cpl.thalesgroup.com

THALES

Migrating from legacy IAM to modern Access Management: Guidelines and Best Practices

White Paper

Contents

Introduction

Businesses are facing increased needs and challenges for managing access and authentication to cloud applications while ensuring employees can securely work from home. Legacy on-premises IAM solutions such as enterprise Single-Sign On (SSO), Virtual Private Network (VPN) or a Web Access Management (WAM) are based on the concept of securing the network perimeter and may limit organizations' ability to enable their employees to securely and efficiently access cloud services. As such, organizations that rely on perimeter on-premises security to protect cloud services are liable to face limitations in their ability to scale effectively and securely in the cloud.

An alternative approach is using a cloud-based Identity-as-a-Service architecture, such as Thales SafeNet Trusted Access, which allows organizations to extend security beyond the network perimeter and protect both on-premises applications that lack modern standards support and public cloud apps.

The goal of this whitepaper is to provide guidelines to companies who want to migrate away from traditional network infrastructure components, including WAMs, VPNs, and legacy SSO in order to benefit from reduced TCO, better and smarter security, and an enhanced user experience made possible by cloud-based access management solutions.

The need for Access Management and Authentication

Enterprises are abandoning traditional business models and adopting digital transformation at a fast pace, embracing cloud, multi-cloud and/or hybrid cloud environments. The adoption rate of cloud applications has been dramatic in recent years, with organizations of all sizes moving to cloud-based delivery models.

While originally it was business needs, such as omnipresence and customer engagement, that pushed towards cloud adoption, nowadays IT services are being migrated to the cloud propelled in large by cloud service providers such as Microsoft, Google and AWS. The majority of orgnizations have already adopted SaaS applications to cater for new ways of working and enhanced employee collaboration.

Although cloud-first initiatives and strategies are a top-notch priority for a majority of businesses, the full-scale transition to the cloud might be a multi-year process to complete. Many enterprises have already transitioned some applications to the cloud while continuing to support indefinitely other on-premises apps and data stores. Regardless of how innovative an organization is, mature enterprises inevitably have legacy resources that rely on the technologies of the previous generation.

These types of hybrid realities are common. Businesses may elect to maintain on-premises infrastructure because they have such customized data stores and associated apps that they are difficult to decouple. Or they may not have adequate resources to devote to the cloud migration. Furthermore, those on-premises applications may be exposed to the business' customer base, and businesses may not be able to sacrifice them because of the inherent revenue risks.

Securing access to these hybrid deployments is critical especially for ensuring business continuity in emergency situations which disrupts normal workflows. Unplanned events like disasters linked to environmental crisis, natural disasters such as earthquakes, business shutdown due to national security reasons or personnel illness due to epidemic phenomena can have a devastating effect on all businesses. The test lies in organizations' ability to enable secure remote access for all employees in a scalable and secure manner.

Security is Critical

As enterprises embrace modern technology trends and cloud computing, security becomes a top concern. This is especially evident in the surge in phishing attacks against cloud services, many of which have led to massive data breaches. As a result, IT teams are seeking streamlined methods of centrally defining and enforcing access controls to manage security and compliance in a consistent manner across their cloud and on-premises applications.

Traditionally, organizations have relied on Virtual Private Networks (VPN), on-premises Single-Sign On (SSO) and Web Access Management (WAM) solutions like CA SiteMinder, Oracle Access Manager, and IBM Tivoli Access Manager to control authentication and authorization to corporate resources.

With the proliferation of cloud-based apps and distributed computing models, these legacy solutions can no longer meet the needs of modern IAM.

