Enterprise Strategy Group™
by TechTarget

REQUIREMENTS FOR A MODERN FIREWALL PLATFORM

Driving Better Outcomes with Flexibility, Ease of Use, and Strong Security



By John Grady
Principal Analyst, Enterprise Strategy Group

AUGUST 2023

This Enterprise Strategy Group eBook was commissioned by SonicWall and is distributed under license from TechTarget, Inc.

© 2023 TechTarget, Inc. All Rights Reserved.

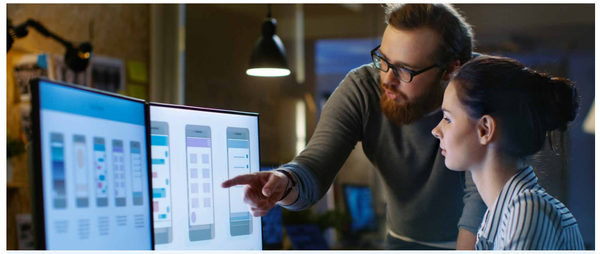
CONTENTS

CLICK TO FOLLOW



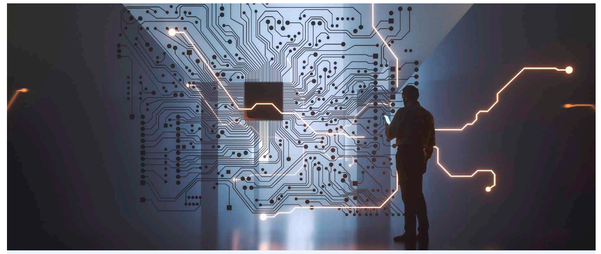
Introduction:
The shift to cloud, proliferation of connected devices...

PAGE 3



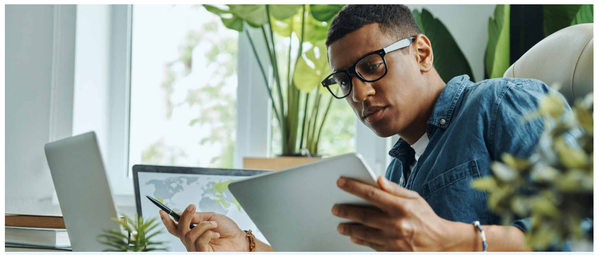
Security Teams Face a Variety of Challenges

PAGE 4



The Need for Firewall Platforms

PAGE 8



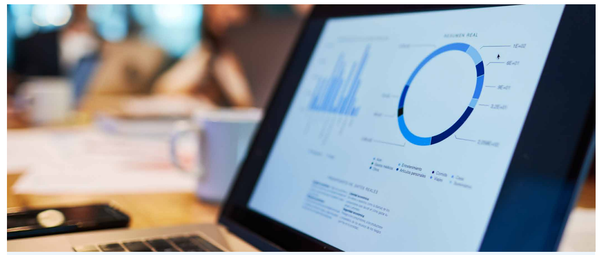
Requirements for Consolidated Firewall Platforms

PAGE 10



The SonicWall Network Security Portfolio

PAGE 15



Conclusion

PAGE 17

© 2023 TechTarget, Inc. All Rights Reserved.

Introduction

The shift to cloud, proliferation of connected devices, expanding threat landscape, and skills shortage have all conspired to make security more difficult than ever. Firewalls remain a critical aspect of any cybersecurity architecture and should help alleviate these problems, not add to them. Consolidated firewall platforms that provide strong security, ease of use, and flexibility can help security teams do more with less and efficiently protect their organization. SonicWall's network security portfolio, consisting of both its enterprise-grade firewalls and Network Security Manager (NSM), helps converge network and security capabilities, supporting more consistent protection across the entire environment and more efficient threat detection and response.



© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Security Teams Face a Variety of Challenges



Threats and Environmental Changes Create Issues

Security teams today have a lot on their plate. As always, they must contend with extremely motivated adversaries, which creates an ever-evolving threat landscape. Ransomware, software supply chain attacks, and sophisticated malware are just some of the notable threats security teams face every day. Yet at the same time, dramatic changes to IT environments have increased complexity and made ensuring a strong security posture more difficult. Respondents to research from TechTarget's Enterprise Strategy Group reported most often that cybersecurity management and operations in their organization are more difficult because of the increase in the number of remote workers accessing the corporate network and applications (41%).[1] As many organizations have shifted to hybrid work models, ensuring consistent protection and secure access regardless of where users are has become a top priority. The proliferation of devices and cloud applications also creates issues. Nearly one-third of organizations (32%) said the increase in IoT devices is most responsible for making cybersecurity more difficult. Accurately accounting for these devices and applying policies to limit their access to sensitive parts of the network or the internet itself is critical but more difficult as scale increases. The same percentage of organizations (32%) cited the increased use of cloud applications as a reason their cybersecurity management and operations are more difficult. As networks have expanded to include infrastructure-as-a-service (IaaS) environments, security teams have struggled to maintain consistent visibility and control. Finally, 31% of organizations cited the increased use of mobile devices to access corporate resources as a key struggle. These challenges impact a wide variety of security disciplines, including network security and the firewall, specifically. Network security solutions that lack scalability, coverage, and strong threat prevention capabilities make it much harder for security teams to overcome these issues.

Top Five Factors Making Cybersecurity More Difficult



41%

An increase in the number of remote workers accessing the corporate network and/or applications



38%

An increase in the threat landscape



32%

An increase in the number of IoT devices with access to the network



32%

An increase in the number of cloud applications our organization uses



31%

An increase in the number of mobile devices accessing the corporate network and/or applications

© 2023 TechTarget, Inc. All Rights Reserved.

1. Source: Enterprise Strategy Group Survey Results, *The State of Zero Trust Security Strategies,* May 2021.

BACK TO CONTENTS

Detecting and Responding to Threats Is More Difficult

Many of these issues have a direct impact on detecting and responding to threats efficiently. Security professionals report a number of factors making threat detection and response (TDR) more difficult. Some of the most important factors cited include:[2]



Workload has increased (45%).

Security practitioners simply have more to do. With more threats and more distributed environments to protect, the process of identifying, triaging, and remediating issues has become more difficult. This makes taking proactive actions more difficult, as many teams spend the majority of their time putting out fires.



Sophistication of threats has increased (37%).

Attackers continue to evolve their methods to evade defenses. Polymorphic malware makes signature detection difficult by making small changes to the code. Fileless attacks that exploit vulnerabilities in common languages and tools such as JavaScript and PowerShell are becoming more common as well.



Inconsistent/incomplete visibility across different security layers (27%).

In many cases, as workloads and applications have expanded to the cloud, teams have had to add additional security tools for different parts of the environment. With regard to firewalls, this may include using different vendors in cloud environments or firewalls from the cloud service providers themselves.



Threat detection/response is dependent on manual processes (25%).

Related to the increased TDR workload, many security teams rely on manual processes to triage alerts and respond to malicious activity. The potential for delays due to this inefficient process can give attackers the critical time they need to establish persistence and make remediation much more difficult.

While a variety of security tools may be used for TDR, many small and midsize organizations rely on their firewalls as key control points to detect potentially malicious activity, perform investigations, and respond via policy modifications to quarantine impacted devices or push updated protections across the organization.

© 2023 TechTarget, Inc. All Rights Reserved.

