wallix

WALLIX Guide

Cómo proteger a la empresa frente a los ataques basados en identidades



Cómo proteger a la empresa frente a los ataques basados en identidades

1. Introducción

La seguridad de identidades es la disciplina encargada de proteger las identidades digitales: las cuentas, credenciales y permisos mediante los que personas, máquinas y servicios acceden a los sistemas de una organización. Es fundamental porque la identidad se ha convertido en una de las principales superficies de ataque. Hoy en día, muchas brechas de seguridad ya no empiezan cuando un atacante consigue atravesar el perímetro, sino con el robo de unas credenciales, una sesión comprometida mediante phishing o el uso indebido de una cuenta con privilegios excesivos.

El robo de credenciales y el phishing siguen siendo dos de los principales puntos de entrada y, cada vez más, consiguen eludir formas básicas de MFA mediante técnicas de adversary-in-the-middle. Una vez dentro, los atacantes aprovechan permisos excesivos o cuentas inactivas para desplazarse lateralmente por los sistemas y escalar privilegios. A esto se suma un problema de escala: en la mayoría de las organizaciones, las identidades no humanas (cuentas de servicio, claves de API o conexiones máquina a máquina) ya superan en número a las identidades humanas, a menudo sin una gestión adecuada ni revisiones periódicas. Cada identidad sin verificar y cada permiso innecesario supone un riesgo permanente.



Ilustración 1 Cómo se desarrolla un ataque basado en la identidad

Si los ataques comienzan en la identidad, la defensa debe empezar por controlar el acceso. Ese es el papel de Identity Access: la capa operativa de la seguridad de identidades que verifica quién se conecta, determina cómo debe autenticarse y controla qué puede hacer, de forma continua y no únicamente en el momento de iniciar sesión. Antes de plantearse controles avanzados o un mayor nivel de madurez en la gobernanza, cualquier organización necesita contar con esta base: autenticación robusta, acceso basado en el principio de mínimo privilegio y un ciclo de vida de las identidades gestionado desde su incorporación hasta su salida.

2. Los principales retos para las organizaciones

2.1 Proliferación y fragmentación de identidades

Pocos entornos de identidad son el resultado de una planificación deliberada. Lo habitual es que hayan ido creciendo con el tiempo en función de las necesidades de la organización en cada momento: una nueva aplicación, una plataforma cloud, una adquisición que incorpora su propio directorio y sus propias normas para conceder accesos. Tras años de crecimiento, el resultado suele ser lo que se conoce como identity sprawl o proliferación de identidades: un mismo empleado con una docena de cuentas desconectadas entre sí, permisos distribuidos entre sistemas que no comparten información y ninguna forma fiable de responder a una pregunta tan básica como quién tiene acceso a qué.



Ilustración 2 Proliferación de identidades: un empleado, una docena de cuentas desconectadas

Los riesgos asociados a esta proliferación son bien conocidos y, en su mayoría, parten del mismo problema: la gestión no está centralizada. La baja de usuarios debe hacerse sistema por sistema, por lo que es habitual que algunas cuentas sigan activas después de que el empleado haya dejado la empresa. Los accesos se van acumulando a medida que las personas cambian de puesto, ya que los permisos se conceden cuando hacen falta, pero rara vez se revisan posteriormente. Ante decenas de inicios de sesión diferentes, los usuarios terminan reutilizando contraseñas porque resulta imposible mantener tantas credenciales únicas y seguras. Al mismo tiempo, las identidades no humanas (cuentas de servicio, claves de API, credenciales de integración, **agentes de IA y otras identidades de máquina**) crecen más rápido que cualquier otra categoría, muchas veces creadas fuera de la visibilidad de los equipos de IT y funcionando durante años con credenciales estáticas.

La fragmentación hace que todos estos problemas sean todavía más difíciles de resolver. Cuando cada sistema aplica la autenticación por separado, el nivel general de seguridad termina siendo el del sistema más débil: basta con una única aplicación legacy sin MFA para crear una brecha. Cuando las políticas de acceso se gestionan desde consolas diferentes, mantenerlas alineadas se convierte en un proceso manual y, al preparar una auditoría, hay que reconstruir la información sistema por sistema. Los equipos de seguridad terminan siendo responsables de una

superficie de ataque de la que solo tienen una visión parcial, y son precisamente esas zonas de conexión entre sistemas las que suelen buscar los atacantes.

