LISTA DE VERIFICAÇÃO DA AKAMAI

Recursos da plataforma Zero Trust

Uma plataforma Zero Trust eficaz consolida soluções pontuais únicas, incluindo ZTNA (Zero Trust Network Access), microssegmentação, firewall de DNS e busca por ameaças, em uma plataforma integrada de console. A implantação rápida e eficaz do Zero Trust significa interromper o ransomware, atender às exigências de conformidade e proteger sua força de trabalho distribuída, assim como sua infraestrutura de nuvem híbrida. Esta lista de verificação pode ser usada para avaliar os recursos do fornecedor ou servir como lista dos requisitos para implementar o Zero Trust com uma única plataforma.

Categoria 1: Requisitos de plataforma

Sua solução de plataforma Zero Trust deve ser flexível, escalável e fácil de administrar.

- [ ] Escalabilidade para atender às demandas de tráfego e fornecer proteção contínua sem perda de desempenho
- [ ] Capacidade de integração com as ferramentas de segurança existentes que os clientes têm atualmente, como SIEM, SOAR, EDR, CMDB e muito mais
- [ ] Cobertura para data centers heterogêneos: ambientes híbridos e multinuvem, sistemas legados, dispositivos de usuário final, clusters de Kubernetes, máquinas virtuais, ambientes IoT/OT e muito mais
- [ ] Modelos de implantação flexíveis compatíveis com diversas arquiteturas híbridas: nuvem, virtual, no local
- [ ] Capacidade de acomodar implantações sem agentes e baseadas em agentes (IoT/OT, PaaS)
- [ ] Suporte para Windows, Linux e macOS, assim como para sistemas operacionais legados
- [ ] Recursos de registro de auditoria para garantir o registro de todas as ações

Categoria 2: Requisitos de visibilidade

A visibilidade profunda é fundamental para entender o ambiente, identificar conexões suspeitas e responder rápida e precisamente às ameaças.

- [ ] Visualização semelhante a um mapa de todos os aplicativos e fluxos de carga de trabalho, assim como acesso de usuário-aplicativo em qualquer ambiente, como contêineres, sem servidor, IaaS ou PaaS, tudo a partir de um único console
- [ ] Fluxos históricos e em tempo real para investigação e perícia forense
- [ ] Interoperabilidade com firewalls e hardware de terceiros, como dispositivos de switch
- [ ] Capacidade de coletar dados de várias fontes de terceiros, como CMDB, EDR e APIs de nuvem para regras e rótulos contextuais
- [ ] Assistência à rotulagem, de preferência aproveitando a IA para ter velocidade e precisão

Categoria 3: Requisitos de política

As políticas leste-oeste (microssegmentação) e norte-sul (ZTNA) são aplicadas a partir de um só lugar, com base em atributos que podem ser usados em diversos casos de uso, como proteção contra ransomware, proteção da força de trabalho remota, resposta a ataques de dia zero e conformidade.

- [ ] Política definida por software e distribuída por toda a empresa sem a necessidade de firewalls físicos internos que criem gargalos
- [ ] Regras criadas com base em vários atributos de carga de trabalho em vez de apenas IPs e portas
- [ ] Políticas granulares centradas em aplicativos para que as cargas de trabalho sejam protegidas ao nível de porta, processo e até mesmo serviço
- [ ] Um mecanismo de recomendação de política com modelos prontos e personalizados, de preferência utilizando IA, que acelera a criação de políticas
- [ ] Políticas impostas com ou sem um agente
- [ ] Controles de política baseados em mapeamento de fluxo abrangente
- [ ] Políticas pré-configuradas para redução global de riscos com base nas práticas recomendadas do setor
- [ ] Política para nuvem híbrida em ambientes virtualizados, IaaS e PaaS
- [ ] Políticas vinculadas à carga de trabalho com a capacidade de acompanhá-la se ela for movida, migrada ou alterada
- [ ] Política de acesso para usuários no escritório e no trabalho remoto

Categoria 4: Requisitos do componente Zero Trust

Das várias funções integradas a uma plataforma Zero Trust unificada, o Zero Trust Network Access e a microssegmentação se destacam como os pilares fundamentais. Essas tecnologias possibilitam que as organizações implantem controles Zero Trust sem afetar negativamente a força de trabalho e a continuidade dos negócios.

- [ ] Mecanismo unificado de acesso e política de rede (controle combinado leste-oeste e norte-sul)
- [ ] Forte imposição de identidade com MFA (autenticação multifator) FIDO2
- [ ] Capacidade de proteger os ambientes de TI e os usuários contra uma ampla gama de ameaças, monitorando e filtrando o tráfego de DNS
- [ ] Detecção contínua de ameaças evasivas e monitoramento da postura de segurança
- [ ] Compartilhamento de sinal entre as ferramentas da plataforma para garantir que um invasor seja bloqueado mesmo que ele consiga atravessar o mecanismo de acesso
- [ ] Adoção de sistemas com tecnologia "deception" capazes de rastrear e colocar os invasores em quarentena
- [ ] Capacidade de consultar pontos de extremidade ou servidores quanto à presença de vulnerabilidades para permitir a rápida mitigação e detecção de ransomware

Categoria 5: Requisitos de IA integrada

Muitos aspectos da implementação eficaz do Zero Trust podem ser simplificados com o uso de IA. Isso agiliza e simplifica a criação de políticas, a conformidade, a resposta a incidentes e a avaliação de vulnerabilidades.

- [ ] Comunicação com logs de rede usando linguagem natural para ajudar a reduzir o tempo de resposta a incidentes, os esforços de escopo de conformidade e muito mais
- [ ] Simplificação de todo o processo de política com IA que sugere rótulos e políticas com base em seus padrões de tráfego exclusivos
- [ ] Tradução de linguagem natural em sintaxe para procurar rapidamente vulnerabilidades em sua rede sem ter que pesquisar IOCs ou escrever consultas personalizadas
- [ ] Mecanismos de IA de busca por ameaças com métodos avançados de detecção para encontrar anomalias e atividades mal-intencionadas que as ferramentas tradicionais deixam passar

Visite a página de segurança Zero Trust da Akamai para saber mais.