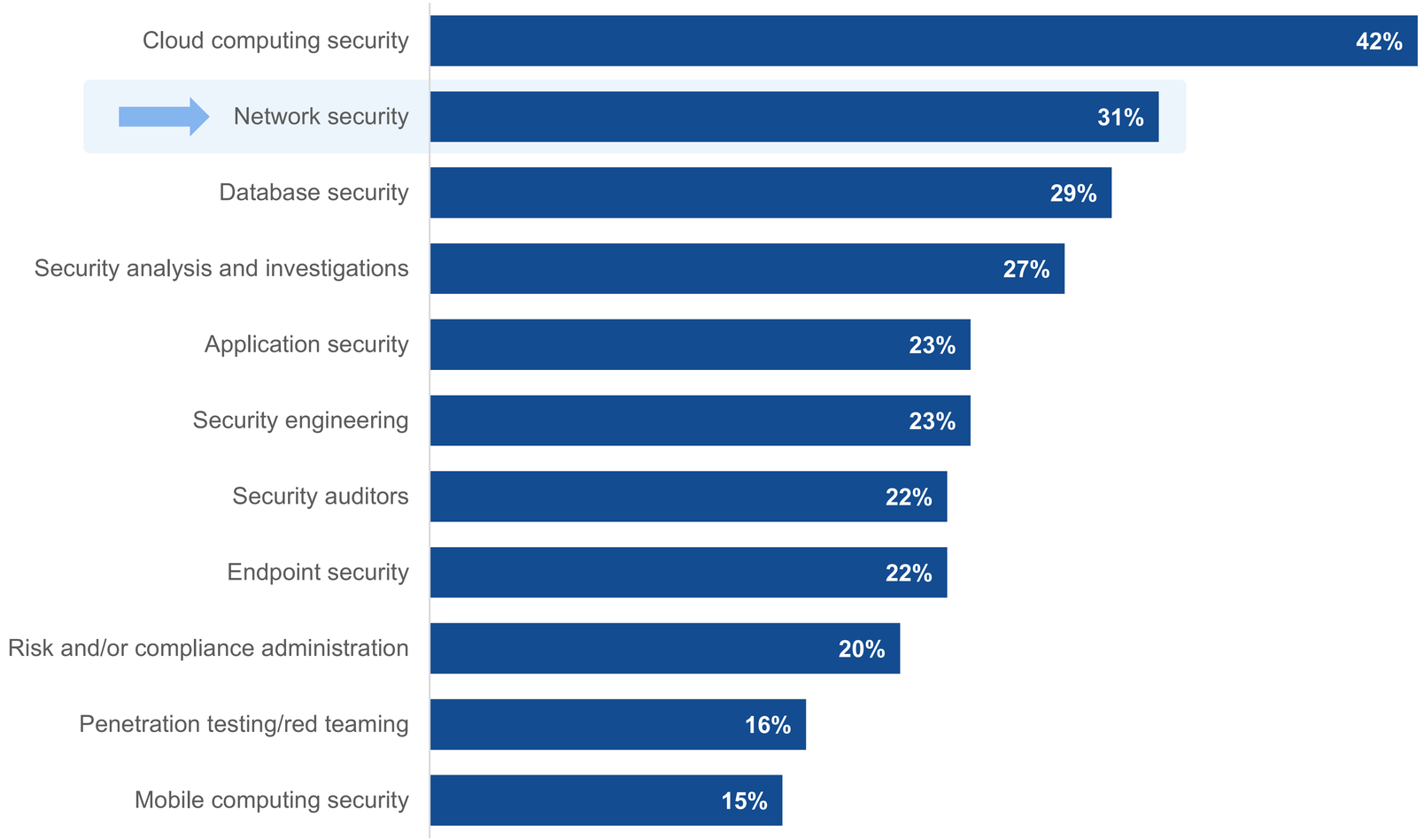
2. Source: Enterprise Strategy Group Research Report, *The Evolving Role of Network Detection and Response*, March 2023.

BACK TO CONTENTS

The Cyber Skills Shortage Looms Large

Further complicating matters, many organizations continue to struggle to find and maintain the right level of cybersecurity skills. When organizations are asked where they have the most acute shortage of IT skills overall, cybersecurity is consistently at the top of the list. In fact, 45% of respondents named cybersecurity as an area in their organization with a problematic shortage of existing skills.[3] This shortage is not limited to new or complex segments of cybersecurity either. While true that cloud security (42%) is most often cited as an area where cybersecurity roles have been the most difficult to fill over the last 12-18 months, network security is close behind, cited by 31% of organizations. This ranked above areas such as application security, security analysis and investigations, and penetration testing/red teaming. With network security generally—and the firewall specifically—being a critical part of the security architecture, organizations require tools that enable them to be more productive, do more with less, and overcome this skills gap.

Areas of Cybersecurity with a Problematic Shortage of Skills



© 2023 TechTarget, Inc. All Rights Reserved.

3. Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

BACK TO CONTENTS

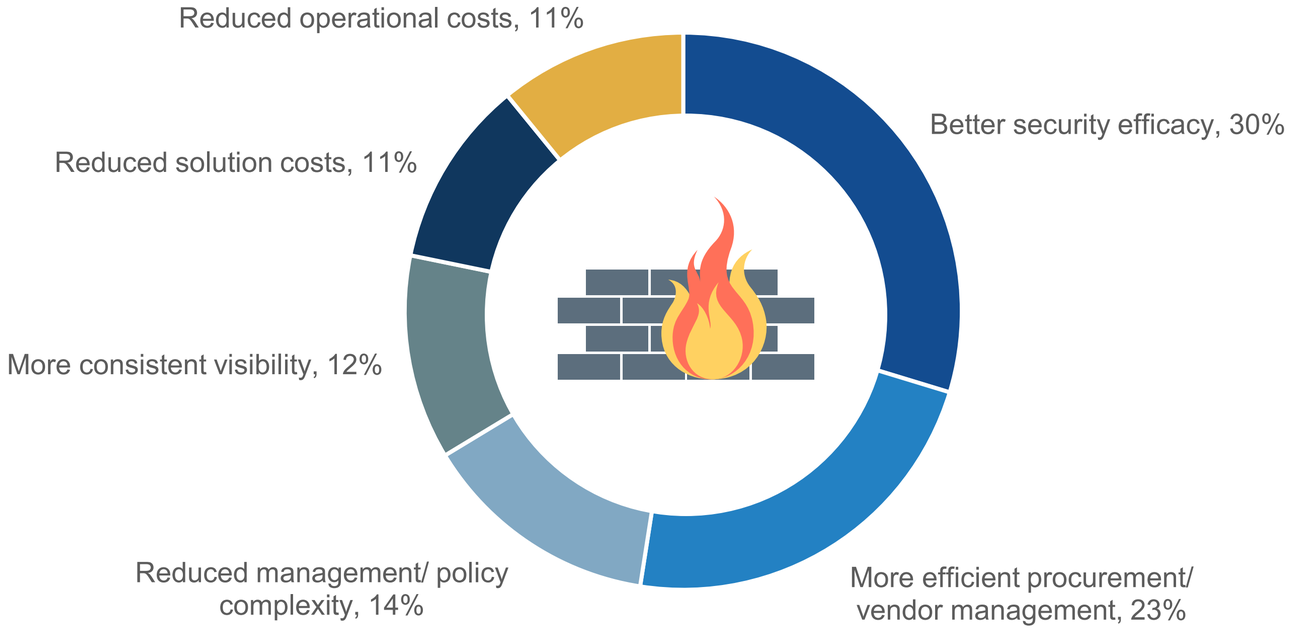
The Need for Firewall Platforms



Security Teams Look to Firewall Platforms to Improve Efficacy and Efficiency and Lower Costs

To alleviate many of these issues, security teams are prioritizing consolidation. This trend is especially prevalent in the network security space, with three-quarters of organizations actively reducing, planning to reduce, or interested in reducing the number of firewall vendors they use.[4] There are a variety of expectations driving security teams toward this convergence. At the top of the list, 30% anticipate that consolidating firewall vendors will provide better security efficacy. By improving previously siloed visibility, the expectation is that threat detection effectiveness will increase. Nearly one-quarter (23%) point to more efficient procurement and vendor management, while 14% cite reduced management and policy complexity as a reason why respondents are consolidating or want to consolidate their firewall vendors. In both of these cases, the need to make the job of security personnel easier and help them be more efficient in the face of the skills shortage is clear.

Reasons for Firewall Consolidation



> “At the top of the list, **30% anticipate that consolidating firewall vendors will provide better security efficacy.”**

© 2023 TechTarget, Inc. All Rights Reserved.

4. Source: Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

BACK TO CONTENTS

Requirements for Consolidated Firewall Platforms



Strong Security, Supported by AI

First and foremost, a firewall platform must provide protection against the most sophisticated attacks. In today's threat environment, this requires a layered approach with multiple analysis engines. A broad install-base from which to source threat intelligence is critical to maintaining a comprehensive signature base to detect common attacks. However, most advanced capabilities are often necessary to identify stealthy threats. Integrations with cloud-based sandboxes can help fill this gap. By running suspicious or unknown executables in a protected environment, and analyzing the code of the file itself, security teams can have more confidence that their organization is protected.

