thalescpl.com

THALES

Los desafíos del acceso de confianza en el ámbito de la nube

Índice de Gestión de Acceso de Thales 2019

Resumen

#AMI2019

Índice

Introducción

Preocupaciones por los servicios en la nube como fuente de ataques cibernéticos

El auge de las identidades y las aplicaciones en la nube ha hecho que los responsables de TI busquen conciliar la velocidad de la nube con las necesidades en materia de seguridad, cumplimiento normativo y escalabilidad de sus empresas. Al mejorar la experiencia que ofrecen las aplicaciones comerciales generales a sus usuarios, las soluciones de gestión de acceso en la nube han surgido para abordar los desafíos multidisciplinares de este nuevo perímetro de identidad.

Tras realizar una encuesta a 1050 responsables de la toma de decisiones de TI de todo el mundo, el Índice de Gestión de Acceso 2019 de Thales reveló que casi la mitad (el 49 %) de las empresas creen que las aplicaciones en la nube las convierten en blanco de ataques cibernéticos. Las aplicaciones en la nube se encuentran entre las tres razones principales por las que una empresa podría sufrir un ataque, inmediatamente después de la infraestructura desprotegida, como los dispositivos de IoT (el 54 %) y los portales web (el 50 %).

Dado que las aplicaciones en la nube son actualmente una parte esencial de las operaciones empresariales diarias, la mayoría (el 97 %) de los directivos de TI considera que la gestión de acceso a la nube es necesaria para que sus empresas adopten servicios en la nube. Sin embargo, a pesar de que cuatro de cada 10 empresas (el 38 %) ya cuenta con un director de seguridad de la información, solo en uno de cada 10 (el 14 %) recae la decisión final sobre la gestión del acceso a la nube implementada en su empresa. De hecho, es más probable que las empresas confíen en una función tradicional de TI, como los directores de sistemas informáticos o CIO (el 48 %) cuando deben ocuparse de este tema. Esto sugiere una desconexión entre la toma de decisiones y la implementación en lo que respecta a la seguridad en la nube.

El rápido aumento de las aplicaciones y los servicios en la nube ha aportado muchas ventajas a las empresas; pero estas conclusiones muestran claramente que, sin la capacidad para proteger adecuadamente los servicios basados en la nube, las empresas se exponen a amenazas innecesarias en materia de seguridad. La tecnología cloud se ha generalizado tanto que su protección debe ser una práctica rutinaria para cualquier empresa. Sin embargo, si no hay un director de seguridad de la información especializado, las empresas pueden carecer del liderazgo necesario para implementar la estrategia o las soluciones de seguridad adecuadas para estar protegidas en la nube.

Aumento del presupuesto en seguridad debido a las filtraciones de datos

La creciente preocupación por las filtraciones de datos de los consumidores ha llevado a las empresas a tomar medidas para aumentar las inversiones en seguridad de TI. Casi todas (el 94 %) han cambiado sus políticas de seguridad en torno a la gestión de acceso en los últimos 12 meses. Es más, los aspectos más importantes de cambios se han centrado en formar al personal en materia de seguridad y gestión de acceso (el 52 %), en aumentar el gasto en gestión de acceso (el 45 %) y en hacer de la gestión de acceso una prioridad para las juntas directivas (el 44 %).

Obstáculos para lograr una gestión de acceso a la nube eficaz

A pesar de las actualizaciones de las políticas de seguridad, la mayoría de los líderes de TI (el 95 %) cree que la gestión ineficaz del acceso a la nube sigue siendo un tema de preocupación para su empresa. De hecho, sus mayores preocupaciones son su impacto en la seguridad (el 48 %), el tiempo del personal de TI (el 44 %) y los gastos operativos generales y de TI (el 43 %). Peor aún, cuando se trata de implementar soluciones de gestión de acceso, los mayores obstáculos mencionados fueron los costes (el 40 %), el error humano (el 39 %) y la dificultad para integrarlas (el 36 %).

