Microsoft

Administrar y proteger el acceso a las aplicaciones con Azure Active Directory

Sección 1

¿Qué es la administración de acceso e identidades?

¿Qué es la administración de acceso e identidades?

Transformación digital

La informática en la nube y los dispositivos móviles transformaron el área de trabajo moderna. Una fuerza laboral cada vez más global tiene la flexibilidad de trabajar desde cualquier lugar gracias a aplicaciones de software como servicio (SaaS) gratuitas y de bajo coste para resolver desafíos de productividad y colaboración. Las empresas grandes migran a aplicaciones e informática a la nube para modernizar su arquitectura, y las líneas de negocios aprovechan los nuevos servicios en la nube para crear aplicaciones personalizadas para sus necesidades específicas. Las grandes empresas se han beneficiado del auge de la nueva tecnología con una mayor productividad, pero la transformación digital también ha presentado tres nuevos desafíos.

¿Qué es la administración de acceso e identidades?

Nuevos desafíos

Riesgo de seguridad: Antes de la revolución de la nube, TI se encargaba de cuidar la tecnología. Las aplicaciones y plataformas que administrabas y protegías se encontraban dentro del perímetro de la red, y todos los inicios de sesión dentro de los recursos corporativos eran validados primero por el firewall. Eso ya no sucede. Tu fuerza de trabajo tiene más control sobre la tecnología que usa, y accede a ella en gran medida a través de Internet. Los ciberatacantes aprendieron a aprovechar esas vulnerabilidades. Incluso cuando un usuario sabe la contraseña correcta de una cuenta, no siempre puedes estar seguro de que sea quien dice ser.

Carga administrativa: La explosión de los puntos de conexión ofrece a los usuarios más formas de conectarse, pero también se convierte una pesadilla para la administración. Muchas empresas no conocen todas las herramientas que usan los empleados, e incluso cuando cuentan con un buen inventario, la sola cantidad de aplicaciones en la nube revela que debes administrar varios sistemas de identidad, lo que aumenta los costes y aumenta los riesgos de seguridad existentes.

Experiencia insatisfactoria del usuario: Los usuarios también padecen las consecuencias. Les encanta la flexibilidad, pero se frustran ante la cantidad de credenciales que deben recordar.

Riesgo de seguridad

Carga administrativa

Experiencia insatisfactoria del usuario

¿Qué es la administración de acceso e identidades?

Administración de acceso e identidades como plano de control central

El denominador común de estos puntos débiles es la ineficacia de los sistemas para verificar la identidad. La identidad reemplazó el perímetro de la red como nuevo plano de control. Necesitas soluciones que conecten distintas herramientas, arquitectura, dispositivos y servicios en la empresa para proteger mejor a la organización y administrar el acceso para empleados y partners externos. Los sistemas de administración de identidad y acceso (IAM) unifican el acceso en un solo sistema, lo que te otorga mayor control. Proporcionan una colaboración perfecta en las fronteras de tu organización y mejoran la seguridad de tus recursos corporativos. Una buena solución de IAM te permite conectar a tus usuarios con sus aplicaciones de trabajo, tanto si se encuentran en la nube como en las instalaciones, a través de un conjunto de credenciales. Las soluciones de IAM están diseñadas para otorgarles a los usuarios acceso solo a los recursos que necesitan y evitar que los usuarios no autorizados accedan a datos que no les corresponden. Administras los derechos y permisos de acceso del usuario desde un portal centralizado, lo que reduce gran parte de los procesos manuales relacionados con el aprovisionamiento y la anulación de aprovisionamiento de cuentas de usuario. Las soluciones de IAM también ofrecen herramientas para administrar directivas de seguridad en tus identidades y aplicaciones. Las mejores soluciones de IAM protegen mejor las identidades, mejoran la experiencia del usuario y aumentan la eficiencia administrativa.

Las soluciones de IAM resuelven estos desafíos

Proteger mejor las identidades

Mejorar la experiencia del usuario

Aumentar la eficiencia administrativa

Sección 2

Información general de Azure AD

Una solución integral

Microsoft Azure Active Directory (Azure AD) es una solución de IAM integral en la nube y un líder en el mercado de la administración de directorios, el acceso a las aplicaciones y la protección de identidades avanzada. Azure AD permite a las organizaciones administrar y proteger identidades para que los empleados, partners y clientes puedan acceder a las aplicaciones y los servicios que necesitan. Azure AD ayuda a millones de organizaciones a administrar y proteger más de mil millones de identidades.

Modernizar el acceso

Administra y protege el acceso a los datos y recursos de tu organización de forma local y en la nube. Conecta a todos tus usuarios, tus aplicaciones y tus dispositivos a la nube para lograr un acceso seguro y perfecto y obtener mayor visibilidad y control. Automatiza flujos de trabajo y permite que las opciones de autoservicio ayuden a mantener los costes bajos y mejoren la productividad de tus usuarios.