Artificial intelligence (AI) is becoming more important to keep pace with the rate of change in attacks. Enterprise Strategy Group research has found that security teams anticipate using AI for a variety of reasons with regard to network detection and response. Nearly two-thirds (61%) expect AI to help with improving detection accuracy,[5] which reduces false positives and ensures that even stealthy threats are identified. Additionally, 59% of respondents anticipate using AI to help improve detection speed. This could be through faster analysis in sandboxed environments or the quicker aggregation and analysis of threat intelligence and available telemetry. Nearly half (47%) see AI helping to identify network devices and entities, which can improve and accelerate policy creation and prevent gaps in defenses. Finally, 47% also expect to use AI to accurately prioritize alerts, making their teams more efficient and helping them focus on what matters most.

Areas of Cybersecurity with a Problematic Shortage of Skills



Improving detection accuracy,
61%



Improving detection speed,
59%



Identifying network devices and entities,
47%



Accurately prioritizing alerts,
47%

© 2023 TechTarget, Inc. All Rights Reserved.

5. Source: Enterprise Strategy Group Research Report, *The Evolving Role of Network Detection and Response*, March 2023.

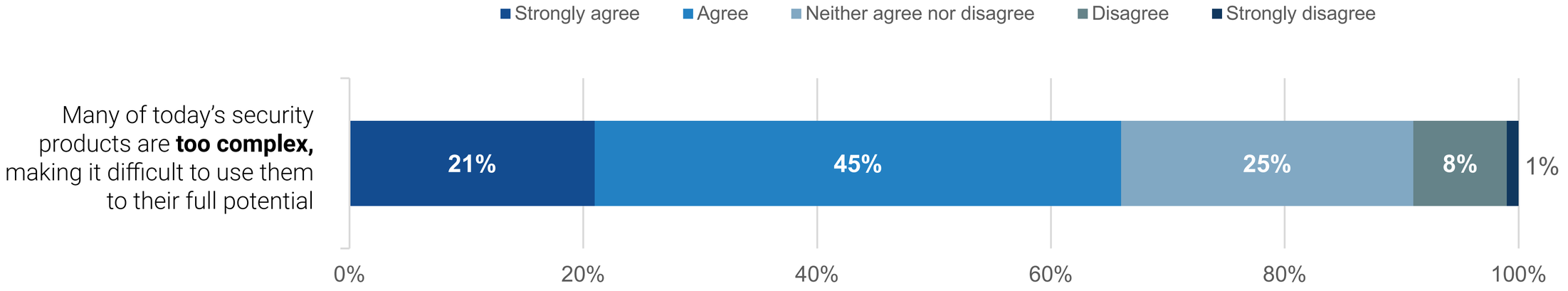
BACK TO CONTENTS

Ease of Use

While strong security is certainly paramount, firewall platforms must provide a high level of usability to help alleviate the skills gap. Two-thirds of Enterprise Strategy Group research respondents (66%) agreed that many of today's security products are too complex, making it difficult to use them to their full potential. Security tools may have advanced functionality, multilayered threat prevention, and even AI, but if they are not properly configured and managed, the value of these capabilities may go unrecognized.

From a firewall perspective, ease of use takes a few forms. First, consolidated firewall platforms must offer centralized, unified policy management across all the deployment models they support. This includes appliance-based branch and data center options, as well as virtual instances for cloud environments, containerized firewalls, and firewall-as-a-service. Additionally, management should be delivered from the cloud to avoid the need for additional infrastructure deployment on premises. Finally, consolidated firewall platforms should provide integrated network and security capabilities, which takes two forms. First, they should provide SD-WAN functionality to help organizations improve bandwidth optimization, reduce connectivity costs, and ensure better user experiences. Especially in the mid-market, organizations may be hesitant to deploy standalone solutions, making SD-WAN functionality on the firewall a significant value-add. Secondly, firewalls should support native threat detection and response activities. Because the firewall sits inline and sees the vast majority of an organization's traffic, it is in a unique position to provide security visibility. However, this data must be easy to understand and use for security teams to take full advantage of the value it offers. Logs certainly provide a story of what is happening in the environment, but for skills-starved security teams, it can be difficult to parse logs for actionable insights. Tools that are able to take logs and present their data in a more usable form offer a clear advantage for security practitioners.