Limitations of Legacy Access Solutions

The mass move to cloud computing and working from home has exposed the weaknesses of on-premises perimeter security for securely accessing cloud applications. These include:

- Directing cloud access traffic through an on-prem solution overloads the network and slows overall network traffic
- Relying on a VPN or WAM for cloud access creates a single point of failure and increases the risk that employees will not be able to access critical cloud apps if the VPN goes down
- Allowing employees to access the entire network with a single credential could prove disastrous from a security perspective if that credential were to be compromised.
- The costs involved in maintaining and expanding legacy on-premises solutions to accommodate hundreds of cloud apps are much higher than implementing a cloud-based solution for secure remote access

Assessing Legacy IAM Solution's Ability to Efficiently Address Cloud Access

Multi-Factor Authentication

Legacy IAM solutions tend to authenticate users with either hardware or software tokens, but this is a binary decision which is taken once, during the initial login process. In the modern business environment, where employees may access corporate assets from almost anywhere, even using their own devices, binary authentication decisions do not adapt the level of authentication in accordance with the risk environment. To be able to provide an agile and granular approach to user authentication, the IAM solution should provide adaptive approaches with step-up as the risk increases based on contextual data gathered from the user's device sensors.

Moreover, software and token-less authentication methods combined with easy, automated token enrollment ensure a seamless log-in experience for all employees. To support all users' needs, the IAM solution should offer a range of passwordless authentication methods that can accommodate varying needs and security levels.

The table below provides an overview of the MFA capabilities offered by legacy and IDaaS authentication solutions.

	Legacy IAM (VPN, WAM, SSO)	IDaaS
Passwordless	Token-based, hardware or software	Token-less: push OTP app, SMS or email code, pattern-based
Authentication decision approach	Binary (yes/no) decision at initial entry	Adaptive decision with step-up as risk increases

Table 1: Multi-Factor Authentication, Comparison of legacy and IDaaS IAM solutions

Enterprise Single-Sign On

Traditional enterprise SSO solutions, like Microsoft AD FS or Ping Federate, are implemented on-premises and usually support federation through protocols such as SAML. These solutions however allow Single-Sign On using a single credential that is presented at the start of a session. If that single credential is compromised, stolen or lost, all enterprise applications would be at risk.

To offer a frictionless logon experience without sacrificing security, organizations should leverage cloud based smart SSO combined with contextual information and step-up authentication. This allows employees to access all their cloud and web applications with a single identity, while these access attempts are assessed in a continuous manner allowing the IT teams to enforce stronger access security in high-risk situations. With smart SSO, end users can maintain business productivity and reduce the hassle of having to re-authenticate to multiple apps.

The table below provides an overview of the Single-Sign On capabilities offered by legacy and IDaaS IAM solutions.

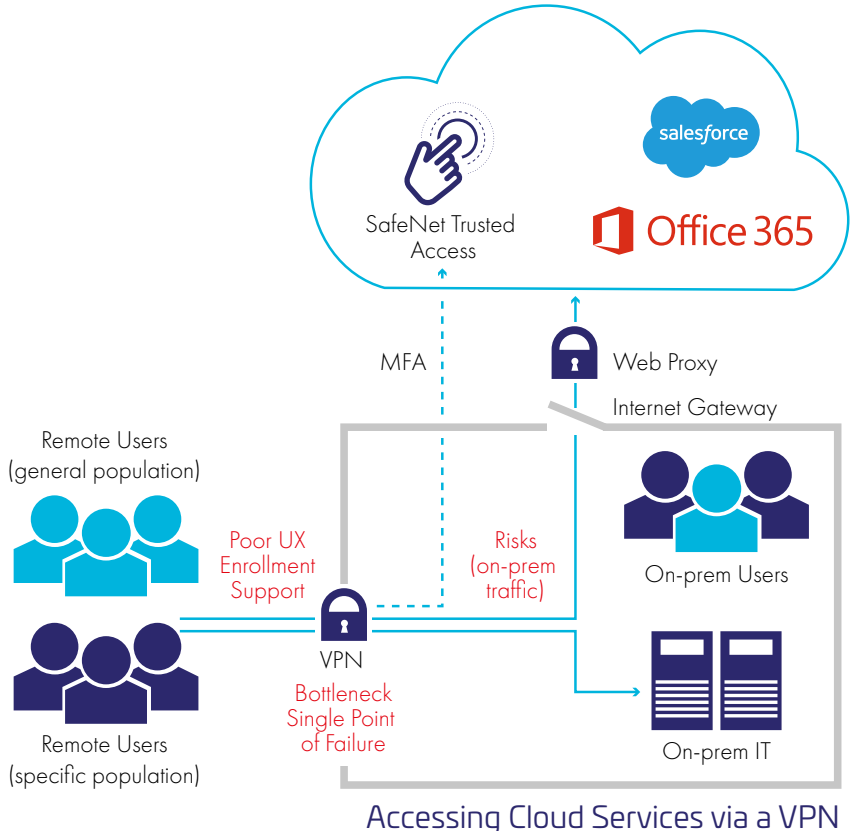
	Legacy (VPN, WAM, SSO)	IDaaS
Implementation	On-premises	In the cloud
Federation	Yes	Yes
Security	Broad SSO, access all apps with the same credential	Adaptive smart SSO, single identity assessed continuously with step-up
Policy Engine	**Open Access** One single access policy for all users and applications	**Policy Driven** Set access policies per business need, application sensitivity and employee function
Authentication	**Point Authentication** User has the same method of authentication to access all services	**Universal Authentication** Apply the step up authentication with appropriate MFA or contextual authentication at each login attempt

