Specops Device Trust: Acceso Zero Trust para entornos de trabajo

La identidad por sí sola no es suficiente. Si el acceso depende únicamente de "quién eres", basta un ataque de secuestro de sesión para comprometer la seguridad (incluso con MFA). Los atacantes roban tokens de sesión, utilizan dispositivos comprometidos y explotan las limitaciones de los controles tradicionales de identidad.

La solución de Specops Device Trust: autenticar y verificar tanto al usuario como al dispositivo en cada inicio de sesión y de forma continua durante toda la sesión.

Autenticación

- Vincula identidades a dispositivos autorizados
- Las credenciales robadas no pueden usarse desde los dispositivos del atacante

Verificación

- Comprueba la postura del dispositivo durante toda la sesión
- Fricción mínima para el usuario sin MDM invasivo

Remediación

- Remediación rápida en autoservicio, sin tickets de TI
- Correcciones con un clic y periodos de gracia para el usuario

Implementación e integración

- **Sistemas operativos:** Windows, macOS, Linux, iOS, Android
- **Integración con proveedores de identidad:** Okta, Azure AD/Microsoft Entra ID, Ping Identity
- **Modelo de implementación:** SaaS en la nube (disponibilidad >99,99%)
- **Impacto en el rendimiento:** No ralentiza los dispositivos de los usuarios
- **Opciones de despliegue:** Implementación gradual por grupo de usuarios, tipo de dispositivo o plataforma de sistema operativo

Cómo se diferencia Infinipoint de las soluciones MDM

Capacidades	Infinipoint	Soluciones MDM
Toma decisiones de acceso en tiempo real durante la autenticación, no se limita a verificaciones periódicas de cumplimiento	✓	✗
Verifica de forma continua durante toda la sesión, no únicamente en el inicio de sesión	✓	✗
Verifica de forma continua durante toda la sesión, no únicamente en el inicio de sesión	✓	✗
Funktioniert mit BYOD ("Bring Your Own Device") ohne invasive Installation	✓	✗
Se integra directamente con los proveedores de identidad (IdP) para una autenticación fluida	✓	✗

Funcionalidades principales

Funcionalidad	Beneficio
Verificación de dispositivo bajo modelo Zero Trust	Verifica la postura del dispositivo en cada solicitud de acceso y de forma continua durante toda la sesión. Incluye cientos de comprobaciones granulares de seguridad.
Autenticación resistente a phishing	Vincula usuarios a dispositivos de confianza. La autenticación solo se permite desde hardware aprobado y registrado, lo que previene ataques basados en credenciales y el secuestro de sesión.
Vinculación usuario-dispositivo	Permite registrar dispositivos autorizados y asociarlos a usuarios específicos. Ofrece control sobre el número de dispositivos, el tipo (escritorio, móvil) y la clasificación (corporativo o BYOD) por usuario o grupo.
Verificación continua de postura	Comprueba la seguridad del dispositivo en el inicio de sesión y cada 10 minutos durante la sesión activa. Detecta amenazas activas, controles de seguridad deshabilitados y fallos de cumplimiento.
Remediación en autoservicio con un solo clic	Permite a los usuarios corregir incumplimiento ("Activar cifrado", "Actualizar sistema operativo", "Activar firewall"), con periodos de gracia configurables. Los flujos de trabajo automatizados reducen la carga del equipo de TI manteniendo la postura de seguridad.
Seguridad de dispositivos de terceros	Ofrece visibilidad completa sobre todos los endpoints, incluidos dispositivos BYOD no gestionados y equipos de contratistas. Distingue entre activos corporativos gestionados y shadow IT que accede a recursos corporativos.
Políticas de acceso basadas en riesgo	Permite definir políticas granulares según grupos de usuarios, tipos de dispositivos, plataformas de sistema operativo y estado de cumplimiento en tiempo real. Las decisiones de acceso se ajustan dinámicamente en función de la salud actual del dispositivo.

Specops Device Trust selbst entdecken

Más información: https://specopssoft.com/es/productos/specops-device-trust/
Solicita una demo: https://specopssoft.com/es/contacto/