OWN YOUR IDENTITY.

inception 2026

De la contraseña al control estratégico:

Passwordless+

Gobernanza + Cumplimiento en la era de identidades híbridas

RSA

5 ataques donde el help-desk o robo de identidad fueron clave (≤5 años)

LECCIONES Y MITIGACIÓN RECOMENDADA

- ✓ Ampliar los controles de soporte
- ✓ Fortalecer protección de identidad
- ✓ Delimitar prívilegios; revisar logs
- ✓ Formar a personal en ingeniería soccial

Observaciones —patrones recurrentes

- **Ingeniería social dirigida al personal**

  (soporte, operadores, equipos de atención) es un vector de alto impacto: un humano engañado puede anular controles técnicos.

- **Riesgo por terceros/partners:** comprometer unproveedor (soporte, outsourcing) suele escalar a múltiples cli ent es
  El ataque muestra que **no basta con**
- **tener medidas básicas de seguridad**; los atacantes evolucionan.

Passwordlesscomo“excusa"

Introducir el modelo sin contraseñas (“passwordless”) en una organización es el momento perfecto para actualizar toda la arquitectura de MFA (autenticación multifactor).

- ¿Cómo se registran los usuarios?
- ¿Qué métodos están permitidos?
  - NIS2,DORA,etc.
- ¿Qué métodos son viables?
  - BYOD(BringYourOwnDevice/ Trae tu propio dispositivo)
- ¿Cómo se maneja el caso “perdí mi autenticador”?
- ¿Qué aplicaciones pueden funcionar sin contraseñas?
- ¿Cuáles no pueden soportar el modelo sin contraseñas?
- ¿Qué requisitos de resiliencia existen?
  - NIS2, DORA

Si tratas el modelo “Passwordless” como solo otro método de MFA… lo estás haciendo mal.

Que es passwordless?

Sin passwords. Sin molestias

Intuitivo & Seguro

Nada a recordar, nada a reusar, nada para atacar por phishing

Que passkey?

Un inicio de sesión seguro, sin contraseñas, **resistente al phishing** y **certificado por FIDO**.

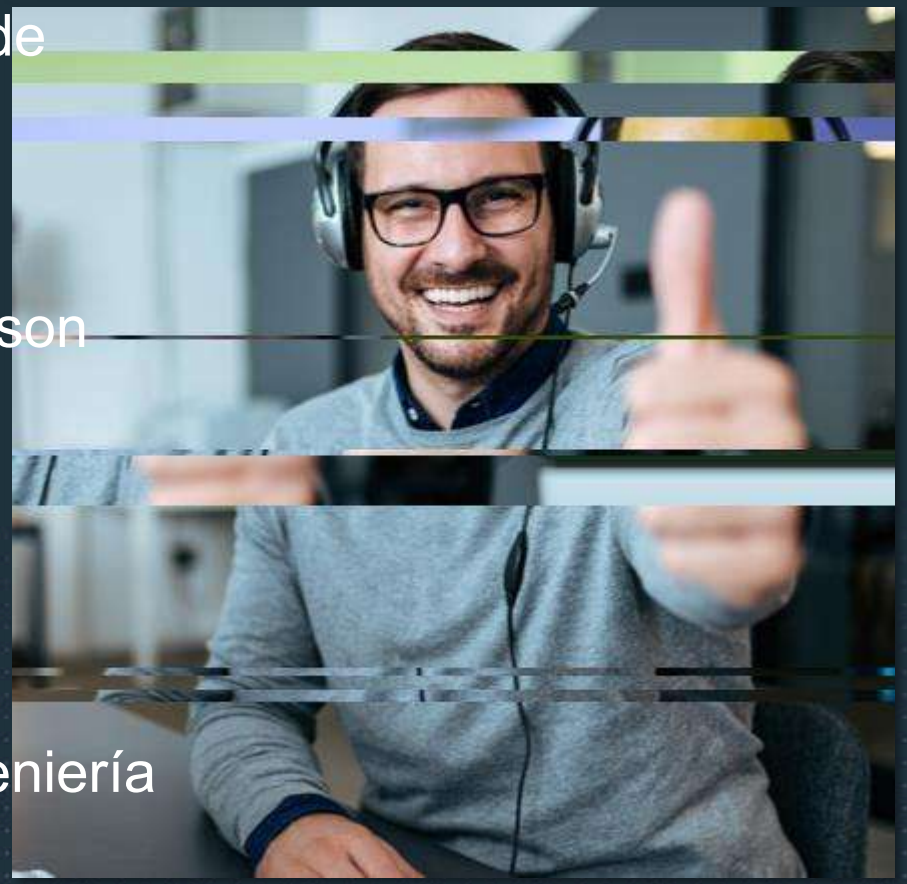
Más fácil para los usuarios. Más fuerte contra los ataques.

