eBook

Connecting Anyone, Anywhere, Securely

The IT Perspective

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Remote Work Isn't a Trend, It's the New Normal.

The need to enable a mobile workforce and allow employees, contractors, and consultants to work from home or outside the office has never been greater. Organizations have rapidly shifted their businesses to operate remotely, and the benefits of doing so are significant.

However, remote work also comes with risks. The reality of working from anywhere means IT has to facilitate secure access for employees from many locations, from many devices for many applications – which complicates the process of ensuring employees are who they say they are.

In today's business environment, constant access to information and services is essential for communication and business, whether in sales, finance, marketing, or the legal profession. This is especially true when we face unanticipated global incidents. Such unplanned events force us to rethink how we work. That's why it's important to ensure employees can collaborate and access corporate applications and information remotely just as securely as they are in the office.

Working remote is 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. In the work-from-anywhere era, it is critical that organizations develop an identity and access management (IAM) strategy that authenticates and authorizes every employee so that they gain access to the business resources they need to stay productive.

The Challenges of Securing a **Remote Workforce**

When we talk about identity and access, it's becoming harder and harder to distinguish the "good guys" from the "bad guys." Organizations must adapt to the evolving risk and threat environment to protect their valuable and sensitive assets. Access security and authentication play an important role.

If there is one lesson we all learned from the pandemic period, it is the ability to adapt to a changing environment. Adaptability is what separates businesses that thrive from those that are still struggling to survive while working remotely. According to a Gartner report, by 2025, the change in the nature of work will include up to 75% of organizations adopting hybrid work strategies. Now, think about that, combined with the fact that up to 80% of the respondents in this survey said they are either very concerned or somewhat concerned about the security risks of working remotely.

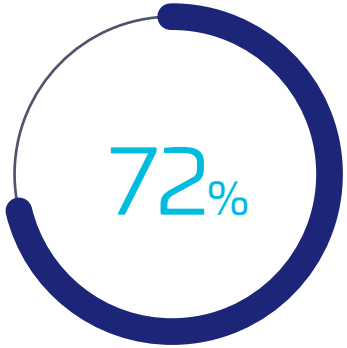
By 2025, massive generational shifts will force **75% of organizations** to adapt their hybrid work strategies to include demands for radical flexibility.

Source: Gartner - Predicts 2022: Digital Workplace Is Foundational for Employee Experience

Key Challenges in Remote Work Security

- Lack of strong cybersecurity tools for remote employees.
- Vulnerability of personal or public Wi-Fi networks without VPN protection.
- Difficulty in maintaining a strong security mindset at home.
- Personal Devices More Prone to Malware: Compared to corporate devices, personal devices are twice as likely to get infected with malware.

How concerned are you about the security risks/threats of employees working remotely?



In 2023, 72 percent of global respondents indicated being very concerned or somewhat concerned about the online security risks of employees working remotely.

Source: Statista https://www.statista.com/statistics/1384003/cybersecurity-concern-level-in-remote-work/?trk=article-ssr-frontend-pulse_little-text-block

