

Partner Playbook

Identity and Access Management Portfolio

A woman with long dark hair is looking down at a tablet computer. The image is overlaid with a semi-transparent blue geometric shape that covers the right side and bottom. The text is white and positioned on the left side of the image.

Thales Cloud Protection and Licensing Story

Today's enterprises depend on the cloud, data and software to keep pace with the cost of doing business in a world that is rapidly digitally transforming. However, they are concerned about business critical and sensitive data being stolen by adversaries such as competitors or cyber criminals. In spite of all their investments in perimeter and endpoint security data breaches continue to occur on a weekly basis. When all else fails, data security has become the last line of defense.

That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive data at rest in on-premises data centers and in public/private clouds, and data-in-motion across wide-area networks. Our solutions enable organizations to migrate to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

We are the worldwide leader in data protection, providing everything an organization needs to protect and manage its data, identities and intellectual property with comprehensive data discovery and classification, data encryption, tokenization, advanced key management, authentication and access management. Whether it's securing the cloud, digital payments, blockchain or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation.

Contents

04	The people we all rely on to make the world go round – they rely on Thales
06	Providing a safer, more secure world powered by the cloud, data and software
07	Thales Identity and Access Management Portfolio
08	Standards-based Security
08	Access Management
09	Introduction to Access Management
10	Cloud Access Management
11	SafeNet Trusted Access (STA)
12	Thales PKI Authentication Portfolio
13	About Thales

The people we all rely on to make the world go round – they rely on Thales



10

largest banks in the world



5

largest software companies in the world



10

largest retailers in the world



10

largest healthcare companies in the world



5

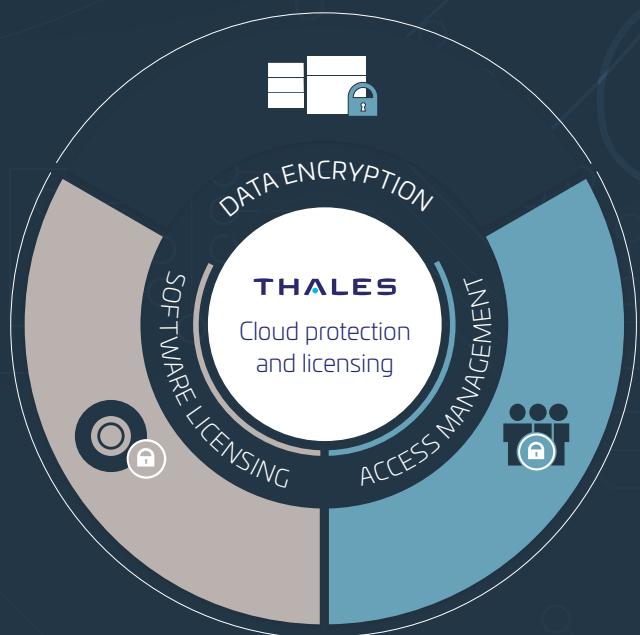
largest cloud service providers in the world



10

of the largest manufacturers in the world

Today's enterprises depend on the cloud, data and software in order to be confident in decisive moments.



What will be your decisive moment to protect your data and software?

Digital transformation is reshaping industries as more and more organizations look to build their businesses using the cloud, data and software. The success of these transformations will ultimately depend on whether these digital services, identities and transactions can be secured and trusted.

At Thales, we are at the heart of making this new digital world possible. As the worldwide leader in digital security, we protect more data, identities, software and transactions than any other company and enable tens of thousands of businesses and organizations to deliver trusted digital services to billions of individuals around the world.



