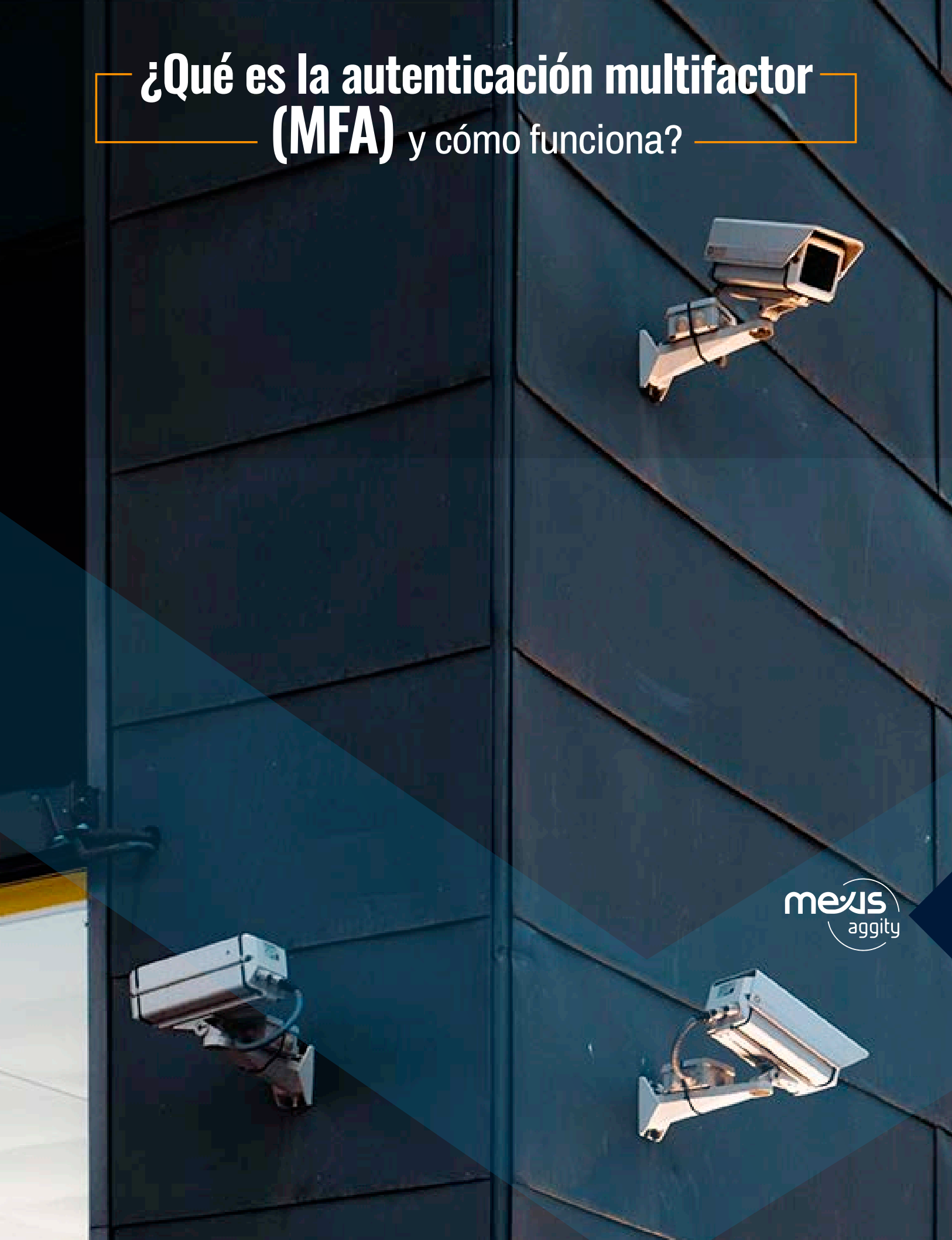
¿Qué es la autenticación multifactor (MFA) y cómo funciona?



Como sugiere el nombre, la autenticación multifactor (MFA) es el uso de múltiples factores para confirmar la identidad de alguien que solicita acceso a una aplicación, sitio web u otro recurso. La autenticación multifactor es la diferencia entre, por ejemplo, ingresar una contraseña para obtener acceso e ingresar una contraseña más una contraseña de un solo uso (OTP), o una contraseña más la respuesta a una pregunta de seguridad.