Security Tools Are Too Complex



© 2023 TechTarget, Inc. All Rights Reserved.

6. Source: Enterprise Strategy Group Research Report, *Technology Perspectives from Cybersecurity Professionals*, July 2022.

BACK TO CONTENTS

Flexibility

Consolidated firewall platforms must provide broad coverage to close visibility gaps and avoid silos. This requires a range of deployment options. Security teams require a variety of appliances to support perimeter use cases for headquarters, regional, and remote/branch office locations, as well as performance-intensive on-premises data centers. Virtual instances are necessary to protect modern software-defined data centers, as well as public cloud IaaS environments. Due to the prevalence of multi-cloud strategies, security teams should look for vendors that, at a minimum, provide virtual firewalls across the major cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. Further, containerized firewalls have become important to protect modern, cloud-native application environments. Similarly, firewall-as-a-service integrated as part of a secure access service edge (SASE) architecture is important as organizations look to shift on-premises controls to the cloud. Vendors that provide coverage across a wide variety of these deployment scenarios can help customers solve both short- and long-term needs.

> “This type of security-as-a-service offering makes it **easier for providers to provision services to customers,** decreasing time to value for end-users.”

Flexibility should also be considered from a consumption and management perspective. While some organizations may have the resources to manage their firewall infrastructure on their own, others may be so short on skills or personnel that a managed service is preferred. As a result, vendors that support the ease-of-use requirements previously discussed, as well as offer a strong network of managed service provider (MSP) and managed security service provider (MSSP) partners to support customers of all types and sizes, can help security teams meet current and future needs as circumstances change. MSPs/MSSPs need flexible, subscription-based pricing models that support the shift from a capital expense model to an operational expense model where it is not necessary to own appliances. This type of security-as-a-service offering makes it easier for providers to provision services to customers, decreasing time to value for end-users.

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

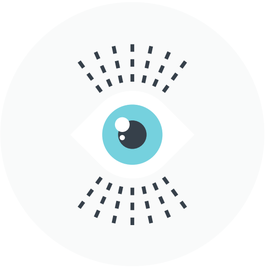
Spotlight – What MSPs and MSSPs Need from a Vendor Solution

There are certainly consistencies across the requirements of end-user organizations and MSPs/MSSPs. The ability to effectively detect stealthy and sophisticated threats is critical across both groups. Because MSPs/MSSPs suffer from the skills shortage just as end-user organizations do and are incentivized to be as efficient as possible to maintain margins, ease of use is also important. Yet there are some specific attributes that service providers should prioritize in addition to these characteristics, all of which center on management capabilities. **These attributes include:**



Scalability.

For MSPs/MSSPs, a cloud-native architecture based on microservices supporting multi-tenancy is critical. This ensures the MSP/MSSP can scale to support thousands of tenants without compromising the privacy or security of any individual customers. This model also allows MSPs/MSSPs to efficiently push updates to all their customers at once rather than having to do so on an individual basis.



Access control.

The level of outsourcing may change from one customer to another. Some customers may want nothing to do with their security management, while others may prefer to have visibility into what's happening in the environment. Role-based access control can enable MSPs/MSSPs to designate specific read-only access to customers so they have the information they need without having the ability to write or modify policy.



Analysis and reporting.

MSPs/MSSPs need the ability to quickly pivot from a specific customer to an aggregated view of the entire customer base to analyze potential threats and incidents and quickly update defenses when attacks are identified. Similarly, firewall platforms that support robust reporting functionality to allow MSPs/MSSPs to quickly audit environments and communicate back to customers gaps in defenses, events that have occurred, how outcomes compare to peers, and actions the MSP/MSSP has taken can help show value and grow the relationship.



Flexible billing.

MSPs/MSSPs have enough on their plate simply delivering core services to their customers. Back-end office functions including invoicing, billing, and contract management can quickly become complex, with providers scrambling to reconcile annual vendor contracts with shorter duration customer agreements. Vendor programs that take this into account and allow service providers to purchase in more flexible increments and shift unused spend credits from one service or customer to another help MSPs/MSSPs manage their business more effectively.