Cloud Security

Confidence in data security is essential, whether it's accessing cloud services or storing data across multiple cloud environments. You can rely on Thales to deliver simple, secure access and encryption solutions to protect sensitive data in any cloud. **How will you secure your data in the cloud?**



Data Encryption & Key Management

Securing sensitive data is a priority for every organization. Whether your data is at rest, in motion, or in use, you can rely on Thales to enable the most effective encryption strategies for your enterprise environments. **Does your enterprise have an encryption strategy?**



Access Management & Authentication

Moving applications to the cloud brings not only increased risks of data breaches but also the challenges of simplifying access for users and enabling compliance. Regardless of the size of your business, you can rely on Thales to deliver secure, trusted access to all cloud services. **Do you have secure access to all of your cloud services?**



Compliance & Data Privacy

Data security regulations present an increasingly complex challenge for global organizations. Wherever you operate and whatever the regulation, you can rely on Thales to help you achieve and maintain compliance, improving your security and managing your risk. **Is your business ready for today's data compliance challenge?**



Software Licensing & Protection

Software is crucial for business performance and new revenue opportunities. As your company shifts from hardware to a software-based business, you can rely on Thales to generate new revenue streams, improve operational efficiency and gain valuable insights from your software. **Can you deliver software the way your customers want to consume it?**

Providing a safer, more secure world powered by the cloud, data and software

Data protection against increasing threats

According to the Thales Data Threat Report, 60 percent of organizations have been breached sometime in their history. This is increasingly serious when nearly all organizations will use sensitive data in digitally transformative technologies. However, less than 30% of companies have deployed encryption to protect data in digital transformation environments. Thales helps businesses and organizations defend their data in a digital world where there is no defined perimeter with advanced encryption, key management and tokenization solutions.

Trusted access in a zero trust world

Traditional security models operate on the assumption that everything inside corporate networks can be trusted. However, given the increasing adoption of cloud services and sophistication of cyberattacks, new security approaches are needed to ensure the individuals accessing cloud services and corporate resources can be trusted, verified and deliver on compliance mandates. Our access management solutions help organizations provide secure, trusted access to cloud services and applications with user friendly single sign-on and robust multi-factor authentication.

Security for a cloud-first world

The cloud gives organizations the agility and efficiency to instantly introduce new services, expand operations, and enter new markets. But the lack of physical control of infrastructure brings a whole host of data security issues, including privileged user abuse, data leakage, regulatory requirements, and many more. Our solutions help organizations secure their cloud transformation, reduce breach exposure and achieve compliance with encryption and key management solutions that keep you in control of your data in any cloud while also providing simple, secure access to cloud services with integrated access management, authentication and single sign-on.

Enabling a world powered by software

Just as important as the cloud, software is increasingly crucial

for business performance and new revenue opportunities. This is especially true for businesses that are shifting away from hardware as their main revenue driver in favor of software. Our software licensing and monetization solutions help manufactures, device makers and software companies license, deliver and protect their software in order to generate new revenue streams, improve operational efficiency, increase customer satisfaction and gain valuable business insights.

Security that integrates with your technology ecosystem

With one of the industry's largest data protection technology ecosystems, Thales solutions integrate with the most widely used technologies to protect and secure access to your mission-critical applications and data. Through the Thales partner program, we have established partnerships with more than 500 global technology organizations who are committed to architecting solutions to meet secure cloud and digital transformation initiatives. Thales partners with leading resellers, system integrators, distributors, managed service providers and technology companies to meet the data protection and compliance needs of the most security-conscious organizations around the world.





Thales Identity and Access Management Portfolio

Cloud-based applications play a vital role in fulfilling productivity and operational needs in the enterprise. However, as new services are added to an organizations' cloud estate, it becomes more difficult to gain unified visibility into cloud access events, more complex to comply with regulations and more onerous for users to remember multiple credentials. And with cloud applications protected, by default, only with weak static passwords, the risk of a data breach rises.

Thales's award-winning suite of SafeNet Access Management and Authentication solutions allow organizations to effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users. Utilizing policy-based SSO and universal authentication methods, enterprises can securely move to the cloud while maintaining access controls to all corporate resources, regardless of the device being used.