Al exigir a las personas que confirmen su identidad de más de una forma, la autenticación multifactor proporciona una mayor seguridad de que realmente son quienes dicen ser, lo que reduce el riesgo de acceso no autorizado a datos confidenciales. Después de todo, una cosa es ingresar una contraseña robada para obtener acceso; otra muy distinta es ingresar una contraseña robada y luego también se le pedirá que ingrese una OTP que se envió por mensaje de texto al teléfono inteligente del usuario legítimo.

Cualquier combinación de dos o más factores califica como autenticación multifactor. El uso de solo dos factores también puede denominarse autenticación de dos factores.

Las tres categorías de métodos de autenticación multifactor.

Un método de autenticación de múltiples factores generalmente se clasifica en una de estas tres formas:

Algo que sepa: PIN, contraseña o respuesta a una pregunta de seguridad.

Algo que tiene: OTP, token, dispositivo confiable, tarjeta inteligente o insignia.

Algo que usted es: rostro, huellas dactilares, escaneo de retina u otros datos biométricos.

Ejemplos de métodos de autenticación multifactor:

Se puede utilizar cualquiera de los siguientes métodos además de una contraseña para lograr la autenticación multifactor.

Biometría: una forma de autenticación que se basa en un dispositivo o aplicación que reconoce un dato biométrico, como la huella digital de una persona, los rasgos faciales o la retina o el iris del ojo.

Presionar para aprobar: una notificación en el dispositivo de alguien que le pide al usuario que apruebe una solicitud de acceso al tocar la pantalla de su dispositivo.

Contraseña de un solo uso (OTP): un conjunto de caracteres generado automáticamente que autentica a un usuario solo para una sesión o transacción de inicio de sesión.

Texto SMS: un medio para enviar una OTP al teléfono inteligente u otro dispositivo de un usuario.

Token de hardware o token duro: n dispositivo generador de OTP pequeño y portátil, a veces denominado llavero

Token de software o token de software: un token que existe como una aplicación de software en un teléfono inteligente u otro dispositivo en lugar de como un token físico.

Los beneficios de la autenticación multifactor.

Mejora de la seguridad: la autenticación multifactor mejora la seguridad. Después de todo, cuando solo hay un mecanismo que protege un punto de acceso, como una contraseña, lo único que tiene que hacer un mal actor para entrar es encontrar una manera de adivinar o robar esa contraseña.

Pero si la entrada también requiere un segundo (o incluso un segundo y un tercer) factor de autenticación, eso hace que sea mucho más difícil ingresar, especialmente si el requisito es algo más difícil de adivinar o robar, como una característica biométrica.

Habilitación de iniciativas digitales: con más organizaciones deseosas de implementar una fuerza laboral remota hoy, más consumidores que optan por comprar en línea en lugar de en tiendas, y más organizaciones que mueven aplicaciones y otros recursos a la nube, la autenticación multifactor es un habilitador poderoso. Asegurar los recursos de la organización y el comercio electrónico es un desafío en la era digital, y la autenticación multifactor puede ser invaluable para ayudar a mantener seguras las interacciones y transacciones en línea.

¿Hay inconvenientes en la autenticación multifactor?

En el proceso de crear un entorno de acceso más seguro, es posible crear uno menos conveniente, y eso puede ser un inconveniente. (Esto es especialmente cierto ya que la confianza cero, que trata todo como una amenaza potencial, incluida la red y cualquier aplicación o servicio que se ejecute en la red, continúa ganando terreno como base para un acceso seguro). Ningún empleado quiere dedicar más tiempo cada vez. día lidiando con múltiples obstáculos para iniciar sesión y acceder a los recursos, y ningún consumidor que tenga prisa por hacer algunas compras o realizar operaciones bancarias quiere verse obstaculizado por múltiples requisitos de autenticación. La clave es equilibrar la seguridad y la conveniencia para que el acceso sea seguro, pero los requisitos de acceso no son tan onerosos como para crear inconvenientes indebidos para quienes lo necesitan legítimamente.

El papel de la autenticación basada en riesgos en la autenticación multifactor.