Cuando se trata de soluciones en la nube, tres cuartas partes (el 75 %) de las empresas ya confían en la gestión de acceso para proteger los inicios de sesión de sus usuarios externos a los recursos corporativos en línea. En concreto, la autenticación de dos factores (el 58 %) es la herramienta que se considera más eficaz para proteger las aplicaciones en la nube y basadas en la web, seguida de la autenticación inteligente de inicio de sesión único o smart SSO (el 49 %) y la autenticación biométrica (el 47 %).

Principales conclusiones

Los servicios en la nube son objetivo de los ataques cibernéticos

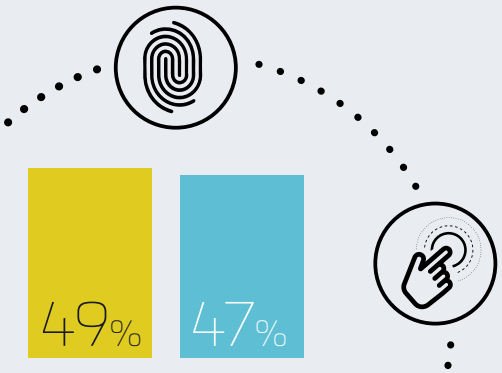
49%

de las empresas considera que las aplicaciones en la nube son el principal objetivo de los ataques cibernéticos

Principales tecnologías de gestión de acceso

58%

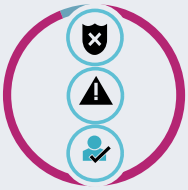
considera que la autenticación de dos factores es la herramienta de gestión de acceso que mejor puede proteger las aplicaciones en la nube y basadas en la web



...mientras que el 49 % considera que es la autenticación inteligente de inicio de sesión único y el 47 % cree que es la autenticación biométrica

Principales conclusiones

Las brechas de datos llevan a la adopción de la gestión de acceso



94%

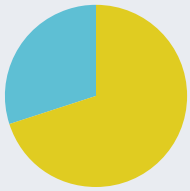
de las políticas de seguridad de las empresas se ha visto influido por filtraciones de datos de consumidores en los últimos 12 meses

62%

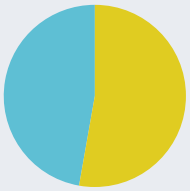
de las empresas sigue operando sin un director de seguridad de la información, a pesar de haber aumentado la preocupación por la ciberseguridad

La gestión de acceso es fundamental para la transformación a la nube

36% utiliza la autenticación inteligente de inicio de sesión único (Smart SSO)



70% utiliza la autenticación de dos factores



53% utiliza la autenticación de inicio de sesión único (SSO)

97%

afirma que la gestión de acceso a la nube para las aplicaciones en la nube favorece la adopción de la nube

95%

considera que una gestión de acceso a la nube ineficaz causa o puede causar problemas a su empresa

Contexto de la gestión de acceso

Como resultado de la realidad de las brechas de datos y la adopción de identidades sociales y en la nube por parte de las empresas, el nuevo perímetro de TI hace que los responsables de la toma de decisiones deban reconsiderar su estrategia de gestión de TI. Motivadas por la comodidad que brinda a los consumidores combinar el inicio de sesión único con políticas basadas en los riesgos, las prácticas de gestión de acceso evolucionan para establecer un puente entre los ámbitos social, móvil y en la nube.

Más de la mitad (el 54 %) de los responsables de TI entrevistados afirman que la infraestructura desprotegida representa una de las principales razones por las que se sufren ataques cibernéticos, mientras que aproximadamente la mitad lo achaca a los portales web (el 50 %) o las aplicaciones en la nube (el 49 %). La seguridad resulta fundamental para las empresas, ya que estas suelen luchar contra más de un motivo de ataques cibernéticos.