Table 2: Smart Single-Sign On, comparison of legacy and IDaaS IAM solutions

Perimeter Control

Legacy perimeter control, like WAMs, VPNs and firewalls, are on-premises solutions. They control traffic through a central, on-premises hub. While this setup may be efficient for on-premises generated traffic, it is not effective for traffic generated or routed to the cloud. Driving traffic from the cloud to an on-premises server to assess security and access requests can create a bottleneck and a single-point of access failure.

When employees are required to work remotely, the modern approach is to implement a zero-trust access evaluation. Businesses need to ensure that nobody is trusted and that access requests are assessed at the access point for each application. This will allow for distributed access decisions per application, per policy and per access scenario. 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, the access management solution should allow for establishing policies that will vary authentication rules according to application.



Accessing Cloud Services via a VPN

The table below provides an overview of the perimeter control capabilities for both the legacy and IDaaS IAM solutions.

	Legacy (WAM, VPN, Firewalls)	IDaaS
Access control	Centrally, on-premises hub	At the access point
Zero-trust	One login for all apps	Access evaluation per app, per policy and per login attempt continuously
Availability	On-premises hub creates a single-point of failure	From the cloud to the cloud
Adaptiveness	Single login for all apps, no step-up	Step up authentication for untrusted networks, ease the level of authentication depending on the risk
Cost	The cost of expanding on-prem infrastructure is high, requiring investment in infrastructure and servers	Cloud-based access management requires no infrastructure investments. And includes support and maintenance

Table 3: Perimeter Control, comparison of legacy and IDaaS IAM solutions

Identity-as-a-Service (IDaaS) solutions support digital transformation and cost savings

Identity-as-a-service (IDaaS) are SaaS-based IAM solutions that allow organizations to use Single-Sign on, authentication and access controls to provide secure access directly to cloud services.

IDaaS has become the preferred delivery method for the vast majority of new access management deployments because it offers a variety of benefits:

- Reduced breach risk by protecting enterprise and cloud apps at the access point
- Reduced identity management complexity by offering seamless access into the required apps either from home or any other location outside the business premises
- Ease of deployment, taking advantage of cloud based delivery
- Increased time to value and cost savings, without investing in servers to support access management functions in a sustainable manner
- High availability and reliability since the IAM services are offered in the cloud, thus avoiding single-points of failure
- Frequent and easy-to-consume functional upgrades

How SafeNet Trusted Access can help businesses implement a modern IAM architecture

A comprehensive IAM platform should cover a range of authentication situations and provide iron-clad access security for all enterprise applications. SafeNet Trusted Access enables organizations to protect enterprise applications and scale securely in the cloud with a broad range of authentication capabilities, while ensuring security with smart Single-Sign On and policy driven access controls.