Una forma de lograr un equilibrio entre lograr la seguridad y garantizar la conveniencia es aumentar o reducir los requisitos de autenticación en función de lo que está en juego, es decir, el riesgo asociado con una solicitud de acceso. Esto es lo que se entiende por autenticación basada en riesgos. El riesgo puede residir en a qué se accede, quién solicita acceso o ambos.

Riesgo que plantea el objeto al que se accede: por ejemplo, si alguien solicita acceso digital a una cuenta bancaria, ¿es para iniciar una transferencia de fondos o simplemente para comprobar el estado de una transferencia que ya se ha iniciado? O si alguien interactúa con un sitio web o una aplicación de compras en línea, ¿es para hacer un pedido o simplemente para verificar el estado de entrega de un pedido existente? Un nombre de usuario y una contraseña pueden ser suficientes para este último, pero la autenticación multifactor tiene sentido cuando hay un activo de alto valor en riesgo.

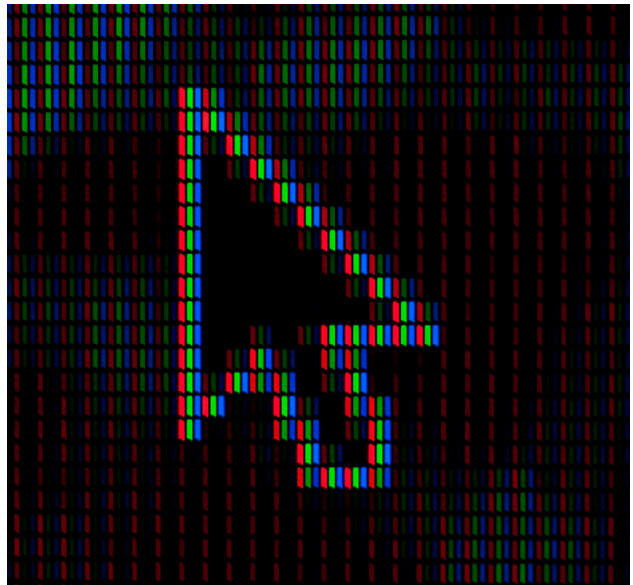
Riesgo que plantea quién solicita el acceso: cuando un empleado o contratista remoto solicita acceso a la red corporativa desde la misma ciudad día tras día, utilizando la misma computadora portátil cada vez, hay pocas razones para sospechar que no es esa persona. Pero, ¿qué sucede cuando una solicitud de Mary en Minneapolis llega repentinamente desde Moscú una mañana? El riesgo potencial (¿es realmente ella?) Justifica una solicitud de autenticación adicional.

El futuro de la autenticación multifactor: IA, ML y más.

La autenticación de múltiples factores evoluciona continuamente para proporcionar un acceso más seguro para las organizaciones y menos inconveniente para los usuarios. La biometría es un gran ejemplo de esta idea. Es más seguro, porque es difícil robar una huella digital o una cara, y más conveniente, porque el usuario no tiene que recordar nada (como una contraseña) ni hacer ningún otro esfuerzo importante. Los siguientes son algunos de los avances que dan forma a la autenticación multifactor en la actualidad.

Inteligencia artificial (IA) y aprendizaje automático (ML): la IA y el ML se pueden utilizar para reconocer comportamientos que indican si una solicitud de acceso determinada es "normal" y, por lo tanto, no requiere autenticación adicional (o, a la inversa, para reconocer un comportamiento anómalo que lo garantiza).

Fast Identity Online (FIDO): la autenticación FIDO se basa en un conjunto de estándares abiertos y gratuitos de FIDO Alliance. Permite que los inicios de sesión con contraseña sean reemplazados por experiencias de inicio de sesión rápidas y seguras en sitios web y aplicaciones.



Autenticación sin contraseña: en lugar de utilizar una contraseña como método principal para verificar la identidad y complementarla con otros métodos sin contraseña, la autenticación sin contraseña elimina las contraseñas como forma de autenticación.

Tenga la seguridad de que la autenticación multifactor continuará cambiando y mejorando en la búsqueda de formas en las que las personas puedan demostrar que son quienes dicen ser, de manera confiable y sin saltarse los obstáculos.

Fuente de información: rsa.com