Además, la proliferación de identidades no adopta siempre la misma forma. La mayoría de los entornos son híbridos por necesidad y combinan aplicaciones cloud con infraestructuras on-premises. En sectores regulados o especialmente sensibles a la soberanía digital, también existen sistemas que no pueden salir del propio perímetro de la organización. Por tanto, una estrategia seria frente a la fragmentación de identidades debe abarcar todo el entorno, no solo las partes más fáciles de conectar.

2.2 Los ataques contra las credenciales se han industrializado

El phishing ya no es una actividad minoritaria ni reservada a atacantes con grandes conocimientos técnicos. Las plataformas de phishing-as-a-service proporcionan infraestructura lista para utilizar con la que imitar páginas corporativas de inicio de sesión, capturar credenciales y eludir algunas formas habituales de autenticación multifactor. Servicios como Tycoon 2FA han permitido utilizar estas capacidades a gran escala, reduciendo la barrera técnica para los atacantes y convirtiendo técnicas avanzadas de phishing en servicios disponibles comercialmente.

Una evolución especialmente relevante es el phishing mediante adversary-in-the-middle (AiTM). En un ataque AiTM, el atacante coloca un proxy entre el usuario y el servicio legítimo de autenticación. La víctima completa el proceso de inicio de sesión real, incluido cualquier código de un solo uso o aprobación mediante notificación push, mientras el atacante captura el token o la cookie de sesión resultante. Esto puede permitirle acceder a la cuenta sin volver a pasar por el proceso de autenticación, incluso cuando se utiliza una forma convencional de MFA. Microsoft registró un aumento del 146 % en los ataques de phishing AiTM observados durante 2024.



Ilustración 3 Anatomía de un ataque de adversario en el medio: la MFA se completa y, aun así, se elude

Otras formas de MFA también tienen limitaciones. Las notificaciones push pueden explotarse mediante solicitudes de aprobación repetidas, mientras que las contraseñas de un solo uso pueden interceptarse o retransmitirse en tiempo real. Por tanto, la cuestión no es únicamente si se utiliza MFA, sino si el método de autenticación es resistente al phishing. Los métodos basados en secretos compartidos, códigos o aprobaciones del usuario ofrecen un nivel de protección muy diferente al de métodos criptográficos como las llaves de seguridad FIDO2 y las passkeys.

Aun así, el uso indebido de credenciales sigue siendo una vía importante de acceso a los entornos corporativos. El Data Breach Investigations Report 2026 de Verizon concluyó que las credenciales robadas representaban el 13 % de la actividad observada de acceso inicial. Cuando un atacante entra utilizando una identidad legítima, sus acciones pueden parecer inicialmente las de un usuario autorizado, lo que dificulta distinguir una actividad sospechosa del comportamiento habitual.

2.3 Presión regulatoria

Los reguladores de los principales mercados convergen cada vez más en una misma exigencia: las organizaciones deben poder demostrar quién tiene acceso a sus sistemas y probar que ese acceso está bajo control. En Europa, NIS2 amplía las obligaciones de ciberseguridad a un mayor número de sectores e incluye el control de acceso y la autenticación multifactor entre las medidas que pueden tener que implantar las entidades afectadas. Al mismo tiempo, DORA exige a las entidades financieras reforzar la gestión del riesgo TIC, incluidos los controles de acceso, las cuentas privilegiadas y los accesos de terceros. El RGPD sigue exigiendo una protección adecuada de los datos personales, por lo que contar con una gestión

documentada de los accesos, realizar revisiones periódicas de permisos y dar de baja las cuentas a tiempo son controles relevantes para el cumplimiento normativo.

