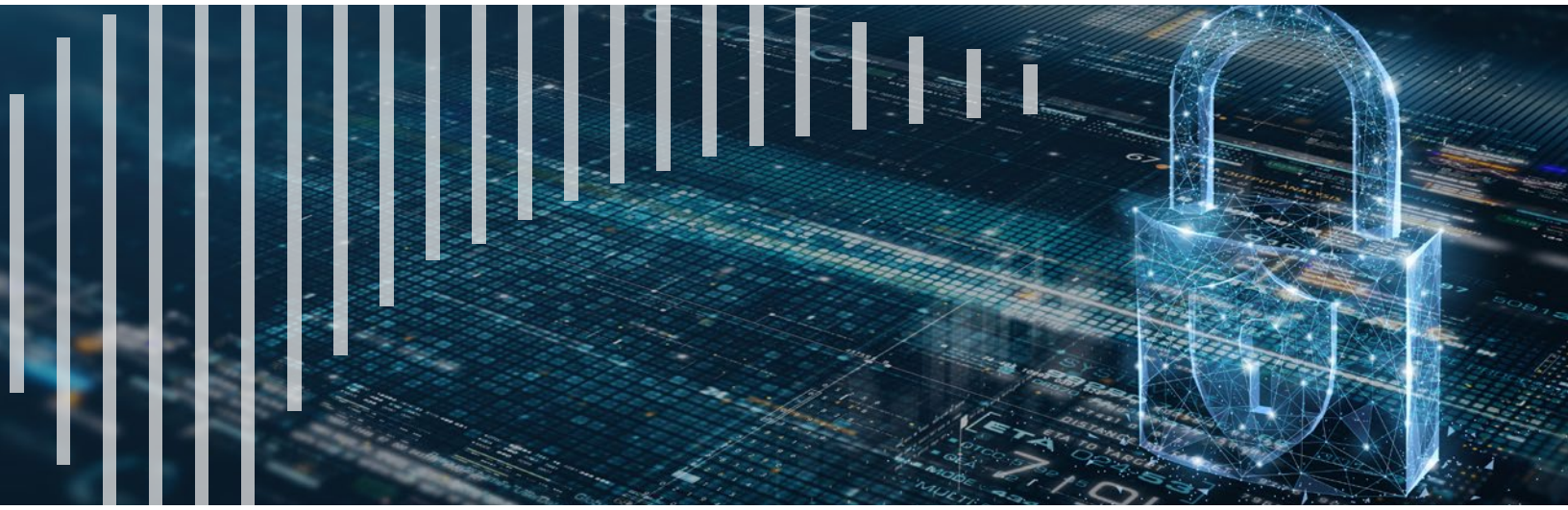
SONICWALL



EXECUTIVE BRIEF

Evolving Threats – Evolved Strategies

Intro

The ever-evolving cybersecurity landscape is rapidly changing, and businesses must change with it.

The massively expanding, distributed IT reality is creating an unprecedented explosion of exposure points for sophisticated cybercriminals and threat actors to exploit.

With hybrid and fully remote environments becoming increasingly more common, cyberattack vectors are also increasing through an influx of new exposure points. Commonplace threats and multi-stage attacks are increasingly becoming more difficult to detect. Many organizations are looking for ways to bolster their cybersecurity and stay ahead of bad actors. There are multiple strategies and technologies businesses can leverage for a stronger security posture to protect their organization.

Implement Multifactor Authentication

Multifactor Authentication (MFA) is an absolute must for both business and personal use. MFA acts as another barrier between networks and cyber criminals. Enabling MFA can make attacks more challenging and even cost-prohibitive for threat actors to attempt. MFA can shut down common attacks like phishing, key loggers, brute force and man-in-the-middle (MITM) attacks. There are different types of MFA:

- Personal device-based: This could be something like a text message or an authenticator app
- Hardware based: This utilizes an actual piece of hardware like a USB, Smart Card or RSA token
- Biological: This could be a fingerprint or a retina scan

As with any technology or software, businesses must conduct the proper research and testing protocols to implement the right MFA policy to fit their security needs.

