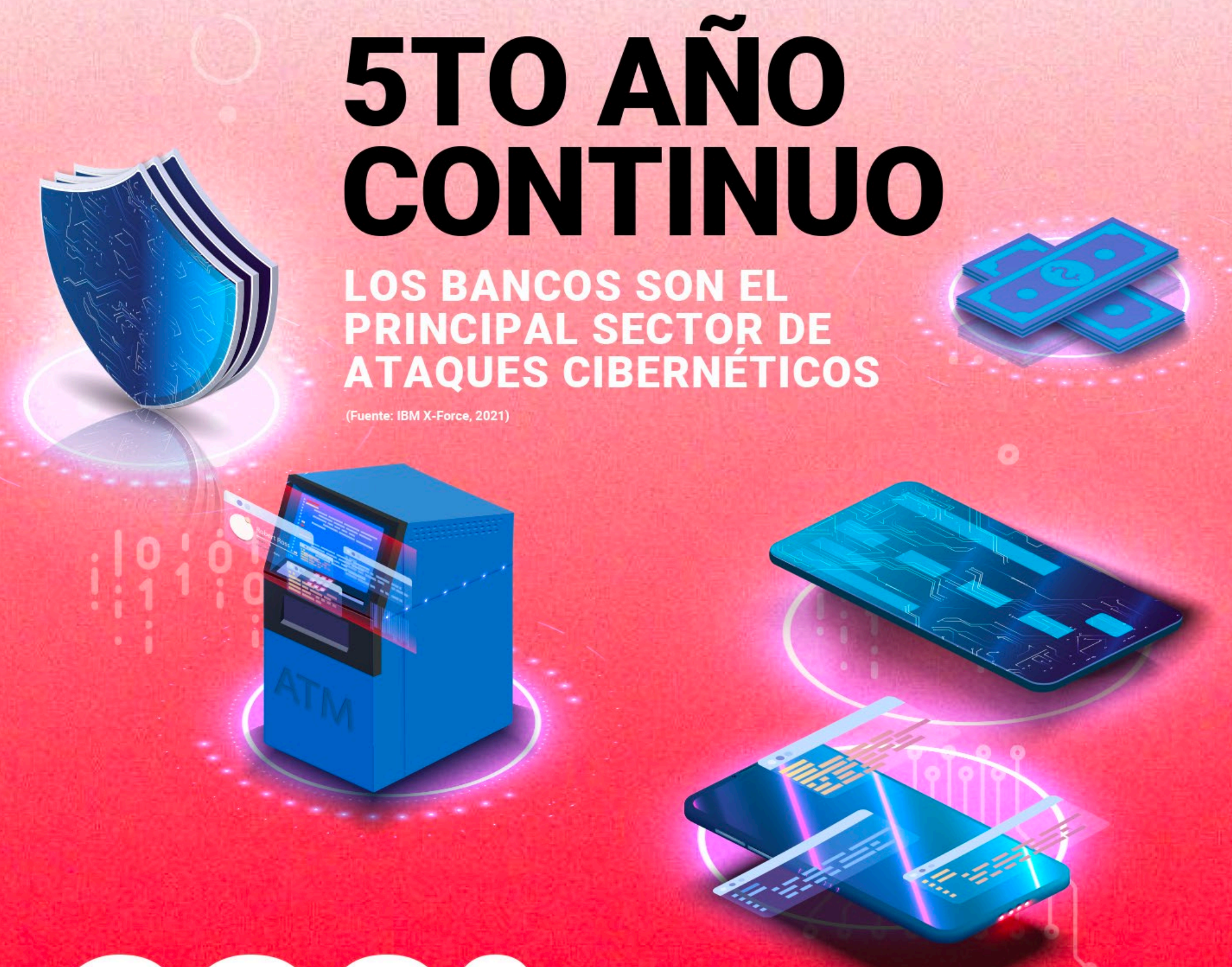
¡AUMENTAN LOS CIBERATAQUES A LA BANCA!



