Product Brief

# Proteggi i Sistemi Critici e Semplifica l'Accesso con SafeNet Authentication Service

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Sebbene la migrazione al cloud sia una tendenza per la maggior parte delle aziende nate nel XXI secolo, molte imprese consolidate hanno scelto consapevolmente e strategicamente di mantenere i propri sistemi on-premises a causa di requisiti di sicurezza e conformità, preoccupazioni legate alla proprietà dei dati o ai tempi di inattività, o semplicemente perché i loro mainframe o applicazioni legacy personalizzate non sono supportati nel cloud.

I fornitori di soluzioni di sicurezza stanno spingendo per un'adozione diffusa delle soluzioni di Identity and Access Management (IAM) basate sul cloud, ma queste spesso non funzionano per le aziende che operano ancora prevalentemente on-premises. Queste organizzazioni necessitano di una soluzione di gestione dell'autenticazione che le supporti nel loro stato attuale e che si integri perfettamente nel loro ambiente.

## IAM Basato su Cloud: Insufficiente per le Organizzazioni che danno priorità alla Sicurezza

### Ambienti IT Ibridi e Frammentati Riducono la Semplicità dell'Autenticazione

Molte organizzazioni rinunciano al controllo in cambio della flessibilità offerta dall'IAM basato sul cloud, ma ciò spesso è in contrasto con le loro priorità in termini di sicurezza e resilienza.

### Un MFA Standard Non Basta

Differenti livelli di sensibilità delle applicazioni, ruoli utente e requisiti di conformità fanno sì che metodi semplici come l'autenticazione a due fattori (2FA), tramite SMS, non siano più sufficienti. Altre soluzioni risultano troppo complesse per alcuni utenti o non abbastanza sicure in altri casi.

### Controlli Sempre Più Rigorosi da Parte dei Regolatori e delle Leggi sulla Sovranità dei Dati

Standard come PCI DSS, NIS 2 e ISO 27001 richiedono il principio del privilegio minimo e l'adozione di policy MFA per l'accesso a dati personali e protetti. Le soluzioni obsolete non riescono a soddisfare efficacemente tali requisiti, esponendo le aziende a multe evitabili.

### Le Credenziali Basate su Password Sono un Bersaglio Facile

Gli hackers continuano a utilizzare metodi consolidati per rubare le credenziali di accesso. L'accesso ad una sola credenziale può portare a gravi conseguenze, poiché consente di muoversi lateralmente nel sistema alla ricerca di dati preziosi.

## SafeNet Authentication Service Private Cloud Edition: Per le Aziende che Non Possono Affidarsi Solo al Cloud

SafeNet Authentication Service Private Cloud Edition (SAS PCE) è un identity provider (IdP) con funzionalità di single sign-on (SSO) e multi-factor authentication (MFA) per applicazioni SaaS e on-premises. Con SAS PCE è possibile:

Aumentare l'adozione della MFA con una vasta gamma di token di autenticazione, basata su azioni dell'utente, livello di accesso ai dati e altro

Ridurre l'attrito per l'utente eliminando richieste di autenticazione ripetute dallo stesso browser e utente

Offrire un'esperienza utente fluida mantenendo elevati standard di sicurezza

A differenza delle soluzioni IAM cloud-native, SAS PCE si integra perfettamente con l'infrastruttura e le applicazioni esistenti, riducendo al minimo le interruzioni e garantendo operazioni fluide.

# I Vantaggi di Thales

## Single Sign-On (SSO) per Tutto il Tuo Ambiente Applicativo

Elimina la frustrazione di gestire credenziali multiple. Con SSO, gli utenti si autenticano una sola volta per accedere a più applicazioni, senza stress né continue interruzioni. Inoltre, sebbene SAS PCE funzioni come IdP on-prem, è possibile integrarlo con un altro IdP per un'esperienza di autenticazione unificata.

## Autenticazione Senza Password

Grazie a metodi avanzati e resistenti al phishing, come FIDO, Windows Hello, PKI e molti altri, la tua organizzazione può abbandonare le tradizionali e vulnerabili password.

## Ampia Suite di Metodi MFA Moderni

- Push OTP
- MobilePASS+ (App Authenticator)
- OTP
- Token hardware
- SMS/Email
- GrIDsure (a pattern)
- Autenticazione basata su certificato
- FIDO

## Policy di Accesso Condizionale

La configurazione di policy avanzate ti consente di applicare le giuste regole di accesso a utenti e applicazioni, garantendo l'integrità di ogni autenticazione.