Proteger y gobernar

Con un elevado volumen de ataques diarios sobre las credenciales de usuarios, la forma de evitar el peligro es hacer un seguimiento constante del comportamiento normal y anormal en el conjunto más amplio posible de señales, aplicar inteligencia artificial y automatizar las respuestas. Equilibra la productividad y la seguridad con el acceso oportuno a los recursos adecuados, las revisiones de acceso periódicas y el cumplimiento de las directivas.

Conectarse y colaborar

Amplía tu negocio con un servicio de nube confiable que puede escalarse a millones de usuarios con seguridad y flexibilidad líder en el sector. Conéctate con tus usuarios externos y proporciónales las herramientas que necesitan para ser productivos con experiencias de autoservicio sencillas y controles de seguridad integrados.

Desarrollar e integrar

Crea aplicaciones que otorgan a los usuarios una forma sencilla de iniciar sesión con sus cuentas personales, profesionales o educativas de Microsoft, o con sus cuentas de redes sociales. Empieza a conectarte a Microsoft Graph, la puerta de entrada a los datos y la inteligencia en Microsoft 365, y crea aplicaciones completas. Permite el inicio de sesión único, automatiza el aprovisionamiento de usuarios y llega a las organizaciones más grandes del mundo.

Sección 3

Azure AD para tus aplicaciones

Azure AD para tus aplicaciones

Una plataforma universal

Azure AD te permite administrar una identidad común para que cada usuario en toda la infraestructura híbrida pueda acceder a las aplicaciones que necesita, incluidas las aplicaciones de línea de negocios locales y en la nube. Administra todas tus identidades desde una plataforma universal para aumentar la eficiencia administrativa y disfrutar de más control. Aplica directivas de seguridad pormenorizadas para cada aplicación que se utiliza en tu organización.

Ahorrar tiempo y dinero

Azure AD ya está integrado en miles de aplicaciones, incluidas opciones populares como Workday, ServiceNow, SuccessFactors, Adobe y Concur, lo que facilita tu tarea de poner esas aplicaciones a disponibilidad de tus usuarios. Con una sola consola, implementa directivas unificadas y supervisa derechos de acceso. Puedes automatizar flujos de trabajo para el aprovisionamiento de usuarios y la administración del ciclo de vida y ahorrar tiempo y recursos con la administración de cuentas de autoservicio. También puedes incorporar información del usuario de las herramientas de RR. HH. como fuente fiable y eliminar así la necesidad de scripts personalizados o procesos manuales para administrar los atributos del usuario.

Las aplicaciones configuradas a través de Azure AD permiten el inicio de sesión único (SSO) para un acceso fluido, lo que significa que los usuarios no tienen que recordar credenciales para cada cuenta de la aplicación ni reutilizar contraseñas inseguras que ponen en riesgo la seguridad de los datos. Las cuentas configuradas para el aprovisionamiento automático otorgan a los usuarios acceso a nuevos recursos sin demoras. Para el aprovisionamiento de entrada, Azure AD garantiza que los nuevos empleados tengan acceso a todos los recursos relevantes el primer día.

Ahorro de tiempo y dinero

Integraciones de SaaS

Inicio de sesión único

Acceso de usuarios desde el primer día

Azure AD para tus aplicaciones

Proporcionar más acceso seguro a todas las aplicaciones

Azure AD te ofrece protección de identidad integral en todas tus aplicaciones, tanto aplicaciones de SaaS y aplicaciones de línea de negocio locales. Tanto si el usuario solicita acceso a Microsoft Word como a Box, Azure AD garantiza que se confirme su identidad antes de otorgar acceso. Puedes instaurar también directivas de gobernanza de acceso para garantizar que los usuarios accedan solo a lo que necesitan, cuando lo necesitan. Puedes exigir que los usuarios soliciten permiso para acceder, y puedes establecer un límite de tiempo para el acceso a la aplicación y realizar revisiones de cumplimiento de acceso periódicas.

Azure AD también aprovecha la potencia de Microsoft Intelligent Security Graph y el aprendizaje automático para analizar billones de señales en tus productos y servicios, a fin de detectar comportamientos atípicos y asignar un riesgo relativo a cada sesión. Azure AD observa el dispositivo, la ubicación y otra información contextual para evaluar el riesgo de inicio de sesión. Puedes establecer las directivas de acceso condicional de Azure AD que aplican automáticamente medidas de seguridad, como bloquear una solicitud de acceso o solicitar un restablecimiento de contraseña cuando un inicio de sesión se considera arriesgado o cuando se cumple con ciertas condiciones particulares de la directiva.

Medidas de seguridad de aplicaciones

Protección de identidades

Acceso a la gobernanza

Directivas de acceso condicional

Sección 4

Cómo administrar y proteger aplicaciones con Azure AD

Azure AD hace que sea sencillo mantener el control y reducir costes mediante la automatización, el autoservicio y el cumplimiento de las directivas.

Cómo administrar y proteger aplicaciones con Azure AD

Integración de las aplicaciones de Azure AD

La galería de aplicaciones de Azure AD hace que resulte fácil configurar y conectar cualquiera de las miles de aplicaciones integradas previamente a tu inquilino. Estas aplicaciones son compatibles con la experiencia de SSO, y es sencillo configurar las aplicaciones para el acceso condicional de Azure AD con directivas por aplicación para toda la empresa. Después de agregar la aplicación y configurarla según tus necesidades, los usuarios con acceso autorizado podrán encontrarla fácilmente en el portal Mis aplicaciones de Azure AD, un portal centralizado para la detección y el lanzamiento de aplicaciones de usuario final.

Si creaste una aplicación o necesitas integrarla a tu organización, también puedes solicitar que aparezca en la galería de aplicaciones de Azure AD.

Explorar las miles de aplicaciones integradas previamente >

Acceso híbrido seguro

Utiliza el proxy de la aplicación Azure AD para proporcionar acceso remoto y seguro a una aplicación web local basada en solicitudes sin necesidad de VPN. El proxy de la aplicación requiere una instalación de conector ligero y ofrece la misma experiencia de TI y usuario final de las aplicaciones de SaaS conectadas a través de la galería de aplicaciones de Azure AD.

O bien, si quieres aprovechar las inversiones en infraestructura existentes, como con partners como F5 ZScaler, SAP, Oracle o Ping Identity, para conectar otros tipos de aplicaciones como las que usan protocolos de autenticación basados en el encabezado o Kerberos, puedes hacerlo sin perder las ventajas de centralización y seguridad de Azure AD.

Más información sobre cómo agregar una aplicación local a través de un proxy de aplicación >

Conectar otras nubes y redes de aplicaciones de partners >

Cómo administrar y proteger aplicaciones con Azure AD

Aprovisionamiento automatizado

Azure AD te permite automatizar la creación, el mantenimiento y la eliminación de identidades de usuarios en aplicaciones de SaaS populares. Puedes crear automáticamente nuevas cuentas en los sistemas correspondientes para nuevos usuarios cuando se unan a tu equipo u organización. Cuando los usuarios abandonen el equipo o la organización, puedes establecer directivas que desactivan automáticamente sus cuentas de los sistemas correspondientes. Al automatizar estas tareas, puedes garantizar que las identidades en tus aplicaciones y sistemas se mantengan actualizadas en función de los cambios en el directorio o el sistema de Recursos Humanos, lo que reduce errores y tiempo.

Más información sobre cómo establecer el aprovisionamiento y desaprovisionamiento automatizado en aplicaciones de SaaS >

Administración de grupos

Azure AD te ayuda a ofrecer acceso a los recursos de tu organización al otorgar derechos de acceso a un solo usuario o a un grupo entero de Azure AD. Usar grupos permite al propietario del recurso establecer permisos de acceso para todos los miembros del grupo, en lugar de tener que otorgar los permisos de uno en uno. Este es un método más seguro ya que hay menos probabilidades de otorgar acceso inapropiado de forma accidental a una persona y permite ahorrar tiempo. También puedes escalar de forma dinámica la administración de grupo al automatizar la inscripción a través de directivas basadas en atributos."

Más información sobre cómo crear un grupo en el portal de Azure >

Cómo administrar y proteger aplicaciones con Azure AD

Autoservicio de usuarios

Algunas tareas no necesitan un profesional de TI para completarse, y Azure AD te permite delegarlas a otros usuarios de la organización. Puedes alentar a los usuarios a crear y administrar sus propios grupos de seguridad en Azure AD. Los propietarios de grupos pueden aprobar o denegar solicitudes de pertenencia, o bien pueden delegar el control de pertenencia a un grupo.

Configurar grupos autoadministrados >

El autoservicio también se extiende a los usuarios. Los usuarios pueden registrarse para obtener una cuenta a través del portal de autoservicio si tienen una dirección de correo electrónico verificada y pueden usar el portal para restablecer la contraseña. Esto puede ahorrarle mucho tiempo y dinero al departamento de soporte técnico.

Configurar el restablecimiento de contraseña para autoservicio >

Modernizar la autenticación

Si actualmente usas autenticación local como los Servicios de federación de Active Directory (AD FS) es posible que te interese migrar tus aplicaciones a Azure AD. Mantienes los mismos beneficios de usuario de SSO, pero mejoras la escalabilidad y los beneficios de seguridad disponibles en la nube, como aplicar controles de acceso pormenorizado por aplicación mediante el acceso condicional de Azure AD u otorgar a los partners acceso a los recursos con la colaboración B2B de Azure AD. Las aplicaciones que usan los estándares SAML 2.0, WS-Federation, OAuth u OpenID Connect para el inicio de sesión federado se pueden migrar.

Crear directivas de acceso condicional de Azure AD para proteger el acceso a las aplicaciones >

Utilizar B2B de Azure AD para colaborar de forma fluida con los partners externos >

Conecta de forma segura cualquier aplicación,
en cualquier nube o servidor, a Azure AD.

Un millón de aplicaciones únicas activas conectadas.

Microsoft

Empieza hoy mismo.

Empieza una prueba gratis durante un mes de Azure AD para ver lo sencillo que resulta administrar el acceso de los usuarios a todas tus aplicaciones y proteger tu empresa.