cpl.thalesgroup.com

THALES
Building a future we can all trust

Supporting Multiple User Authentication Journeys Enables Modern Access Security

White Paper

Contents

Executive Summary

Organizations are compelled to adapt to the evolving risk and threat environment to protect their valuable and sensitive assets. Access security and authentication plays an important role. However, organizations are facing many challenges that prevent them from mitigating expanding threats against identity theft. This paper provides an overview of the emerging authentication landscape and the challenges towards a modern, dynamic access security. It also examines how supporting a range of user authentication journeys can help organizations balance strong security with a smooth user experience.

Why is there a need for a different approach to user authentication?

Remote work norms create security challenges

If there is one lesson learnt from the turbulent pandemic period that businesses should cherish for the years to come 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 whilst working remotely. Surveys indicate that two-thirds of global enterprises will continue to support work from home arrangements for the foreseeable future. In addition, according to a recent Gartner report, by the end of 2024, the change in the nature of work will increase the total available remote worker market to 60% of all employees.

> **"By the end of 2024, the change in the nature of work will increase the total available remote worker market to 60% of all employees."**
>
> **– Gartner, August, 2021**

It is evident that hybrid working environments will continue to create further security challenges. Dispersed employees are increasing the threat landscape and the inherent business risk. Part of the threat is that in today's attack landscape the identities of remote users have become a lucrative target. Cyber criminals are looking for the weakest link to get into a corporate network. Once inside they will elevate privileges of the compromised identity to take control of other accounts and finally either exfiltrate sensitive data or disrupt operations.

Every user is a potential target

As organizations move to the cloud, entire employee groups that previously didn't require remote access, now must go beyond the traditional perimeter to access sensitive info. When using cloud apps, everyone is literally an outsider, even when a user is accessing the application from within the business network.

> **" In the current business and risk landscape, every employee is a potential target."**

In the current business and risk landscape, every employee is a potential target. However, organizations seem to have not realized the potential threat. The Thales Access Management Index (AMI) 2021 report indicates that when it comes to multi-factor authentication (MFA) adoption, only 34% of internal, non-IT employees are affording enhanced authentication control through MFA. In addition, 48% of the global businesses are deploying MFA to protect only the privileged employees and IT administrators.

It's clear that organizations need to shift their security investments to improve their security posture with more modern authentication technologies and approaches for all users and applications.

Not all users are equal

To reduce the overall risk, organizations are investing in access security. However, relying on a 'one size fits all' approach is not adequate to protect access to an enterprise's most valuable assets. Data, services, and applications are now located and delivered from multiple cloud platforms outside the corporate boundaries. Without a defined perimeter to defend, it is time for businesses to redefine their access security strategy.

As enterprises adopt cloud-delivered services, more diverse types of users have emerged. In the past, employees were grouped per role and responsibility. You had the executives, HR staff, budgeting officers, IT staff, and office workers. But today, this model seems outdated.

In addition to their responsibilities, employees need to be classified using a wide range of factors to include their location, their device, the location of data they request access, etc. **This diversity of user profiles demands better and more adaptive authentication policies and controls, which will span across all enterprise users.**

Access can no longer be granted based on a static authentication decision which is not affected by the environment where the user is located. In an environment where users are changing devices and networks, accessing data from either business premises or their home, the access decision cannot be static.

Given these dynamics, organizations and security teams are faced with a complex authentication problem to require a dynamic, yet balanced approach. What you need is a solution that can integrate into your IT environment - cloud, on-premises, even existing IAM solutions - easily and flexibly without harming user experience.

What is the emerging authentication landscape?

Although enterprises were always supporting some sort of remote working for various social or health reasons, the current business landscape is much more complex, creating new challenges for the security teams in their effort to protect data against their adversaries:

Sheer volume and diverse types of remote employees

In today's new work normal, the majority of employees choose to work remotely even partly. Hybrid working models are the norm, creating challenges for effectively validating employees trying to access remotely corporate resources. During the pandemic, many organizations faced difficulties scaling their existing authentication and access solutions to accommodate all their remote employees.

In addition to the growing number of employees, we are witnessing an increasingly diverse type of employee. There are users accessing on-premises data from their home using their private laptop. Others may access data through a cloud app using the corporate network and laptop while their colleagues could be logging onto services via an insecure Wi-Fi network in an airport through their mobile phone. How can you accommodate all these different authentication requests using a monolithic approach to access security?

The **2021 Thales Data Threat Report** indicates that only 20% of the respondents were very prepared to handle the security risks and the diverse authentication needs of their employees caused by the pandemic.

The 2021 Thales Data Threat Report indicates that only 20% of the respondents were very prepared to handle the security risks and the diverse authentication needs of their employees caused by the pandemic. Not surprisingly, 82% of global businesses were very concerned about the access security risks of employees working remotely. The lesson learnt is simple - those businesses that are better positioned to address these access challenges can also make a smoother adjustment to the new requirements.