HW Passkey

Mobile P ass key (d evic e-bo und)

Bonus? Resistente al Phishing es un *Bonus*?

- MFA es simplemente demasiado bueno. Hace un par de años era suficiente tener cualquier MFA implementado.
- Ya no: los atacantes aprendieron.
- Los usuarios y los flujos de trabajo alrededor del MFA son ahora el objetivo:
  - Bombardeo de solicitudes / Fatiga de MFA
  - Registro y recuperación
  - Fraude en el servicio de asistencia (HelpDesk)
  - …
- El phishing es solo uno de los muchos ataques de ingeniería soci al.



“Passwordless” requiere comprender el panorama de usuarios y aplicaciones.

Sign-in es solo uno de los retos

- ¿Cómo se asignarán los diferentes autenticadores a las identidades (registro)?
  –La contraseña existente (de Active Directory) no funcionará… ya no hay contraseña

- ¿Cómo pueden los usuarios iniciar la recuperación de autenticadores extraviados, perdidos o robados?

- ¿Cómo puede el servicio de asistencia (HelpDesk) asegurarse de que está hablando con la persona correcta?

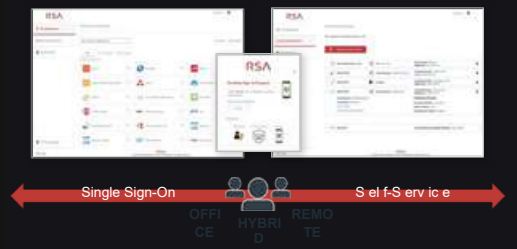
Acceso Seguro & Conveniente contra ataques MFA

Administracion de accesos Passwordless desde el dia uno

/enrola

EnrolamientoSeguro

Para *nuevos usuarios* con **0 autenticadores registrados**
Disponibilidad de IDV