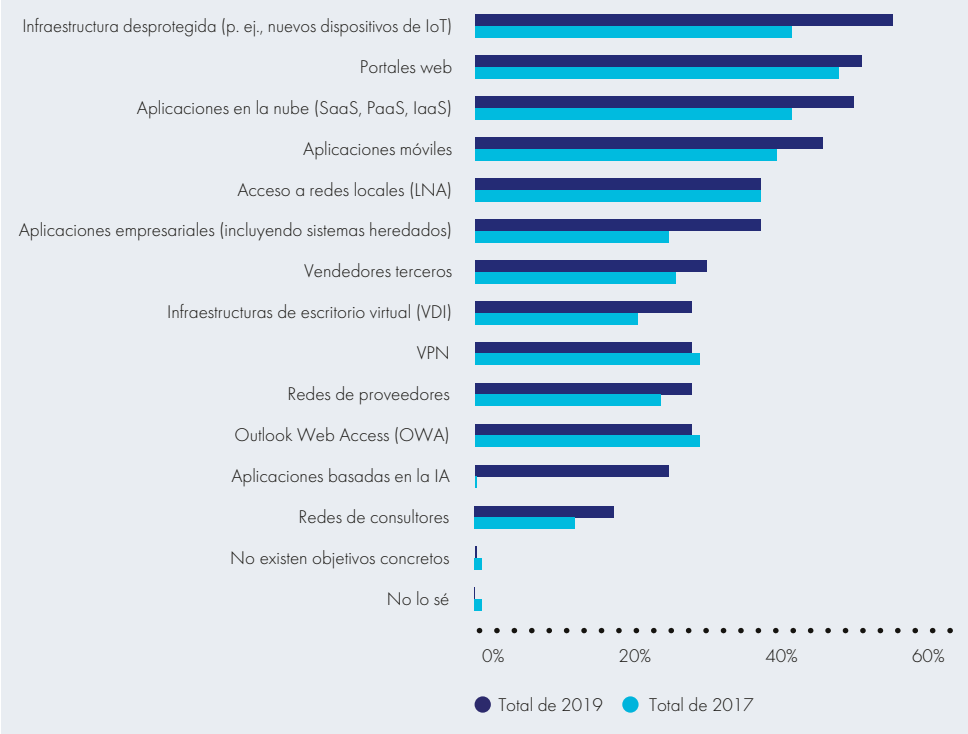


Figura 1
"En general, ¿cuáles de las siguientes opciones considera que son los principales objetivos de los ataques cibernéticos?", repartido entre los datos históricos y preguntado a todos los encuestados (1050 encuestados)

Casi todos los encuestados (el 94 %) afirman que las políticas de seguridad relacionadas con la gestión de acceso de sus empresas se han visto influidas por las filtraciones en los servicios prestados a los consumidores en los últimos 12 meses. A pesar de este enfoque, tres de cada cinco encuestados (el 56 %) permiten que los empleados inicien sesión en los recursos corporativos con las credenciales de redes sociales, a pesar de tener presente recientes filtraciones de seguridad.

Parece ser que se está produciendo actualmente un cambio de percepción en cuanto a la importancia de la seguridad de TI. Más de un tercio de los encuestados (el 36 %) indica que le resultó difícil convencer a la junta directiva de la necesidad de implantar seguridad de TI hace un año, mientras que solo el 20 % afirma estar pasando por este proceso en la actualidad.

Tendencias en la gestión de acceso a la nube

Las empresas están experimentando una mayor presión para implementar una solución de gestión de acceso a la nube. La inmensa mayoría declara que los principales factores que motivan esta implementación son las preocupaciones en materia de seguridad y la amenaza de filtraciones a gran escala. Con la gestión de acceso, los usuarios conservan una única identidad para todos los recursos gracias a la autenticación de inicio de sesión único SSO en la nube, y protegen esa identidad a través de políticas basadas en los riesgos y la autenticación de dos factores. Esto permite a las empresas proteger el acceso a los servicios basados en la nube sin sacrificar la velocidad.

