Microsoft Security

Una fuerza de trabajo moderna requiere una seguridad integrada e impulsada por la identidad

Protección contra el phishing y otros ataques basados en la identidad sin comprometer la productividad de los empleados

Contenido

Introducción

Por mucho tiempo los usuarios que acceden a los activos empresariales a través de redes domésticas inseguras y dispositivos no administrados han sido objetivos atractivos para los ciberataques. Ahora, con los entornos de trabajo remotos e híbridos convirtiéndose en una práctica común en muchas organizaciones, **las amenazas son cada vez más sofisticadas**. Como resultado, los equipos de seguridad adoptan cada vez más modelos de seguridad basados en la identidad para ofrecer acceso seguro a los activos empresariales sin afectar la experiencia del usuario ni la productividad.

La estrategia correcta implica un enfoque moderno e integrado que combina una autenticación sólida, un control de acceso basado en políticas adaptables y una detección y una corrección proactivas del compromiso de identidad y el uso indebido.

La necesidad de una seguridad sólida basada en la identidad

Incluso antes de la aparición del COVID-19, los líderes de seguridad buscaban alternativas a la seguridad tradicional basada en el perímetro para adaptarse a una fuerza de trabajo cada vez más móvil y a la migración continua de datos, aplicaciones e infraestructura de TI a la nube. El cambio al trabajo remoto, impulsado por la pandemia, amplió aún más la superficie e hizo a las organizaciones más vulnerables a ataques y filtraciones.

Para los ciberdelincuentes, el cambio presentaba nuevas oportunidades de ingreso y salida para acceder a los datos empresariales y filtrarlos. En el **informe de defensa Digital de Microsoft** se descubrió que los actores de los estados naciones están adoptando técnicas de reconocimiento más sofisticadas, además de la recolección de credenciales y vulnerabilidades de la red privada virtual (VPN). A medida que los datos confidenciales pasaron de instalaciones empresariales seguras a hogares, sistemas y redes de empleados con una protección débil, los controles y las políticas de seguridad tradicionales detrás del perímetro de la red se volvieron más difíciles de aplicar.

La actividad de amenazas relacionada con la identidad ha aumentado significativamente desde que comenzó la pandemia. Solo en marzo de 2020 **Microsoft detectó** 4.900 millones de inicios de sesión impulsados por atacantes y más de 150.000 cuentas comprometidas. También se produjo un **fuerte aumento en los ataques** que involucran métodos de fuerza bruta y compromiso de correo electrónico empresarial (BEC) para obtener las credenciales de la empresa. En una **encuesta de Microsoft** realizada en 2020, el 28 % de las empresas informaron algún ataque exitoso de suplantación de identidad dentro de su organización. A menudo, las credenciales comprometidas se han utilizado para acceder a los datos empresariales o facilitar ataques futuros. Por ejemplo, los adversarios cibernéticos han usado credenciales de identidad robadas para **apuntar y falsificar a personas de alto valor** e iniciar fraudes, incluidos pagos ilegítimos y transferencias bancarias.

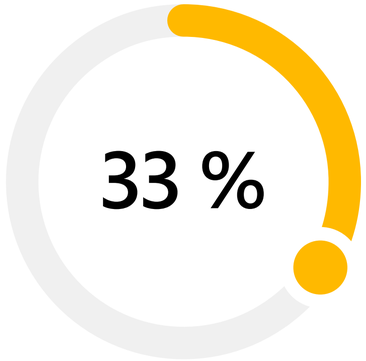
4.900 millones

Inicios de sesión impulsados por atacantes solo en marzo de 2020

+ de 150.000

cuentas atacadas

Los administradores de seguridad son conscientes de la mayor necesidad de controles de acceso y protección de la identidad más fuertes. Se dan cuenta de que, a partir de la protección de los datos detrás de la red empresarial, los equipos de seguridad deben detectar y responder a las amenazas en el perímetro extendido de la fuerza de trabajo remota. En el **estudio 2020 Security Priorities** (Prioridades de seguridad 2020) de IDG, el 33 % de los profesionales de seguridad sostuvo que mejorar los controles de identidad y acceso fue una de sus principales prioridades de seguridad en 2021 debido a un aumento en los ataques basados en la identidad dirigidos a los trabajadores remotos.



El 33 % de los profesionales de seguridad dijo que mejorar los controles de identidad y acceso fue una de sus principales prioridades en 2021

Los beneficios de la seguridad integrada basada en la identidad

Para ofrecer a los trabajadores remotos un acceso seguro y sin problemas a los recursos locales y hospedados en la nube, las organizaciones necesitan una estrategia de seguridad integrada y basada en la identidad que combine una autenticación sólida con capacidades proactivas de protección contra el uso indebido de la identidad.

Los componentes críticos incluyen autenticación multifactor (MFA) para proteger el acceso a los recursos empresariales, junto con soporte para las directivas para controlar qué, cuándo y cómo un usuario específico puede acceder a la información y los sistemas mediante información contextual en tiempo real sobre el usuario, el dispositivo, la ubicación y el riesgo de la sesión. Además, la solución debe integrar mecanismos para detectar y responder de manera inteligente a cuentas comprometidas y amenazas mediante capacidades de IA y automatización basadas en la nube.