Este mismo patrón se repite fuera de Europa. En Estados Unidos, SOX y HIPAA exigen controles de acceso demostrables en sus respectivos sectores, mientras que las directrices federales de Zero Trust están impulsando a organismos públicos y proveedores hacia el uso de MFA resistente al phishing. En Reino Unido, el RGPD británico convive con las normas de resiliencia operativa de la FCA y con Cyber Essentials, que establece requisitos de control de acceso y MFA para acceder a numerosos contratos con el sector público. En Oriente Medio, las normativas de protección de datos, como la PDPL de Arabia Saudí, están evolucionando rápidamente, y organismos como SAMA establecen requisitos específicos de identidad para el sector financiero. Asia-Pacífico sigue una evolución similar, desde la APPI de Japón y la PDPA de Singapur hasta las directrices de MAS sobre acceso privilegiado. Por encima del ámbito nacional, PCI DSS e ISO 27001 acompañan a las empresas allí donde operan, convirtiendo la gestión de accesos en una exigencia contractual además de regulatoria.



Ilustración 4 Marcos diferentes, una expectativa común

Cada marco tiene su propio alcance y sus propios plazos. Pero, vistos en conjunto, todos apuntan en la misma dirección: los controles de identidad y acceso ya no son simplemente una decisión interna de seguridad, sino una obligación externa que las organizaciones deben poder demostrar cuando se les requiera.

2.4 La trampa de la experiencia de usuario

Por último, cuando los controles de seguridad generan demasiada fricción, los usuarios tienden a buscar formas de evitarlos. Las solicitudes frecuentes de autenticación fomentan los atajos. Los requisitos de contraseña demasiado complejos llevan a reutilizar contraseñas, crear variaciones predecibles o almacenarlas de forma insegura. Y los procesos lentos para solicitar acceso aumentan la probabilidad de que se compartan credenciales o se utilicen soluciones alternativas no gestionadas.

No es simplemente una cuestión de disciplina por parte de los usuarios, sino un problema de diseño. La seguridad del acceso de los empleados funciona mejor cuando la opción más segura es también la más sencilla. Los usuarios deberían poder autenticarse una sola vez, acceder a las aplicaciones necesarias para su función, utilizar factores más rápidos y seguros que las contraseñas y resolver las necesidades habituales de acceso sin retrasos innecesarios. Una solución que considere la usabilidad como algo secundario terminará generando precisamente los comportamientos que pretende evitar.



Ilustración 5 La fricción genera el comportamiento que pretendía evitar; elimínala desde el diseño

3. Sectores donde estos retos son más críticos

Estos desafíos afectan a la mayoría de las organizaciones, pero resultan especialmente importantes en sectores que combinan entornos complejos, sistemas sensibles y estrictos requisitos regulatorios.

Sector público y administraciones

Las administraciones públicas utilizan entornos de aplicaciones amplios y heterogéneos, que van desde servicios cloud modernos hasta sistemas que llevan décadas en funcionamiento. El acceso a estos sistemas se reparte entre ministerios, organismos y administraciones locales, a menudo sujetos a requisitos estrictos de auditoría, soberanía y control sobre dónde se almacenan los datos de identidad.

Para estas organizaciones, la prioridad es ofrecer una autenticación coherente en todo el entorno de aplicaciones, implantar métodos de autenticación robustos de acuerdo con los requisitos aplicables al sector público y mantener bajo su control un registro completo de la actividad de acceso.

Infraestructuras críticas e industria

Los operadores de los sectores de energía, transporte, agua, fabricación y otros ámbitos industriales deben proteger entornos en los que la disponibilidad es esencial. Pueden trabajar con redes de tecnología operacional segregadas, ubicaciones remotas con conectividad limitada y sistemas legacy difíciles de sustituir o modificar.

En estos entornos, la autenticación debe seguir funcionando de forma fiable sin depender por completo de servicios externos. Además, debe integrarse con los sistemas industriales y legacy existentes y generar los registros necesarios para auditorías y supervisión regulatoria. El objetivo es ofrecer una autenticación coherente de los empleados en oficinas, plantas y ubicaciones remotas sin introducir una dependencia operativa inaceptable.

Servicios financieros

Las entidades financieras están sujetas a amplios requisitos relacionados con la gestión del riesgo TIC, la resiliencia y la supervisión de terceros. Empleados, contratistas, proveedores de servicios y partners tecnológicos pueden necesitar acceso controlado a sistemas sensibles.

