SonicWall Secure Mobile Access for BYOD

Using converged solutions to ensure mobile workforce management and mobile security management

SONICWALL™

Introduction

Businesses are transforming their mobile strategies. They're moving from supplying company-owned devices to a bring-your-own-device (BYOD) approach. And along with this shift has come a change in the way IT secures its mobile devices and connected networks.

Converged technology combines the best of management and security capabilities to enhance mobile productivity.

Mobile risks

Mobility and BYOD come with a number of inherent risks:

- Lost or stolen devices
- Compromised or leaked data — especially when personal and business data is co-mingled
- The increasingly complicated threat of malware

Also, consumer data protection laws and regulations in some countries require IT to respect employees' personal data privacy on devices that are also used for work, adding another layer of complication to IT demands.

Some companies have tried layering disparate technologies to protect devices and networks independently, but that approach has not been effective.

Security tools

Today, IT can implement a number of solid mobile workforce management and mobile security management tools to help secure mobile data and devices:

- Mobile device management (MDM)
- Mobile application management (MAM)
- Secure Sockets Layer virtual private network (SSL VPN)
- Network access control (NAC)

Individually, each of these tools has benefits and drawbacks.

To save money and reduce complexity, security tools need to work with business data flows, protecting data in flight, at rest and via access gateways.

