thalesgroup.com

THALES

Secure Remote Access for Employees

Guidelines to Ensuring Secure Access and Data Protection for Remote Employees

White Paper

Contents

Introduction

The need to enable a mobile workforce and allow employees, contractor and consultants to work from home or outside the office has never been greater.

In today's business environment, constant access to information and services is essential for communication and getting business done whether you are in sales, finance, marketing or the legal profession. This is especially true when we face un-anticipated global incidents. Such unplanned events force us to rethink how we work. That's why it's important to ensure employees can not only collaborate, but that they can access corporate applications and information remotely in the same, secure way as if they were in the office.

Working remotely seems like the answer to many of the problems raised during crisis periods. Remote commuting must be a strategic decision followed by careful planning to eliminate all data security loopholes. Good planning can help businesses minimize the potential impact of such events, especially when it comes to protecting sensitive data.

Approaches to Remote Working

There are different approaches organizations can take to offering a secure remote office.

- Cloud services like Office 365 and SFDC for example, are delivered in SaaS model, and can be deployed rapidly, making it easier than ever for people to work remotely
- VPN access to the network, when most apps are still delivered on-premises
- Remote desktop or virtual environments

In reality, most organizations will have a mixture of on-premises and cloud services that employees will need to access.

Unfortunately, businesses still rely on simple username and passwords, making these phishing campaigns serious security issues. Even organizations that have migrated their email to cloud services, such as Microsoft O365, are still susceptible because, in the majority of cases, cloud-based email and other cloud services are only protected by simple passwords. Indeed, cyber hackers are earning $2 billion dollars from business email scamming, according to the FBI.

Given the threats to an organization when it exposes its assets to external access, there are some basic best practices that can make the path smoother for CISOs and IT security teams who need to maintain business continuity in a hurry by enabling employees to work securely from home.

Secure Remote Access: A Key Component of Business Mobility

Implementing a cloud-based access management and multi-factor authentication solution to secure access to both cloud services and on-premises apps can protect enterprise and cloud applications at the access point by keeping the bad guys out, while still offering your employees an easy way to log into the applications they need - from home, or any other location outside the office.

The most effective way to provide users with secure access to all the apps they need is to rely on a cloud-based IDaaS solution, such as SafeNet Trusted Access, instead of relying on a VPN, WAM, or on-premise access management and single sign on solutions. Cloud-based access management and authentication services offer tangible advantages over on-premises solutions such as a VPN, WAM, or on-premises SSO, including:

- They are easier, faster and simpler to deploy than on-premises solutions
- User access is achieved from the cloud to the cloud, meaning you are avoiding any on-premises bottlenecks
- They don't have the complexity of a VPN which typically requires client software to be installed and configured which is not easy to do in case of emergency
- The user experience is more intuitive and better than with a VPN, since authentication is part of the login workflow

Guidelines to assessing an IDaaS solution that meets your needs

When you need to get a new system up and running quickly in a crisis, selecting an IDaaS solution can be stressful. Below are a few basic considerations when assessing an access management and authentication service so your employees can work remotely and securely from home.

When you need to get a new system up and running quickly in a crisis, selecting an IDaaS solution can be stressful.

Efficiency and Deployment

A cloud-based solution will allow you to get up and running quickly without the need for heavy on premises installations. When assessing your solution, it is advisable to check how many on-premises components you will need to install, and how many servers you will need, and how the additional servers you'll need in order to maintain redundancy. In this regard, a solution's support for cloud-based RADIUS, and a cloud-based IDP are significant factors in your ability to get up and running quickly. Likewise, solutions that require the installation of on-premises gateways will require additional implementation lead time, servers and maintenance.

Automation

Especially in a crisis, you need to enroll users quickly, with minimum friction and help desk calls. By subscribing to a service that provides automated token enrollment workflows and one-click token installment for end users, your organization will be able to self-enroll quickly and reduce IT burdens. Instead, businesses should avoid a multi-step, manual token enrollment which is error prone and resource consuming.

Authentication and Token Flexibility

Software and token-less authentication methods are ideal for remote employees. And when combined with easy, automated token enrollment, will ensure your users have a seamless log-in experience. To support all users' needs, look for a solution that can offer a range of authentication methods that can accommodate varying needs and security levels. These include: Push OTP app (which can be installed on a mobile device or desktop); SMS or email code sent to a mobile device or email address; pattern-based authentication, a token-less method that does not require users to install any software on an end device. Look for a solution that can centrally manage and provision a variety of software and token-less authentication methods to users remotely. Avoid any solution that offers only one or two methods of user authentication.

Ability to Access all Apps and Cloud Services

Does the remote cloud access management service support the applications your enterprise regularly uses? While working from home, you might need to access Salesforce, Dropbox, Confluence or other services. Consider implementing an access management service that can manage several apps within the same platform and secure your VPN with remote access. Look for a solution that can secure access to apps via SAML, RADIUS and non-standards-based apps and avoid any solution that can only secure cloud and web-based apps. This way you will be able to protect all apps with a single solution and offer convenience with single-sign-on.