Prevent breaches

Deter unauthorized access and apply universal authentication methods for all apps

Enable cloud transformation securely

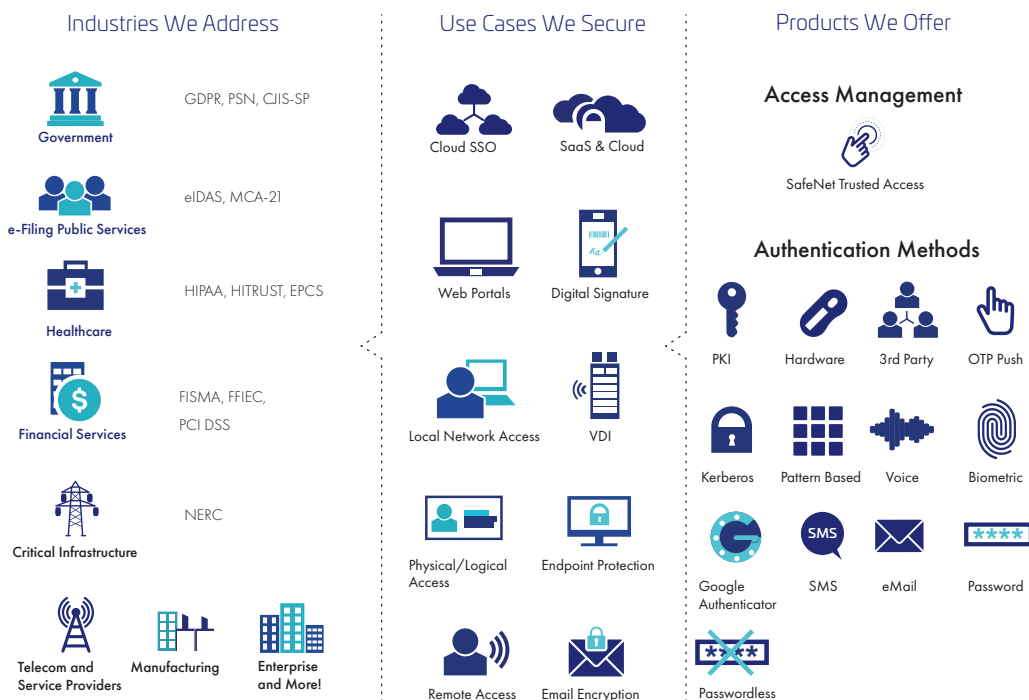
Transform your business and operate securely by applying consistent access policies to all on prem and cloud apps

Simplify the login experience

Make it simple for users to log into multiple apps with cloud SSO, elevating trust only when needed

Simplify compliance

Remain compliant as you grow your environment by setting policies that adapt to new regulations



Standards-based Security

Thales's SafeNet Access Management and Authentication solutions offer unparalleled standards-based security:

- FIPS 140-2 validated software and hardware tokens
- Common Criteria certified hardware tokens
- ISO 27001:2013 accreditation
- AICPA SOC-2 recognition
- DSKPP-secured provisioning of software tokens
- ANSSI certified libraries within software tokens
- Hardware-based root of trust
- Field-programmable tokens

Access Management

Over the years, you may have heard a lot about access management. In fact, we tended to use the terms "authentication" and "access management" pretty much to mean the same thing. But in fact there are differences between the two. While authentication validates a user's identity, access management determines that a user has the permission to access a certain resource and enforces the access policy that has been set up for that resource.

Access management is very important when it comes to managing access to cloud resources. Nowadays, a person typically has to access numerous cloud apps throughout the day. This is a hassle for both users and IT: Users have to remember countless passwords; while IT need to endlessly reset forgotten passwords. The solution to this problem is SSO: By having one credential for all cloud apps, users can easily login once to several apps while IT saves precious time over password resets.

Since that single identity is only as secure as the authentication used to verify it, the method of verifying users' identities becomes paramount to maintaining cloud access security. To this end, access management solutions and single-sign on solution offer granular control over the access policies defined per application.

By requiring an additional authentication factor in high risk situations, a frictionless user experience is maintained.



