Descripción del producto

Garantice la seguridad de su fuerza laboral y proteja a su empresa con SafeNet Trusted Access

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Siendo algunas de las organizaciones técnicamente más avanzadas y eficientes del mundo, las empresas que priorizan a la nube han establecido un nuevo estándar para las fuerzas de trabajo modernas. Mientras que las fuerzas laborales globales requieren un acceso continuo a aplicaciones y servicios basados en la nube, esto ha supuesto también un desafío para los equipos de seguridad a la hora de proteger sus datos y aplicaciones más confidenciales. Además, con la idea errónea de que el acceso seguro significa una gran fricción para el usuario, a los profesionales de la seguridad les resulta difícil lograr la aceptación para implementar un nuevo enfoque para la autenticación de la fuerza laboral.

Las empresas nativas de la nube no deberían tener que renunciar a ello. Con la solución adecuada, usted puede proteger el ingreso a aplicaciones y datos sin interrupciones, ofreciendo una experiencia de usuario fluida, al tiempo que mantiene los estándares de seguridad a los que se ha comprometido como organización.

La autenticación tradicional y la gestión de accesos no se han adaptado al panorama de amenazas modernas.

La MFA universal deja huecos importantes.

Con diferentes niveles de confidencialidad en aplicaciones, roles de usuario, requisitos de cumplimiento, entre otros, las políticas generales de la MFA conducen a una menor adopción por parte de los usuarios, demasiada fricción en algunas situaciones y huecos importantes en otras.

Una fuerza laboral híbrida y remota presenta complejidades de acceso

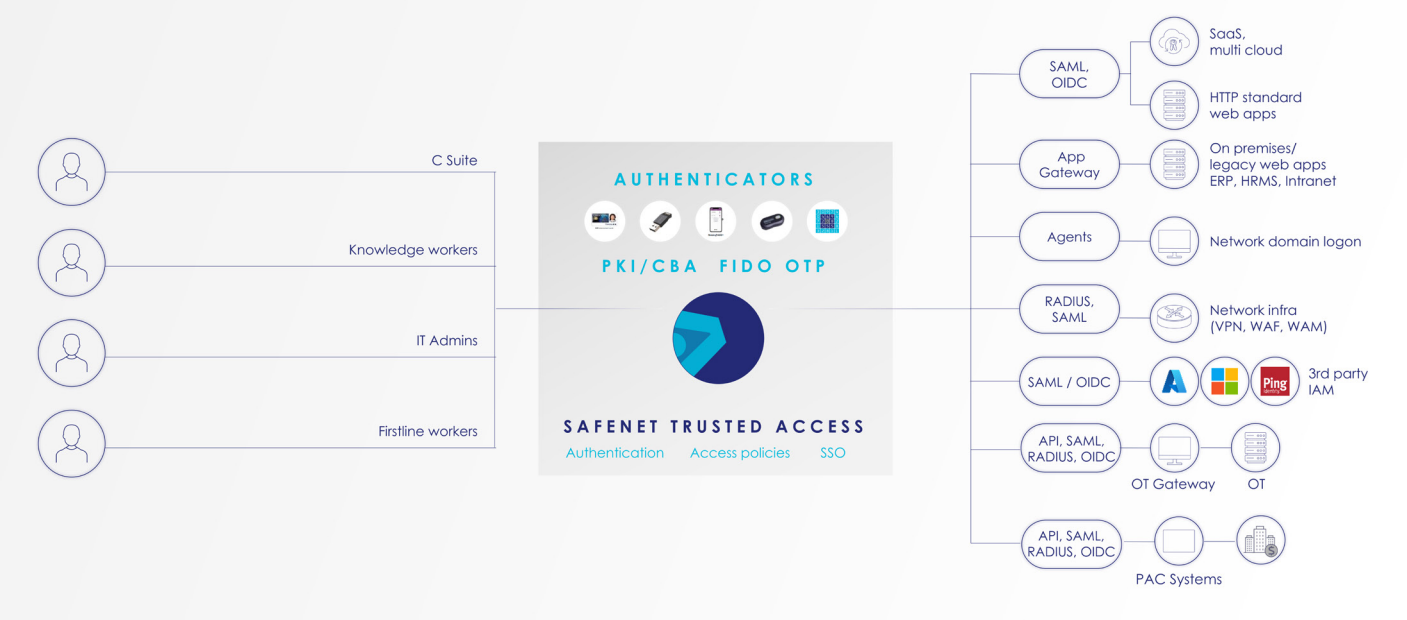
Muchas herramientas locales de gestión de acceso no han evolucionado para satisfacer para satisfacer las necesidades modernas que permiten el ingreso a una fuerza laboral cada vez más remota e híbrida.

