LISTA DE COMPROBACIÓN DE AKAMAI

Capacidades de una plataforma Zero Trust

Una plataforma Zero Trust eficaz debe combinar soluciones distintas que tradicionalmente han funcionado por separado, como el acceso de red Zero Trust (ZTNA), la microsegmentación, el firewall de DNS y la búsqueda de amenazas, en una plataforma integrada con una única consola. Si se logra implementar un modelo Zero Trust de forma rápida y eficaz, se logra detener los programas de secuestro, cumplir con las exigentes normativas y proteger tanto a los empleados ubicados en distintos puntos del mundo como la infraestructura de nube híbrida. Esta lista de comprobación puede utilizarse para evaluar las capacidades del proveedor o consultar los requisitos de implementación de enfoques Zero Trust con una única plataforma.

Categoría 1: Requisitos de la plataforma

Su solución de plataforma Zero Trust debe ser flexible, escalable y fácil de gestionar.

- [ ] Escalabilidad para responder a los picos de tráfico y proporcionar protección continua sin que afecte al rendimiento
- [ ] Capacidad de integración con las herramientas de seguridad existentes que los clientes tienen en marcha, como SIEM, SOAR, EDR o CMDB, entre otras
- [ ] Cobertura para centros de datos heterogéneos: entornos híbridos y multinube, sistemas heredados, dispositivos de usuario final, clústeres de Kubernetes, máquinas virtuales, entornos de IoT/OT y mucho más
- [ ] Modelos de implementación flexibles compatibles con diversas arquitecturas híbridas (en la nube, virtuales o locales)
- [ ] Capacidad para adaptarse a implementaciones basadas en agentes y sin agentes (IoT/OT, PaaS)
- [ ] Compatibilidad con Windows, Linux y macOS, así como con sistemas operativos heredados
- [ ] Funciones de registro de auditoría para garantizar el registro de todas las acciones

Categoría 2: Requisitos de visibilidad

Tener una amplia visibilidad es fundamental para comprender el entorno, identificar conexiones sospechosas y responder de forma rápida y precisa a las amenazas.

- [ ] Vista de mapa de todas las aplicaciones y flujos de carga de trabajo, así como acceso de usuario a aplicaciones en cualquier entorno (contenedores, sin servidor, IaaS o PaaS), todo desde una única consola
- [ ] Flujos históricos y en tiempo real para investigación y análisis forenses
- [ ] Interoperabilidad con firewall y hardware de terceros, como dispositivos de conmutación
- [ ] Capacidad para recopilar datos de distintas fuentes ajenas, como CMDB, EDR y API en la nube para etiquetas y reglas contextuales
- [ ] Asistencia para el etiquetado, preferiblemente mediante el uso de IA para aumentar la velocidad y la precisión

Categoría 3: Requisitos de las políticas

Tanto las políticas este-oeste (microsegmentación) como las políticas norte-sur (ZTNA) se aplican desde un solo lugar, en función de atributos que se pueden utilizar en diversos casos de uso, como la protección frente a programas de secuestro, la protección de los teletrabajadores, la respuesta ante ataques de día cero y el cumplimiento normativo.

- [ ] Política definida por software y distribuida por toda la empresa sin necesidad de firewall internos físicos que creen obstáculos
- [ ] Reglas basadas en distintos atributos de carga de trabajo en lugar de solo IP y puertos
- [ ] Aplicación de políticas detalladas centradas en las aplicaciones para proteger las cargas de trabajo a nivel de puerto, procesos e incluso servicios
- [ ] Un motor de recomendación de políticas con plantillas personalizadas y listas para usar, preferiblemente mediante IA, que acelera la creación de políticas
- [ ] Directivas aplicadas con o sin agente
- [ ] Controles de políticas basados en una asignación de flujos exhaustiva
- [ ] Políticas preconfiguradas para la reducción de riesgos globales basadas en prácticas recomendadas del sector
- [ ] Política para la nube híbrida en entornos virtualizados, IaaS y PaaS
- [ ] Políticas vinculadas a la carga de trabajo con la capacidad de seguirla si se mueve, migra o cambia
- [ ] Política de acceso para los usuarios de la oficina y que trabajan de forma remota

Categoría 4: Requisitos de los componentes Zero Trust

Entre las diversas funciones integradas en una plataforma unificada Zero Trust, el acceso a la red Zero Trust y la microsegmentación destacan como pilares fundamentales. Estas tecnologías permiten a las organizaciones implementar controles Zero Trust sin que esto afecte negativamente a la plantilla ni a la continuidad del negocio.

- [ ] Motor de políticas de red y acceso unificado (control combinado este-oeste y norte-sur)
- [ ] Aplicación sólida de la identidad con autenticación multifactor (MFA) FIDO2
- [ ] Capacidad de proteger los entornos de TI y los usuarios de una amplia gama de amenazas mediante la supervisión y el filtrado del tráfico de DNS
- [ ] Detección continua de amenazas evasivas y supervisión de la situación de seguridad
- [ ] Uso compartido de señales en las herramientas de la plataforma para garantizar que un atacante se detenga incluso si logra perforar el mecanismo de acceso
- [ ] Adopción de sistemas de engaño dinámicos capaces de rastrear y poner en cuarentena a los atacantes
- [ ] Capacidad para consultar terminales o servidores con el fin de detectar vulnerabilidades y mitigar rápidamente la detección de programas de secuestro

Categoría 5: Requisitos de IA integrada

Muchos aspectos de la implementación eficaz de Zero Trust se pueden optimizar con el uso de la IA. Esto acelera y simplifica la creación de políticas, el cumplimiento, la respuesta a incidentes y la evaluación de vulnerabilidades.

- [ ] Comunicación con registros de red mediante lenguaje natural para reducir el tiempo de respuesta a incidentes, los esfuerzos de alcance de cumplimiento y mucho más
- [ ] Optimización de todo el proceso de políticas con IA que sugiere etiquetas y políticas basadas en los patrones de tráfico exclusivos
- [ ] Traducción del lenguaje natural en sintaxis para buscar rápidamente vulnerabilidades en la red sin tener que investigar IOC ni escribir consultas personalizadas
- [ ] Mecanismos de búsqueda de amenazas mediante IA para métodos de detección avanzados con el fin de detectar anomalías y actividades maliciosas que las herramientas tradicionales no detectan

Visite Seguridad Zero Trust de Akamai para obtener más información.