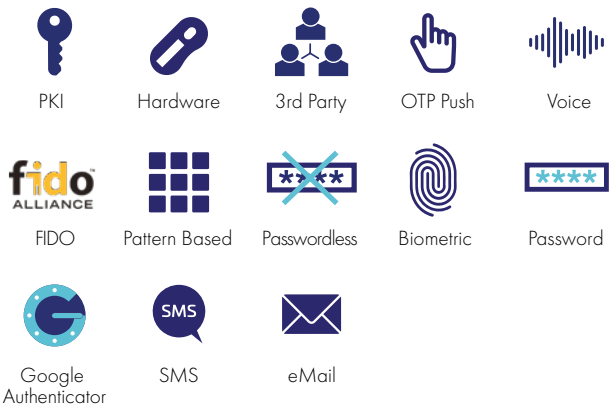
Multi-Factor Authentication

SafeNet Trusted Access offers comprehensive authentication capabilities with step-up, risk-based authentication, making it easier to implement MFA across the entire application portfolio for an enterprise. A key benefit of SafeNet Trusted Access is its support for a wide range of MFA form factors, including hardware and software, SMS and email, push notification and biometrics, and numerous authentication methods including OTP, PKI (certificate-based), adaptive and pattern-based authentication.

SafeNet Trusted Access supports authentication standards, including RADIUS, OpenID and SAML – all delivered from the cloud. In addition, SafeNet Trusted Access supports passwordless authentication via FIDO in a variety of methods, including via PUSH OTP, certificate-based authentication, FIDO authentication and Windows Hello.

SafeNet Trusted Access

Universal authentication methods



Utilize the MFA schemes already deployed

Extend PKI authentication to the cloud

Offer the appropriate level of assurance

Offer convenience with Passwordless authentication

Figure 1: Thales' SafeNet Trusted Access authentication methods

Smart Single-Sign On

One of the core strengths of SafeNet Trusted Access is its policy engine, which allows for setting access policies that are extremely flexible. Security policies cater for the creation of very granular and specific rules to constantly reassess users during an open session, rather than only for certain events such as authentication time-outs. If the level of risk changes, SafeNet Trusted Access forces the user to re-authenticate or step up to a stronger form of authentication.

Policies can be set per application, apply to network ranges, operating systems, and user collections and geolocations. Authentication rules can be established as dynamic and as context specific as needed: for example, they can be set to check at every access attempt or for particular circumstances, such as requiring step-up authentication under riskier conditions.

To provide integrated identity corroboration capabilities for continuous and adaptive access management, SafeNet Trusted Access supports the following functional requirements:

- Context-based "conditional" access control.
- Integration between applications and other sources of risk context information.
- Continuousness. Risk and trust are automatically assessed for every interaction throughout every session, and this can come only through integration with applications.

Perimeter Control

SafeNet Trusted Access was born and lives in the cloud. Hence, it is not dependent on on-premises infrastructure and can control access in the cloud avoiding bottlenecks. In addition, since all authentication and access management services are provided at the access point, SafeNet Trusted Access enables a perimeter-less security for distributed network environments enabling the implementation of zero trust approaches.

This perimeter-less approach ensures that security is not jeopardized by single-points of failure and that an adaptive and risk-based authentication is applied per application, wherever that application is.

Next Steps: Migrating from legacy IAM solutions to SafeNet Trusted Access

This section will provide a step-by-step guide to migrate on-premises and cloud services from traditional IAM solutions to SafeNet Trusted Access. Acknowledging that many organizations are not on in a position to undertake a massive migration for all their apps, we propose a phased approach which is based on the needs of specific groups within your organization.

Step 1.

Map out all on-premises and cloud services to have a clear visibility on what is to be protected.

Step 2.

Once you have full visibility into your services, it is recommended to:

- Assess the protocols each service and app supports. Determine whether the application supports a modern standard such as SAML or OpenID Connect. Many enterprise-focused web applications have a built-in SAML capability, but some may need proprietary or non-standard integration.
- Map out the users who typically access these apps. For example, are they privileged users, C-suite users, or regular users?
- Determine the sensitivity of these apps and ascertain the appropriate level of authentication that should be applied for each app

Step 3.