Mayor escrutinio por parte de las reguladoras de cumplimiento

Estándares como el PCI DSS, el NIS 2 y el ISO 270001 exigen principios de privilegio mínimo y la activación de políticas de autenticación multifactor (MFA, por sus siglas en inglés) para acceder a cualquier información personal identificable (PII, por sus siglas en inglés), así como a otros tipos de datos protegidos. Las soluciones obsoletas no lo hacen de forma eficaz, lo que conlleva multas evitables.

Los inicios de sesión basados en contraseñas son blanco de muchos ataques

Los atacantes aún utilizan sus métodos de eficacia comprobada para robar credenciales de inicio de sesión. Obtener acceso a tan solo una credencial facilita el movimiento lateral al recorrer múltiples sistemas para acceder a una fortuna de datos valiosos.



SafeNet Trusted Access protege el ingreso a su entorno único de aplicaciones

SafeNet Trusted Access (STA) es una solución de inicio de sesión único (SSO, por sus siglas en inglés), de autenticación multifactor autenticación multifactor (MFA, por sus siglas en inglés) y gestión de acceso para aplicaciones tanto en la nube como locales. Con la solución STA usted puede:

Mejorar la adopción de la MFA con una amplia gama de tokens de autenticación basados en la acción del usuario, el acceso a los datos y más

Automatizar flujos de trabajo adaptados a las necesidades, comportamientos y características específicas de los diferentes usuarios

Nunca poner en riesgo la experiencia del usuario mientras mantiene un alto estándar de seguridad.

A diferencia de las herramientas básicas de autenticación y gestión de accesos, STA le permite a las organizaciones proteger el ingreso a sus aplicaciones en la nube y locales, protegiéndolas contra el acceso no autorizado, sin sacrificar la experiencia del usuario. Como solución de autenticación moderna, STA ayuda a aumentar la adopción de la MFA para cualquier tipo de usuario de la fuerza laboral.

Lo que obtiene: La ventaja de Thales

Inicio de sesión único (SSO, por sus siglas en inglés) sin interrupciones para todo su entorno de aplicaciones

Elimine las complicaciones y la frustración de administrar varios inicios de sesión. Con SSO, los usuarios pueden autenticarse una sola vez, y acceder sin problemas a múltiples aplicaciones: no más cansancio causado por las contraseñas ni interrupciones constantes. Además, puede habilitar una experiencia de autenticación unificada, integrando STA con su proveedor de identidad (IdP, por sus siglas en inglés) preferido.

Autenticación sin contraseña

Gracias a métodos de autenticación avanzados y resistentes al phishing, como FIDO, Windows Hello, PKI y muchos otros, su organización ya no tendrá que depender de contraseñas tradicionales que son altamente vulnerables.

Amplia gama de métodos modernos de MFA

- OTP Push en dispositivos móviles y computadoras de escritorio
- OTP Hardware
- Autenticación basada en patrones
- Fuera de banda a través de correo electrónico y mensajes de texto
- Autenticación contextual y adaptativa
- FIDO 2
- Tarjetas inteligentes y credenciales PKI
- Google Authenticator
- Autenticación sin contraseña
- Biometría
- Voz

Puntuación de Riesgo y Acceso Condicional

La potente configuración de políticas, la puntuación de riesgos y las evaluaciones de riesgos de terminales garantizan que usted imponga las políticas de acceso correctas para las aplicaciones y los usuarios correctos, y que mantenga la integridad de todas las autenticaciones.

Autoinscripción iniciada por el usuario y de rápido tiempo de obtención de valor

Creada teniendo en cuenta la usabilidad y ofrecida como una solución SaaS, STA le permite a las organizaciones configurar e implementar políticas de acceso rápidamente. La función de autoinscripción proporciona una guía paso a paso para que los usuarios configuren e inscriban sus tokens de autenticación, lo que reduce la carga de TI.

Conocimientos basados en datos e integración perfecta del flujo de trabajo

Con registros de eventos detallados exportados automáticamente a su SIEM, usted puede obtener un contexto más profundo de los intentos de acceso fallidos, informando así las futuras políticas de autenticación.

Arquitectura de distribución flexible y resistente

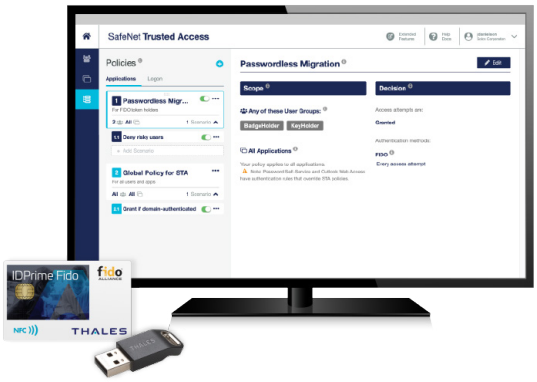
Garantice el acceso ininterrumpido a los datos y la continuidad del negocio a través de Access Continuum, nuestro confiable mecanismo de respaldo, incluso durante interrupciones o cortes del servicio.