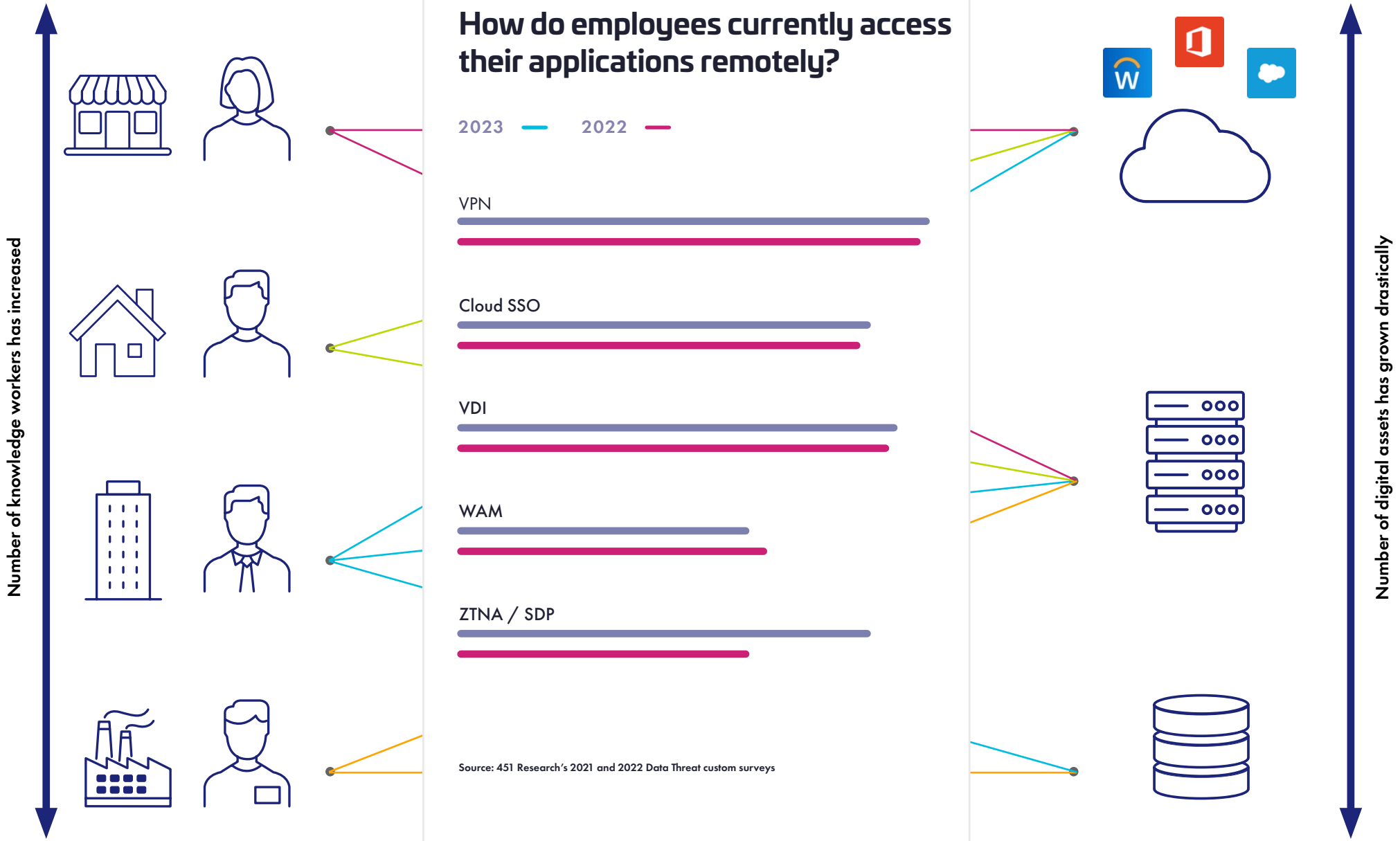
From the **IT Perspective**

Simple, secure authentication continues to be top-of-mind for many organizations and their IT teams. The need to balance security and the ability for users to access resources quickly is a top of mind priority. Authentication processes present a clear breach target; credential misuse or authentication weakness is more often than not a root cause.

For IT teams, the loss of control is a big challenge. Managing where and how people access business resources and at what level adds complexity to the IT environment, and these complex networks are getting harder to secure. Allowing remote access to the network widens the surface of attack for cyber criminals. Attackers don't need to break in, they flash their credentials and walk through the door, which complicates remote access for everyone.

These issues expose significant gaps in authentication protocols, and shine light on the need for methods that can stand up to the evolving threat landscape from any point of entry.

As well as maximizing security, IT teams must minimize the friction and complications for employees. Organizations face challenges from the variety of authentication systems used on a daily basis — industry estimates can be up to four on average. This means multiple, varying sign-on requirements that employees must remember and use, adding friction and frustration in their day-to-day work.


How do employees currently access their applications remotely?
2023
2022
VPN
Cloud SSO
VDI
WAM
ZTNA / SDP
Source: 451 Research's 2021 and 2022 Data Threat custom surveys
Number of knowledge workers has increased
Number of digital assets has grown drastically

Remote Work - the Employee Perspective

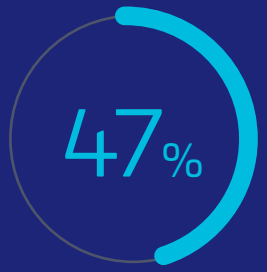
Today's workforce wants flexibility and connectivity to their digital resources from anywhere with multiple devices. Therefore, IT teams must provide a secure way to delegate access as well as minimize complications for employees. Usability is key so choosing solutions that facilitate collaboration and quick access to documents should be a priority.

