SONICWALL™

Executive Brief: Ready or not, mobile workers and BYOD are here to stay

IT struggles to embrace mobile workers and BYOD while maintaining data security

Abstract

Mobility and BYOD in the workplace have increased dramatically. Employees demand the freedom to choose the best mobile devices they need to do their work. When they have that flexibility, they're more productive. However, IT must balance allowing greater freedom in mobile access with the demands of mobile security.

The evolving mobility landscape

The way business professionals work has changed dramatically over the last several years, and continues at a rapid pace. According to IDC, the U.S. mobile worker population will increase to 105.4 million in 2020, and account for 72.3% of the U.S. workforce. So, clearly, many employees aren't just sitting at their desk in the office. Instead, they're often on the move, working from different locations across different hours with different devices. This allows them access to the data and applications needed to perform their jobs, while providing for their own work/life balance.

For example, many workers wake up each day and immediately check their email and voicemail for new messages using their smartphones or tablet devices. They continue to do this throughout the day regardless of their location usually right up to bedtime. We've become an "always-on" society.

We also find ourselves doing more work remotely, such as at a coffee shop, on a train to work, on a business trip from a hotel room, on the road while meeting with customers or working from our home office. Employees want and need to do their jobs wherever and whenever, using whatever device best suits them.

What workers want and need

Workers want the freedom to use the devices they prefer, including smartphones, tablets, laptops or other devices. Their choice may change throughout the day depending on where and when they're working, and what level of data and applications they need. For instance, employees often check

> The choice between mobile access and mobile security can be a tough balancing act for IT.

their email using a smartphone, but use a laptop or PC to create presentation slides or spreadsheets. The key is that workers want to use the devices they're most comfortable with depending on the situation at the moment. Tech Pro Research shows that 74% of organizations either already or plan to allow employees to bring their own devices to work. Meanwhile, Gartner reports that 70% of mobile professionals will conduct their work on personal smart devices by 2018.

Workers also want to choose the applications they use – no matter if they're employer-issued or personally owned. And, most importantly, they must have access to the data they need for their jobs, whether it's online through the internet or behind their company's intranet firewall – regardless of where they are, when they want it and where it exists.

When employees can use the devices they prefer to securely access the applications and data they need – anytime and anywhere – they're significantly more productive. According to IDC, mobility has become synonymous with productivity both inside and outside the workplace, and the mass adoption of mobile technology in the U.S. has cultivated an environment where workers expect to leverage mobile technology at work. Employees also view this opportunity to have a work/life balance as a true benefit of working for their employer, which helps HR retain top talent and attract more.

Significant risks and concerns for IT

While IT recognizes mobile workers and BYOD are here to stay, this proliferation of devices in the workplace (both employer-issued and personally owned) has increased the demand on organizations to enable secure mobile access to company applications, data and resources. Often, remote and mobile workers rely on the same device for both business and personal use, resulting in intermingling of business and personal data and applications.

This creates an increased risk of security breaches for organizations, such as:

- Unauthorized users gaining access to company networks and systems from lost or stolen devices
- Devices infected by malware and ransomware that act as a conduit to infiltrate company systems
- Interception of company data in-flight on unsecured public Wi-Fi networks
- Loss of business data stored on devices if rogue personal apps or unauthorized users gain access to data

Customers need the ability to react as quickly as possible to minimize the window of exposure before an attacker can potentially cripple the organization.

This can be challenging for IT. For example, IT could just open everything up so it's easy for workers to get to anything they want. But, that also makes it easy for them to access data and resources in inappropriate and/or insecure ways. Or worse, it makes it easier for bad guys to access your data and resources.

Alternately, IT could lock everything down tightly with all kinds of controls and technologies. However, this could make it so difficult for workers to access data and resources that they find ways around these security measures, or just look for a job at a more user-friendly company.

Learn more about how to solve these concerns regarding enabling secure mobile access over BYOD. Read our Secure Mobile Access for BYOD e-book.

© 2016 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.

About SonicWall® Solutions

SonicWall® solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, SonicWall solutions mitigate risk and reduce complexity so you can drive your business forward.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com