



Authentication Management

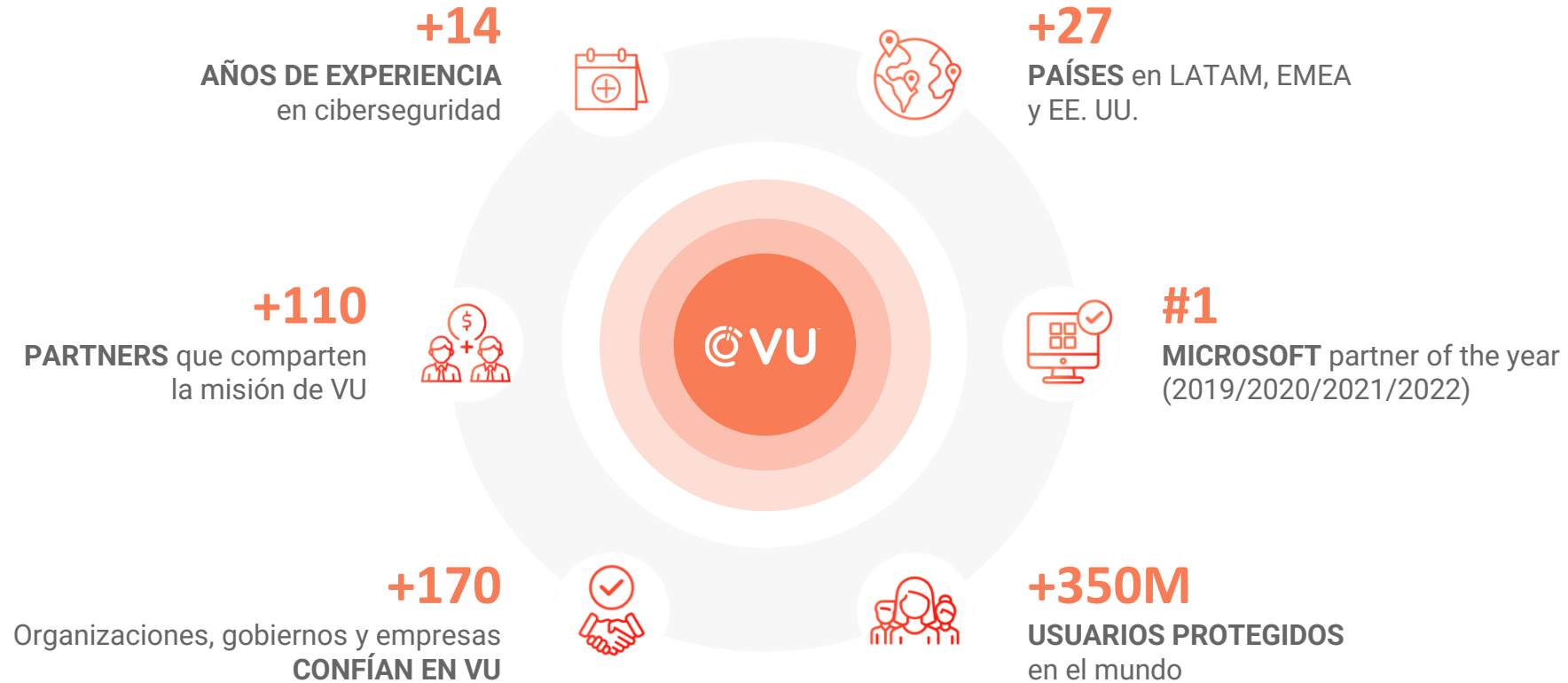
Ciberseguridad como habilitadora de negocios
Protección de identidad y prevención de fraude

VU es una empresa de ciberseguridad

especializada en protección de la identidad y prevención de fraude.