Employee and user expectations

Technology has enabled employees to opt for a diverse way of working remotely. Employees have realized that flexibility in work provides them with many options to accommodate their personal or family needs. Some are choosing the coziness of their home, while others are becoming digital nomads and work from the breathtaking beaches in the Greek islands. Some other employees decided to move from the city to the country to benefit from more affordable housing and open spaces for their kids. Finally, those employees who haven't left their homes may still select to work from the coffee shop around the corner, the local park, or the library instead of going into an office. Security teams need to secure this diverse way of connecting to corporate resources, and they need to do so in a frictionless manner.

Attackers are targeting credentials

According to Verizon's 2021 Data Breach Investigations Report, 90% of all data breaches start with compromised credentials. The Threat Horizon report from Google's Cybersecurity Action Team indicates that 48% of compromised instances were attributed to actors gaining access to public cloud platforms which had either no password or a weak password for user accounts or API connections. Cybercriminals have become very sophisticated in compromising and using these stolen credentials to launch lateral attacks traversing the on-premises and cloud environments. Compromised credentials offer criminals the ability to become undetected and elevate privileges to steal sensitive data. It is clear that protecting only sensitive users and apps is not enough to safeguard organizations – especially when everyone is now remote.

2021 VERIZON REPORT

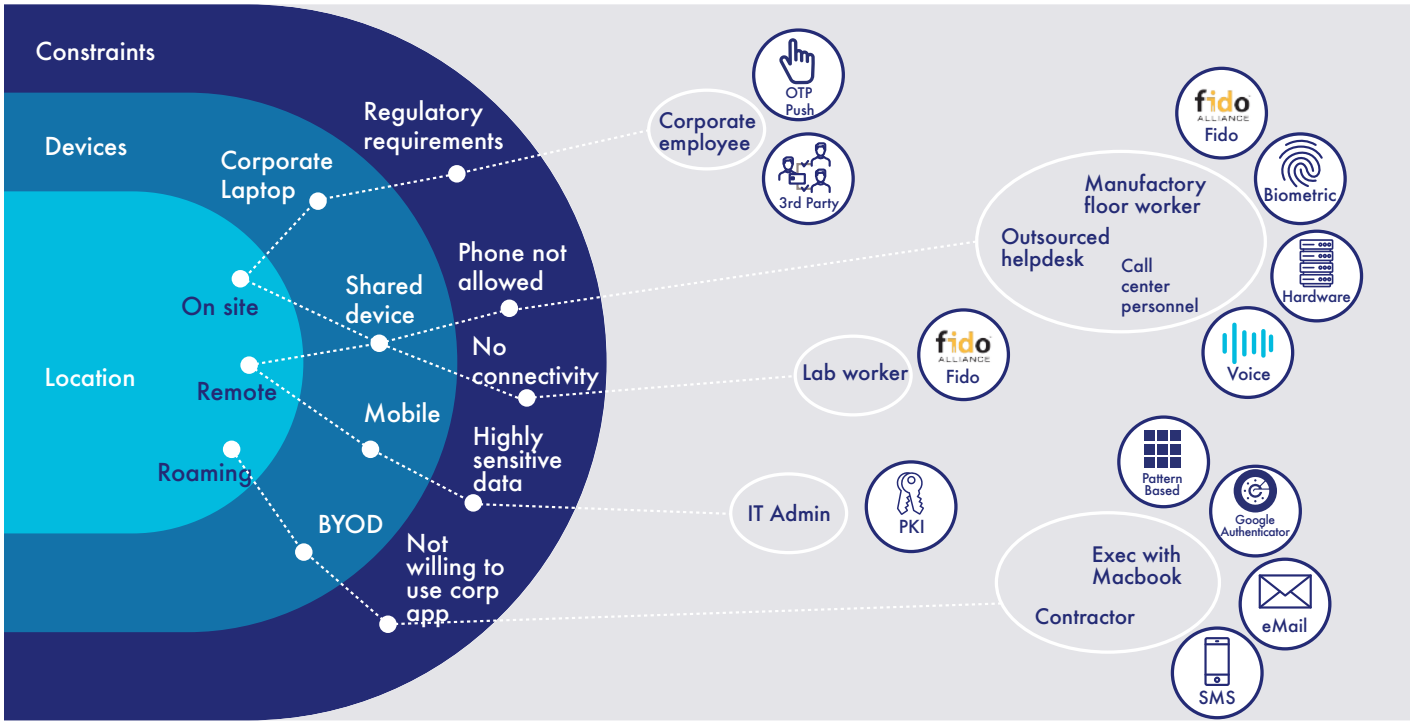
90% of all data breaches start with compromised credentials.

User authentication journeys explained

Security teams need to realize that not all users are equal, and they shouldn't be treated as such. An enterprise employs executives, IT admins, contractors, factory floor workers, office workers, or even third-party suppliers. All these different users have different requirements. Deploying a monolithic authentication solution will leave both security gaps and users feeling unhappy and counter-productive.