Introduction to Access Management

Authentication and Access Management solutions are composed of Identity Governance and Administration (IGA) functionality and Access Management (AM) functionality. IAM solutions provide a methodic framework for granting (and requesting) access to applications (IGA), enforcing access controls (AM) and ensuring visibility into access events (AM). Given that most organizations deploy the IGA and AM components separately of each other, these disciplines are being increasingly evaluated as distinct, standalone solution families, rather than as composite functionalities of a single Authentication and Access Management suite.

Access management is a functionality that enables determining whether a user has permission to access a certain resource, and enables the enforcement of the access policy that has been set up for that resource.

Access management is implemented based on access policies that

are defined by IT administrators and include such information as which groups of users (e.g. Sales, R&D, HR) are allowed access to which cloud applications (e.g. Salesforce, Office 365, Jira, Taleo), as well as the set of user attributes required to access each application (e.g. trusted network, password, OTP).

The access policy can require more or less user attributes to be assessed depending on the sensitivity of a cloud application. These attributes are assessed using riskbased or context-based authentication, which is central to enforcing the different access policies defined for each cloud application. (For more details, see context-based authentication.)

Also central to cloud access management is single sign-on, which enables the use of a single username and password set or 'identity' to log in to all one's cloud applications. (For more details, see single sign-on.)



Click [here](#) to learn more and download the Access Management Handbook

Cloud Access Management

Cloud applications are excellent at providing organizations the best technology at a quick time to value, zero maintenance overhead and infinite scalability. The immediate fulfillment and instant productivity provided by cloud apps comes, however, with a price tag. IT departments lose visibility into who is accessing what application, when—and what authentication method is being used.

Compliance risk increases as apps are managed from multiple disparate consoles, while help desk tickets owing to password resets abound.

The most important person in the process—the end user—suffers from password fatigue, frustration and downtime as they fret to keep their copious identities in order.

To address these cloud adoption hurdles, cloud access management solutions have emerged to streamline cloud access provisioning, eliminate password hassles for IT and users, provide a single pane view of access events across your cloud estate and ensure that the right access controls are applied at the right time to the right user.

- **Optimized cloud security** - By enforcing scenario-based access controls using finegrained policies, organizations optimize security and reduce the risk of a breach
- **Ease of Management** - Access management provides administrators with a single point of management, a single pane of glass, from which to define access policies once and enforce them throughout
- **Visibility** - Access management solutions enable IT to answer the questions “Who has access to what?” “Who accessed what and when?” and “How was their identity verified?” By gaining a central view of access events and visibility into which applications are being accessed also saves businesses money as it enables identifying which app licenses are underutilized
- **Access Management Benefits** - Implementing cloud access management solutions increases enterprise access security, removes the ambiguity associated with cloud security and compliance risk—and no less important—ensures the most frictionless user experience.
- **Enhanced user convenience** - Access management solutions offer cloud single sign on, which lets your users log in just once in order to gain access to all their cloud applications, using the familiar enterprise identity they already use today
- **Cloud access management ensures that the right people have access to the right applications at the right level of trust**
- **Cloud access management solves the challenges faced by enterprises in their quest for broader cloud adoption.**

Value proposition:



Click [here](#) to access the Access Management Primer fact sheet



Click [here](#) to access the 4 Steps to Cloud Access Management guide



SafeNet Trusted Access (STA)

Thales offer access management and authentication solutions which prevent data breaches and enable cloud adoption by simplifying and securing access to all your apps. STA is an access management and authentication service. By helping to prevent data breaches and comply with regulations, STA allows organizations to migrate to the cloud simply and securely.

Value proposition

- Prevent breaches - Apply different MFA methods and control accesses for each app while eliminating passwords
- Enable cloud transformation securely - Extend existing access controls to cloud apps and apply consistent access policies to all cloud resources
- Simplify compliance - Prove compliance with a real-time audit trail of who is accessing which app and how
- STA prevents data breaches, allowing organizations to migrate to the cloud simply and securely

STA core capabilities

- Access Management
- Authentication
- Smart Single Sign On

Target customers

- CISO
- IT Manager
- Support
- End User
- Finance

Supported authentication methods

- OTP Push
- OTP App
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- PKI credentials
- FIDO
- Google Authenticator
- Passwordless authentication
- Biometric
- Voice
- 3rd party



Click [here](#) SafeNet Trusted Access product brief

Smart questions

- Organizations who planning to use cloud apps, or that are already using several cloud apps will be the most likely customers for STA. The purpose of the questions below is to help us understand where our customer is in terms of cloud adoption. The first thing to verify is whether the customer already is using an IDaaS or SSO solution. Those that are not, will more likely be potential customers for STA.

