# Los siete elementos de una arquitectura de confianza cero de gran éxito

Guía del arquitecto de Zscaler Zero Trust Exchange

## Las arquitecturas de seguridad tradicionales dejan vulnerables a las empresas

Los enfoques de seguridad de statu quo, que utilizan cortafuegos y VPN, conectan a los usuarios a la red, lo que permite a los atacantes comprometer a los usuarios, dispositivos y cargas de trabajo, y se mueven lateralmente para alcanzar activos de alto valor y extraer datos confidenciales.

## El lugar de trabajo híbrido actual requiere un enfoque de confianza cero para la seguridad

Para proteger sus organizaciones, los líderes empresariales innovadores recurren a la confianza cero, un enfoque de seguridad integral basado en el acceso con privilegios mínimos y la idea de que ningún usuario o aplicación debe ser fiable de forma inherente.

## ¿Cómo se implementa una arquitectura de confianza cero?

La verdadera confianza cero se entrega a través de **Zscaler Zero Trust Exchange**, una plataforma nativa de la nube integrada que conecta de forma segura a los usuarios, los dispositivos (IoT/OT) y las cargas de trabajo a las aplicaciones sin conectarse a la red.

## Siete elementos forman la base de una verdadera arquitectura de confianza cero

Con este enfoque único, Zscaler elimina la superficie de ataque, evita el movimiento lateral de las amenazas y protege su empresa frente al riesgo y la pérdida de datos.

### 1. ¿Quién se está conectando?

Finaliza la conexión solicitada, luego verifica el usuario, el dispositivo IoT/OT o la identidad de la carga de trabajo.

### 2. ¿Cuál es el contexto de acceso?

Valida el contexto del solicitante de conexión, analizando atributos como el rol, la responsabilidad, el tiempo de solicitud y las circunstancias de la solicitud.

### 3. ¿Hacia dónde va la conexión?

Confirma que el destino es conocido, comprendido y categorizado contextualmente para el acceso. Si se desconoce el destino, marque para realizar más análisis.

### 4. Evalúe el riesgo

Aprovecha la IA para calcular dinámicamente una puntuación de riesgo asociada a la conexión en función de factores como la postura del dispositivo, las amenazas, el destino, el comportamiento y la política.

### 5. Prevenga riesgos

Inspeccione el tráfico y el contenido en línea para identificar y bloquear contenido malicioso.

### 6. Prevenga la pérdida de datos

Inspeccione el tráfico saliente para identificar los datos confidenciales y evitar su exfiltración.

### 7. Aplique las políticas

Aplica la política por sesión y determina la acción condicional que debe tomarse con respecto a la conexión solicitada. Si se toma la decisión de permiso, se establece una conexión segura con Internet, la aplicación SaaS o la aplicación interna.

¿Está preparado para aprender a aplicar estos siete elementos fundamentales de un diseño de confianza cero a su negocio para **eliminar su superficie de ataque, evitar el movimiento lateral de amenazas** y **proteger a su organización contra la vulneración y la pérdida de datos?**

Lea el libro electrónico



Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.es