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:

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



To better understand the user authentication journey concept, let us examine two real world use cases – a hospital doctor and a factory worker.

Use case: Julia, Hospital Doctor

Julia is a surgery doctor living in Vienna. She works at the city's Central Hospital and also sees patients at the municipal health clinic. She needs to access her patients' medical records to advise on treatments.

Seeing patients at the hospital

Using a shared desktop provided by the hospital IT department, Julia needs to access patient records to determine the best treatment. In this situation, Julia can use a PKI-based smart card to authenticate herself to the hospital medical data system. The smart card supports high assurance multi-factor authentication (MFA) which is required to comply with healthcare privacy and security regulations.

Seeing patients at the municipal health clinic

Julia also works at the municipal health clinic seeing her patients. She needs to access the patients' data using her private laptop to consult on the individual's medical history. Security and privacy regulations for medical data require that Julia uses multi-factor authentication. However, since Julia's personal laptop is not equipped with a smart card reader, she is not able to use PKI-based authentication. In this case she could use a FIDO device to meet the required authentication assurance level.

Working her shift at the hospital

When Julia is working on the hospital wards she needs to access the patients' medical records using the hospital's shared tablet. Again, a FIDO device meets the requirement for strong MFA.

In the case of Julia, the fact that she was able to use a smart card that supports both FIDO authentication and PKI was instrumental in her ability to meet stringent security requirements while maintaining a convenient login experience with a single authentication device.

Use case: Mike, Factory Worker

Mike works in a car manufacturing factory in Detroit overseeing the maintenance of business critical machinery. Mike has various responsibilities that require different authentication journeys - fault finding, system maintenance, team supervisor organizing shifts. During his shifts Mike needs to log into several terminals to perform his duties.

Report a fault on a machine on the factory floor

Mike needs to log a fault on one of the machines on the factory floor using a shared terminal. Pattern-based authentication is the only viable option since the factory floor is a hands-free environment. Pattern-based authentication allows users to derive a unique one-time code, without the needs to install software, which removes the necessity for a traditional password or static PIN code.

Perform system maintenance on an assembly robot on the factory floor

Mike is tasked to review log data of an assembly robot through a special user interface. In this case he would need to use a certificate-based authentication or FIDO authentication to meet the regulatory requirement for strong MFA when accessing critical operational systems.

Organize monthly shifts from the factory café

In another situation, Mike is at the factory cafeteria drinking coffee with his colleagues and needs to review the shift rotation patterns. Since Mike is accessing a non-classified shared terminal which is not connected to critical business systems, he can use passwordless, biometric-based authentication.

How modern authentication can support user authentication journeys

Each user travels its own unique authentication journey, every day, several times per day. How can you make these journeys smooth and safe? Adopting a 'Discover, Protect, Control' approach to access security is a start.

Step 1: Discover the various user authentication journeys

The first step is to identify the specific authentication needs of your users and uncover where there are authentication gaps. To do that, you need to:

- Identify the users in your enterprise – executives, IT administrators, office workers, etc. Take into account that user constituencies in your organizations will likely grow, as you adopt more cloud services.
- Identify the access context and map all roles, responsibilities, and system access requirements. For example, this includes, user location, app delivery location, constraints such as access to cellular networks, constraints on use of mobile phones
- Identify the resources – systems, data, applications - the users need to access and determine their criticality.
- Doing the above exercise will help you understand your specific authentication needs and uncover gaps that need to be addressed.

Step 2: Protect

Once you have completed the Discovery phase, you will be in a better position to support all identified user authentication journeys, balancing security and convenience. To do that, you need to:

- Transform your authentication solution into a modern one – dynamic and flexible – based on passwordless authentication, policy based contextual access, and continuous risk assessment.
- Offer your users a choice of multiple authentication methods to accommodate all their needs.
- Optimize security and convenience using step up, conditional access.
- Allow your users to enroll at their own convenience, manage your solution remotely, and scale your solution easily.

Step 3: Control

As organizations expand in the cloud, the need for scalable access security and authentication increases. The ability to flexibly add new services into your access security regime, gain visibility into access events and fine-tune policies as your environment grows, is fundamental to delivering efficient business outcomes.

Conclusion

Businesses need to invest in a modern and flexible authentication and access control solution to support varying user authentication needs and close potential security gaps. In increasingly complex hybrid IT environments, taking a 'once size fits all' approach to authentication can create vulnerabilities by creating easy targets for cyber-criminals. Adopting a "Discover, Protect, Control" approach to access security will enable organizations to identify the user authentication journeys each employee takes, address their specific authentication needs, and continuously enforce a strong access control regime as they scale in the cloud.

To dive deeper into the technical aspects of authentication go to https://cpl.thalesgroup.com/access-management

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.

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 <