It's true that today's workforce doesn't just sit behind a desk. Organizations must consider how their employee's roles, functions and the environment in which they operate. And more so, the data and resources they need to access.

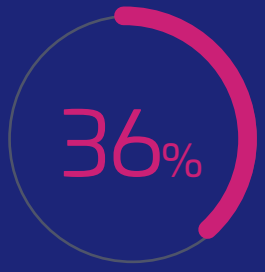
Employees must have the freedom and flexibility to work from anywhere. This can also have a high impact on employee retention. Plainly said, employees stick with employers when they have remote work options.

Employers also benefit as they can recruit and hire from anywhere, retain staff, and increase employee happiness, all while reducing costs.

The Remote Workplace: **Freedom to Come and Go**



of employees surveyed say working from home improves their productivity



say it's too arduous to access their work profile to do so

believe that their employer values the importance of a good digital experience for employees.

Employees value a new approach that blends in-office time with remote opportunities.

Not All Users Are Created Equal

One of the challenges we observe very often with Identity and Access Management is that it means different things to different people – remote work creates security challenges as dispersed employees increase the threat landscape.

Not all users are equal, and they shouldn't be treated as such since a wide range of factors must be considered: location, device, where's the data, and everything in between.

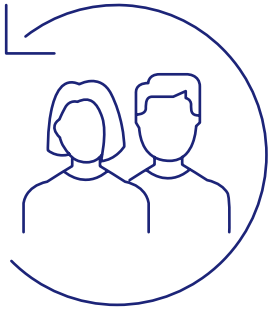
Remote work norms create security challenges

Dispersed employees increase the threat landscape

Identities of remote users are a lucrative target

Every user is a potential target

MFA is not widely adopted yet, as only 34% of internal, non-IT employees are using MFA according to recent surveys



Not all users are equal

Organizations cannot rely on "one-size-fits-all" approach

There's **No One-Size-Fits-All** Soluton for all Authentication Journeys

An enterprise employs executives, IT admins, contractors, factory floor workers, office workers, or even third-party suppliers. All these different users have different requirements. To deploy an authentication solution that really works for all your employees and helps mitigate the increasing risk of cyber-attacks, you need to identify all these factors shaping a user's authentication journey.

These factors include:

1. **The user persona – role and responsibilities of the user**
2. **The user location – on-site, remote, or roaming**
3. **The user devices – corporate laptop, shared device, mobile, BYOD**
4. **The assets the user is required to access and how critical these are**
5. **The compliance environment or any other constraints like lack of connectivity or phone-not-allowed policies**

