SONICWALL®

EXECUTIVE BRIEF

SECURING YOUR REMOTE WORKERS ACCESS: A STRATEGIC MISSION IMPERATIVE

Mobile access ensures that mission-critical operations and services are not disrupted in an uncertain, dynamic world

Abstract

Globally, the remote workforce is here to stay – and on the rise. The benefits in agility, continuity, and productivity make secure mobile access strategically imperative for today's government agencies and departments. However, to effectively support this workforce, IT is faced with several challenges, including an explosion of endpoints, smarter threats and the need to access mission critical resources, all while operating on a lean budget.

Introduction

Each day's headlines can bring disruptive challenges that require dynamic technology solutions. Public health emergencies; natural events such as earthquakes, tsunamis, hurricanes and blizzards; and political crises can all restrict mission-critical staff from travel or accessing resources at a physical site. To ensure mission continuity, agencies must have the agility to conduct operations from anywhere, at any time.

Case in point: In response to COVID-19, the Office of Management and Budget issued with a mandate to "Maximize telework across the nation for the Federal workforce (including mandatory telework, if necessary), while maintaining mission-critical workforce needs."

Even when not faced with pandemics, many agencies seek to benefit from increasing team workforce productivity as well as minimizing operational overhead costs of maintaining physical office facilities, by empowering personnel to work safely and securely from anywhere, at any time.

As a result, government agencies have increasingly relied upon remote access to resources from both authorized and BYOD devices outside of their traditional network perimeters.

Effective cybersecurity must include secure mobile access

Providing remote 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.

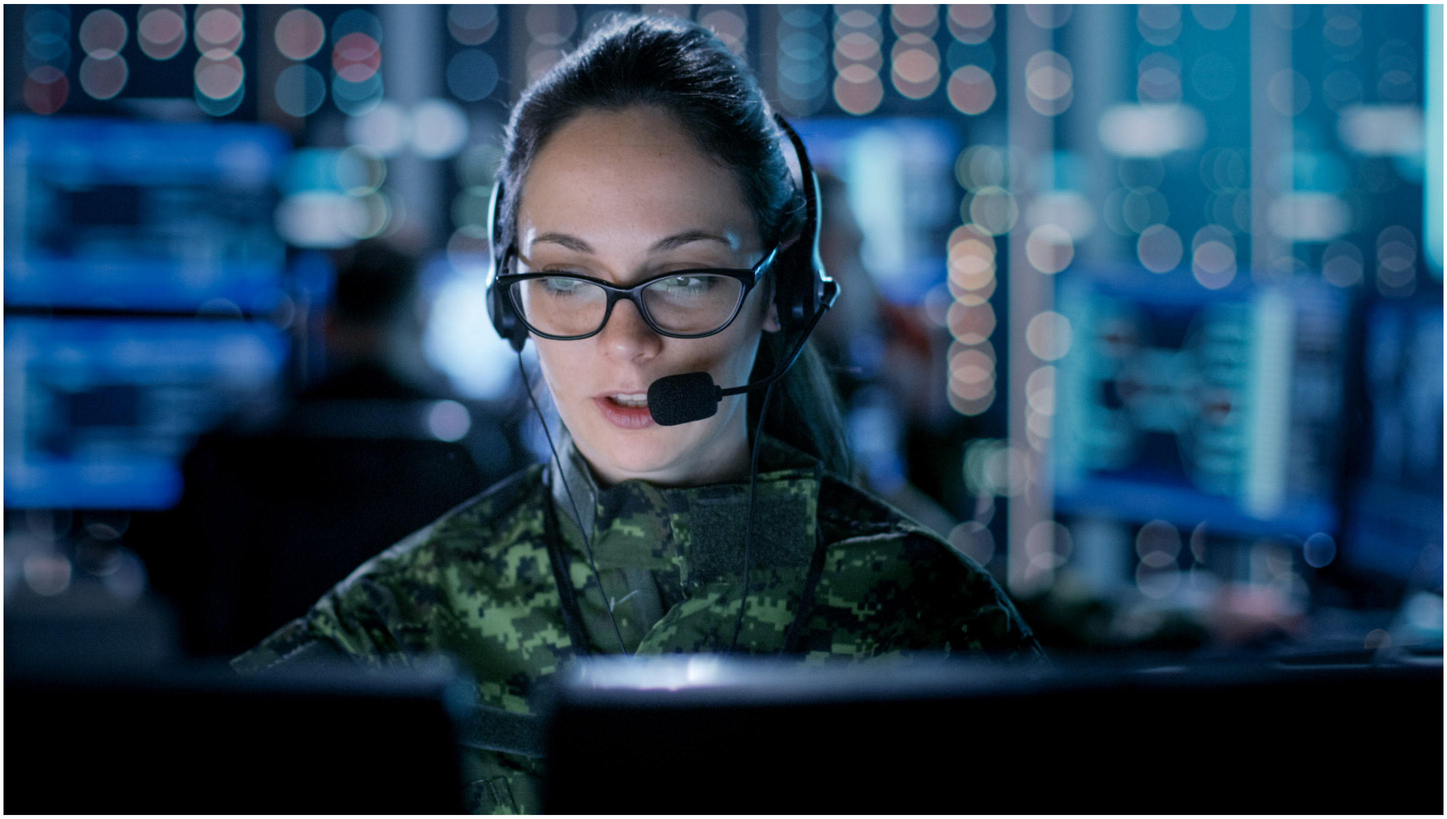
Ultimately, the security of your remote network must match that of your wired network. This requires a zero-trust posture regarding any remote device attempting to connect with agency resources, whether those resources be on-prem or in the cloud. Secure mobile access is a core component of a zero-trust approach to secure 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. To be effective, cybersecurity must provide remote employees with easy and secure 24/7 access to key agency resources in an agile, easy-to-use, cost-effective and scalable way.

Conclusion

Whether for ensuring operational continuity or enhancing workforce productivity, secure mobile access is a mission business imperative. The SonicWall Secure Mobile Access (SMA) 1000 series enables secure anywhere, anytime access across hyper-distributed operations. This gives your agency the agility to stay operational regardless of what tomorrow's headlines may bring.

Learn more at www.sonicwall.com/products/remote-access.



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

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.