## Time-to-Value Rapido e Registrazione Guidata dall'Utente

Dopo l'integrazione con le directory esistenti, il deployment di SAS PCE è guidato dagli utenti, accelerando l'adozione e riducendo il carico sull'IT. Gli utenti ricevono istruzioni dettagliate per registrare i fattori MFA e abilitare l'SSO.

## Analisi dei Dati e Integrazione con i Flussi di Lavoro

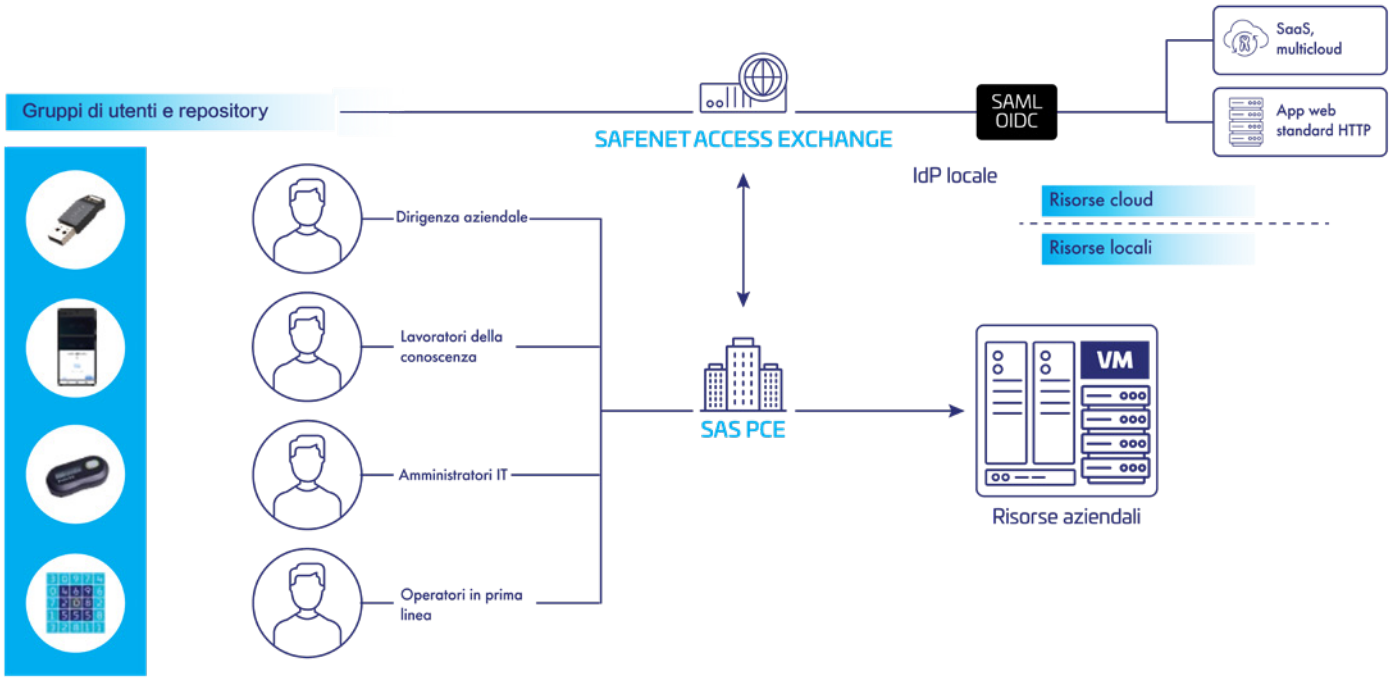
Con fino a 30 giorni di log degli eventi esportati automaticamente nel tuo SIEM, puoi analizzare i tentativi di accesso non riusciti per perfezionare le policy di autenticazione future.

## Supporto Esteso a Diversi Protocolli

- SAML
- OIDC
- WS-Fed
- RADIUS
- Agent
- API REST e SCIM
- Application Gateway
- Applicazioni legacy

## Supporto di Backup per IdP Cloud-Based

SAS PCE può fungere da meccanismo di fallback per altri IdP basati sul cloud, come Okta, Ping e EntraID, garantendo continuità di accesso in caso di interruzioni.



## Informazioni su Thales

Leader globale nella cybersecurity, Thales protegge dati sensibili, identità, applicazioni e software per i brand più affidabili al mondo. Attraverso crittografia avanzata, gestione degli accessi e delle identità, sicurezza delle applicazioni e gestione delle licenze software, Thales protegge gli ambienti cloud, difende dalle minacce informatiche, garantisce la conformità normativa e consente esperienze digitali sicure e affidabili.


cpl.thalesgroup.com/it

**Contattaci –** per tutti i recapiti e per conoscere l'ubicazione dei nostri uffici, visita cpl.thalesgroup.com/contact-us