Sobre VU



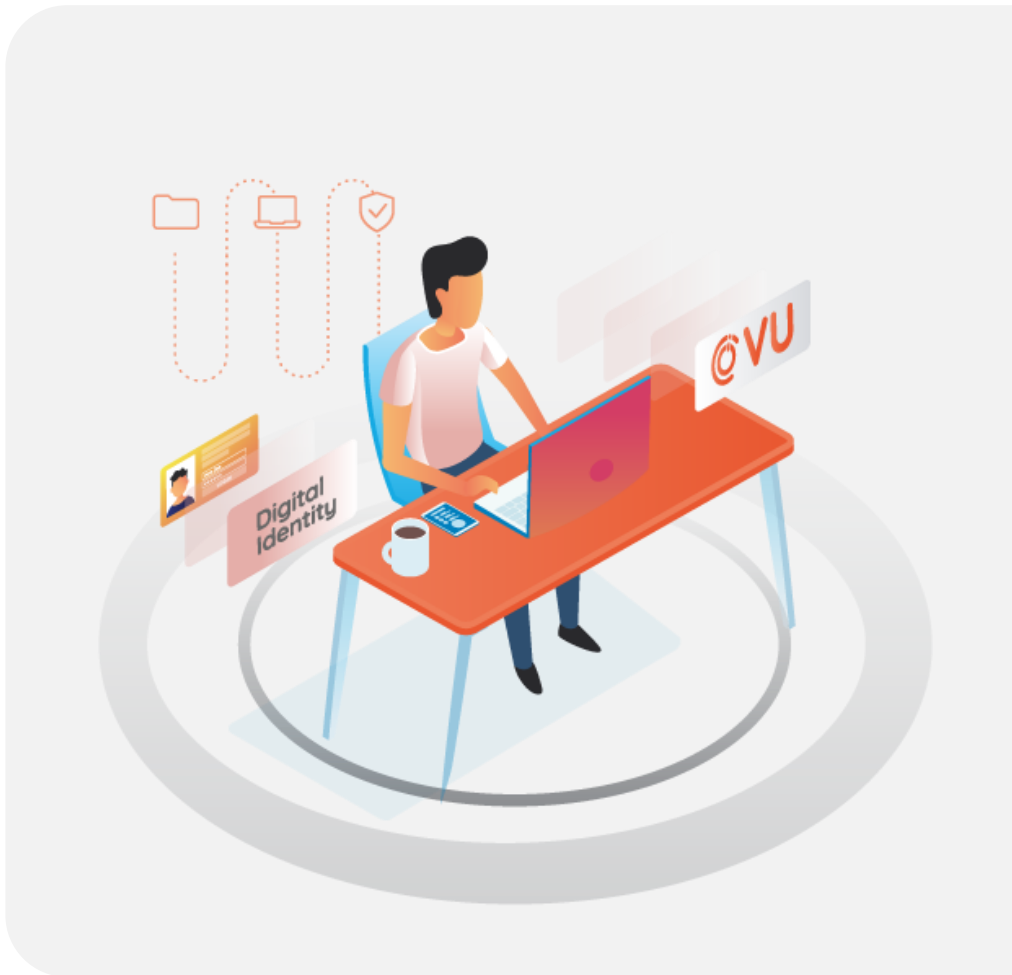
La misión de VU

es proporcionar **experiencias digitales seguras y sin fricciones** para los ciudadanos, así como para las empresas y organizaciones, durante el proceso de transformación digital.



Authentication Management

Evolución del producto



Seguridad Zero-Trust para entorno cloud, híbrido u on-premise. Mediante la autenticación multi-factor se garantiza que el legítimo propietario de las credenciales sea la entidad que está accediendo al sistema.

Capa extra de seguridad en los procesos de autenticación.

Single Sign-on y federación de identidades en un solo paso se logra autenticar a los usuarios en diversas aplicaciones y sistemas corporativos.

Active Directory capacidad de integrarlo.

Cualquier recurso corporativo incluidos VPNs, Intranets, aplicaciones y Office 365.

Integraciones y protocolos más reconocidos como SAML2, OIDC, Radius, API y App.

Múltiples canales OTP Correo electrónico, SMS, notificaciones push a aplicaciones móviles y notificaciones sync.

Wallets de identidad Microsoft Authenticator o Google Authenticator.

¿Qué es?

Una **solución MFA** (Múltiple Factor de Autenticación) que asegura que **solo el usuario autorizado se conecte a aplicaciones o infraestructura crítica de la empresa.**

La seguridad adicional se genera implementando un **segundo factor de autenticación** -token de seguridad- a los **servicios y aplicaciones.**

¿Cómo funciona?

Las personas **validan su identidad ingresando su usuario y una clave dinámica de única vez (OTP)**, recibida vía email o por la aplicación que previamente instalaron en su teléfono móvil, que puede reemplazar al password tradicional o ser un factor adicional de seguridad. La empresa gestiona a través de un backend el enrolamiento de usuarios, políticas, sincronización con AD, etc.

¿A quién está dirigido?

Empresas de diversas industrias, segmentos y tamaños, con más de 100 usuarios internos o externos.

Puntos clave



Evita el robo de identidad, así como ataques de phishing y pharming.



Garantiza que la persona que accede al sistema es quien está autorizada.



Brinda un sistema de auditoría.



Muchas gracias