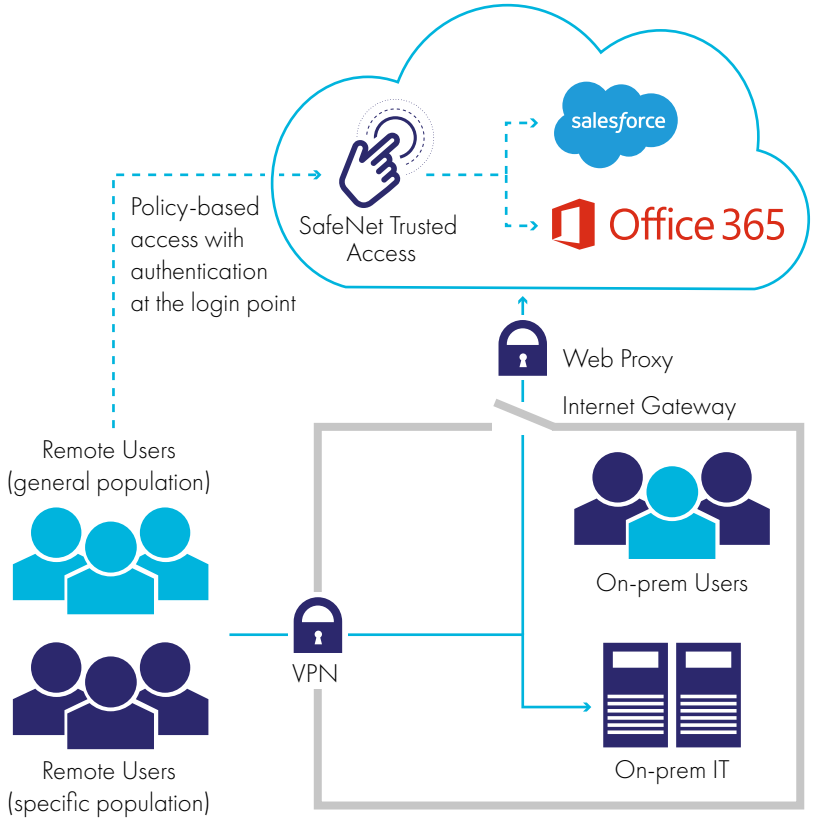
Identify the IAM solution used to provide authentication and access control to each service. Are they behind WAMs, VPNs or on-premises SSO?

Step 4.

Prioritize the apps and user groups that should be implemented first. A good place to start is to prioritize cloud apps that are being accessed via a VPN or WAM and those apps that are being accessed by passwords. By enabling direct access to cloud services through SafeNet Trusted Access for most of your users, you will be able to immediately reduce traffic on your network and secure these services at the access point. Phase 2 of implementing SafeNet Trusted Access will involve prioritizing the on-premises apps that will be protected. A good way to prioritize these apps, is by starting out with the ones that support Radius, OIDC or SAML. Since SafeNet Trusted Access offers federation wizards, supporting these applications will be straightforward to set up. Phase 3 will involve moving over legacy apps that do not support modern federation protocols. These will likely use integration that relies on agents or APIs.

Deployment KPIs: What is Achievable on Day 1 of SafeNet Trusted Access Implementation?

- Set up cloud-based MFA service
- Federate apps defined in phased 1 priority list, using wizard based federation templates
- Set up access policies based on the risk assessment carried out for each app
- Monitor and adjust policies as needed



Accessing Cloud Services with SafeNet Trusted Access

Conclusion

The ability to scale securely in the cloud, enable employees to work from home and reduce costs is now more critical than ever. Indeed, according to Gartner 74% of companies plan to permanently shift to more remote work post COVID-19[1] in order to offer mobility and reduce costs.

Continued adherence to legacy identity and access management tools will not be sufficient to support modern architectures and enable organizations to benefit fully from cloud efficiencies. By implementing a modern, cloud-based access management platform such as SafeNet Trusted Access, organizations can accelerate their business evolution and reduce the risk of data breach, while ensuring agility and cost savings.

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.

1 Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently
https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

THALES

Contact us

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

> cpl.thalesgroup.com <