HOJA DE DATOS

Autenticación de dos factores de Starling

Verificación de identidad segura y simple

Beneficios

- Aumenta la seguridad para prácticamente cualquier sistema o aplicación.
- Simplifica la administración continua, ya que no requiere los costos de infraestructura ni genera los problemas de las soluciones locales.
- Facilita la adopción de los usuarios al proporcionar opciones de autenticación simples de usar, como autenticación mediante notificaciones, SMS y llamados telefónicos.
- Posibilita que el servicio técnico responda rápidamente a problemas de autenticación del usuario desde cualquier navegador web.
- Disminuye el riesgo de violación de la seguridad de credenciales de autenticación robadas o comprometidas.
- Proporciona un registro de auditoría integral para satisfacer los requisitos de cumplimiento.

Información general

Independientemente de la manera en que se vean afectadas las contraseñas, ya sea por comportamiento cuestionable del usuario, uso de contraseñas débiles o si simplemente fueron robadas, esto afectará la reputación y los resultados de su empresa. Existe una forma simple de aumentar la seguridad y evitar la violación de datos al requerir la autenticación de dos factores para obtener acceso a los recursos de su red.

Con la autenticación de dos factores de Starling, una solución basada en SaaS, usted puede proteger a su organización, hacer que los usuarios sean más productivos y reducir significativamente el volumen de solicitudes de restablecimiento de contraseñas que se envían a su servicio de ayuda.

Proteja y simplifique el acceso del usuario

La autenticación de dos factores (TFA) es la manera más simple y segura de resolver el problema de las contraseñas. Sin embargo, no todas las soluciones de dos factores son iguales. Usted debe considerar cómo opera su empresa, cómo podrían hacerse más eficientes los procesos de autenticación, qué factores en forma de token necesitará y qué funcionará con su infraestructura y pila de aplicaciones existentes.

La autenticación de dos factores de Starling soluciona el problema de las contraseñas sin los costos de capital en los que puede incurrir con las soluciones locales tradicionales. Gracias a un panel de administración fácil de usar y a las opciones de autenticación flexibles para los usuarios finales, permite a las empresas verificar de manera rápida y sencilla la identidad de los usuarios.

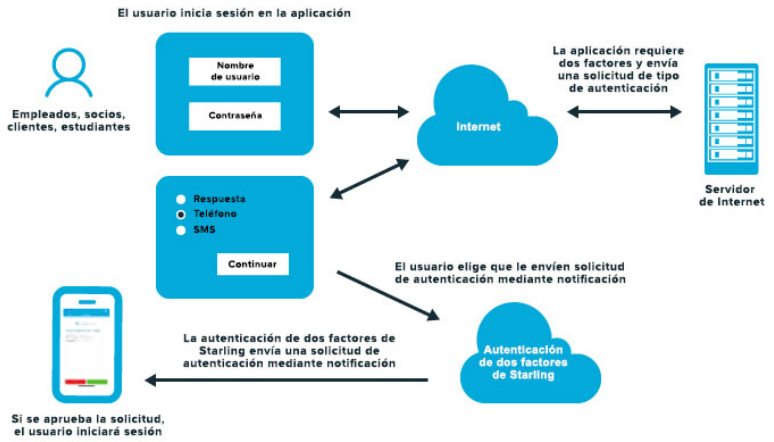

Figura 1. Arquitectura y módulos de la autenticación de dos factores de Starling.

Características

Panel de administración fácil de usar

El panel de administración basado en roles con aprobaciones de flujo de trabajo garantiza que los administradores y los asociados de soporte técnico reciban las tareas o derechos adecuados, a la vez que les facilita la administración de cuentas de usuarios finales, la generación de códigos de respuesta temporales y la ejecución de comprobaciones de estado para verificar que la aplicación móvil esté funcionando correctamente.

Métodos de autenticación múltiples

Los usuarios pueden generar contraseñas de un solo uso con las aplicaciones de dos factores de autenticación de Starling para iOS, Android y Chrome o recibir una contraseña de un solo uso a través de SMS o llamado telefónico.

Autenticación mediante notificaciones

Permita que la autenticación de dos factores sea aún más sencilla para sus usuarios: estos pueden omitir la contraseña de un solo uso si seleccionan la autenticación mediante notificaciones después de introducir el nombre de usuario y contraseña en una aplicación. Se enviará una verificación por SMS a la aplicación móvil para que los usuarios aprueben o rechacen la solicitud de inicio de sesión en la aplicación. Una vez aprobada la solicitud, iniciarán sesión automáticamente en la aplicación.

Token

La autenticación de dos factores de Starling incluye varias opciones; entre ellas, aplicaciones móviles para iOS y Android, Chrome, SMS o llamados telefónicos.

Desarrollo de marca del token

A través del panel de Starling, los administradores pueden personalizar fácilmente la apariencia del token en la aplicación, para que coincida con la marca de la empresa.

Adaptador ADFS

Permite a las empresas implementar la autenticación de dos factores en las aplicaciones que usan el protocolo WS-Federation de Microsoft, como Office 365. Además, es compatible con otros protocolos de federación, incluido SAML 2.0 para soportar inicios de sesión para aplicaciones en la nube, como Google Apps y salesforce.com.

Agente de RADIUS

Permite a las empresas soportar la autenticación de dos factores en todo lo que utilice el protocolo RADIUS para la autenticación.

Agente de HTTP

Implemente protección de autenticación de dos factores a sitios web con IIS.

Inicio de sesión de escritorio

Mejore su entorno: agregue autenticación de dos factores a las computadoras y servidores de los usuarios al unificar los inicios de sesión de los usuarios y consolidar la autenticación.

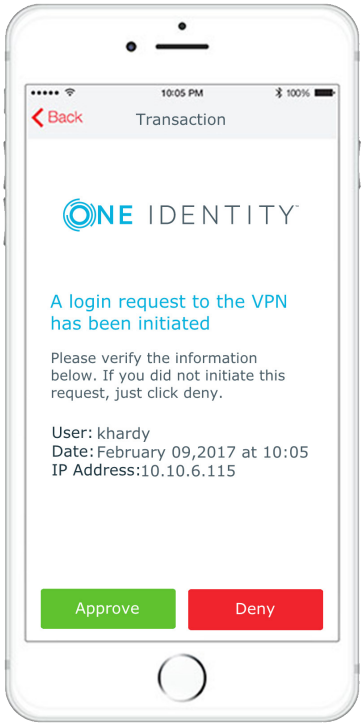

Figura 2. La autenticación mediante notificaciones simplifica y protege el proceso de inicio de sesión del usuario.

Acerca de One Identity

One Identity permite que las empresas se ocupen correctamente de la administración de identidades y acceso (IAM). Con nuestra exclusiva combinación de ofertas, incluido un portafolio de gestión de identidades, administración de accesos, administración privilegiada e identidades como soluciones de servicio, las empresas pueden alcanzar su máximo potencial sin impedimentos de seguridad, ya que estarán protegidas contra las amenazas. Más información en OneIdentity.com