Product Brief

Secure Your Workforce and Protect the Enterprise with SafeNet Trusted Access

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

As some of the most technically advanced and efficient organizations in the world, cloud-first companies have set a new standard for modern workforces. While global workforces require continuous access to cloud-based applications and services , it has also introduced a challenge for security teams to protect their most sensitive data and applications. Additionally, with the common misconception that secure access means heavy user friction, it makes it difficult for security professionals to get buy-in to implement a new approach to workforce authentication.

Cloud-native businesses shouldn't have to compromise. With the right solution, you can protect access to applications and data without disruptions—delivering frictionless user experience while upholding the security standards you've committed to as an organization.

Traditional Authentication and Access Management Hasn't Evolved for the Modern Threat Landscape

One-Size-Fits-All MFA Leaves Significant Gaps

With different application sensitivity, user roles, compliance requirements, and more, blanket MFA policies lead to lower user adoption, too much friction for some situations, and gaping holes in others.

A Hybrid and Remote Workforce Introduces Access Complexities

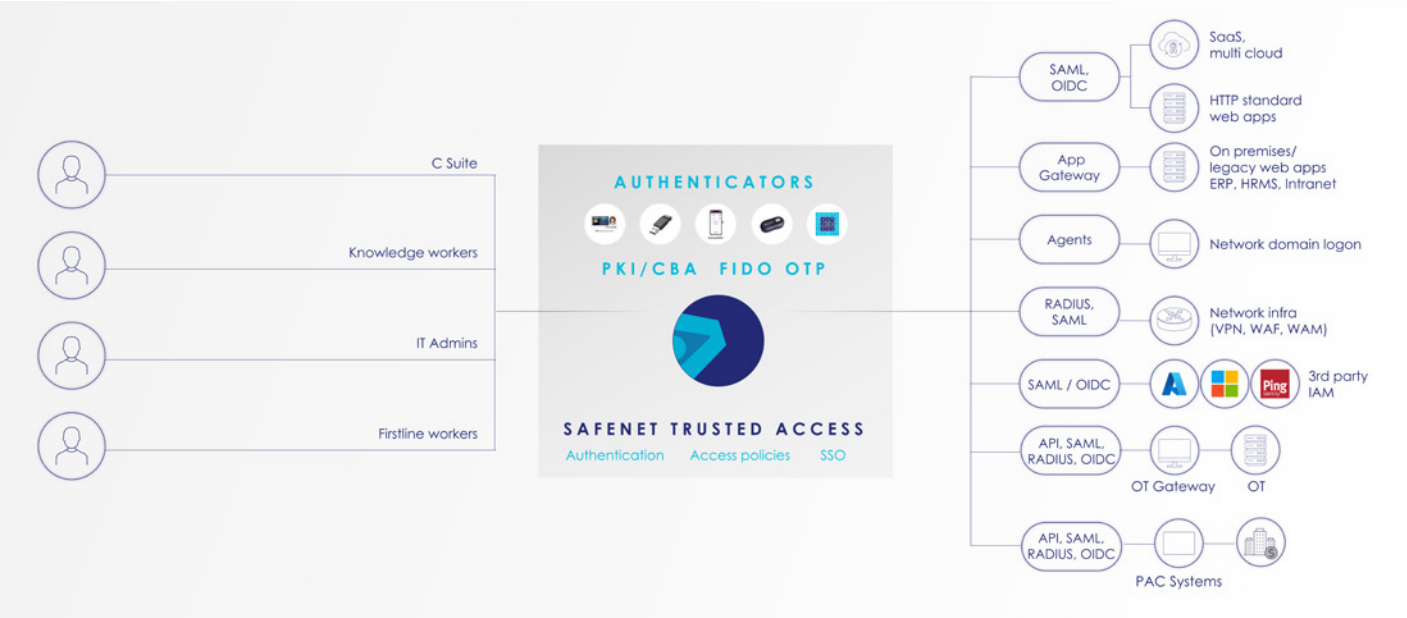
Many on-premises access management tools have failed to evolve to meet modern needs of enabling access for an increasingly remote and hybrid workforce.

Increased Scrutiny from Compliance Regulators

Standards like PCI DSS, NIS 2, ISO 27001 require least privilege principles and enabling MFA policies for accessing any PII and other forms of protected data, which outdated solutions fail to do effectively, leading to avoidable fines.

Password-based Logins Are Highly Targeted

Attackers still use their tried-and-true methods of stealing login credentials. Gaining access to just one credential paves way for lateral movement as they traverse multiple systems to access a goldmine of valuable data.



SafeNet Trusted Access Secures Access to Your Unique Application Environment

SafeNet Trusted Access (STA) is a single sign-on (SSO), multi-factor authentication (MFA), and access management solution for both cloud and on-premises applications. With STA you can:

Improve MFA adoption with a wide range of authentication tokens based on user action, data access, and more

Automate workflows tailored to the specific needs, behaviors, and characteristics of different users

Never compromise on user experience while maintaining a high standard of security

Unlike basic authentication and access management tools, STA enables organizations to secure access to their cloud and on-premises applications by protecting against unauthorized access, without sacrificing user experience. As a modern authentication solution, STA helps increase MFA adoption for any type of workforce user.

What You Get: The Thales Advantage

Seamless Single Sign-On (SSO) for Your Whole Application Environment

Eliminate the hassle and frustration of managing multiple logins. With SSO, users can authenticate once and seamlessly access multiple applications—no more password fatigue or constant interruptions. Plus, you can enable a unified authentication experience by integrating STA with your IdP of choice.

