Descrizione del prodotto

Tieni al sicuro la tua forza lavoro e proteggi l'azienda con SafeNet Trusted Access

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Le aziende che mettono il cloud al primo posto sono tra le più avanzate a livello tecnico e le più efficienti a livello organizzativo al mondo e hanno rivoluzionato gli standard della forza lavoro moderna. Se da una parte la forza lavoro distribuita a livello mondiale necessita del continuo accesso alle applicazioni e ai servizi basati sul cloud, dall'altra questa presenta per i team che si occupano di sicurezza una sfida per assicurare la protezione dei dati e delle applicazioni più sensibili. Inoltre, un errore comune è pensare che un accesso sicuro porti a un massimo attrito per gli utenti, il che rende difficile ai professionisti della sicurezza ottenere l'approvazione necessaria per implementare un nuovo approccio di autenticazione della forza lavoro.

Le attività commerciali cloud-native non dovrebbero accontentarsi. Con la soluzione giusta è possibile proteggere l'accesso alle applicazioni e ai dati senza interruzioni funzionali, garantendo agli utenti esperienza d'uso migliorata attriti e gli standard di sicurezza ai quali l'azienda deve attenersi.

L'autenticazione e la gestione degli accessi di tipo tradizionale non si sono evolute per stare al passo con i rischi della realtà moderna

Una soluzione di MFA unica non è adatta a tutti gli scenari

A causa degli svariati aspetti relativi alla sensibilità dell'applicazione, ai ruoli dell'utente, ai requisiti di conformità e a molto altro ancora, politiche MFA generalizzate portano a una diminuzione dell'adozione da parte degli utenti, attriti esagerati in alcuni casi e divari troppo ampi in altri.

Una forza lavoro ibrida e da remoto introduce complessità al controllo degli accessi

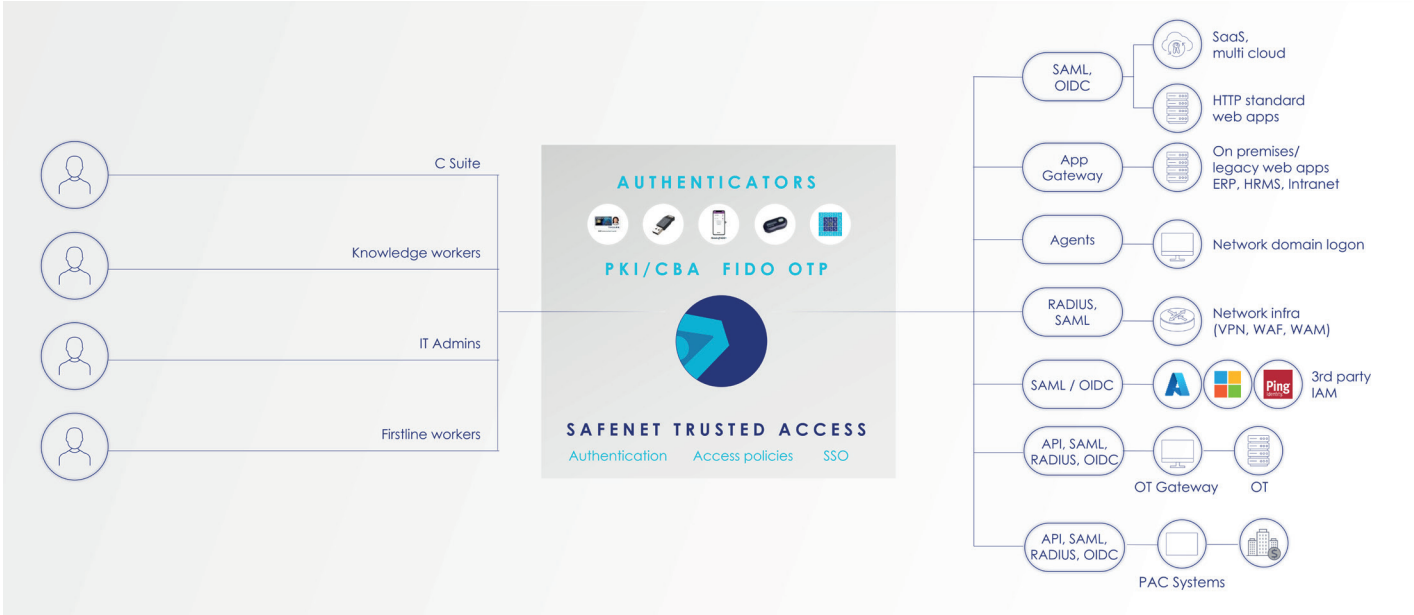
Molti strumenti di gestione degli accessi on-premises non sono riusciti a restare al passo con la necessità odierna di consentire l'accesso a una forza lavoro sempre più da remoto e ibrida.