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

The SonicWall Network Security Portfolio



SonicWall's Enterprise-grade Firewalls and NSM Provide Strong Security, Flexibility, and Ease of Use for End-users and MSPs

SonicWall has provided network security solutions to enterprises, governments, and SMBs worldwide for over 30 years. Over that time, the company has shipped more than 3 million of its firewalls, which now span four product families:



Customers have the flexibility to deploy NSv firewalls on AWS and Azure public/government clouds and protect private cloud workloads on VMware ESXi, Microsoft Hyper-V, Nutanix, and KVM. The SonicOSX operating system is the core of both SonicWall's physical and virtual appliances and supports the company's patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection and patent-pending Real-Time Deep Memory Inspection (RTDMI) technologies, SD-WAN, real-time visualization, and high-speed virtual private networking, alongside other security features. The OS also provides Secure SD-WAN to enable organizations to build high-performance networks across remote sites using readily available, low-cost public internet services.

A complete range of security services are available across all these models, including intrusion prevention, application control, gateway anti-malware, content filtering services, comprehensive anti-spam, DNS security, and SSL decryption. Further, SonicWall's Capture Advanced Threat Protection (ATP) service protects customers from evasive advanced threats and malware. Capture ATP uses sandboxing technology to block unknown or suspicious files at the gateway until they are cleared as benign. The service uses multiple engines in parallel, including static analysis, RTDMI, emulation, and hypervisor analysis. This multi-engine approach helps reduce false positives while increasing the speed of detection and the organization's confidence in its security efficacy.

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

> “This combination provides real-time snapshots of the security posture in the environment.”

To support ease of use, SonicWall provides centralized management of its firewalls through NSM. NSM can be consumed as a SaaS offering or deployed on premises if customers prefer. It allows security teams or MSPs/MSSPs to deploy and manage all devices, device groups, and tenants they have responsibility for and synchronize security policies across the environment. When coupled with SonicWall Analytics, NSM transforms firewall traffic log data into actionable insights across users, applications, and networks. This combination provides real-time snapshots of the security posture in the environment and enables security responders to identify and investigate critical data points to expose hidden risks and intervene early to help avoid costly incidents.

Additionally, SonicWall offers both customers and MSPs/MSSPs ease of procurement through a variety of avenues. SonicWall Security-as-a-Service allows customers to fully outsource their network security to an experienced security provider. Updates, monitoring, alerting, hardware upgrades, and reporting are included. SonicWall’s MSP Monthly program allows customers purchasing through MSPs to forgo typical 1-, 3-, or 5-year contracts and subscribe on a monthly basis. Partners are not required to make any upfront purchases, with billing done in arrears. Partners are simply charged based on their consumption at the end of the month, and end-users only pay for what they use. Finally, SonicWall FlexSpend allows partners to cut procurement down to one step. As long as SonicWALL FlexSpend Credits are available in a partner’s account, the partner can enable multiple services instantly on multiple units at once, all without having to purchase and activate a large number of individual service SKUs. Partners can also transfer previously allocated, yet-unused FlexSpend Credits across different units.

Conclusion

While some in the industry have talked about the demise of the perimeter, and as a result the diminished importance of the firewall, the reality on the ground is vastly different. There is no question that enterprise environments are vastly different than they were just a few short years ago, and that has certainly impacted the perimeter. Now, rather than having a handful of ingress points to the network, security teams must protect a myriad of these access points across branch offices, remote sites, and cloud infrastructure. This doesn’t mean the firewall lacks value, but rather that firewalls must evolve to better meet the needs of todays’ distributed enterprise. The key to this is providing strong security, ease of use, and flexibility to help security teams do more with less and efficiently protect their organization. With SonicWall’s broad range of enterprise-grade firewalls, switches, and access points and its holistic approach of managing them through NSM, security teams can provide more consistent protection across the entire environment and more efficient threat detection and response.

© 2023 TechTarget, Inc. All Rights Reserved.