/mypage

Acceso & Single Sign-On

Para usuarios *existentes* con autenticadores registrados

/recupera

Recuperacionde crede ncia les

Para usuarios *existentes* con **1 autenticador registrado**

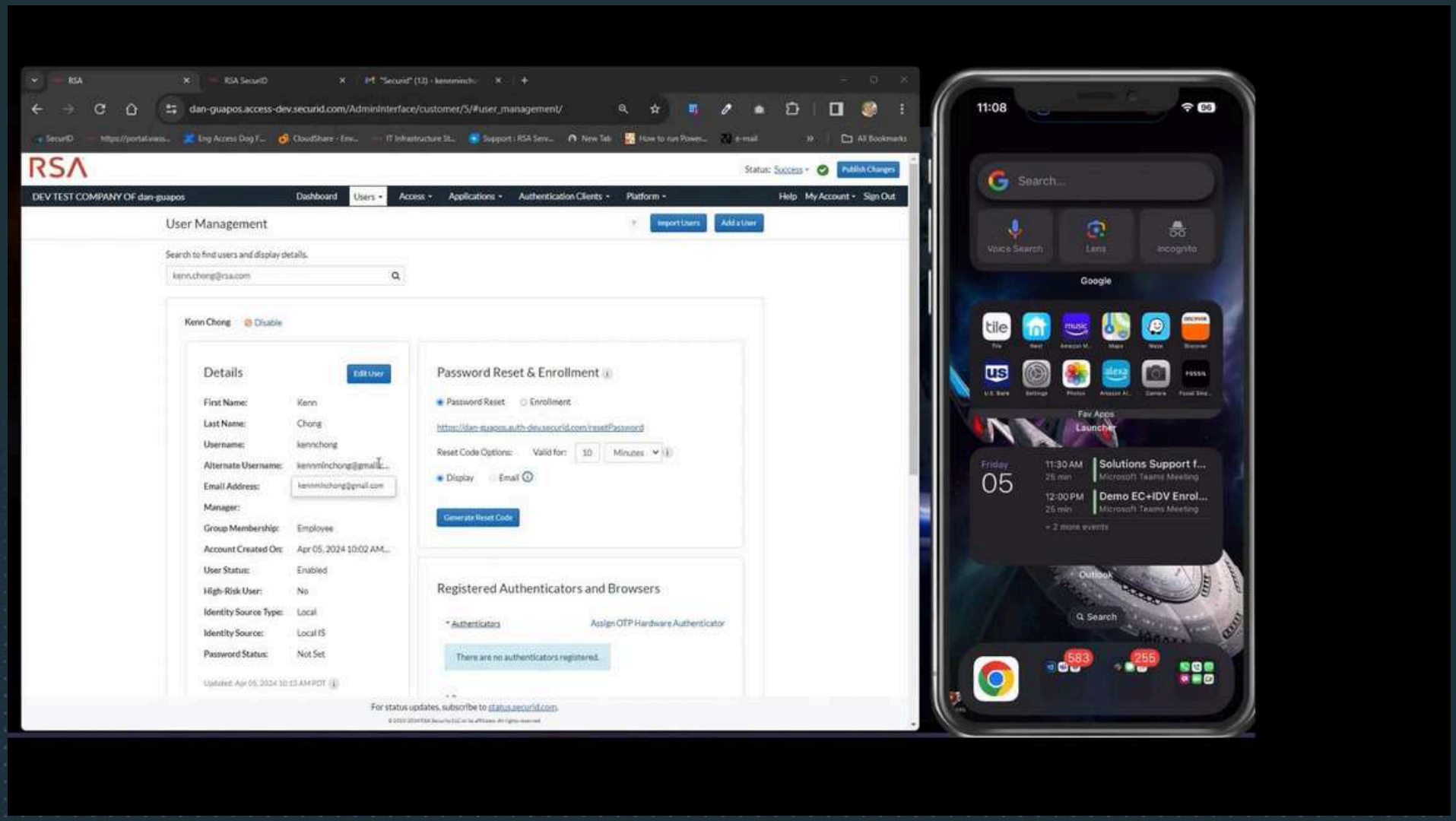
/verifica

Verificacion de identidad

Para usuarios *existentes* con acceso a **cualquier** autenticador

PASSWORDLESS

EXPERIENCIA – Verificacion de identidad



Hay un antes y un después de “Passwordless”

Nube fuera?!? Ahora qué?

NIS2&DORA / Directivos&Negocioquisieransabertu respuesta

- Una interrupción de un servicio MFA en la nube puede tener muchas causas diferentes:
  - Falla real de la solución MFA
  - Falla del proveedor de nube subyacente
  - Interrupción de la conexión con la nube
  - Pérdida repentina de confianza en el proveedor de MFA
  - …
- Potencialmente, todas las aplicaciones (locales o en la nube) podrían dejar de estar disponib
  - Correo electrónico
  - VPN
  - CRM
  - …

Felicidades ! Es Hibrido!

- Un verdadero sistema MFA híbrido garantiza que las aplicaciones —especialmente las locales (on-premise)—se mantengan seguras y disponibles.
- Si la nube del MFA no está disponible… la parte local (on-premise) del sistema MFA híbrido continúa f unci ona ndo .

- Todo esto sin las desventajas de tener un sistema MFA separado, por ejemplo:
  - –Autenticadores duplicados
  - –Gestión del ciclo de vida
  - –Reglas de acceso

“Passwordless” debe ser resiliente frente a interrupciones. No solo por cuestiones regulatorias (NIS2, DORA).

Una historia completa Passwordless

1 Acceso Seguro que empodera productividad

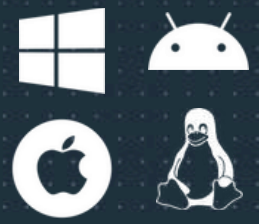
- Passwordless
- Resistente al Phishing
- Resistentea Malware
- Resistente a Fraude
- Resistentes a ataques de FuerzaBruta
- Resistentes a Bypass
- Resistentes al Outage

2 Verdadero Passwordless En cualquier momento

- Secure Enrollment
- Desktop Logon
- SaaS S ig n-o n
- Access Requests
- Secure Recovery
- O ffline Access

3 Una experiencia, Fuerza de trabajo unificada

Todos los usuarios



Cualquier plataforma

Cualquier ambiente