História do cliente da Akamai

Uma empresa de saúde dos EUA evitou 4.000 ataques cibernéticos em um único dia

Engenheiros de rede usaram visibilidade de camada 7 e políticas inteligentes via microssegmentação para reduzir os riscos cibernéticos

Preveniu ransomware

Ganhou visibilidade aprofundada

Melhorou as políticas

Conectando pacientes aos cuidados essenciais

Imagine tentar proteger uma rede que impacta diretamente a vida dos pacientes enquanto se mantém à frente de ataques cibernéticos cada vez mais sofisticados. Essa era a realidade de uma empresa de saúde de médio porte. Sua equipe de engenharia de rede enfrentava crescentes ameaças de ransomware e uma necessidade de maior visibilidade, por isso, a equipe recorreu à Akamai Guardicore Segmentation para fortalecer a postura de segurança da empresa.

Expandindo a arquitetura Zero Trust

A organização tinha uma visão ousada: fortalecer seu ambiente de TI com os princípios do Zero Trust, enquanto atendia aos requisitos de conformidade HIPAA e SOC 2. Como as apostas eram altas, os objetivos da equipe de engenharia de rede incluíam:

- Manter aplicativos críticos online mesmo durante incidentes de segurança
- Reduzir o impacto de ataques de ransomware, limitando sua propagação
- Obter visibilidade detalhada da rede, muito além dos firewalls tradicionais

A organização precisava de uma solução de microssegmentação escalável e econômica que não exigisse a substituição da infraestrutura de TI existente. Além disso, a solução precisava ser simples o suficiente para ser gerida por uma equipe enxuta e escalável para acompanhar o crescimento da empresa.

Como explicou um engenheiro de rede: "O ransomware atinge a saúde. Quanto mais rápido conseguirmos isolar e eliminar essas ameaças, melhor".

Healthcare Company

Localização

Estados Unidos

Setor

Saúde e ciências biológicas

Solução

Akamai Guardicore Segmentation

Akamai

Encontrando a solução de microssegmentação ideal

Após descartar rapidamente a opção de uma abordagem em contêineres, a empresa avaliou soluções de microssegmentação. "Queríamos os mesmos recursos que vemos nos firewalls de última geração, ou seja, visibilidade na camada de aplicativo", explicou o engenheiro de rede.

Após avaliar várias soluções, a organização encontrou a Akamai Guardicore Segmentation. Uma demonstração positiva, juntamente com o suporte prático dos engenheiros da Akamai, selou o acordo. A solução atendeu a todos os requisitos, incluindo:

- **Visibilidade aprofundada:** inspeção da camada 7 e insights completos da rede
- **Facilidade de implantação:** agentes baseados em software sem hardware adicional
- **Resiliência:** nenhum ponto único de falha na rede principal
- **Flexibilidade:** suporte para diversos sistemas operacionais

De acordo com o vice-presidente de infraestrutura de TI e segurança da informação, a Akamai Guardicore Segmentation oferece uma grande vantagem para equipes enxutas. "Imediatamente após iniciar a implantação, vimos benefícios em relação à visibilidade e ao controle."

"Não precisamos comprar e gerenciar vários firewalls leste-oeste (proporcionando uma enorme economia de custos) e ainda obtemos um nível de visibilidade que não seria possível com firewalls", acrescentou o gerente de infraestrutura de TI.

Parando o ransomware no seu caminho

Os resultados foram imediatos e impressionantes. Ao cercar melhor seus aplicativos e usar as políticas de prevenção de ransomware prontas para uso da Akamai Guardicore Segmentation, a equipe neutralizou 4.000 ataques cibernéticos no primeiro dia. A solução ainda adaptou as políticas para atender às necessidades específicas da organização.

"Para políticas intermediárias, usamos o modo de alerta para sinalizar incidentes sem causar tempo de inatividade. É uma ótima maneira de refinar as políticas sem interrupções", compartilhou o engenheiro de rede.

> A Akamai Guardicore Segmentation nos ajudou a fazer mais do que apenas lidar com nossas preocupações com ransomware: ela elevou nossa abordagem à cibersegurança.
>
> **– Engenheiro de rede**

> "Escalar a 'montanha do Zero Trust' é incrivelmente desafiador. A Akamai Guardicore Segmentation nos ajudou a subir rapidamente essa montanha enquanto reduzia os desafios de custo e complexidade."
>
> — Vice-presidente de infraestrutura de TI e segurança da informação

Obtendo uma visão incomparável na camada 7

De acordo com o gerente de infraestrutura de TI, a Akamai Guardicore Segmentation oferece valiosas visualizações dos fluxos de tráfego entre diferentes aplicativos. Isso revelou um tesouro de dados para a equipe. Agora, a equipe pode inspecionar detalhes granulares além dos logs da camada 4: IDs de usuários, entradas de linha de comando e até correlações de serviços.

"Nossa equipe de rede pode analisar o fluxo de tráfego para solucionar problemas e fornecer à nossa equipe de segurança as informações necessárias para investigar totalmente os incidentes", observou o engenheiro de rede.

Essa visibilidade foi útil durante uma violação inesperada de política. Um novo funcionário conectou um PC diretamente ao CPE (Equipamento nas Instalações do Cliente) do provedor em vez de a uma porta LAN protegida por um roteador doméstico. Isso foi estritamente proibido, já que o CPE atribuiu ao PC um IP público, tornando-o suscetível a varreduras públicas da internet.

Como explicou o engenheiro de rede da organização: "A Akamai Guardicore Segmentation detectou o problema instantaneamente, permitindo-nos isolar o PC e resolver a situação antes que ela se escalasse. Além disso, isso nos inspirou a criar uma política para prevenir que esse tipo de incidente ocorra no futuro".

Rotulagem mais inteligente, melhores políticas

Graças à rotulagem intuitiva e à criação de políticas, a equipe de engenharia de rede conseguiu mapear facilmente o tráfego e aplicar regras de segurança. De acordo com o engenheiro de rede: "Podíamos decidir o que funciona melhor para o nosso ambiente. Esse recurso nos impressionou muito mais do que esperávamos e nos ajudou a criar políticas de forma eficiente".

Por exemplo, a equipe limitou o acesso aos servidores de impressão, permitindo apenas zonas confiáveis: uma solução rápida que melhorou a postura geral de segurança da organização. "Isso nos possibilitou solucionar os problemas mais simples de imediato", continuou o engenheiro.

Visibilidade que transmite confiança

Um benefício inesperado? Uma visão clara do fluxo de tráfego interno e do comportamento dos aplicativos. Essa nova visibilidade permitiu uma melhor colaboração com os proprietários dos aplicativos e facilitou as janelas de manutenção. Por exemplo, a equipe agora pode mostrar aos proprietários de aplicativos se o tráfego deles está sendo bloqueado.

"No passado, a solução de problemas e a preparação para o futuro eram um problema. Agora, durante as mudanças, podemos confirmar com confiança quando o tráfego foi transferido dos servidores antigos para os novos. Isso nos permitiu desativar sistemas legados com certeza", disse o engenheiro de rede.

O vice-presidente de infraestrutura de TI e segurança da informação da organização concluiu: "A Akamai Guardicore Segmentation já teve um impacto e se tornou um produto essencial em nossa prática de segurança. Estou ansioso para expandir sua implementação em toda a organização".