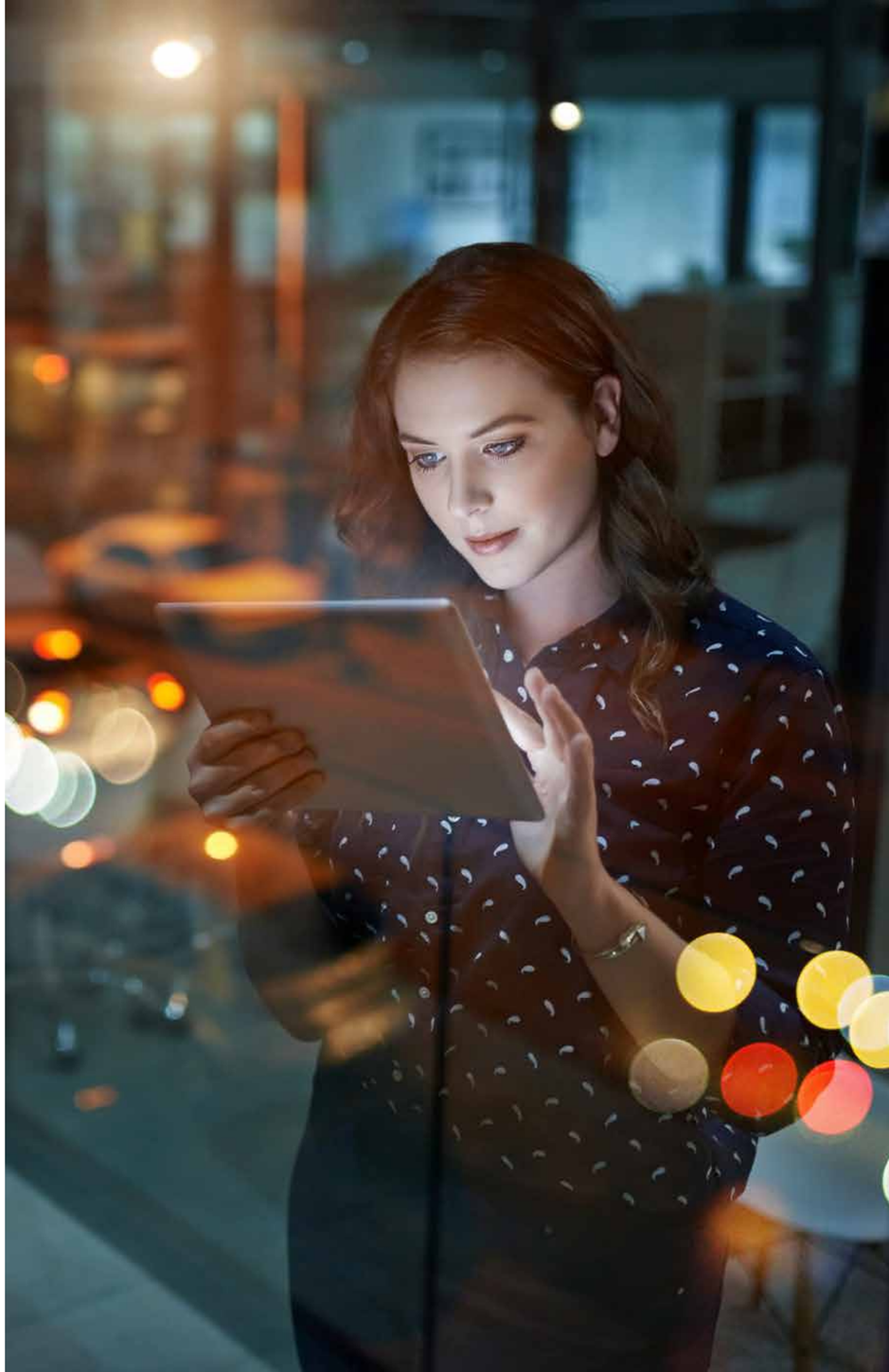
BACK TO CONTENTS

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.

LEARN MORE

For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.



ABOUT ENTERPRISE STRATEGY GROUP

TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2023 TechTarget, Inc. All Rights Reserved.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2023 TechTarget, Inc. All Rights Reserved.