HISTÓRIA DO CLIENTE DA AKAMAI

Empresa de manufatura de capital aberto padroniza controles de segurança e economiza tempo com a Akamai Guardicore Segmentation

A empresa de manufatura precisava de uma solução global segura

Visibilidade abrangente da rede

Segmentação entre infraestruturas de TI

Resposta a ameaças de ransomware

O cliente

Essa empresa líder em manufatura é negociada publicamente na NYSE e atende mercados em todo o mundo.

O desafio

Proteger uma empresa global

O grupo de segurança de TI é responsável por vários locais em todo o mundo. A maioria dos quais são instalações de uso misto para escritório e fábrica. Para garantir uma postura de segurança forte, a equipe precisava padronizar os controles de segurança em toda a organização e fornecer proteção consistente em todas as regiões geográficas em que está distribuída.

"Queríamos mudar de uma rede aberta e plana para uma arquitetura segmentada com as práticas recomendadas", explicou o arquiteto de infraestrutura que lidera o projeto de segmentação.

Como muitas organizações, essa empresa industrial inicialmente recorreu aos firewalls para o projeto.

No entanto, o gerenciamento de várias regras baseadas em infraestrutura, alterações e atualizações de estações de trabalho em toda a rede rapidamente se tornou demorado, mesmo em um único local. Além disso, embora a visibilidade tenha melhorado, ela permaneceu restrita a zonas específicas, dificultando a obtenção de uma visão completa e centralizada da atividade da rede e das dependências entre os ativos.

Interrupção da movimentação lateral não autorizada

Embora os firewalls oferecessem alguns controles de segmentação básicos, eles não conseguiam resolver outra preocupação importante da equipe de segurança: as comunicações ponto a ponto não gerenciadas. Por isso, era essencial estender a proteção e a visibilidade até essa área específica. Não abordá-la deixaria a organização vulnerável a ataques pass-the-hash, ransomware e outras ameaças que dependem da movimentação lateral entre os pontos de extremidade para se propagar.

Manufacturing Company

Localização
Estados Unidos

Setor
Fabricação

Solução
Akamai Guardicore Segmentation

Principais impactos

- Mitiga a propagação de malware por meio de movimento lateral
- Fornece visibilidade granular
- Protege os pontos de extremidade com segmentação
- Facilita a resposta a incidentes

Akamai

A escolha da solução

Depois de várias implantações complicadas de controle de firewall, a equipe descobriu a Akamai Guardicore Segmentation e iniciou discussões internas sobre os benefícios e as possibilidades de uma segmentação de última geração.

Foi necessário realizar um estudo abrangente de todas as novas soluções que a empresa implementou. Dessa forma, a equipe também avaliou as diversas alternativas. Depois de um processo completo de verificação, a equipe prosseguiu com a Akamai Guardicore Segmentation. "Nenhuma das opções ofereceu uma solução tão completa como a [Akamai] com monitoramento de tráfego, rotulagem flexível e visibilidade avançada no nível da aplicação usando apenas a pegada digital de um único agente em um cliente", disse o arquiteto de infraestrutura.

> Com um único agente em uma máquina, resolvemos definitivamente o problema de um ataque de ponto de extremidade por movimentação lateral.
>
> Arquiteto de infraestrutura, empresa manufatureira

Akamai Guardicore Segmentation

Na primeira fase do projeto, a empresa implantou Akamai Guardicore Segmentation em aproximadamente 2.000 estações de trabalho. Assim que a solução entrou em vigor, a equipe de segurança de TI descobriu um novo nível de visibilidade da rede e de seus fluxos de comunicação.

Novas percepções e segmentação em ação

"Com os mapas de tráfego [Akamai], nossa visibilidade está 1000% melhor agora e inclui comunicações de PC para PC", disse o arquiteto de infraestrutura.

A capacidade de se aprofundar na atividade de um computador individual e, ao mesmo tempo, entender a atividade geral no nível da aplicação ajudou a organização a tomar melhores decisões relacionadas à segurança da informação. Por exemplo, alguns usuários haviam instalado aplicações de suas impressoras domésticas nos notebooks da empresa. Foi possível descobrir que muitas dessas aplicações verificavam continuamente a rede corporativa em busca de dispositivos compatíveis. Baseada nessa nova percepção de visibilidade da Akamai, a equipe conseguiu interromper as verificações.

Akamai Hunt: aproveitando a Akamai Guardicore Segmentation para detecção de ameaças

Essa nova compreensão da atividade de rede também ajudou a empresa a deter agentes de ameaças externas. Por exemplo, logo após a implantação da plataforma, o serviço Akamai Hunt detectou a comunicação de um ativo com um arquivo com características de um malware conhecido chamado GoldenSpy. A equipe Hunt notificou a equipe de segurança de TI da empresa sobre a ameaça detectada. O cliente também recebeu uma análise do escopo da infecção, dos riscos potenciais (que correspondem às informações da MITRE sobre o GoldenSpy), da perícia forense (usando o Insight) e recomendações para investigação e mitigação internas. Em seguida, a empresa usou a política de controle da Akamai para colocar o sistema infectado em quarentena e impedir que o malware se movesse lateralmente para novas máquinas.

Padronização e economia de tempo

Agora, essa empresa também pode criar e gerenciar políticas centralmente, como uma política de estação de trabalho global central e tem a flexibilidade para criar exceções únicas quando um caso de uso exigir. Isso garante uma aplicação consistente nos locais onde exista um agente Akamai e reduz o risco de erros e atrasos na configuração.

Além disso, o tempo gasto com políticas também diminuiu drasticamente na organização. Por exemplo, alterar os controles de firewall antes da nova plataforma era um processo que poderia levar dias. Usando os novos modelos de política da Akamai como guia inicial, a equipe de segurança de TI pode criar controles de segurança até mesmo para os casos de uso mais complexos em menos de uma hora e aplicá-los a toda a base instalada em segundos.

O futuro com a Akamai

Embora o foco inicial do projeto fosse a padronização dos controles de segurança para segmentação e acesso dos pontos de extremidade, há planos para abordar casos de uso adicionais com a Akamai. As partes interessadas estão discutindo uma expansão da proteção para incluir servidores e aplicações essenciais, como o sistema ERP da organização.

Independentemente do que os planos futuros podem incluir, o projeto original já é considerado um sucesso pela empresa e reduziu significativamente a superfície de ataque e o risco das estações de trabalho da empresa. A equipe confia muito mais na postura de segurança da organização contra ataques que se movem lateralmente de um ponto de extremidade para outro. Como a liderança do projeto explicou, "Agora, com um único agente em uma máquina, resolvemos esse problema de vez e podemos passar de uma estação de trabalho sem políticas para uma implementação completa de controles de segurança em 30 segundos".

> Com os mapas de tráfego [Akamai], nossa visibilidade está 1000% melhor agora e inclui comunicações de PC para PC.
>
> Arquiteto de infraestrutura, empresa manufatureira

Acesse akamai.com/guardicore para obter mais informações.