Un enfoque eficaz debe tener en cuenta todas las identidades, aplicar los métodos de autenticación adecuados, restringir y supervisar los accesos privilegiados y de terceros, y permitir aportar evidencias cuando sea necesario. El objetivo no es únicamente impedir accesos no autorizados, sino también demostrar que los accesos se gestionan de forma continua.

4.2 Una autenticación preparada frente a los ataques actuales

La autenticación multifactor exige que los usuarios presenten factores de distintas categorías, como algo que conocen, algo que poseen o algo que son. Esto dificulta que una cuenta se vea comprometida, pero el nivel de protección depende en gran medida de los factores utilizados.

Las contraseñas de un solo uso pueden interceptarse o retransmitirse. Las notificaciones push pueden terminar aprobándose tras múltiples solicitudes o mediante técnicas de ingeniería social. Los ataques adversary-in-the-middle pueden interponerse en una sesión de autenticación legítima y capturar el token de sesión resultante, incluso cuando se utilizan determinadas formas de MFA. Por tanto, utilizar MFA no garantiza por sí solo protección frente al phishing.

La autenticación resistente al phishing permite abordar esta debilidad. Los métodos FIDO2 y WebAuthn, incluidas las llaves de seguridad físicas y las passkeys, vinculan la autenticación al servicio legítimo mediante criptografía de clave pública. No existe ningún código reutilizable ni secreto compartido que el usuario pueda revelar en una página fraudulenta. La autenticación basada en certificados, incluidas las tarjetas inteligentes, proporciona una protección similar y sigue estando ampliamente implantada en administraciones públicas, defensa y otros entornos con elevados requisitos de seguridad.

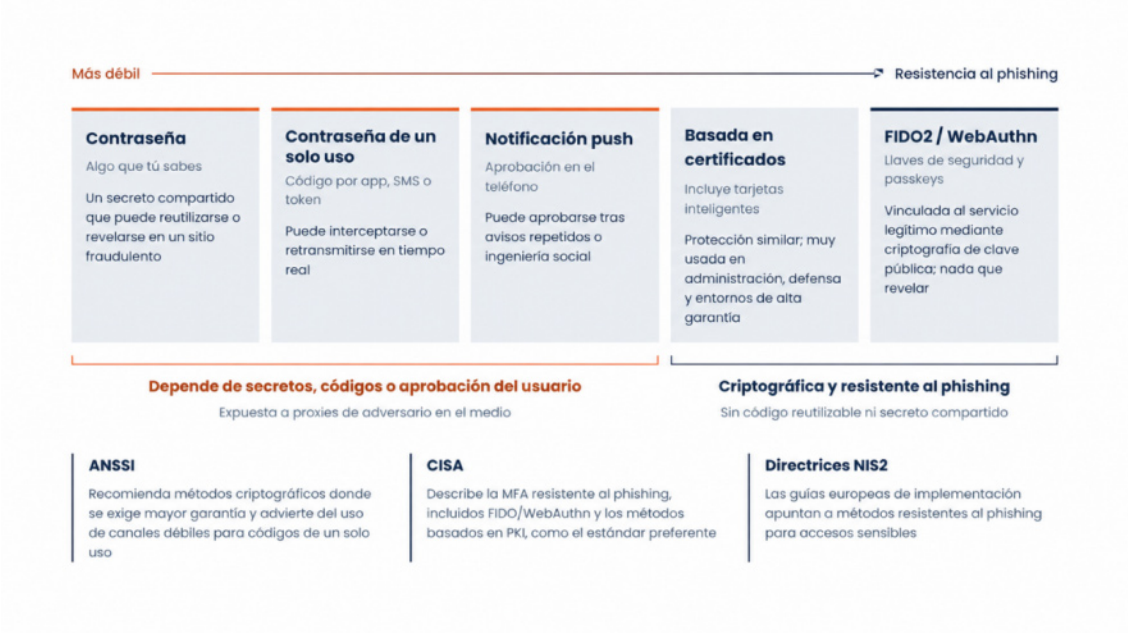


Ilustración 7 No todos los métodos de MFA son iguales: cómo se posicionan los métodos más comunes frente al phishing

Las recomendaciones regulatorias y técnicas reconocen cada vez más esta diferencia. ANSSI recomienda métodos de autenticación criptográfica cuando se necesita un mayor nivel de garantía y advierte de los riesgos de utilizar canales más débiles para los códigos de un solo uso. CISA considera la MFA resistente al phishing, incluidos FIDO/WebAuthn y la autenticación basada en PKI, como el estándar recomendado. Las directrices europeas relacionadas con la implantación de NIS2 también orientan a las organizaciones hacia métodos resistentes al phishing para proteger accesos sensibles.