Maggiore scrutinio da parte delle autorità che si occupano di conformità

Standard quali PCI DSS, NIS 2 e ISO 27001 richiedono privilegi ridotti minimo e consentono alle politiche MFA di accedere a ogni PII e altre forme di dati protetti, cosa che le soluzioni obsolete non sono riuscite a risolvere efficacemente, portando a sanzioni evitabili.

I login tramite password sono un bersaglio facile

Negli attacchi alla sicurezza si usano ancora i metodi brevettati per rubare le credenziali di login. Ottenere accesso anche solo a una credenziale consente movimenti laterali che attraversano diversi sistemi, fino ad arrivare a una miniera d'oro di dati vulnerabili.



SafeNet Trusted Access garantisce un accesso sicuro all'ambiente dell'applicazione unico per l'azienda

SafeNet Trusted Access (STA) è un'autenticazione multifattoriale (multi-factor authentication, MFA) ad accesso unico (single sign-on, SSO) e una soluzione di gestione degli accessi sia per le applicazioni su cloud che on-premises. Con STA è possibile:

Migliorare l'adozione di MFA con un'ampia gamma di token di autenticazione basati sulle azioni degli utenti, sugli accessi ai dati e non solo

Automatizzare i flussi di lavoro in base a esigenze, comportamenti e caratteristiche specifici di diversi utenti

Non scendere a compromessi sull'esperienza dell'utente, mantenendo uno standard di sicurezza elevato

A differenza degli strumenti di autenticazione e gestione degli accessi di base, STA consente alle aziende di proteggere le proprie applicazioni su cloud e on-premises dagli accessi non autorizzati, senza compromettere l'esperienza dell'utente. In quanto soluzione di autenticazione moderna, STA permette una maggiore adozione di MFA per qualsiasi tipo di utente.

Cosa si ottiene: Il vantaggio di Thales

SSO impeccabile per l'intero ambiente applicativo

Basta con la seccatura e la frustrazione di dover gestire multipli login. Con SSO gli utenti possono effettuare l'autenticazione una sola volta e accedere senza problemi a diverse applicazioni. Non servono più innumerevoli password e non c'è più lo stress legato a interruzioni costanti. In più si può attivare un'esperienza di autenticazione unificata, integrando STA con l'IDP selezionato.

Autenticazione senza password

Utilizzando metodi di autenticazione avanzati e resistenti a phishing quali FIDO, Windows Hello, PKI e molti altri ancora, l'azienda non deve più dipendere dalle tradizionali password altamente vulnerabili.

Un'ampia suite di moderni metodi di MFA

- Push OTP su dispositivi mobili e desktop
- Hardware OTP
- Autenticazione basata sui modelli
- OOB via e-mail o SMS
- Autenticazione contestuale e adattativa
- FIDO 2
- Smart card e credenziali PKI
- Google Authenticator
- Autenticazione senza password
- Biometria
- Voce

Punteggi relativi ai rischi e accesso condizionato

La configurazione avanzata dei criteri, nonché i punteggi e le valutazioni del rischio degli endpoint, garantiscono l'applicazione dei criteri di accesso adatti per ogni applicazione e utente, mantenendo l'integrità di tutte le autenticazioni.

Concretizzazione rapida del valore e auto-registrazioni a iniziativa dell'utente

Creato per soddisfare le necessità di utilizzo e per offrire una soluzione SaaS, STA consente all'azienda di impostare e adottare rapidamente i criteri di accesso. La funzione di auto-registrazione include istruzioni che guidano l'utente passo per passo nell'impostazione e nella verifica dei token per l'autenticazione, riducendo le richieste ricevute dall'IT.

Informazioni basate sui dati e integrazione impeccabile del flusso di lavoro

Un registro eventi dettagliato è esportato automaticamente nel SIEM per una maggiore chiarezza sui tentativi di accesso non riusciti, ed è uno strumento essenziale per informare i futuri criteri di autenticazione.