Passwordless Authentication

Using advanced, phishing-resistant authentication methods such as FIDO, Windows Hello, PKI, and many others, your organization no longer has to rely on traditional, highly vulnerable passwords.

Extensive Suite of Modern MFA Methods

- OTP Push on mobile and desktop
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS
- Contextual and adaptive authentication
- FIDO 2
- PKI smart cards and credentials
- Google Authenticator
- Passwordless authentication
- Biometric
- Voice

Risk Scoring and Conditional Access

Powerful policy configuration, risk scoring, and endpoint risk assessments ensure you enforce the right access policies for the right apps and users and maintain the integrity of all authentications.

Fast Time-to-Value and User-Initiated Self-Enrollment

Built with usability in mind and delivered as a SaaS solution, STA enables organizations to setup and deploy access policies rapidly. The self-enrollment feature provides step-by-step guide for users to setup and enroll their authentication tokens, reducing the burden on IT.

Data-Driven Insights and Seamless Workflow Integration

With detailed event logs automatically exported to your SIEM, you can get deeper context into failed access attempts, informing future authentication policies.

Flexible and Resilient Delivery Architecture

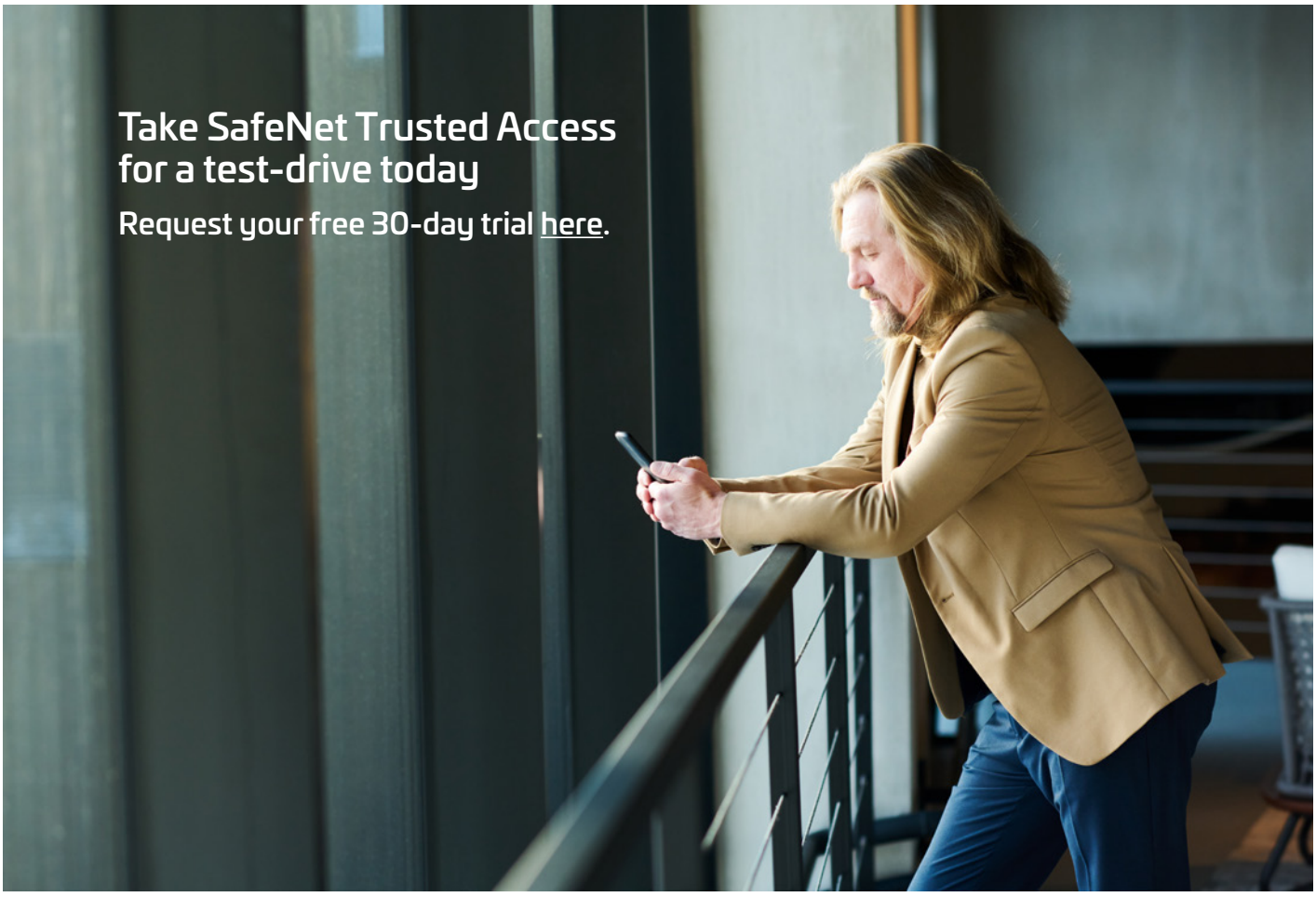
Ensure uninterrupted data access and business continuity through Access Continuum, our reliable fallback mechanism, even during disruptions or service outages.

Support for Broad Range of Protocols

- SAML
- OIDC
- WS
- Fed
- Cloud-based RADIUS
- Agents
- REST and SCIM APIs
- Application gateways
- Legacy applications

About Thales

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management, application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.



cpl.thalesgroup.com

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