El despliegue debe realizarse en función del nivel de riesgo. Los administradores, usuarios privilegiados y usuarios que acceden a sistemas críticos deberían ser los primeros en adoptar estos métodos, para después ampliar su uso a medida que los dispositivos y procesos lo permitan. La solución debe facilitar esta evolución mediante un marco de políticas común, sin exigir una migración inmediata en toda la organización.

4.3 Federación sobre la infraestructura existente, sin tener que sustituirla

Las organizaciones llevan años invirtiendo en sus infraestructuras de directorio. Active Directory y LDAP contienen el registro de referencia de quién trabaja en la empresa, dónde y con qué función, y están integrados en multitud de procesos de RR. HH., IT y seguridad. Una solución de acceso para empleados que obligue a abandonar esta base parte con una desventaja desde el principio.

Lo que se necesita es federación: la solución utiliza los directorios existentes como fuentes de identidad de referencia, se sincroniza con ellos y amplía su alcance a las aplicaciones mediante protocolos estándar: SAML y OpenID Connect para aplicaciones web modernas, RADIUS para equipos e infraestructuras de red y SCIM para automatizar el aprovisionamiento de usuarios en servicios compatibles. Las identidades, grupos y estructuras organizativas existentes se mantienen intactos y todo el entorno de aplicaciones, incluidos los sistemas que nunca fueron diseñados para la federación, pasa a estar accesible a través de una única capa de autenticación.



Ilustración 8 La federación amplía los directorios que ya tienes mediante protocolos estándar

Este enfoque también permite llevar a cabo un despliegue realista dentro de los plazos de cumplimiento normativo. Cuando existen fechas límite, no hay margen para migraciones de directorios que duren varios años. Una solución que se integra sobre la infraestructura actual puede aplicar una autenticación robusta en todo el entorno en cuestión de meses.

4.4 Gestión del ciclo de vida de las identidades sin carga manual

Toda identidad tiene un ciclo de vida: incorporación, cambios de función y salida. Cada una de estas etapas puede provocar que los accesos se desvíen progresivamente de lo que deberían ser. La solución debe permitir gestionar todo este ciclo desde un único punto: crear las cuentas desde el primer día con los accesos correspondientes a cada función, ajustar los permisos cuando cambie el puesto y revocar todos los accesos cuando la persona abandone la organización.

La administración aplicación por aplicación se sustituye por políticas centralizadas basadas en grupos y roles.

De este modo se evitan dos de los problemas habituales de la administración manual: la acumulación progresiva de privilegios y las cuentas huérfanas que siguen activas después de que sus propietarios hayan abandonado la organización. Además, un coste operativo recurrente pasa a convertirse en un proceso

gobernado: los accesos que tiene una persona son los que corresponden a su función y pueden demostrarse en cualquier momento.

4.5 Evidencias de auditoría integradas

Todas las normativas mencionadas en este documento terminan planteando las mismas preguntas: ¿quién tiene acceso a qué?, ¿cómo se protege ese acceso? y ¿puedes demostrarlo? Una solución de acceso para empleados debe poder responder a estas preguntas a partir de sus propios registros: logs completos de autenticación, una visión actualizada de los permisos de cada usuario sobre cada aplicación e informes preparados para los auditores, no únicamente para los administradores.