Al ser preguntados por las mejores herramientas de gestión de acceso para proteger las aplicaciones en la nube y basadas en la web, casi tres de cada cinco encuestados (el 58 %) indica que la autenticación de dos factores es una de las mejores opciones, seguida de la autenticación inteligente de inicio de sesión único (el 49 %) y la autenticación biométrica (el 47 %).
Casi todos los encuestados (el 97 %) consideran que la gestión de acceso a la nube para las aplicaciones web y en la nube es un factor que favorece la adopción de la nube. Además, el 75 % de las empresas de los encuestados protege el acceso de los usuarios externos a los recursos corporativos en línea mediante la gestión de acceso, lo que demuestra que esta puede repercutir más allá del ámbito exclusivo de los usuarios inmediatos.

Aunque la autenticación aporta ventajas, el 96 % de los encuestados admite que existen desafíos para la autenticación y seguridad basadas en la nube. Los desafíos más destacados son el coste de las soluciones de seguridad (el 40 %) y el error humano en la gestión de las soluciones (el 39 %). Asimismo, casi todos (el 95 %) afirman que una gestión de acceso a la nube ineficaz por parte de sus empresas afecta o puede afectar a sus recursos web/en la nube.

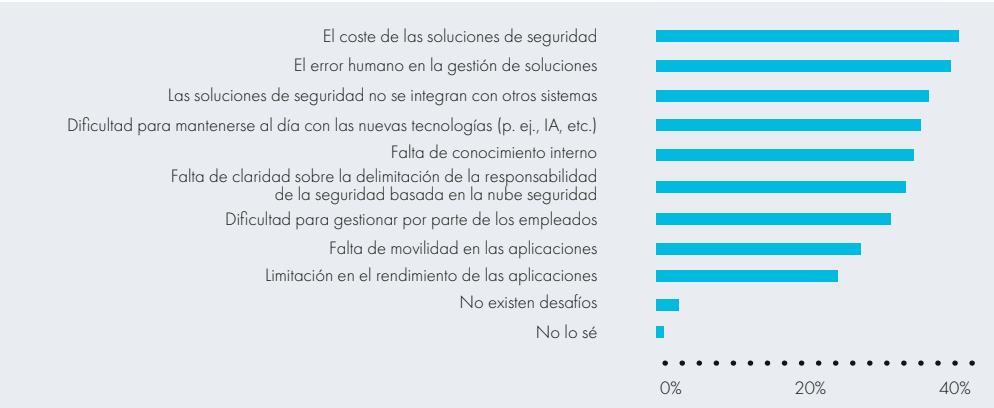


Figura 2
"¿Cuáles considera que son los desafíos de la autenticación y la seguridad basadas en la nube?", preguntado a todos los encuestados (1050 encuestados)

Autenticación inteligente de inicio de sesión único (smart SSO)

La autenticación inteligente de inicio de sesión único, o smart Single Sign-On, permite a los usuarios iniciar sesión en todas las aplicaciones en la nube con una misma identidad, eliminando la necesidad de recordar varias contraseñas, la frustración, los restablecimientos de contraseñas y el tiempo de inactividad, al tiempo que se garantiza la protección del acceso en todo momento. El uso inteligente del inicio de sesión único, basado en autenticaciones previas en la misma sesión SSO y en la política contextual específica para cada intento de acceso, permite a los usuarios autenticarse solo una vez para acceder a todas las aplicaciones en la nube, así como realizar autenticaciones adicionales cuando resulte necesario.

