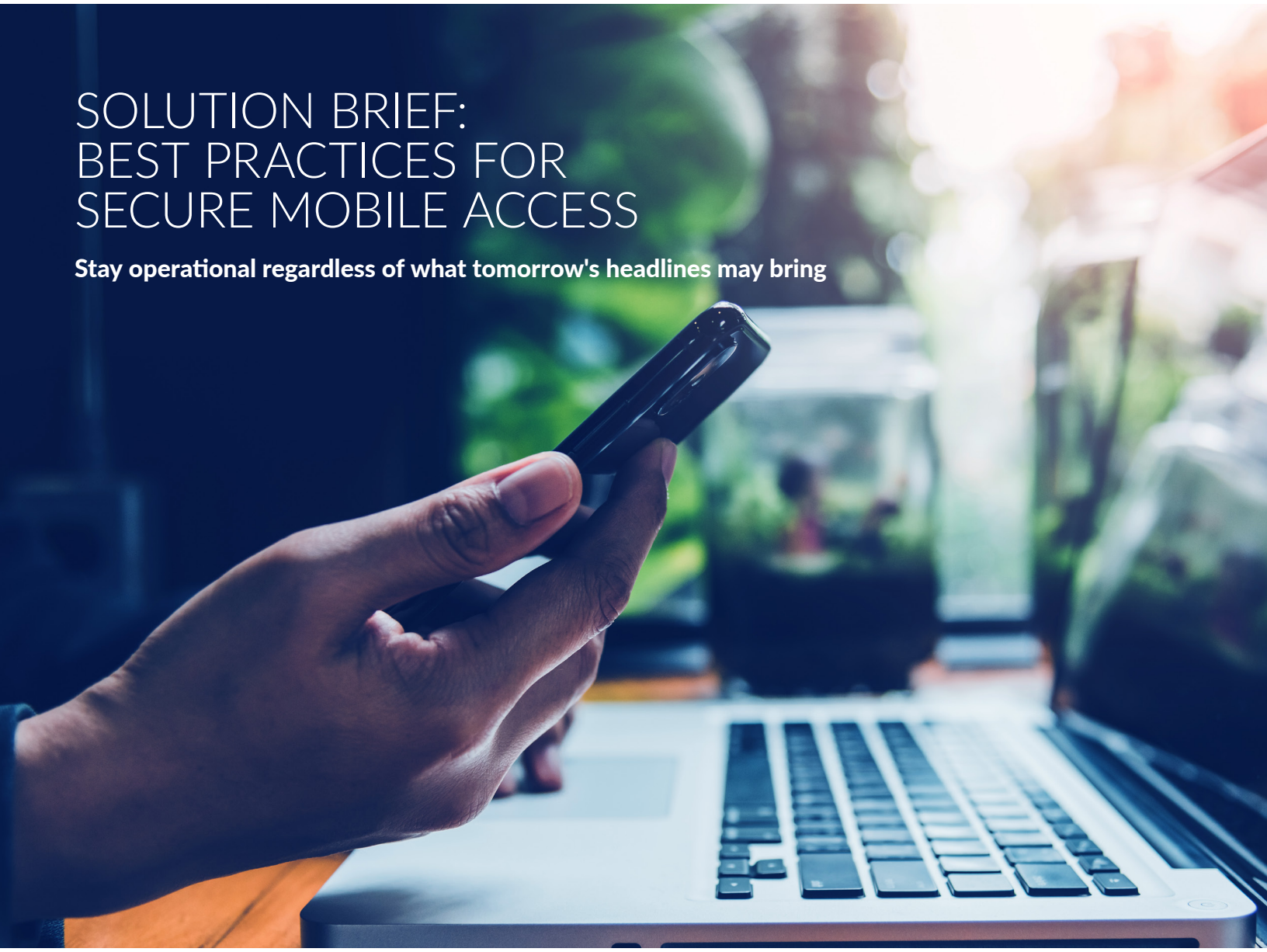
SONICWALL

SOLUTION BRIEF: BEST PRACTICES FOR SECURE MOBILE ACCESS

Stay operational regardless of what tomorrow's headlines may bring



Abstract

Supporting business goals for today's digital workspace requires secure mobile access, yet obstacles stand in the way of balancing security, access, performance and value. Best practices for effectively implementing a protected mobile workforce include maintaining high security, connectivity, robust performance, and low total cost of ownership. This solution brief details practical steps to achieve those best practices.

Introduction

Whether for ensuring business continuity or enhancing workforce retention and productivity, more organizations are embracing mobility, work-at-home and flex-time for their employees. To achieve business goals with a mobile and remote workforce, having a robust and reliable access security service has never been more critical. A key element of ensuring reliable mobile access is maintaining security updates, but maintenance can disrupt service and performance. Organizations need to maintain a flexible work environment without losing availability, but deploying a highly available service can be complex, costly and time consuming.

Effective cybersecurity must include secure mobile access

Providing mobile access in today's anywhere/anytime, hyper-distributed world opens an explosion of exposure points over a myriad of potentially insecure mobile endpoint devices.

Human fallibility and risky online behavior mandate that employees cannot be trusted to ensure the security of their own mobile devices.

Moreover, the array of threat types is expanding, deepening and getting smarter, including targeted ransomware, never-before-seen threats, memory-based malware, side-channel attacks and encrypted threats.

Ultimately, the security of your mobile network must match that of your wired network.

Stay operational regardless of what tomorrow's headlines may bring.

Best Practices: Simple, safe and agile mobility

To be effective, cybersecurity must provide mobile employees with easy and secure 24/7 access to key business resources in an agile, easy-to-use, cost-effective and scalable way.

This requires a zero-trust posture regarding any mobile device attempting to connect with corporate resources, whether those resources be on-prem or in the cloud. Secure mobile access is a core component of a zero-trust approach to anywhere, anytime access.

IT must also secure access from these mobile endpoints with limited budgets and skilled staff resources.

This means streamlining deployment, availability and support to lower total cost of ownership.

SonicWall Secure Mobile Access

The SonicWall Secure Mobile Access (SMA) solution enables anywhere, anytime access across hyper-distributed enterprises. This gives your business the agility to stay operational regardless of what tomorrow's headlines may bring.

The SonicWall SMA 1000 Series provides distributed enterprises with comprehensive end-to-end secure remote access to corporate resources hosted across on-prem, cloud and hybrid datacenters. It applies identity-based, policy enforced access controls, context-aware device authentication, and application level VPN to grant access to data, resources and applications after establishing user and device identity and trust. Flexibly deployed as a hardened Linux appliance or virtual appliance in private clouds on ESXi or Hyper-V, or in AWS or Microsoft Azure public cloud environments. It supports up to 20,000 concurrent connections with a single unit and scale upwards of hundreds of thousands of users through horizontal clustering.

SMA streamlines your company's flex work initiatives with:

- Always-On VPN
- Single Sign On (SSO) using SAML Identity Provider
- High Availability
- Multi-Factor Authentication (MFA)
- Capture Advanced Threat Protection (ATP) sandboxing
- TLS 1.3 Support
- Flexible and Scalable Deployment
- Centralized management
- Low TCO

Conclusion

Best practices for mobile security include zero-trust access control, seamless dependability and low total cost of ownership. Fortunately, there is a viable solution to help you implement all of these best practices.

To learn how you can be more successful in maintaining a healthy access security environment while achieving zero downtime, visit www.sonicwall.com/products/secure-mobile-access.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 28 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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