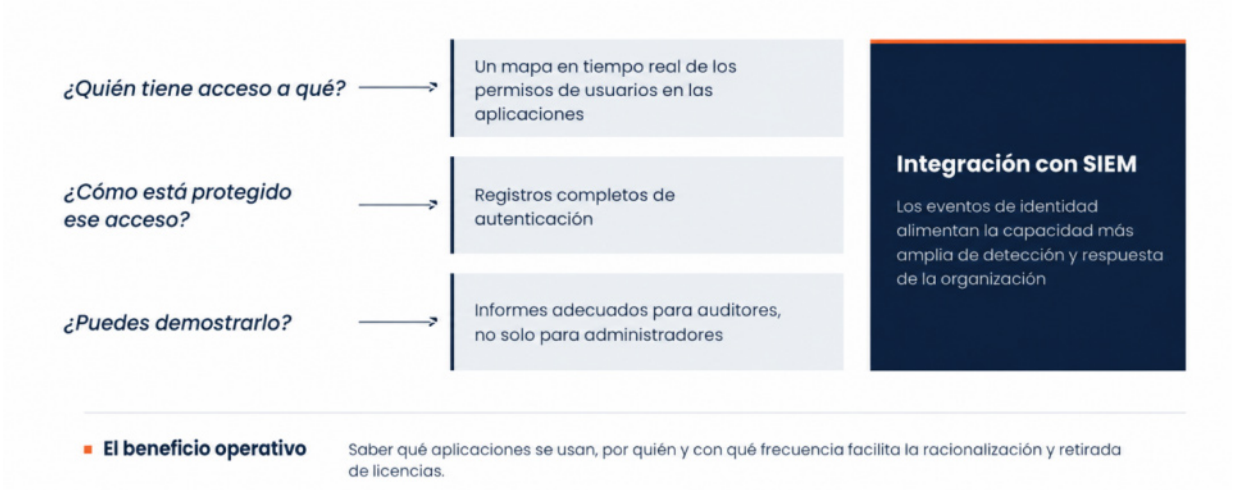


Ilustración 9 Las tres preguntas del auditor, respondidas a partir de los propios registros de la solución

La integración con plataformas SIEM permite incorporar los eventos relacionados con identidades a las capacidades generales de detección y respuesta de la organización.

Más allá del cumplimiento normativo, esta visibilidad también aporta ventajas operativas. Saber qué aplicaciones se utilizan realmente, quién las utiliza y con qué frecuencia proporciona a los equipos de IT la información necesaria para optimizar licencias y retirar aquellas herramientas que la organización ya no necesita.

5. Una plataforma, el modelo de despliegue que necesitas

Las capacidades descritas anteriormente definen qué debe hacer una solución de acceso para empleados. El lugar donde se ejecuta es una decisión diferente, que depende del contexto regulatorio, la infraestructura y el nivel de riesgo de cada organización, no de las funcionalidades de la propia solución.

Como servicio (SaaS).

La opción más rápida para empezar a utilizar estas capacidades: no necesitas desplegar infraestructura, el proveedor se encarga de la operación y las actualizaciones y el escalado se realiza de forma transparente. Está pensado para organizaciones que quieren disponer de seguridad para el acceso de sus empleados en cuestión de semanas y prefieren consumir el servicio en lugar de gestionarlo directamente.

Como appliance on-premises.

Las mismas capacidades, desplegadas dentro de la infraestructura de la propia organización. Los datos de identidad, los flujos de autenticación y los logs permanecen completamente bajo tu control: dentro de tu perímetro, tu jurisdicción y tu responsabilidad operativa. Está pensado para organizaciones con requisitos de soberanía, licitaciones reguladas que no permiten servicios de identidad prestados desde la nube y entornos industriales, aislados (air-gapped) o con conectividad limitada, en los que la autenticación debe seguir funcionando sin depender de servicios externos.

Hay dos preguntas que determinan qué modelo es el adecuado. ¿Dónde deben almacenarse los datos de identidad? Si la normativa, las políticas internas o la sensibilidad de las operaciones exigen que las identidades permanezcan bajo el control directo de la organización, el appliance ofrece una respuesta estructural a una cuestión que las garantías contractuales solo pueden resolver parcialmente. ¿Qué situaciones debe ser capaz de soportar la autenticación? Si el entorno debe seguir funcionando aunque se pierda la conectividad externa (por ejemplo, una planta industrial, un barco o una red clasificada), la autenticación no puede depender de la disponibilidad de un servicio cloud.

