EXECUTIVE BRIEF:
WHY SECURE MOBILE ACCESS IS A STRATEGIC BUSINESS IMPERATIVE

Mobile access ensures your business keeps productive in a disruptive, dynamic world

Abstract
Globally, the mobile 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 business. However, to effectively support this workforce, IT is face with several challenges, including an explosion of endpoints, smarter threats and the need to access both internal and SaaS resources access, 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 revenue continuity, companies must have the agility to conduct business from anywhere, at any time.

At the same time, many companies seek to benefit from increasing staff productivity and retention, as well as minimizing operational overhead costs of maintaining physical office facilities, by empowering personnel to work from anywhere, at any time.

According to a global 2019 IWG survey of over 15,000 professionals from a range of different industries in 80 countries:

- 85% confirmed increased productivity due to greater flexibility
- 65% say flex work helped reduce CAPEX/OPEX and manage risk
- 75% consider flex work to be the new normal
- 62% of companies worldwide currently have flex work policies
- Over half of employees worldwide work remotely more than 2.5 days a week
• Over 80% of workers would choose a flex-work job over a non-flex job

• The U.S. economy alone could see a $4.5 trillion boost through flex work

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

**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. 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. 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.

**Conclusion**

Whether for ensuring business continuity or enhancing workforce retention and productivity, secure mobile access is a strategic business imperative. 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.

Learn more at [www.sonicwall.com/products/remote-access](http://www.sonicwall.com/products/remote-access).
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.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 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