5TO AÑO CONTINUO

LOS BANCOS SON EL PRINCIPAL SECTOR DE ATAQUES CIBERNÉTICOS

(Fuente: IBM X-Force, 2021)

238%

Fue el porcentaje de ataques cibernéticos contra los bancos en el primer semestre de 2020

(Fuente VMWare Black)

SECUESTRO DE DATOS ATAQUES para frenar los sistemas y extorsionar por grandes pagos

FRAUDE FÍSICO como robar tarjetas

FRAUDE CIBERNÉTICO POR IRRUMPIR EN LOS sistemas y redes

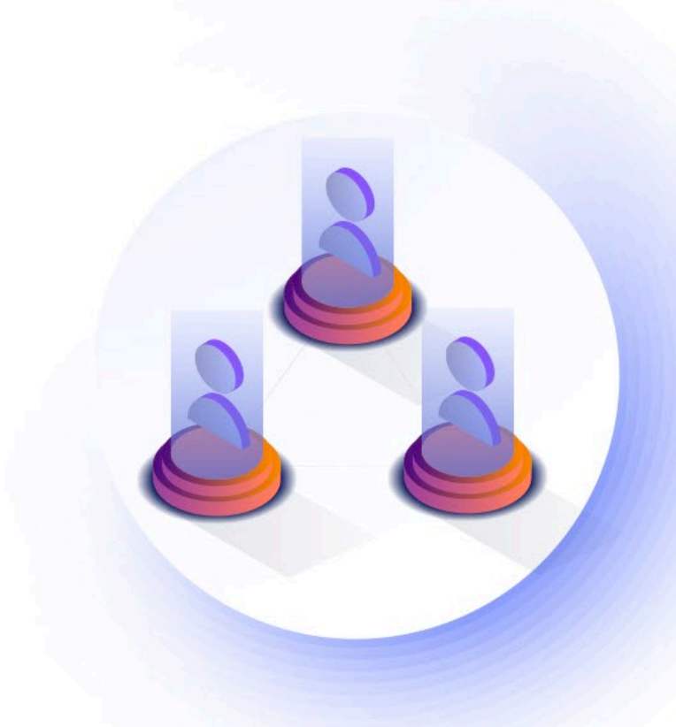
ATAQUE DE INTERMEDIARIO cuando un ciberdelincuente intenta secuestrar una operación en un dispositivo de autoservicio

ATAQUES LÓGICOS cuando un dispositivo de autoservicio es engañado dispensando dinero

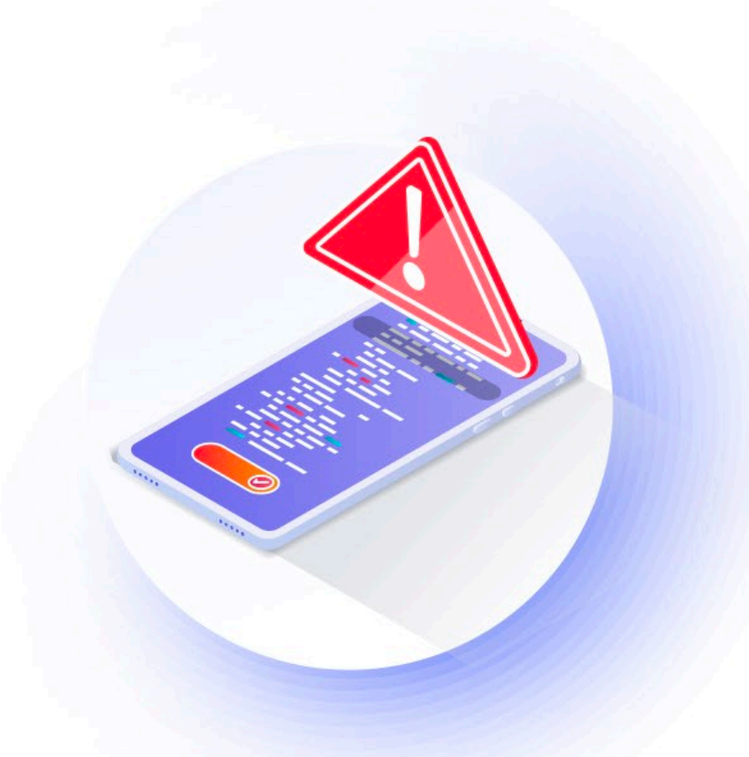
ATAQUE DE CAJA NEGRA al conectar un dispositivo en el cajero automático