De media, el 23 % de los empleados de las empresas de los encuestados utilizan la autenticación inteligente de inicio de sesión único. Sin embargo, este porcentaje podría aumentar hasta el 46 % en el plazo de dos años, ya que, a pesar de todavía no ser un método de autenticación habitual en las empresas, parece que lo será en el futuro. Además, el 96 % de los encuestados afirma que le gustaría ver implementada una solución de autenticación inteligente de inicio de sesión único (smart SSO). Esta tendencia a adoptar este tipo de autenticación se ve reflejada en que casi todos los encuestados (el 97 %) consideran que el uso de la autenticación inteligente de inicio de sesión único aporta o puede aportar ventajas a sus empresas. Las ventajas más probables son la sensación de que se protegen los datos de los empleados (el 54 %) o de los clientes (el 52 %), y la prevención de filtraciones de datos (el 50 %).

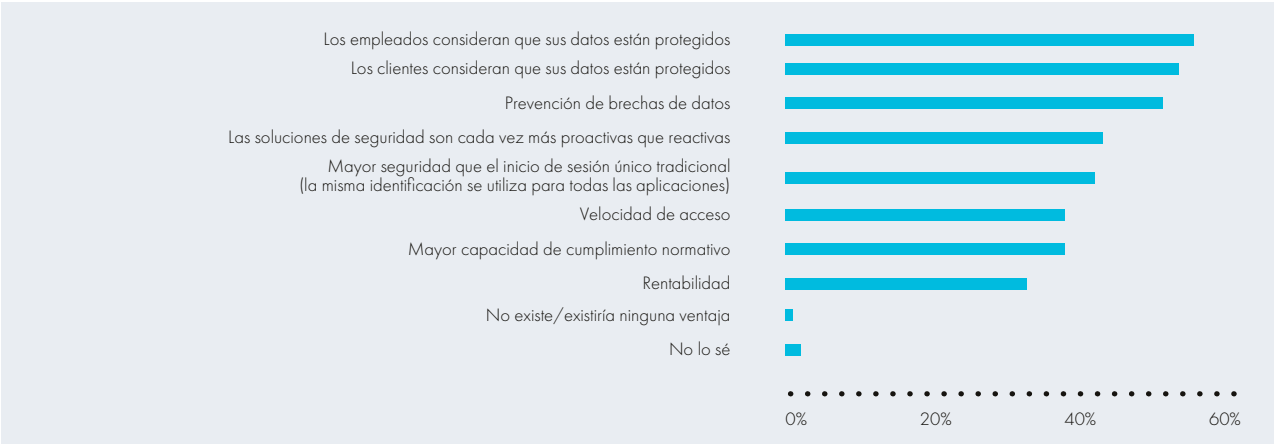


Figura 3
"¿Cuáles son o serían las ventajas que el uso de la autenticación inteligente de inicio de sesión único aporta o puede aportar a su empresa?", preguntado a todos los encuestados (1050 encuestados)

Esta tendencia a adoptar este tipo de autenticación se ve reflejada en que casi todos los encuestados (el 97 %) consideran que el uso de la autenticación inteligente de inicio de sesión único aporta o puede aportar ventajas a sus empresas. Las ventajas más probables son la sensación de que se protegen los datos de los empleados (el 54 %) o de los clientes (el 52 %), y la prevención de brechas de datos (el 50 %).

Tendencias en la autenticación de dos factores

La autenticación de dos factores forma parte integral de la gestión de acceso, ya que sirve como primera línea de defensa frente a filtraciones de datos, por lo que se espera que aumente su uso en todos los ámbitos de las empresas en los próximos dos años. La mayoría de los líderes de TI gestionan la autenticación de dos factores de manera centralizada para todas sus aplicaciones empresariales, ya sea en la nube, redes privadas virtuales, entornos de escritorios virtuales, portales web o aplicaciones móviles.