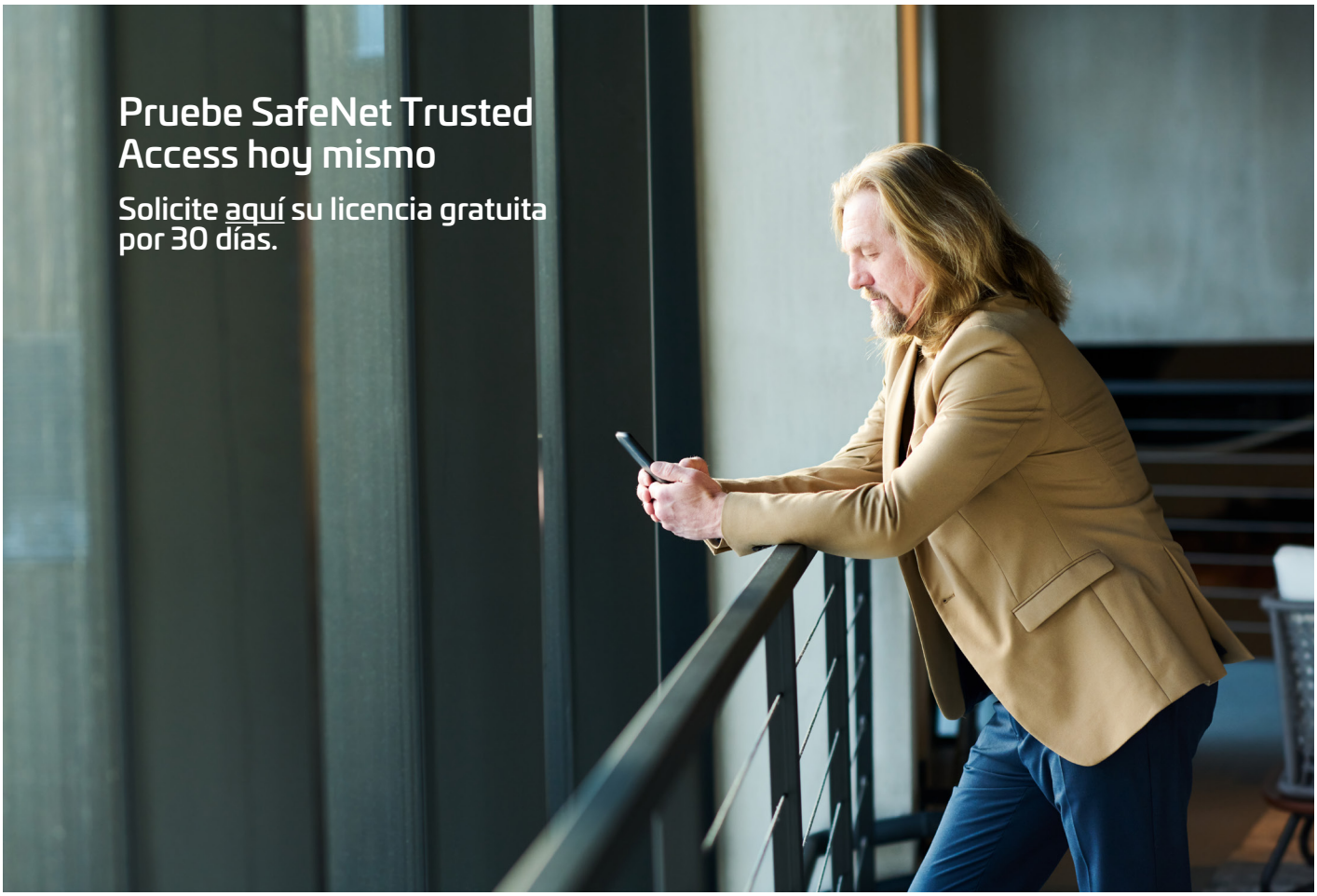
Compatibilidad con una amplia gama de protocolos

- SAML
- OIDC
- WS
- Fed
- RADIUS basado en la nube
- Agentes
- APIs REST y SCIM
- Puertas de enlace de aplicaciones
- Aplicaciones heredadas

Acerca de Thales

Como líder mundial en ciberseguridad, Thales protege datos confidenciales, identidades, aplicaciones y software de las marcas de más confianza en el mundo. A través del cifrado avanzado, la gestión del acceso a identidades, la seguridad de las aplicaciones y los derechos de software, Thales protege los entornos de nube, defiende contra las ciberamenazas, garantiza el cumplimiento y permite experiencias digitales confiables.





cpl.thalesgroup.com

Contáctenos: para conocer todas las ubicaciones de las oficinas y la información de contacto, visite cpl.thalesgroup.com/contact-us