LOS DISPOSITIVOS DE AUTOSERVICIO SON UN ESLABÓN DÉBIL DE SEGURIDAD

Los dispositivos de autoservicio contienen información delicada



Demasiadas personas tienen derechos de administrador



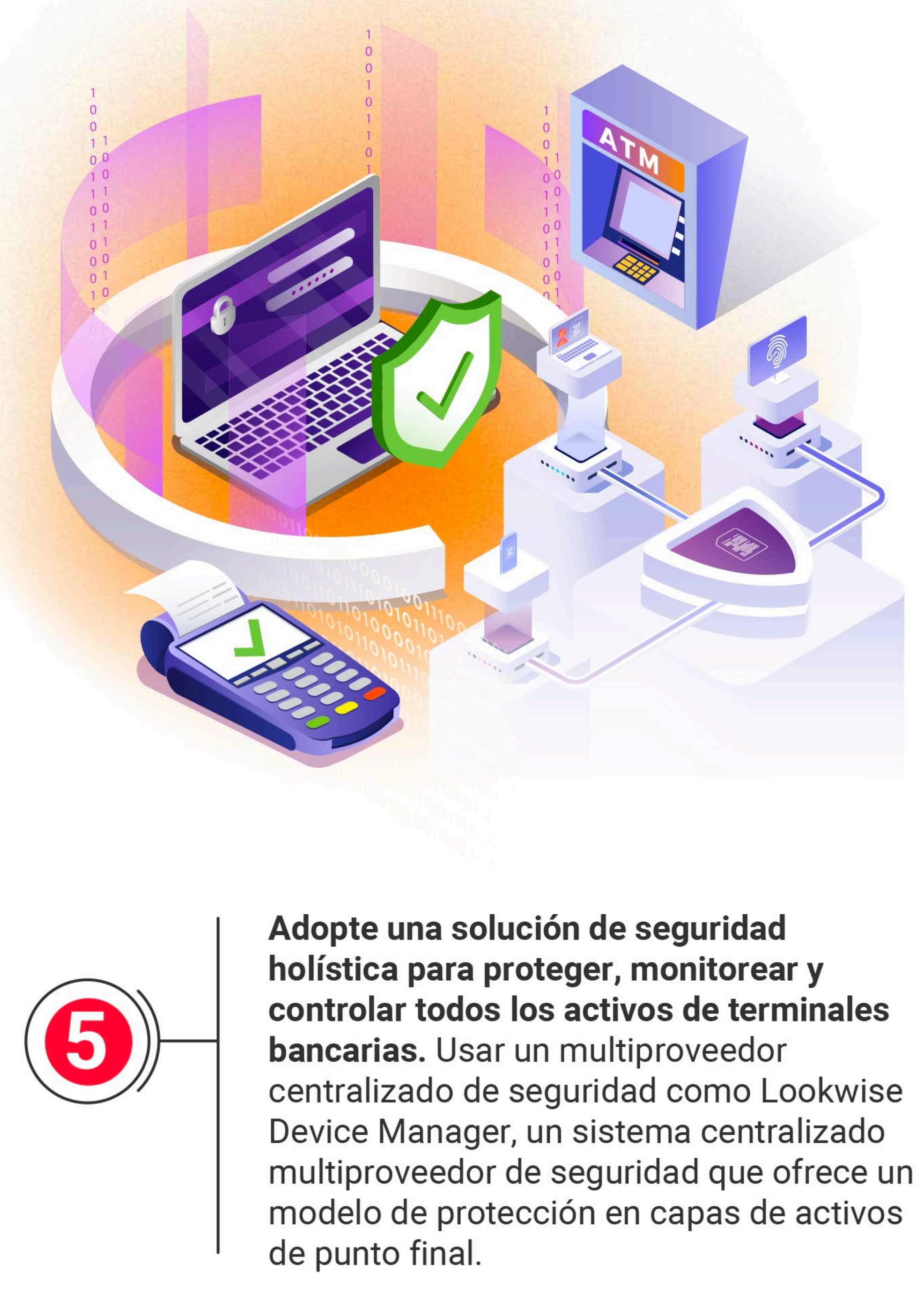
Los dispositivos de autoservicio comprenden diferentes hardware y software que hacen que sea difícil obtener una completa vista de lo que está pasando en condiciones de seguridad

Algunos dispositivos de autoservicio utilizan tecnología más antigua que los hacen menos seguros

Los dispositivos de autoservicio están mal monitoreados. Los bancos, muy a menudo, no saben qué tan seguros son los dispositivos

