

# Implementar la autenticación y los controles de acceso para Office 365



La solución SafeNet Trusted Access de Thales hace que sea fácil implementar los controles de acceso y autenticación fuerte con Microsoft Office 365, al ofrecer una sólida protección de aplicaciones que sea también conveniente para los usuarios finales.

## Office 365: los desafíos

La implementación de Office 365 crea una nueva realidad para las organizaciones en la que los empleados, estén en la oficina, desde casa o en la carretera, pueden acceder a los sistemas empresariales de forma remota. Por defecto, la única protección que ofrecen estos servicios en línea son contraseñas que de por sí son débiles y estáticas. Casi el 60% de los datos sensibles de las organizaciones se almacenan en la nube y más del 71% de las implementaciones experimentan al menos una cuenta comprometida cada mes<sup>1</sup>. En este contexto, se vuelve crucial poder implementar controles de acceso que evalúen los perfiles de riesgo e implemente una autenticación fuerte.

## SafeNet Trusted Access: la solución

SafeNet Trusted Access de Thales es un servicio de gestión de acceso inteligente que permite a los clientes llegar al equilibrio perfecto entre la comodidad del usuario y el acceso seguro a todas las aplicaciones de su organización.

## Principales beneficios



### Reducción del Coste Total de Propiedad (TCO)

- Aprovecha la infraestructura existente y reduce los gastos generales de gestión a través de la automatización.
- Implementa una autenticación multifactor fuerte que reduce la fatiga relacionada con las contraseñas y reduce los costos del servicio de asistencia.



### Mejora de la productividad

- Ofrece a los usuarios una experiencia de inicio de sesión único (SSO) cómoda y sin complicaciones
- Políticas de autenticación adaptativa que evalúan los riesgos y el equilibrio entre la conveniencia y la seguridad.



### Administración simplificada

- Elimina la integración compleja y garantiza una gestión fácil con un servicio en la nube que se puede configurar y ejecutar en un par de horas



### Protección completa

- Protege el acceso a Office 365 y todas las demás apps en la nube / web con un servicio de gestión de acceso único

<sup>1</sup> Source: Office 365 Adoption Rate, Stats, and Usage

SafeNet Trusted Access ofrece una gestión de acceso flexible a través de un motor de políticas fácil de usar que brinda a los clientes control en tiempo real sobre la capacidad de aplicar estrategias a nivel de usuario individual, grupo o aplicación. El motor de políticas admite una amplia gama de métodos de autenticación, incluidos los que ya están implementados, lo que permite a las organizaciones aprovechar sus inversiones actuales y usarlas para proteger los servicios en la nube y basados en la web.

Al combinar el SSO, estrategias basadas en el riesgo y métodos de autenticación universal, SafeNet Trusted Access brinda a las organizaciones el poder y la flexibilidad para proteger el acceso a todas las aplicaciones, simplificar la experiencia de inicio de sesión y administrar el riesgo de manera efectiva.

## Proteger el acceso a Office 365: ¿Cómo funciona?

SafeNet Trusted Access aprovecha las inversiones en infraestructura existentes y simplifica el proceso de implementación de controles de acceso para validar las identidades de los usuarios. A través de una integración SAML 2.0 simple basada en plantillas, SafeNet Trusted Access actúa como el proveedor de identidad confiable para Office 365 y otras aplicaciones basadas en la nube y en la web de terceros, brindando a los administradores de TI la capacidad de implementar fácilmente una solución de administración de acceso en todos sus entornos. SafeNet Trusted Access es un servicio basado en la nube que garantiza una implementación rápida y un mantenimiento sencillo, sin gastos administrativos adicionales ni cambios en las infraestructuras existentes.

## Acerca de las soluciones SafeNet de Identity & Access Management de Thales

Las soluciones de gestión de identidad y acceso de Thales permiten a las empresas administrar y asegurar de forma centralizada el acceso a las aplicaciones empresariales de TI, web y basadas en la nube. Utilizando un SSO basado en políticas y métodos de autenticación universal, las empresas pueden gestionar eficazmente los riesgos, cumplir con las normativas, obtener visibilidad de todos los eventos de acceso y simplificar la experiencia de inicio de sesión para sus usuarios.

### Características principales

- Una consola de gestión intuitiva permite a los administradores configurar y ajustar políticas para aplicaciones y grupos de usuarios de forma rápida y sencilla.
- Al optimizar la seguridad con la comodidad del usuario, los administradores pueden optar por aplicar la autenticación simple o de factores múltiples a través de estrategias de acceso definidas y pueden aplicar capas de opciones de autenticación para aumentar o reducir los requisitos donde sea necesario. Los usuarios pueden acceder a todas sus aplicaciones e iniciar una sesión de SSO desde un portal de aplicaciones personalizado.
- La solución admite numerosos métodos de autenticación que brindan a las organizaciones una amplia variedad de opciones para mitigar el riesgo. Las opciones de autenticación universal admitidas incluyen autenticadores fuera de banda (OOB) de tipo PUSH o SMS, autenticador basado en matriz (PIP), factores de forma de contraseña única (OTP) basada en hardware y software, autenticadores de terceros, autenticación basada en certificado PKI, y Kerberos.

