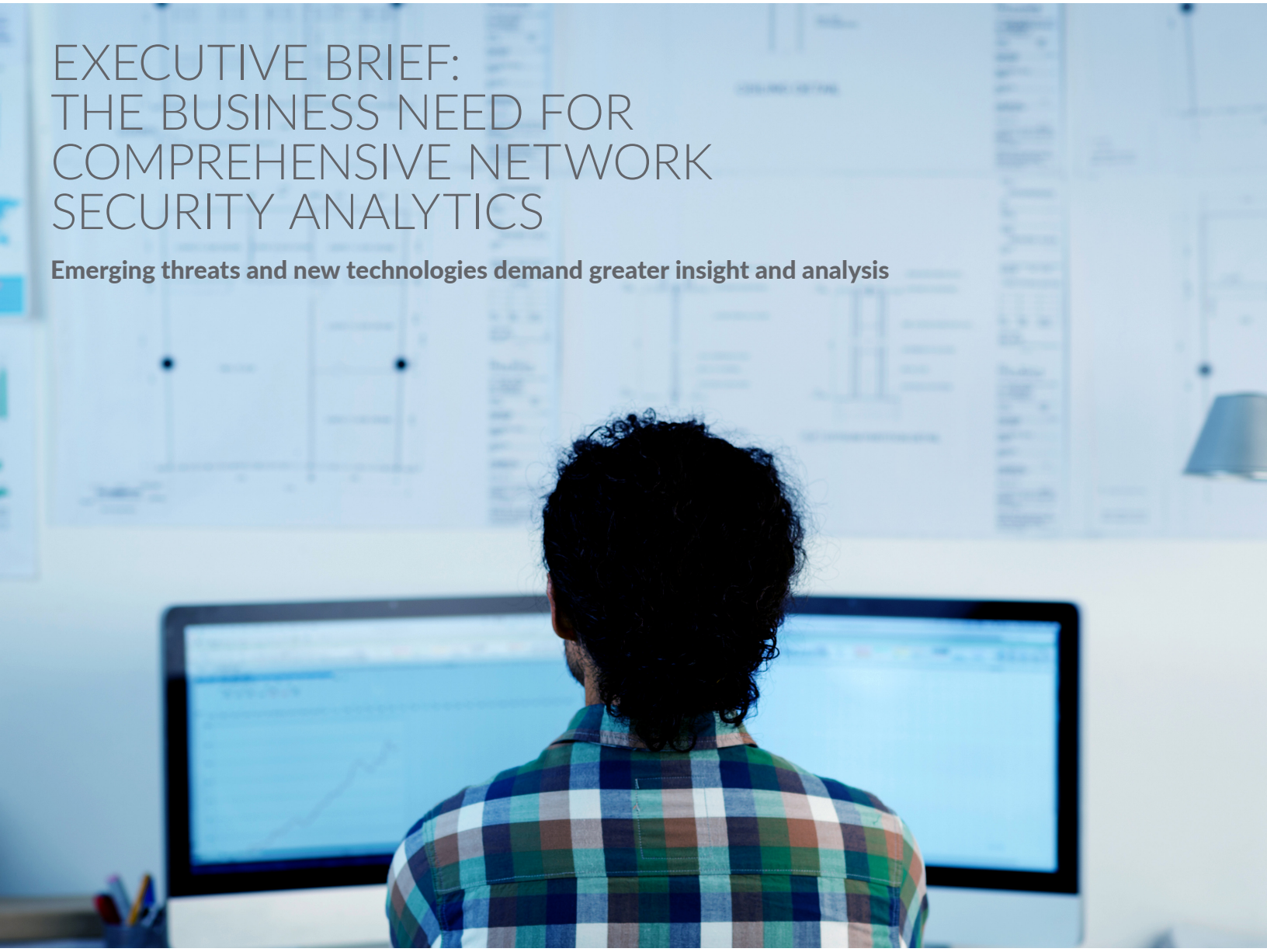
SONICWALL

EXECUTIVE BRIEF: THE BUSINESS NEED FOR COMPREHENSIVE NETWORK SECURITY ANALYTICS

Emerging threats and new technologies demand greater insight and analysis



Abstract

Disastrous attacks can happen quickly in today's highly disruptive and unpredictable cyber threat landscape. To keep the organization running and users' productivity at an optimal level, network security personnel need to constantly monitor and maintain the health and defense of networks and services.

The state of today's cyber crime

It is not uncommon for any organization's network to be the victim of security breaches. These might include unauthorized intrusions, insider threats and any number of malware or phishing attacks that could spread ransomware within the organization. These attacks slow an entire organization's momentum, as key personnel divert their focus from key business priorities to damage control.

Network security stakeholders should be concerned with the rising risks created by the speed at which cyber criminals develop new types of threats using new attack vectors. Up to 84 percent of cyber attacks target the application layer[1], while 37 percent of cyber threats target emerging attack surface areas such as databases, IoT devices and appliances and micro services.[1] Emerging cyber attacks make organizations the victims of mobility, wireless, cloud and even IoT, rather than the beneficiaries of these new technologies. Attacks and malware can be hidden inside encrypted traffic to bypass firewall inspection. Attackers can gain access to multiple parts of the network. Ransomware can enter via malvertising, webmail phishing attacks or exploits. The inability to address rapidly emerging threats can hamper an organization's ability to protect sensitive information, meet compliance and maintain normal service operations.

Critical Network Insight

- North-South Traffic
- East-West Traffic
- User Access
- Connectivity
- Web Usage
- Application Usage
- State of Security Assets
- Real-Time Security Events
- Threat Profiles
- Relevant Security-Related Data

A dire need for insight and analysis

Ultimately, the network security team may have only very limited visibility and insight into everything that goes on in the organization's network security environment. This includes north-south and east-west network traffic, user access, connectivity, web and application usage, state of security assets, security events, threat profile and other security related data.

The lack of aggregation, normalization, correlation, and contextualization of disparate security data can lead to an incomplete and disjointed view of what is truly happening on the networks. The absence of this structured data leaves the organization at risk and further impairs the network security team's ability to recognize and solve security problems. The organization needs to know all the risks and how to plan for them. As many as 94 percent of data breaches are preventable by practicing proper cyber hygiene and proactive risk management.[1]

Without the insight provided by analytics, the network security team finds it nearly impossible to do accurate security planning, make informed policy decisions, and respond to security incidents at the speed required to meet organizational initiatives. According to Forrester, 74 percent of global enterprise security decision-makers rate improving security monitoring as a high or critical priority.[2] Without complete awareness and understanding of the network security environment, it is very difficult to keep the security risk down to a minimum, ensure network uptime, service delivery and workforce productivity, and conforms to compliance regulations. These are key challenges security operations face today.

Conclusion

As the pace of cyberattacks accelerates, network security stakeholders need to be concerned about their capacity to stay apprised of their threat posture, protect sensitive information, meet compliance and maintain normal service operations for all business locations and users, while safely moving the company's digital transformation forward.

Learn more. Read our Solution brief A comprehensive approach to network security analysis.

[1] "The New Enterprise Security Model: How to Operationalize Cyber Risk Management in Today's Dynamic Threat Landscape," *RiskSense*
[2] The Forrester Wave™: Security Analytics Platforms, Q1 2017

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