Architettura di fornitura flessibile e resiliente

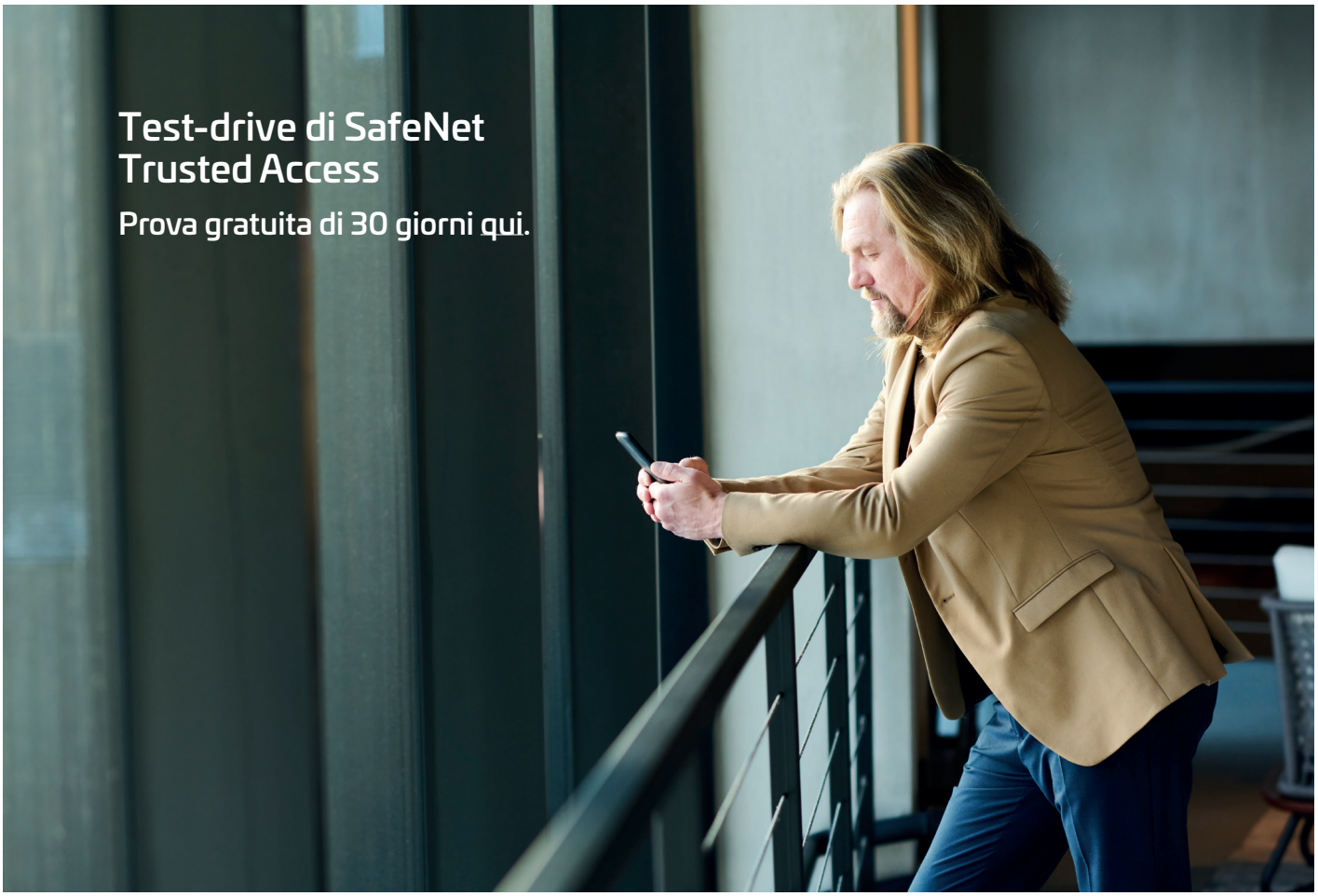
Per garantire un accesso ai dati ininterrotto e una continuità operativa, ci affidiamo a un accesso in continuum, un affidabile meccanismo di sicurezza che rimane funzionale anche durante temporanei disagi o interruzioni di servizio.

Assistenza per un'ampia gamma di protocolli

- SAML
- OIDC
- WS
- Fed
- RADIUS su cloud
- Agents
- REST e SCIM API
- Gateway a livello di applicazione
- Applicazioni legacy

Informazioni su Thales

In quanto leader mondiale nella sicurezza informatica, Thales protegge dati, identità, applicazioni e software sensibili dei marchi più apprezzati al mondo. Grazie alla crittografia avanzata, alla gestione delle identità di accesso, alla sicurezza dell'applicazione e ai diritti d'uso del software, Thales protegge gli ambienti cloud, difende dai potenziali rischi informatici, garantisce la conformità e consente esperienze digitali affidabili.



cpl.thalesgroup.com

Contatti: per tutti i recapiti e per conoscere l'ubicazione dei nostri uffici cpl.thalesgroup.com/contact-us