Aproximadamente ocho de cada diez encuestados (el 81 %) afirman que sus empresas utilizan la autenticación de dos factores para proteger las aplicaciones móviles, mientras que un porcentaje similar lo hace para proteger las aplicaciones empresariales (el 81 %) o las aplicaciones en la nube (el 85 %). Se prevé que este uso aumente, ya que el 96 % espera que se extienda el empleo de la autenticación de dos factores por parte de sus empresas en el futuro. Esto podría no tardar en producirse, ya que más de tres de cada cinco (el 61 %) afirma que su uso aumentará en el plazo de un año.

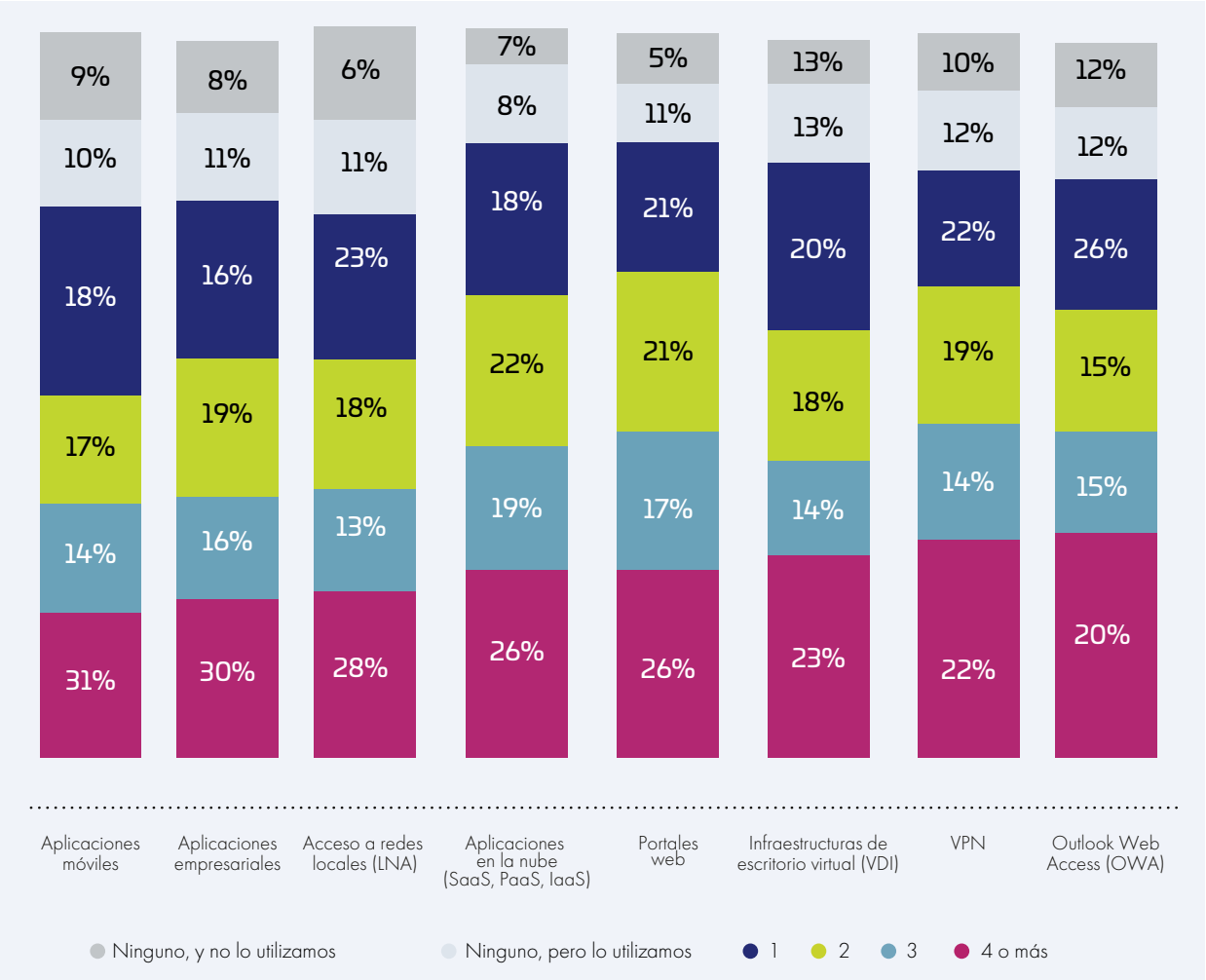


Figura 4
"¿Cuántas de las aplicaciones anteriores están protegidas actualmente por una autenticación de dos factores en su empresa?", preguntado a todos los encuestados (1050 encuestados)