Smart SSO for Optimal Security and Convenience

To offer the most frictionless experience possible without sacrificing security, organizations can leverage cloud SSO combined with contextual information and step-up authentication. This allows users to access all their cloud and web applications with a single identity, while IT only needs to enforce stronger access security in high-risk situations. Therefore, look for a solution that offers step up and conditional access based on access policies, while avoiding any solution that offers broad SSO allowing access to all apps with the same credential. With smart SSO, end users can maintain business productivity and reduce the hassle of having to re-authenticate to multiple apps.

Provide Flexible Policies

While you will want your employees to be able to work at home, your access management service might not consider their remote IP addresses or geographical regions as a trusted network. By subscribing to a cloud access management service with flexible policies, you can whitelist or blacklist groups of users according to IPs and receive reports regarding login activities. Such a service will be able to step up authentication for untrusted networks and ease the level of authentication method required for the whitelisted networks. Similarly, you can establish policies that will vary authentication rules according to application.

Transparent Licensing Model

Many services on the market today have very complicated pricing models. Some vendors' licensing packages are bundled with numerous services that you may not need--meaning you will be paying a premium for capabilities that won't be used. Other vendors use a 'pay per feature' model that turn out to be very costly. Both approaches make it difficult to calculate how much you will be paying at the end of the day, and what features you will get. When under pressure to purchase and implement a solution quickly, you don't have the time for in-depth cost projections. Therefore, you should look for a dedicated access management and authentication solution with a transparent pricing model and the features you need.

Secure your Corporate Data

Securing your employees' remote access to corporate resources and apps is not enough. You will need to plan how to protect your most precious asset, your data, while it is either in transit or at rest. Data breaches are usually privacy breaches, since most of this data is about employees, customers, financial data or even PII. Privacy breaches can result in severe penalties under data protection regulations such as GDPR or CCPA.

Even if a data breach is not a privacy violation, it may entail industrial espionage by state-sponsored actors who may take advantage of the crisis to steal precious sensitive or secret data. In either case, any data breach will harm your business' reputation significantly, which also means loss of revenue when customer trust is damaged.

Below are a few tips to consider for protecting your corporate data while it is being accessed remotely by your employees.

Discover and Classify your Data
Before implementing any cybersecurity strategy, businesses must first conduct a data sweep. This helps them understand what data they have collected or produced and where the most sensitive and valuable parts are. If businesses don't know what data they possess and produce, they can't even begin to start protecting it.

Understand the Risks related to Data
Once a business understands the data it has and produces, it then must understand the risks associated with it. While there is not a silver bullet to defend against a cyber-attack, having a risk-based approach is essential to employ the appropriate best practices to mitigate these breaches. It's about focusing on the need to protect the data at its source, rather than preventing a breach entirely.

Encrypt all Sensitive Data
While it is crucial that businesses restrict who can access sensitive data, it is encryption that ensures this data cannot be used in the event it is accessed by unauthorised personnel. Therefore, businesses must understand where their most valuable data is stored before this step can occur. Regardless of where it is stored – on their own servers, in a public cloud, or a hybrid environment – encryption must always be used to protect data.

Securely Store your Keys
When data is encrypted, an encryption key is created. These keys are necessary to unlock and access encrypted data. Consequently, businesses must ensure that these keys are securely stored. Encryption is only as good as the key management strategy employed, and companies must keep them in secure locations, such as external hardware away from the data itself, to prevent them being hacked.

Introduce Two-Factor Authentication
Next, businesses should adopt strong two-factor authentication, to help ensure only authorised employees have access to the data they need to use. Two-factor authentication involves an individual having something they possess – like a message on their smartphone – and something they know, rather than simply relying just on one protection such as a password, which can be easily hacked.

Back up your Business Data
However, these previous steps only protect business' data from attempts to steal it. When it comes to disaster recovery, such as earthquakes or flooding, it may be required to transfer operations to alternate locations. The best way to mitigate this potential situation is to back up all critical business data. Back up is also important as a countermeasure to attacks such as ransomware. Having a good, working back up of your company's critical data can ensure a return to normal operations quickly, whether in a disaster situation or in a cyber incident. The backed-up data should be stored either in the cloud or offsite and kept secure with two factor authentication and encryption.

Ask for Help
Businesses shouldn't be afraid to ask for assistance if they feel their company doesn't have the expertise or the resources to manage their security needs. Partnering with a third party, like a cloud service provider or a specialized cybersecurity company, can take that strain off and allow them to focus on running the business.

Last but not least: Leadership Buy-in is Crucial

To ensure the effectiveness of the above steps, IT security professionals should seek leadership buy-in. Only if the C-Suite understands the importance and fully supports the implementation of these security precautionary measures will they be successful. Otherwise, they will be just another plan hidden in dusted drawer. Business executives need to realize that business agility is a corporate responsibility and that any security risks are enterprise risks.

The suggestions for access management and data protection presented in this article should be considered carefully by all businesses wishing to maintain secure remote access and mobility. Adapting to a secure digital workplace is a core component of offering ease of use for employees when they access apps and services from home.

Learn more about how Thales can help your organization prepare to respond in a crisis by contacting our specialists.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <