

Access challenges for the IT department:

- New access model for Hybrid IT
- Multiple authentication mechanisms
- Additional Infrastructure components
- Complex user workflows
- Compliance & DLP

user access experience, and ensure that the users have the right access to be productive. In addition, IT needs the agility to enable businesses by rapidly onboarding and deploying new SaaS applications.

- **Multiple authentication mechanisms:** Increasing number of applications also means managing multiple user authentication methods across domains. For example, cloud-based applications may use SAML 2.0 or OpenID, while on-premises applications may use RADIUS or Kerberos. For IT, managing a combination of authentication mechanisms while ensuring proper security controls becomes an inefficient overhead. For users, this translates to multiple login URLs with separate credentials.
- **Additional infrastructure components:** User directories are considered as the “keys to the kingdom.” Organizations are reluctant to migrate their on-premises user directories to the cloud due to sensitive data moving out of the corporate network. In addition, organizations lose control over data that leaves their network, and that poses a significant security and compliance risk. Therefore, IT has to maintain multiple application-centric user directories every time they on-board a new SaaS application. New infrastructure components are required to ensure that these directories and access rules are in-sync at all times, increasing installation and maintenance costs, and complicating the IT architecture.
- **Complex user workflows:** Most organizations today embrace mobility and BYOD, and wish to empower employees with the freedom to choose the best mobile devices they need to do their work. In the traditional IT model, employees were given access to a set of on-premises applications from their workstations. Today, employees

also choose to work from their personal laptops, smartphones and tablets when away from their workstations. This makes it difficult for IT to configure workflows based on user identities and access policies based on devices. The IT department needs to be able to enforce access rules based on the state of the endpoint device, user location and application being accessed.

- **Compliance & DLP:** IT is a key stakeholder for audit and compliance. Proper controls must be set in place to track, monitor and report who is accessing what data. New regulations, such as the EU GDPR, require proof that organizations have taken proper precaution against breaches by demonstrating that effective security and data loss prevention (DLP) solutions are in place.

Organizations embark upon cloud transformation to grow their businesses. But moving to the cloud also means introducing new secure access into your network. Often times, the IT department runs into one or more of the above challenges resulting in bad security practices, shadow IT and loss of productivity.

Conclusion

To successfully move to the cloud, organizations need a centralized access security solution that supports new access models inherent with the hybrid IT approach and simplifies workflows for seamless access to all applications whether hosted in the cloud or in a local datacenter.

[Read our technical brief](#) to find out how SonicWall SMA enables organizations to securely move to the cloud while reducing complexities and IT overhead in managing the hybrid IT environment.

© 2017 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 Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

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