommended feature sets for a comprehensive and scalable endpoint solution approach.

Endpoint security challenges for global operations

The management and security of endpoints is increasingly critical for today's global enterprises and managed security service providers (MSSPs). The growth of ransomware and the persistent use of credential theft have made endpoints the battleground of today's threat landscape. With the proliferation of mobility and BYOD, global operations also struggle with the visibility and management of their security posture. Yet global operations face greater-than-ever challenges in protecting their endpoint devices.

Endpoint security products have been on the market for years. However, there is a continuous struggle with:

- End users working both in and out of the network with their devices
- Encrypted threats reaching endpoints unchecked
- Knowing if endpoint security products up to date or what versions are installed
- Creating and enforcing policies and compliance on a global scale
- Getting reports from specific environments as well as across all environments

- Understanding and managing alerts and remediation steps
- Visibility into the scale of unpatched vulnerabilities
- Remediating any issues on endpoints which impact operational costs and detracts time from other customers

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.

What is needed

Enterprises and MSSPs need a quick snapshot into the health of their tenants, with the ability to see infections and present vulnerabilities, as well as the version of endpoint security installed on endpoints. Additionally, as more employees work from home, companies want more control over the content workers are accessing on their devices. They want to have visibility into what is being blocked, and if there are any statistical outliers (e.g., certain webpages or employees). Organizations want to extend this visibility into which devices are online and in operation as well.

The art of managing multiple tenants depends on how well organizations can adapt current policies on a global scale, while simultaneously spinning up new tenants. When new threats are detected, they want to quickly add new definitions to all tenants quickly. If a certain non-productive website is dominating bandwidth and impacting employee performance, an Enterprise or MSSP IT administrator would like to amend their content filtering policies on-the-fly across all tenants.

Use-Case 1: Rolling out a new version with minimal disruption

The biggest challenge MSSPs and large enterprises have with new agent versions is balancing between keeping up but also ensuring that new versions do not disrupt end user productivity. A typical approach is to apply the new version to a small pilot set of endpoints (e.g. a lab tenant) to validate that all is well. Once this is satisfied, organizations usually adopt one of two approaches.

1. Immediately push the agent out to all tenants with their own update schedule, or
2. Roll out within batches of tenants to better control any field issues

This requires flexible version management that can be automated for scale, and with enough control over who gets the new versions and when.

Use-Case 2: Immunizing endpoints from a new threat across all customers

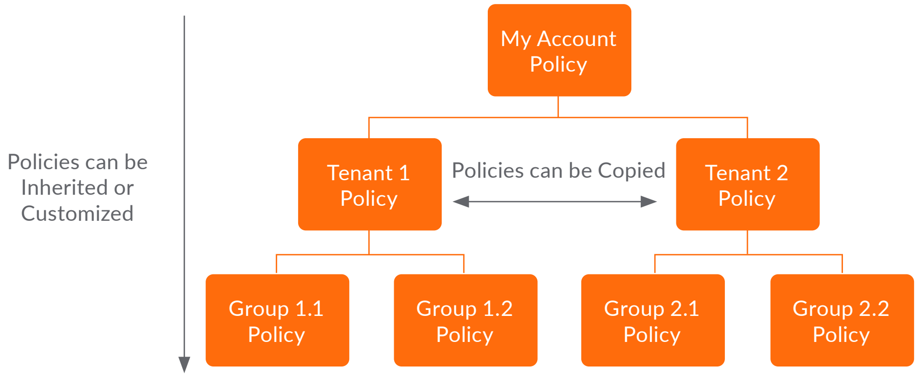
MSSPs and large enterprises leverage threat intelligence from third-party source (commercial, community-driven or open-sourced) that help them stay ahead of the latest malware threats. One of the most common uses of threat intelligence is to immunize endpoints from new threats by simply marking the hash value of a file as “Known Malicious”. But using this in a SOC system for hunting or analytics isn’t enough. It is also important to proactively notify all endpoints across all tenants at machine speed. This requires a top-down push of new configurations to all endpoints irrespective of who they belong to and where they are.

Use-Case 3: Controlling web browsers via content filtering for various tenants and groups of users

Managing content filtering across multiple tenants of diverse businesses and user types is not an easy task. Admins have to offer flexibility to allow all content, block some content types, and even maintain exceptions for specific websites. This requires the ability to define a global baseline (to allow all content) and enforce inheritance of settings across tenants. Moreover, it must still allow custom policies for specific tenants (e.g. blocking adult content for K-12 and Higher Education customers) or even for specific groups in a tenant (e.g. blocking social media for research professionals).

How does SonicWall Help?

To address the endpoint security needs of global enterprise operations, SonicWall Capture Client offers a unified client platform that delivers multiple endpoint protection capabilities, including next-generation malware protection and support for global visibility and management. It leverages cloud sandbox file testing, content filtering, and enforcement for endpoint protection.



Policy Types

- Client Policy
- Threat Protection
- Trusted Certificates
- Web Content Filtering
- Blacklists
- Exclusions
- Device Control

Additionally, it provides consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

Global Dashboard

Capture Client's Global Dashboard gives MSSPs a snapshot into the health of their tenants within a global view through the addition of more data than before. From this screen, administrators can see the health of each tenant. This is judged by the number of infections, vulnerabilities present, and the version of Capture Client installed. They can also see what and who is being blocked the most by Content Filtering (option available on Capture Client Advanced). This dashboard can also tell you which devices are online and operating as well.

Accounts and Account Policies

Accounts are a new concept that allow clustering of tenants that have common security configuration requirements. Account Policies allows administrators to apply a single baseline policy to all tenants in the account (effectively a global policy) which makes it easier to spin up new tenants. This also allows for administrators to quickly create protections for new threats across all tenants on this policy. When the Inheritance option is activated, all new tenants will acquire the account policy. When turned off, unique policies can be created and modified for individual tenants. By default, all Capture Client tenants are clustered under a common account, however MSSPs and distributed enterprises managing multiple tenants can request for their own Account.

Conclusion

Managing endpoint security in MSSPs and global enterprise operations is a daunting task, requiring a comprehensive best-practice approach. Fortunately, for each challenge, there are suitable security technologies available to help. SonicWall endpoint solutions, including Capture Client, provide effective tools to implement endpoint security for global enterprise operations.

Learn more.
Visit www.sonicwall.com/endpoint.

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