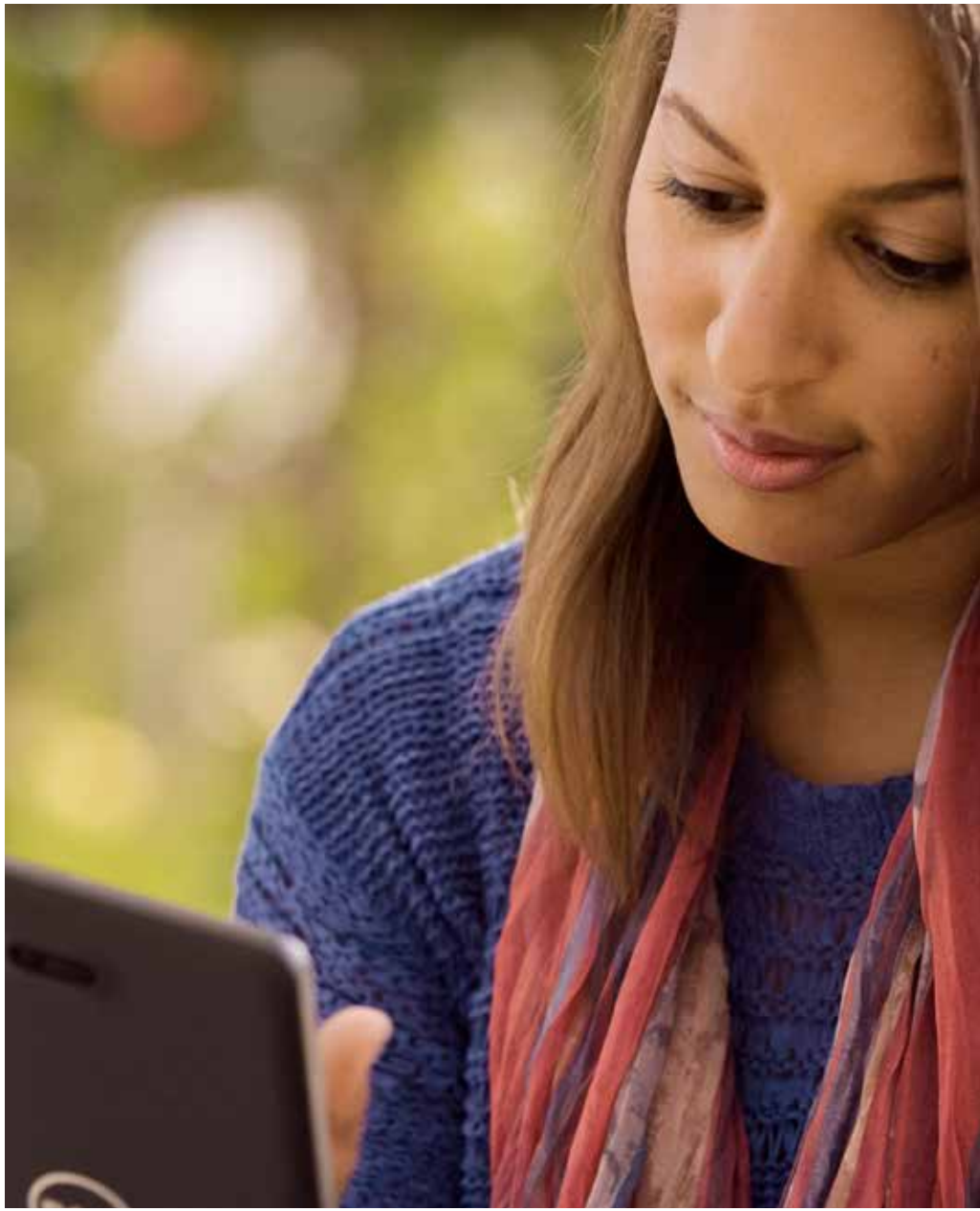
SONICWALL™

Mobile device management

MDM provides a single point of contact and control for the management of mobile devices. An MDM solution typically includes a device-level agent and management software. It enables device-level management including software distribution, security, policy and inventory management, and service management.

MDM offers the ability to wipe a device's data when the device is lost. But it adds IT management and administration of personal devices, which users may resist to protect their own privacy. Also, data can be leaked if it's transferred to other devices because MDM typically creates policies at the user level rather than for applications. MDM also can't block information-sharing via cloud services or other third-party applications.

MDM provides a single point of contact and control for the management of mobile devices.



