SONICWALL

EXECUTIVE BRIEF: SECURING ACCESS WHEN MIGRATING TO CLOUD

Abstract

Moving to the cloud and enabling mobility are top IT priorities for organizations of all sizes. Today, most businesses have adopted a hybrid IT model, which includes legacy on-premises applications in local data centers and popular Software-as-a-Service (SaaS) applications hosted in the cloud. Securing this hybrid IT environment, while providing a consistent experience with "anytime, any device, any application" access to authenticated users, remains a key challenge for the IT department.

Impact of hybrid IT in securing access

According to an IDC report, cloud IT infrastructure will grow at a five-year compound annual growth rate (CAGR) of 11.7%. That accounts to over 50% of the IT budget spend moving away from traditional data center to a cloud based IT infrastructure by 2021.

Organizations want to be able to plan and move to the cloud securely in a phased manner. Currently, all of the functionalities provided by on-premises solutions cannot be completely replicated by cloud-based applications. Therefore organizations are taking a phased step-by-step (rather than a big-bang) approach, migrating a set of applications and testing them. According to an IDG report, 70% of organizations have implemented at least one cloud application. This has created a Hybrid IT environment with new set of requirements for secure access to any application, on any device, at any time.

- **New access model for Hybrid IT:** Organizations are increasingly adopting SaaS applications, but they are not completely replacing the legacy applications. Today, organizations have deployed a blend of legacy, web and cloud/SaaS applications and services. This blend of application types requires a blended approach for secure access, irrespective of where the application is hosted. IT must provide a consistent

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.

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