Ninguno de los dos modelos supone una renuncia. Son dos formas de desplegar una misma plataforma, y la elección correcta es la que mejor se adapta a las necesidades de tu entorno.

6. WALLIX Identity Access

Nuestra solución ofrece las capacidades de seguridad de identidades descritas en este documento: Single Sign-On para las aplicaciones; autenticación multifactor, incluidos métodos resistentes al phishing; federación de identidades sobre las infraestructuras existentes de Active Directory y LDAP mediante protocolos estándar; gestión centralizada del ciclo de vida de las identidades; y visibilidad

completa para auditorías. Está disponible tanto como servicio como mediante un appliance on-premises, con las mismas capacidades y el mismo modelo de gestión.

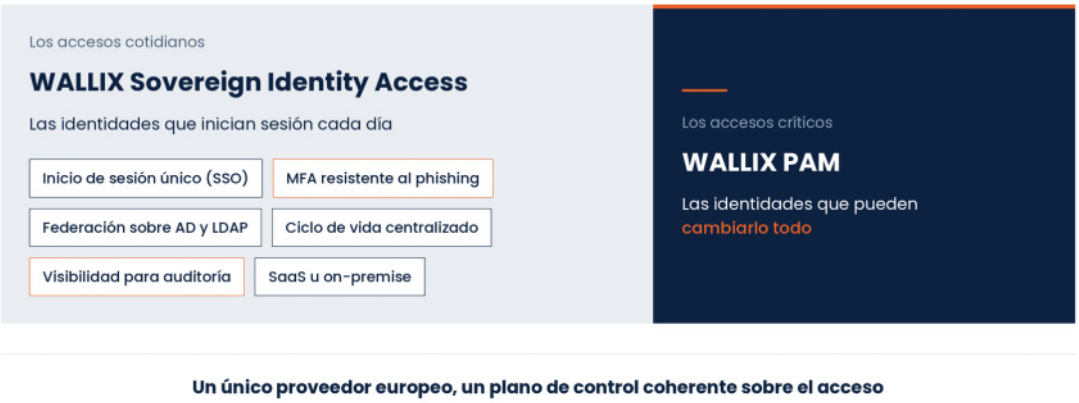


Ilustración 10 Dos components para resolver un problema

WALLIX Identity Access forma parte de la plataforma WALLIX, junto con WALLIX PAM. La seguridad de identidades y el acceso privilegiado son dos caras de un mismo problema: las identidades que inician sesión todos los días y aquellas que tienen capacidad para modificar los sistemas más críticos. Proteger ambas a través de un único proveedor europeo permite disponer de un punto de control único y coherente sobre todos los accesos, desde los más cotidianos hasta los más críticos.

7. Conclusión

El acceso basado en identidades es uno de los puntos clave de la organización moderna: es lo que permite trabajar y, al mismo tiempo, el punto de partida de muchas brechas de seguridad. Las organizaciones que consiguen protegerlo comparten un mismo enfoque: identidades centralizadas en lugar de dispersas, una autenticación capaz de resistir el phishing, una infraestructura existente que se amplía en lugar de sustituirse y evidencias del control de los accesos disponibles cuando se necesitan.

Las capacidades ya existen. Los plazos regulatorios están definidos. Lo que queda es tomar la decisión de tratar el acceso de los empleados como el perímetro de seguridad en el que ya se ha convertido y desplegar ese control allí donde tu organización necesite que funcione.

Acerca de WALLIX

WALLIX (Euronext: ALLIX, cotizada desde 2015) es un proveedor europeo de soluciones de ciberseguridad para identidades y accesos, líder en la gestión de accesos privilegiados (PAM), que ayuda a las organizaciones a reforzar su seguridad y su soberanía digital. Arraigada en los valores europeos de seguridad y libertad, y reconocida por las principales firmas de análisis por la excelencia tecnológica de su plataforma WALLIX One, WALLIX presta apoyo a más de 4.000 organizaciones en todo el mundo. WALLIX protege las identidades, los accesos y los privilegios en entornos IT y OT, permitiendo a las organizaciones evolucionar con confianza en un mundo digital más seguro.

WWW.WALLIX.COM

wallix