

La autenticación multifactor adaptativa frente a las políticas de seguridad básicas

No todas las soluciones de autenticación de doble factor o Multifactor (MFA, por sus siglas en inglés) se han diseñado de la misma forma, sino que sus niveles de seguridad varían en función de los factores que emplean, aunque la falta de visibilidad y la incapacidad de integrar distintas herramientas de seguridad siguen produciendo puntos ciegos de seguridad. Además, una autenticación segura debe resultar sencilla tanto para los usuarios como para los administradores.

Puntos débiles más comunes en las organizaciones de hoy



Garantizar la productividad de forma segura

El empleado actual trabaja desde una amplia variedad de dispositivos, ubicaciones y redes, lo que debe llevarse a cabo de manera segura.



Métodos de ataque modernos

Los métodos de ataque actuales obligan a las organizaciones a proteger la autenticación y el acceso a todas sus aplicaciones, aunque la falta de visibilidad y la incapacidad de integrar distintas herramientas de seguridad siguen produciendo puntos ciegos de seguridad.



Una seguridad sencilla

Cualquier solución de seguridad debe ser también fácil de usar y adoptar para obtener buenos resultados.

LA SOLUCIÓN:

La autenticación multifactor adaptativa de Okta

La AMF adaptativa de Okta agrega una capa de seguridad a todos los activos de su organización, no solo a los críticos.



Autenticación segura para toda su empresa

La AMF cierra una gran brecha de seguridad para sus empleados, socios y clientes con una autenticación adaptable para todas sus aplicaciones, sistemas y dispositivos.



Políticas inteligentes que permiten la gestión de accesos contextual

Cree políticas inteligentes basadas en la red, el dispositivo, la ubicación y el contexto de riesgo que limiten la necesidad de identificación a los intentos de inicio de sesión arriesgados.



Fácil de usar para los administradores y usuarios finales

El aprovisionamiento automatizado hace que la configuración, administración y gestión resulten sencillas y transparentes (existen más de 5500 integraciones de VPN y SAML disponibles en la Okta Integration Network).



Ampliable a toda su organización

Mejore tanto la productividad como la seguridad de sus equipos. Las herramientas de elaboración de informes y API ofrecen a los profesionales informáticos una visibilidad total de la seguridad, de manera que se reduce la zona de ataque y se posibilitan respuestas rápidas ante las amenazas.

Autenticación multifactor adaptativa de Okta

A continuación, encontrará un ejemplo de cómo la autenticación multifactor adaptativa de Okta hace que el trabajo en línea sea más seguro, cómodo y productivo.

Políticas de seguridad básicas

VS.

Autenticación multifactor adaptativa (AMF adaptable)



John

trabaja para una empresa con sede en EE. UU. que no utiliza Okta.



Jane

trabaja para una empresa con sede en EE. UU. que ha implementado la AMF adaptable de Okta.

John/Jane se encuentra en una conferencia en Reino Unido

cuando recibe una llamada urgente de un cliente que necesita que modifique una propuesta multimillonaria lo antes posible.

John

conecta su ordenador portátil al wifi público y gratuito para acceder a Salesforce.com, pero se percató de que necesita iniciar primero la VPN.



John intenta acceder a la VPN, pero se le solicita un código de su token de hardware. Se acuerda de que lo dejó en la oficina.

John llama al número de emergencia del servicio de asistencia técnica de la empresa, que le facilita una contraseña temporal.



Tras acceder a la VPN, John vuelve a Salesforce.com, pero ha olvidado la contraseña. Comprueba las notas adhesivas que tiene en su ordenador, pero la contraseña de Salesforce se ha caído.

Salesforce.com le envía las instrucciones para restablecer la contraseña a su cuenta de correo electrónico de la empresa. Una vez restablecida la contraseña, John obtiene los detalles que necesita y puede comenzar a actualizar la propuesta, que se encuentra en el servidor de SharePoint.



John busca su contraseña de Sharepoint en otra nota adhesiva e inicia sesión para recuperar el documento más reciente de la propuesta.



John

completa la propuesta y la envía por fin al cliente, que ha esperado impacientemente.

Jane

conecta su ordenador portátil al wifi público y gratuito y accede a Okta, que utiliza para acceder a todos sus servicios relacionados con el trabajo.



Al no encontrarse en la red corporativa, el servicio de autenticación multifactor adaptativa de Okta le pide a Jane que se identifique utilizando la aplicación Okta Verify en su teléfono.



Jane desbloquea su teléfono con su huella dactilar, aprueba la autenticación correctamente en un solo toque y obtiene acceso al panel de control de Okta.



A continuación, Jane sencillamente hace clic en Salesforce para obtener los últimos detalles del cliente y en Sharepoint para acceder a su propuesta.



Jane

completa la propuesta y la envía al cliente, que está gratamente sorprendido por su inmediata respuesta.