Customers who are NOT using an SSO or IDaaS solution:

- How many cloud apps are deployed in your organization?
- Is there a "cloud first / cloud adoption" strategy direction in your organization? Do you have many issues with users having to manage multiple passwords for the various apps? How do you handle that currently?
- Do you want to be able to apply 2FA and SSO to all cloud apps?
- Customers who ARE already using an SSO or IDaaS solution:
- What are you using today?
- How does it allow you to set policies per application and per user?
- What type of 2FA methods can you use?
- What applications does it protect?
- What additional features would you like to see in your current solution that are not available?
- What types of other solutions are you looking into at this time?
- How are you protecting O365?

Access Management for Leading Applications

SafeNet Trusted Access supports hundreds of applications, including the following:



Thales Authentication Portfolio

Universal Authentication Capabilities

Thales delivers fully-automated, highly secure next generation authentication capabilities with flexible authentication options tailored to the unique needs of any organization. Our platforms support a broad range of authentication technologies and form factors as outlined below:

OTP

- One-time passwords are supported via PUSH notifications generated on mobile devices, on apps installed on desktops and via hardware tokens.

Certificate-based authentication

Thales' range of certificate-based solutions offer strong multi-factor authentication and enable organizations to address their PKI security needs. Thales' virtual smart card solution, hardware smart cards and USB authenticators offer a single solution for strong authentication and high assurance applications such as digital signing and email encryption. They also support network logon, as well as corporate ID badges, magnetic stripes and proximity.

Thales offers a broad range of certificate-based PKI authentication solutions. These include:

- SafeNet IDPrime Virtual - A virtual smart card solution that facilitates mobility by enabling PKI-based security on all devices and reduces the operational overheads associated with hardware based authentication devices.
- Smart Card hardware form factor
- USB token form factor

PKI authentication solutions are enabled by SafeNet Authentication Client middleware and CMS solutions that manage certificate life cycle management and provisioning.

Adaptive authentication

Thales' context-based authentication offers convenient, frictionless strong authentication while maintaining the flexibility and agility to add protection with stronger methods of security in higher risk situations.

Combined with "step-up" authentication, context-based authentication optimizes a layered approach to access security by assessing user login attributes and matching them against pre-defined security policies.

SMS and eMail

- Numerical passcodes can be delivered to all devices via SMS or eMail

Pattern-Based Authentication

Thales' GrIDsure flexible authentication method allows an end-user to generate a one-time password without the requirement for hardware tokens or software applications. GrIDsure tokens work by presenting the end-user with a matrix of cells which contain random characters, from which they select a 'personal identification pattern' (PIP).

FIDO Authenticators

SafeNet FIDO2 Devices offer enterprises strong and secure passwordless authentication to any environment.

SafeNet IDPrime 3940 FIDO (Smart Card) and SafeNet eToken FIDO (USB token enable organizations to secure cloud adoption and bridge secure access across hybrid environments via an integrated access management and authentication offering.

Third Party Authenticators

Thales solutions support OATH tokens and other third party authenticators.



Questions and Special Requests

If you have any questions or special requests, please contact Gemma.Ainsley@ThalesGroup.com

You can discover the latest and greatest sales and marketing resources by visiting the Accelerate Partner Portal via <https://thales.webinfinity.com>

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: CPL_Sales_AMS_TG@thalesgroup.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: CPL.Sales.APAC.TG@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: CPL_Sales_EMEA_TG@thalesgroup.com

> cpl.thalesgroup.com <

