RESUMO DA SOLUÇÃO AKAMAI

Simplificação e proteção com um modelo Zero Trust completo

Zero Trust é uma abordagem estratégica de cibersegurança que protege uma organização removendo a confiança implícita entre usuários, dispositivos, redes, dados e aplicações. Em vez de pressupor que todos os elementos por trás do firewall empresarial são seguros, a abordagem Zero Trust pressupõe uma violação a qualquer momento e aplica o acesso de menor privilégio a todas as solicitações, independentemente da origem.

Por que a Zero Trust é importante agora?

A Zero Trust se tornou uma prioridade para as organizações que precisam se adaptar de modo mais eficaz ao ambiente moderno em constante mudança. Essas organizações estão procurando um novo modelo de segurança que englobe a força de trabalho híbrida e proteja usuários, dispositivos e aplicações em qualquer lugar.

Princípios da arquitetura moderna Zero Trust

- Verificar explicitamente, sempre no contexto
- Aplicar o privilégio mínimo explicitamente
- Monitorar continuamente

A consolidação é essencial

Abordagem completa e integrada

Uma abordagem holística à Zero Trust deve se estender a todas as entidades da organização, incluindo identidades, redes e aplicações. A Zero Trust serve como uma estratégia completa, por isso requer a integração de todos os elementos. A utilização de várias soluções pontuais e não muito bem integradas não se alinha a essa abordagem estratégica.

A Akamai montou um portfólio holístico e robusto para fornecer todas as soluções Zero Trust essenciais para a organização moderna. Em vez de instalar, executar e corrigir vários produtos de segurança, as organizações podem confiar em um só fornecedor para disponibilizar todas as tecnologias necessárias e desfrutar de custos reduzidos e eficiências operacionais aprimoradas.

Compartilhamento de sinal entre soluções

A Akamai trabalhou com automação integrada em seu portfólio Zero Trust, reduzindo significativamente a complexidade e a personalização. Dessa forma, os produtos do portfólio podem compartilhar conhecimentos sobre ameaças entre si, o que os torna mais seguros. Se um produto identificar uma ameaça, outro produto poderá ser alertado para mitigá-la.

Benefícios

- **Força de trabalho distribuída**
  Permita que os usuários trabalhem com mais segurança em qualquer lugar, a qualquer momento e em qualquer dispositivo
- **Migração para nuvem**
  Forneça controle de acesso seguro em ambientes de nuvem e de nuvem híbrida
- **Mitigação de riscos**
  Interrompa ameaças e minimize o movimento lateral de ransomware e outros tipos de malware
- **Conformidade**
  Suporte à conformidade com microperímetros em torno de dados confidenciais

Akamai

Um portfólio holístico completo: usuários, aplicações e rede

Proteja a carga de trabalho

Akamai Guardicore Segmentation Zero Trust para aplicações

A Akamai Segmentation fornece a solução de microssegmentação líder do setor, projetada para limitar a propagação de ransomware e outros malwares. O produto fornece visibilidade e compreensão das cargas de trabalho, processos e aplicações, bem como implementação de políticas de acesso.

Proteja a rede

Enterprise Application Access: acesso à rede Zero Trust

A tecnologia Zero Trust Network Access da Akamai foi projetada para substituir a tecnologia tradicional de VPN para uma forte identidade de usuário. Em vez de colocar toda a rede em risco, o Enterprise Application Access permite o acesso de usuário com base no app específico que o usuário precisa acessar para executar uma função. O Enterprise Application Access oferece visibilidade sobre a identidade dos usuários e uma sólida aplicação de identificação e autenticação.

Proteja o usuário

Secure Internet Access: acesso Zero Trust à internet

O Secure Internet Access é uma solução de gateway web segura baseada em nuvem. O Secure Internet Access inspeciona todas as solicitações da Web feitas pelos usuários e aplica inteligência de ameaças em tempo real e técnicas avançadas de análise de malware para garantir que apenas conteúdo seguro seja entregue. Solicitações e conteúdos mal-intencionados são bloqueados de maneira proativa.

Autenticação multifator: sólida identidade Zero Trust

A Akamai MFA protege as contas dos funcionários contra phishing e outros ataques de máquina no meio. Isso garante que apenas funcionários devidamente autenticados possam acessar as contas de sua propriedade, que outros acessos sejam negados e a invasão de contas de funcionários seja evitada.

Rastrear e monitorar

Hunt: serviços de segurança

Ao adotar uma abordagem de "sempre presumir um estado de violação", a equipe de elite de caçadores de ameaças da Akamai procura continuamente comportamentos de ataque anômalos e ameaças avançadas, que muitas vezes escapam às soluções de segurança padrão. Nossos caçadores de ameaças notificam você imediatamente sobre qualquer incidente crítico detectado na rede e trabalham em conjunto com sua equipe para corrigir a situação.

A vantagem da Akamai

A Akamai oferece algumas vantagens que a diferenciam dos outros fornecedores de Zero Trust. Nós oferecemos a cobertura mais ampla: sistemas legados e modernos; Windows e Linux; local e virtualizada, contêineres e muito mais. Devido aos nossos recursos incomparáveis de visibilidade, os usuários têm o contexto completo e sabem o que cada carga de trabalho está fazendo. E nossos serviços internos de caça a ameaças de elite ampliam os recursos de qualquer equipe de segurança e permitem que sua organização fique à frente das ameaças.

Para saber mais sobre Zero Trust e como começar, visite akamai.com.