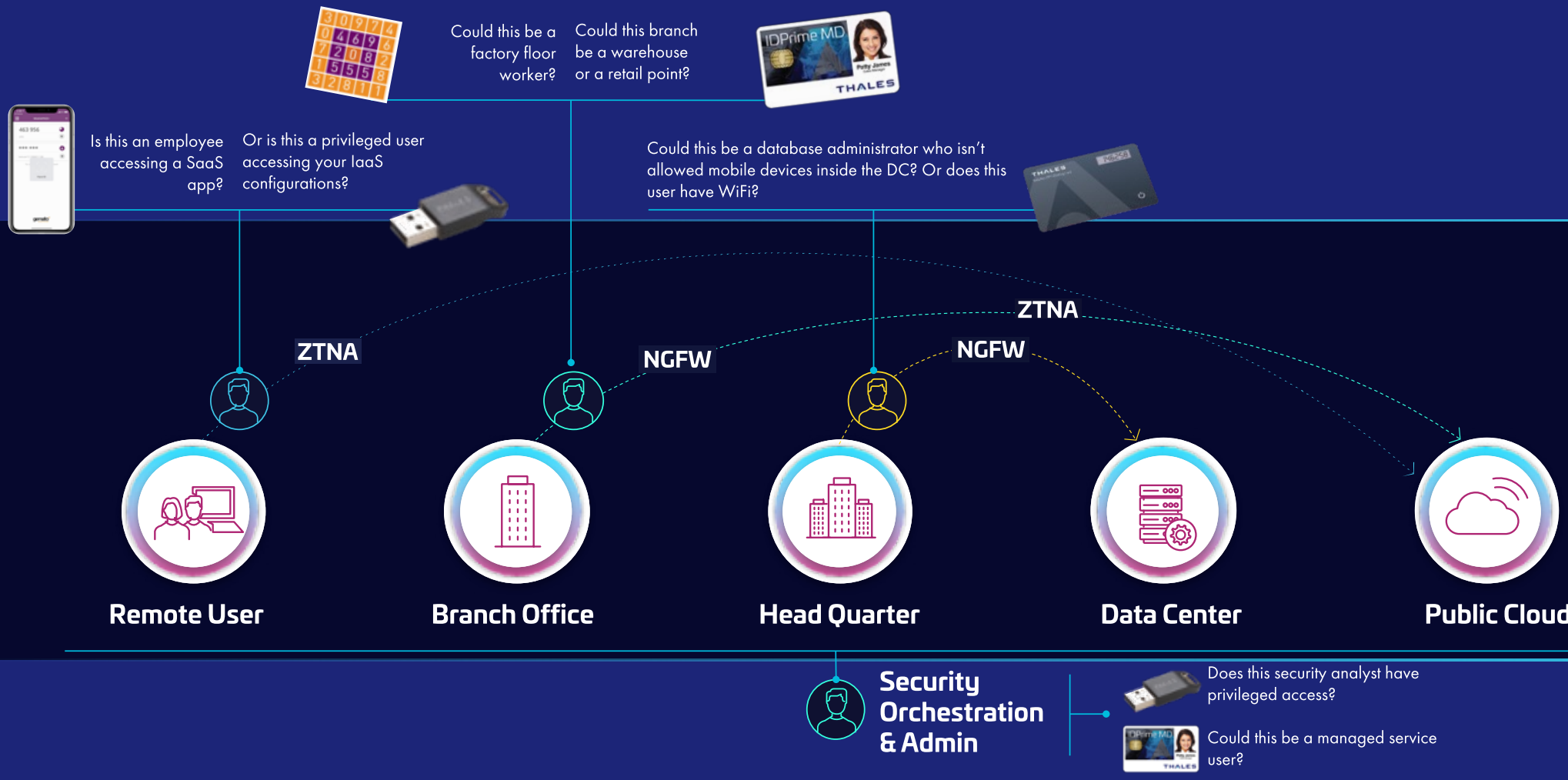
What Data or Resource are They Accessing?

Productivity Application

Database Server

Factory Floor Terminal

Authentication Journeys: **Right Sizing Least Privileges**



Mapping Users and Their Needs to a **Secure Authentication**

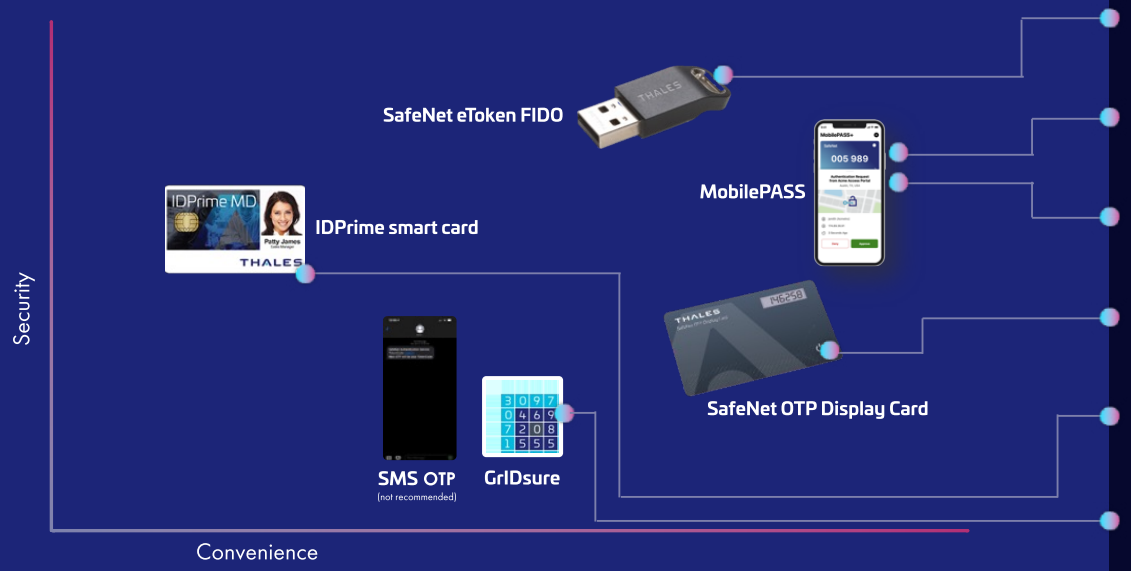
Understanding the balance between security and convenience is a key component to adopting the right MFA for each use case.