De manera positiva para las empresas, más de nueve de cada diez encuestados (el 94 %) considera que la autenticación de dos factores para las aplicaciones en la nube facilita la adopción de la nube. Pero, además de aumentar los niveles de seguridad, la autenticación de dos factores también contribuye a allanar el camino para la adopción de la nube.

Consideraciones clave

Si bien las organizaciones se están familiarizando con las soluciones de gestión de acceso, los responsables de TI y de la toma de decisiones empresariales deben asegurarse de que entienden los riesgos de sus soluciones en la nube con el fin de implementar las soluciones pertinentes. Estas soluciones deben prescindir de perímetros, ser compatibles con un modelo de tipo zero-trust, además de ser flexibles y adaptables, para aprovechar al máximo tecnologías punteras como la autenticación inteligente de inicio de sesión único (smart SSO). Sin herramientas eficaces de gestión de acceso, las empresas se enfrentan a un mayor riesgo de filtraciones y a falta de visibilidad, además de incurrir en gastos adicionales debido a una nube mal optimizada. Entre las consideraciones clave que se extraen del informe de este año, se incluyen las siguientes:

- Casi tres de cada cinco encuestados (el 56 %) declaran que permitirían a los empleados de su empresa iniciar sesión en los recursos corporativos con las credenciales de redes sociales.
- El 94 % de los profesionales de TI afirma que las políticas de seguridad relacionadas con la gestión de acceso de sus empresas se han visto influidas por las brechas en servicios para consumidores en los últimos 12 meses.
- Un porcentaje importante las empresas de los encuestados ha adoptado soluciones de gestión de identidad y acceso (el 62 %), de identidad como servicio o IDaaS (el 58 %), de inicio de sesión único en la nube (el 54 %) o de autenticación inteligente de inicio de sesión único o smart SSO (el 46 %). Solo el 20 % de los profesionales de TI afirma que actualmente resulta difícil convencer a la junta directiva de la necesidad de implantar seguridad de TI.
- Casi la mitad de los profesionales de TI (el 49 %) considera que la autenticación inteligente de inicio de sesión único es la mejor herramienta de gestión de acceso para proteger las aplicaciones y los servicios en la nube y basadas en la web.
- En el plazo de dos años, prácticamente la mitad de los usuarios de las empresas utilizarán la autenticación inteligente de inicio de sesión único (smart SSO).

Acerca de Thales

Las personas a las que confía la protección de su privacidad confían en Thales para proteger sus datos. Las empresas se enfrentan a un número cada vez mayor de momentos decisivos relacionados con la seguridad de los datos. Tanto si se trata de elaborar una estrategia de cifrado, migrar a la nube o cumplir los requisitos normativos, puede confiar en Thales para proteger su proceso de transformación digital.

Tecnología decisiva para momentos decisivos

THALES

Continente americano
2860 Junction Avenue, San Jose, CA 95134, EE. UU.
Tel.: +1 888 744 4976 o +1 954 888 6200
Fax: +1 954 888 6211 | Correo electrónico: sales@thalesesec.com

Asia-Pacífico
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel.: +852 2815 8633
Fax: +852 2815 8141 | Correo electrónico: asia.sales@thales-esecurity.com

Europa, Oriente Medio y África
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ, Reino Unido
Tel.: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
Correo electrónico: emea.sales@thales-esecurity.com

> thalescpl.com <