UNA ESTRATEGIA PARA DEFENDERSE

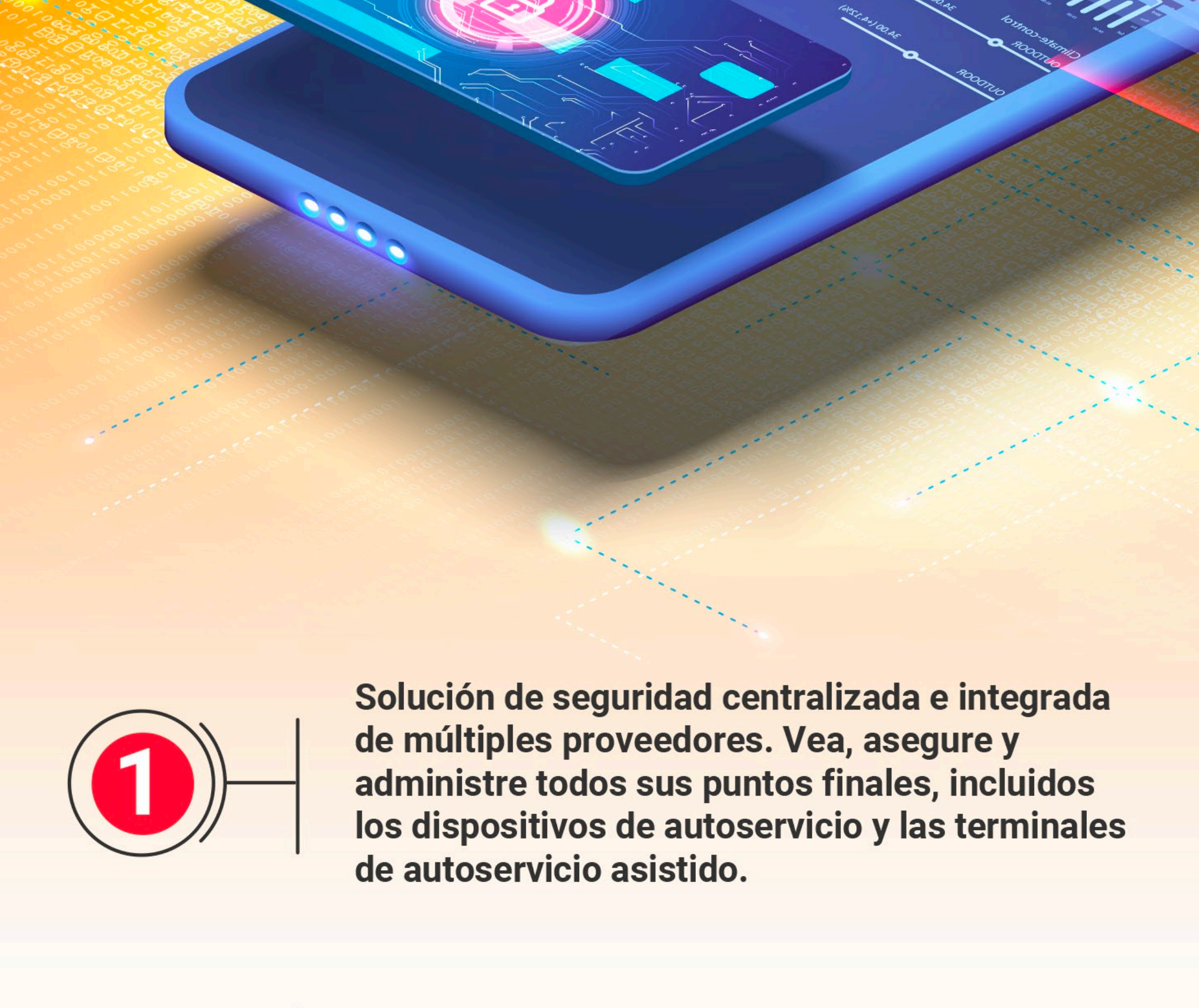
1. **Operaciones de control**
   - Controle completamente y reduzca el tiempo de la implementación de imágenes SW en el sitio del despliegue de actividades
   - Controle y supervise completamente las actividades de mantenimiento de dispositivos de autoservicio en el sitio
2. **PREVENCIÓN Y MONITOREO** de actividades imprevistas en el sitio
3. **MAXIMICE LOS DISPOSITIVOS DE AUTOSERVICIO EN EL TIEMPO DE ACTIVIDAD**
4. **PLAN PARA #NEXTGENBRANCH** asegurar los canales de banca digital, estaciones de trabajo remotas del personal y terminales de autoservicio asistido