Learn to Better Assess Risk

To build an effective security strategy, businesses must know how to accurately assess risks, which is different at every organization. A government agency may be safe-guarding global assets and matters of national defense. A small business may be growing their brand reputation and locking down their financial assets. No matter the size of your organization, many security professionals look to the National Institute of Standards and Technology (NIST) to ensure standards and regulatory best practices. While frameworks can set a solid foundation, organizations must assess their unique risks for their environments. Businesses must have a broad perspective along with nuanced details concerning their own risk. Leaders from cross-functional departments can provide their perspectives. Cybersecurity professionals may find that the other departments have different, valid perspectives on risk. Once the organization has a thorough understanding of risk across its entire ecosystem, security professionals can map a path forward to implement a stronger security posture.

Address the Skills Gap

Businesses need qualified professionals to defend the organization's infrastructure from cyber-attacks. As the complexity of the network grows, so does the need for solid support staff. Most organizations discover they need highly qualified people to effectively protect company hardware, software and networks from cybercriminals. Attracting top

talent is a business imperative, but many organizations may experience staffing challenges. Hiring and retaining cybersecurity professionals has proven to be a daunting task. SonicWall has a large partner network that can be utilized to help businesses of all sizes achieve their security goals and objectives.

Choose the Right Technology

Security defenses have advanced which has increased IT management teams' capabilities to safeguard their assets and keep networks safe. A solid strategy includes multi-layer protection and seamless coverage across all attack surfaces.

Threat actors are trying to target your organization using a growing footprint of applications, devices, networks and infrastructure. They're attacking with everything from phishing and never-before-seen malware variants to ransomware, side-channel attacks, IoT attacks and more – all of which can be especially difficult to detect.

SonicWall helps you eliminate blind spots and secure a "boundless" workforce across all environments. You can see everything, everywhere and act fast on the events that matter.

Our Capture Security Center eliminates siloed visibility. Using a single-pane-of-glass and unified point of control, you can see every attack surface across multiple generations of IT infrastructure (on premises, cloud, endpoints and Secure Network as a Service.)

Real-time, around-the-clock threat awareness reveals vulnerabilities in the landscape as they happen and always knows what they are and what they are trying to breach. Personalized risk meters further minimize exposure and prioritize actions according to risk profile while actionable analytics and reporting accelerate response times and help shape your strategy.

SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) blocks zero-day and unknown threats at the gateway — even those that hide via encryption or don't exhibit malicious behavior. The technology is built to understand how threat actors are operating. Zero-day threats won't have an attack signature until after the first time they're used, rendering businesses vulnerable. RTDMI detects those threats and enables a level of visibility that allows you to see those changes in attacker behavior.

Expect More

Organizations need to know that their vendors are taking proper security measures when developing their products. Ideally, vendors should have systems like software composition analysis and static application security testing in place. It is critical to have visibility into the development pipeline to understand your risk exposure to multiple vulnerabilities. Threat actors know the perimeter is going to be the hardest place to access within the organization. They look for vulnerabilities across the entire organization – and that includes third-party software and hardware. Companies can create vendor questionnaires that assess standards the vendors must meet for consideration. Vetting multiple vendors through questionnaires provides ample data to decide which vendor fits your business best. Requiring higher vendors can help organizations strengthen their overall cybersecurity posture.



Conclusion

Threat actors are constantly changing their plans of attack to infiltrate businesses and cause as much havoc as possible. In a world where the cybercriminals are constantly changing their attacks to catch organizations off guard, those same organizations can implement strategies that will keep them one step ahead.

- Implement Multifactor Authentication to make it more difficult for threat actors to infiltrate networks.
- Develop better risk assessment strategies to make sure the business is protected across all potential points of entry
- Hire and develop highly qualified staff to optimize and maintain all security systems
- Select the best technology across networks, endpoints, and access points protecting data and users
- Enact stringent requirements for vendors to ensure the business isn't importing vulnerabilities from third-party hardware and software.

Ultimately, it's the responsibility of each organization to determine what cybersecurity strategies will work best for their business. To learn more about how to build, scale and manage security across cloud, hybrid and traditional environments, contact a SonicWall Security Expert today.



About 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. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

© 2023 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.

ExecBrief-EvolvedThreats_EvolvedStrategies-US-JK-7925