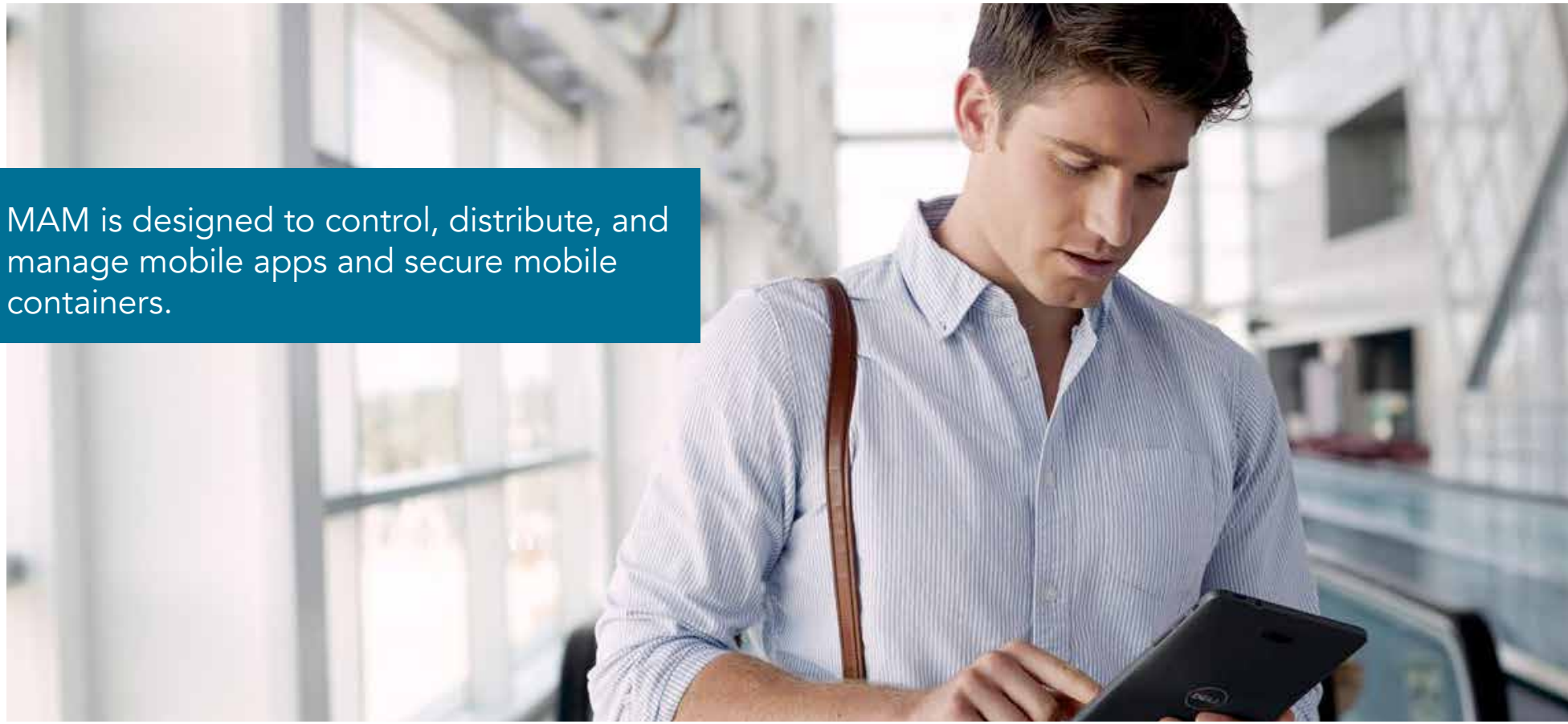
SONICWALL™

Mobile application management

MAM gives IT the ability to provision secure containers, apps and application data on any mobile device that is given corporate network access, and allows the isolation of business and personal apps and data.

MAM allows policies to be set at the application level, but not all applications can be managed by MAM, which may require proprietary applications and custom app development. It also may not be popular with mobile users who want application and service choice.

MAM is designed to control, distribute, and manage mobile apps and secure mobile containers.



Secure Sockets Layer virtual private network

In the mobile workplace, SSL VPN creates secure communications between the mobile device and the VPN gateway. An SSL VPN access gateway helps authenticate and control users trying to access a network when a device is lost, and provides a key security layer for employees who need to access the network from unsecure locations outside the corporate parameters.

SSL VPN uses encryption to create a secure communications option for data transmitted between two endpoints.

SONICWALL™

Network access control

NAC manages and enforces end-point security policy. NAC may rely on information from MDM to confirm that a device is policy-compliant before allowing it access to the network. NAC can also help authenticate and control users trying to access a network when a device is lost.

SONICWALL™

Growth of BYOD

It can be difficult, if not impossible, to install and use security technologies when IT no longer owns or manages the mobile devices. But BYOD strategies are becoming the status quo, and organizations need to find ways to address security risks in this new business context.

By 2018, Gartner predicts twice as many employee-owned devices used for work than enterprise-owned devices.*

Gartner Inc. Nov 2014

SONICWALL™

BYOD and data protection

To protect business data flows for BYOD, mobile management and security technologies are converging. The focus is shifting from protecting the device to protecting business data and applications, both at rest and in-flight. For example, Apple's recent iOS releases make application-level management easier.

Secure access gateways now combine user authentication with device inspection and security policy to validate security state and app-level VPN access controls. This gives IT the tools it needs in a single platform to provide policy-enforced secure mobile access for BYOD users, while protecting against rogue access and malware threats. And if on-device business data protection is needed, adding enterprise mobile management completes a comprehensive solution.

Maturation of mobile operating systems and technologies is making more granular security management possible.

SONICWALL™

Converged solution

Some organizations make use of one or more of the existing mobile security technologies — MDM, MAM, SSL VPN and NAC. But it's only when elements of all four are implemented as a converged solution that IT managers can be sure corporate applications, data, networks and devices are fully protected. Combined, these technologies provide comprehensive protection at all access gateways:

- MDM and MAM— protects the device and data on the device
- SSL VPN — secures data in flight
- NAC — helps enforce endpoint security and network access policy and guards the corporate network and servers

A converged solution lowers the risks of BYOD and mobility while giving users what they want — the use of the devices they love with access to the data and applications they need.

SONICWALL™

Faster, simpler mobile security management

SonicWall solutions provide IT teams with the level of management and security they need to meet their business requirements. End users get the functionality and features they need and want to do their jobs. With our solutions, IT departments no longer need to buy, install and maintain multiple, disparate, mobile solutions from multiple vendors, which ultimately saves time and reduces complexity. SonicWall's Secure Mobile Access and Enterprise Mobility Management solutions enable IT teams to:

- Secure and manage endpoint devices, workspaces, and containers
- Provide secure access from mobile devices
- Increase overall IT efficiency with powerful granular access control capabilities
- Enable mobile worker productivity while protecting resources from threats.

SONICWALL™

How can I learn more?

Visit our web page, "Secure your mobile access to business data and applications".

Please send feedback on this ebook or other SonicWall ebooks or white papers to feedback@sonicwall.com.

SONICWALL™

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future. www.sonicwall.com

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

SonicWall
5455 Great America Parkway,
Santa Clara, CA 95054
www.sonicwall.com

Refer to our Web site for regional and international office information.

Ebook-SecureMobileAccess-US-VG-20449

SONICWALL™