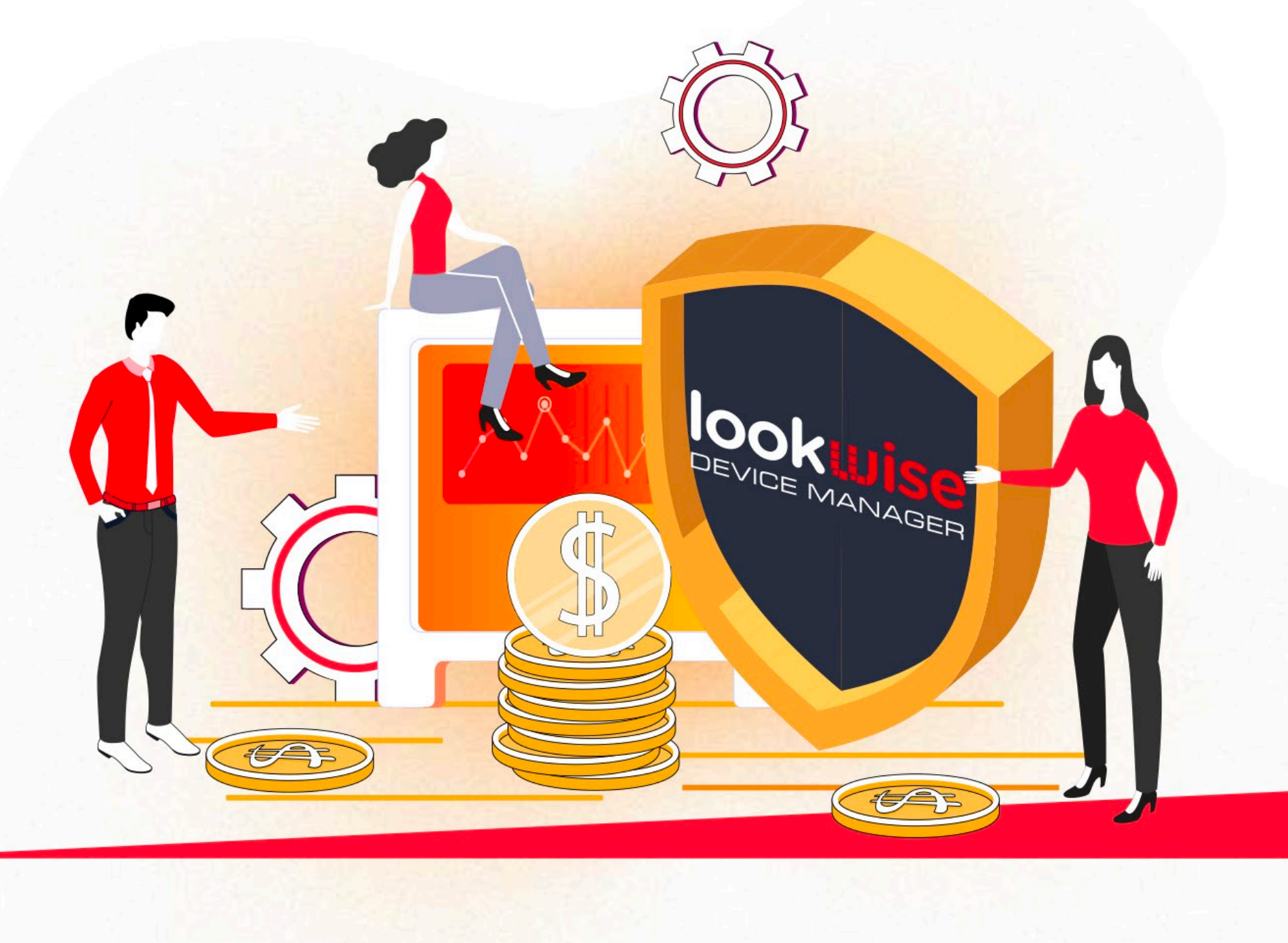
5. **Adopte una solución de seguridad holística para proteger, monitorear y controlar todos los activos de terminales bancarias.** Usar un multiproveedor centralizado de seguridad como Lookwise Device Manager, un sistema centralizado multiproveedor de seguridad que ofrece un modelo de protección en capas de activos de punto final.

lookwise® DEVICE MANAGER

CÓMO DEBE SER UNA CIBERSEGURIDAD EFECTIVA PARA LAS SUCURSALES DE PRÓXIMA GENERACIÓN



1. **Solución de seguridad centralizada e integrada de múltiples proveedores. Vea, asegure y administre todos sus puntos finales, incluidos los dispositivos de autoservicio y las terminales de autoservicio asistido.**
2. **En tiempo real puede ver y proteger todo con un modelo de protección en capas para dispositivos de autoservicio**
3. **Monitoreo proactivo, realizar bloqueos, detectar y solucionar fraudes e incidentes de seguridad rápida y efectivamente**
4. **Ahorro de tiempo y dinero gracias a las operaciones de ciberseguridad remotas y centralizadas en una sola GUI**
5. **La fuerte seguridad cibernética no se interpone en el camino de cómo ofrecer servicios interconectados y fáciles de usar**
6. **Puede ejecutar la ciberseguridad en dispositivos de forma remota, segura y controlada**
7. **Habilita la banca en sucursales de próxima generación omnicanal modernas y centradas en el cliente**



AURIGA the banking e-volution

lookwise® DEVICE MANAGER