Below are examples of different roles within a typical organization. On the far left is the axis between security and convenience. Of course, at the high end of security are users who must authenticate every time, no matter the convenience factor. Then, we move down through the user groups and show the different authentication methods that will allow them access while also considering the security policy.

Look at your users, their needs, and how you can weave that into an effective authentication journey.

Then, protect those users with access policies and secure authentication across your environment. And control the risk with real-time policy enforcement.

Right-Sizing Privileges and MFA for Zero Trust



Securing the Remote Workplace

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

Cloud services like Office 365 and SFDC, for example, are delivered in SaaS model

Remote desktop or virtual environments

VPN access to the network, when most apps are still delivered on-premises

Considerations for **Securing the Remote Workplace**

Efficiency and Deployment

A cloud-based solution will allow you to get up and running quickly without needing heavy on-premises installations. When assessing your solution, it is advisable to check how many on-premises components you will need to install, how many servers you will need, and how many additional servers you'll need in order to maintain redundancy.

Automation

Enroll users quickly, with minimum friction, and help desk calls.

Authentication and Token Flexibility

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; and pattern-based authentication. Look for a solution that can centrally manage and provision a variety of software methods to users remotely.

Go Passwordless

The Benefits of Passwordless Security

It's true that many businesses still rely on simple usernames and passwords, making phishing campaigns serious security issues. Even organizations that have migrated their email to cloud services, such as Microsoft O365, are still susceptible because, in most 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.

Passwordless authentication and passkeys bring a measurable positive impact to an organization's security, IT and business operations. A recent survey revealed that 65% of people reuse passwords across accounts, and nearly half hadn't changed their passwords in over a year, even after a known breach. Growing awareness of this fundamental security flaw has made passwordless authentication, including passkeys, one of the biggest trends in cybersecurity.

Fully passwordless authentication — where no password or similar secret is shared between the person and service — is far more secure than password-based authentication. Credentials never leave the user's device and are not stored on a server, so they are not vulnerable to phishing, password theft or replay attacks.

1. **Eliminate Phishing, Password Reuse and Credential Stuffing**
2. **Reduce Ransomware and Data Breach Risk**
3. **Eliminate Password Reset Costs**
4. **Improve the User Experience and Increase Workforce Productivity**
5. **Meet MFA Compliance**

Passwordless Authentication **Enables Zero Trust**

Zero Trust security is widely accepted as being a security model based on the principle of 'trust no one, verify everywhere' – i.e., no entity can be trusted. When applications are being delivered from multiple clouds and delivery points – authentication plays a key role because the access point becomes the front line of security. The access point is the entryway for a user to access enterprise information and applications. The Zero Trust security framework defines how users inside and outside an organization must be authenticated. It effectively abolishes perimeter-based protection schemes by assuming that any user, device, or service could be compromised.

A pillar of any Zero Trust initiative is phishing-resistant MFA as the gatekeeper, and the strength of that gatekeeper affects the security of the entire Zero Trust architecture. Unfortunately, organizations often find gaps in employee MFA adoption, especially among those who work remotely or travel often.

To enact Zero Trust principles without a negative impact on the user experience, organizations can consider FIDO Certified passwordless authentication, as it builds trust in the identity. This ensures that authentication processes are in alignment with Zero Trust.

Final Thoughts:
IAM is Critical to Secure a Remote Workforce

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

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.

In order to secure your network and ensure ease of use for remote workers, it's important to leverage SSO, SSO, MFA, and Access Management.

As the future approaches, IAM will continue to increase in importance and necessity. A network is easier to secure when you know who's connected. IT teams can maintain control of users and their access levels by choosing IAM solutions that consolidate identities and logins.

Remote working is the new normal, and businesses need a long-term, robust IAM strategy to secure their remote workforce. The associated risks and challenges mean that a remote work IAM strategy is a critical priority. With the right IAM strategy in place, you can fully manage employee access, add layers of silent security, and make it easy for workers to collaborate with one another from anywhere.

The benefits of IAM

- Access controls are fully managed
- Easy access from anywhere
- Reduce IT costs
- Simplify auditing and reporting

Every Digital Interaction **Begins with Identity**

THALES

Delivering One Platform for Every Identity

Discover IAM

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

© Thales - May 2024 • BBv3