Un enfoque integrado de la seguridad puede optimizar la administración de identidades, ya que proporciona a los administradores una vista unificada de los datos, de múltiples fuentes, a través de una sola consola. Ofrece a las organizaciones una forma de usar tanto las señales relacionadas con la identidad como las señales en todos los dispositivos, aplicaciones y redes de una empresa, lo que permite directivas coherentes para el control de acceso.

Un enfoque integrado optimiza la seguridad en entornos locales y de varias nubes, abarcando todos los puntos de conexión, las aplicaciones y las cargas de trabajo.

Una fuerza de trabajo moderna requiere una seguridad integrada e impulsada por la identidad

Enfoque integrado de la seguridad de Microsoft: desde la identidad hasta la protección contra amenazas

Seguridad impulsada por la identidad

La solución de administración de identidades y acceso de Microsoft, Azure Active Directory, integra capacidades para una autenticación sólida y control de acceso granular mediante directivas de adaptación en tiempo real y detección y corrección automáticas de riesgos de identidad. Microsoft Azure Active Directory ayuda a las organizaciones a proteger el acceso a los recursos y los datos mediante la autenticación sólida y las políticas de acceso adaptable basadas en el riesgo en tiempo real.

Azure AD ayuda a las organizaciones a proteger el acceso a los recursos y los datos mediante una autenticación sólida. Permite el inicio de sesión más simple a través de métodos de autenticación sin contraseña, como Microsoft Authenticator y Windows Hello, que permiten a los usuarios autenticarse de forma segura en dispositivos móviles y en la web. El acceso condicional en Azure AD permite a las organizaciones controlar a qué puede tener acceso un usuario, cuándo y cómo, en función de factores como el dispositivo, la ubicación y la información de riesgo en tiempo real.

Azure AD Identity Protection puede detectar y responder automáticamente a cuentas comprometidas y otros riesgos basados en la identidad. Azure AD utiliza capacidades avanzadas de machine learning, análisis de comportamiento de usuarios y entidades (UEBA), además de inteligencia conectada sobre el comportamiento del usuario para supervisar continuamente la actividad sospechosa y proteger en tiempo real las filtraciones de identidades perdidas o robadas.

Protección integrada contra amenazas

La interoperación con otros productos de seguridad Microsoft como Microsoft 365 Defender, Azure Defender y Azure Sentinel puede ayudar a proporcionar más contexto para detectar, analizar y responder a las amenazas en los recursos, no solo en la identidad, con el respaldo de las capacidades de IA para ayudar a unir las señales e identificar lo más importante. La integración permite a las organizaciones comparar señales sobre usuarios, inicios de sesión y otros eventos riesgosos con datos de amenazas en entornos híbridos que comprenden aplicaciones locales y en la nube.

La protección contra amenazas integrada es fundamental porque los atacantes explotarán cualquier vulnerabilidad que puedan encontrar en dispositivos, servicios en la nube y usuarios. Cuando un atacante encuentra una oportunidad, usará ese punto de apoyo inicial para escalar los privilegios y moverse lateralmente a través de una red hasta dar con su objetivo. Un sistema de seguridad integrado y basado en la identidad puede ayudar a detectar y responder a dicha actividad, en todos los puntos de conexión, las aplicaciones y las cargas de trabajo, en varios entornos de nube y locales, a través de un único panel.

Los analistas de seguridad pueden usar un solo panel para identificar las actividades de los usuarios sospechosos y correlacionar los datos entre múltiples conjuntos para detectar y responder a ataques de varias etapas. Los equipos de seguridad pueden visualizar una brecha y obtener contexto sobre cómo un ataque entró y se propagó en la infraestructura, para ayudar a prevenir ataques futuros.

Seguridad integrada en acción, impulsada por la identidad

La integración completa, habilitada con un modelo de seguridad basado en la identidad, proporciona muchos beneficios a las organizaciones de todos los sectores. Estos son tres ejemplos.

✓ Vaya más allá de las decisiones simples de permitir/bloquear a controles de acceso más detallados:

Lumen Technologies aprovecha el soporte para las directivas de acceso condicional en Azure Active Directory para definir a qué aplicaciones y a qué datos pueden acceder los empleados desde casa o cuando viajan al extranjero.

✓ Evaluación de riesgos en tiempo real y mitigación de las amenazas basadas en la identidad:

Bridgewater Associates utiliza la herramienta Identity Protection en Microsoft Azure Active Directory para identificar intentos de inicio de sesión inusuales y riesgosos y para bloquear a los usuarios, restablecer contraseñas o requerir autenticación multifactor en función de señales como ubicaciones y direcciones IP.

✓ Desarrolle la resiliencia al permitir la evaluación y supervisión continuas de acceso:

La empresa mundial de logística de contenedores Maersk ha implementado la protección de identidad de Azure AD y las herramientas de acceso condicional para marcar comportamientos de riesgo y tomar medidas, como la revocación de acceso, rápidamente y antes de que esta se convierta en un problema importante.

Primeros pasos

Cierre las brechas entre las soluciones puntuales y obtenga cobertura en todo su entorno multiplataforma y de varias nubes.

Obtenga más información

Microsoft