SONICWALL

SOLUTION BRIEF: A UNIFIED APPROACH TO MANAGING GOVERNANCE, RISK AND COMPLIANCE

Integrating global management of network security

Abstract

A connected approach to security orchestration, control, analytics and reporting is not just fundamental to good preventative security practice, but it's also the basis for a unified security governance, compliance and risk management strategy.

A simpler, coherent big picture

Simplicity in security management practice promotes better security coordination and decisions. This requires freeing the clutter and manual routine from daily operations.

One of the best ways to remove these complexities is to employ smart management software as the foundation. This software must be systematic in its methods and workflow to reduce the number of personal interventions when managing the security environment. Rather than scrambling to react when systems develop problems or unauthorized changes are made to firewall rules, the intelligent software automatically recognizes and reports these types of security risks and helps to resolve them quickly.

Moreover, not having a coherent, big-picture view of the whole security ecosystem leaves organizations at risk to preventable cyber-attacks or compliance violations. The adoption of this common platform gives organizations of any sizes, including distributed enterprises and service providers, deeper insight to make more informed security decisions. It also empowers security teams to move fast and drive collaboration, communication and knowledge across the shared security framework.

Integrated, secured and extensible management

To simplify and unify, **an optimal solution would provide** an integrated, secured and extensible cloud-based architecture to manage the entire security portfolio. This unified cloud platform would enable security teams to easily consolidate the management of security appliances and federate all operational aspects of the security infrastructure. This includes centralized policy management and enforcement, real-time event monitoring, user activities, application control, data usage, drill-down data and flow analytics as well as forensics, compliance and audit reporting, and more. It would also meet the firewall change management requirements of enterprises through a workflow automation feature.

Governance, compliance & risk management

A comprehensive approach forms the foundation for a unified security governance, compliance and risk management strategy. You would want to establish a holistic, connected approach to security orchestration to federate all operational aspects of your network security ecosystem. It should simplify and automate various tasks to promote better security coordination to reduce the complexity, time and expense of performing security operations and administration. Such tasks include:

- Security and network provisioning
- Policy enforcement
- Patching
- Device discovery
- Inventory
- Configuration and diagnostics
- Monitoring
- Reporting
- Analytics
- Auditing
- Security statistics collection

Workflow automation

The workflow process assures the correctness and the compliance of policy changes through rigorous validation and enforcement procedures prior to deployment. Approval groups should be flexible and in conformance with the company personnel security guidelines. This will help mitigate risk, reduce errors, improve efficiency and ensure high security effectiveness. With proper workflow automation and auditing of policy changes, security teams would have the agility and confidence in deploying the right firewall policies, at the right time and in conformance with compliance regulations.

Zero-touch deployment

By leveraging the cloud, an ideal solution would simplify and speed the deployment and provisioning of firewalls remotely. This would reduce the time, cost and complexity associated with device configuration. At the same time, security and connectivity could occurs instantly and automatically. Administrators could operationalize large number of firewalls at scale with minimal user intervention. From a single web-based management console, for example one could push policies, perform firmware upgrades and synchronize licenses.

Analytics

An effective solution would enable IT to perform deep investigative and forensic analysis of enriched security data. It would empower stakeholders with single-pane visibility and situational awareness of the network security environment.

Security teams should have the agility and confidence in deploying the right firewall policies at the right time and in conformance with compliance regulations.

This would empower them to make informed security policy decisions based on time-critical and consolidated threat information. IT could calibrate security policies and controls as potential risks and threats are uncovered. As a result, it would reduce incident response time with real-time, actionable threat intelligence.

Conclusion

With the right cloud-based security management platform, organizations and service providers can establish a fully coordinated security governance, compliance and risk management strategy. The right platform can also reduce the operating expenses and complexities of supporting a solely-owned infrastructure while providing the ultimate in visibility, agility and capacity to govern the entire SonicWall network security ecosystem with greater clarity, precision, and speed – all from one place.

Learn how the SonicWall Capture Security Service can enhance your bottom line at sonicwall.com/capture-security-center.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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