RESUMO DA SOLUÇÃO DA AKAMAI

Destaque de detecção de violação por vários métodos: Uso de políticas de segmentação para detecção de violações em data centers

Com as violações do data center não dando sinais de diminuir, é hora das equipes de segurança focarem mais atenção no coração do data center, onde as aplicações estão conversando entre si e executando funções de missão essencial. À medida que mais organizações distribuem cada vez mais ativos de data center em vários ambientes virtualizados, as defesas de perímetro não são mais adequadas. Os administradores de segurança precisam de um meio eficiente de proteger o tráfego interno leste-oeste contra ataques que já conseguiram violar as defesas do perímetro.

O firewall atinge uma parede

Os firewalls têm sido tradicionalmente usadospara proteger comunicações dentro e fora dos data centers. No entanto, colocar firewalls no centro do data center é problemático. Incapazes de se adaptar a grandes quantidades de tráfego leste-oeste, eles se tornam um gargalo para o desempenho. O firewall no nível do servidor consome grandes quantidades de recursos de computação do host, que já é altamente sobrecarregado. Também requer a implantação de várias soluções para abranger os vários tipos e marcas diferentes de sistemas operacionais no data center, dificultando o gerenciamento.

Até recentemente, a implementação de políticas de segurança no nível do processo L7 também era um desafio. Isso porque ela requer visibilidade de todas as aplicações e processos que se comunicam no seu ambiente. Ela exige ainda uma compreensão holística de como os processos devem funcionar juntos dentro da aplicação e do data center. Sem essas percepções, a implementação de políticas de segurança no nível do processo pode ser arriscada e as chances de algo dar errado são muito elevadas.

Para proteger ativos essenciais no data center e, ao mesmo tempo, melhorar a detecção e a resposta a violações, as equipes de segurança precisam dos meios para:

- Visualizar todas as aplicações e processos em execução em seus data centers em tempo real
- Implementar políticas de segurança granulares sem impedir processos essenciais
- Detectar comunicações não autorizadas que possam indicar uma violação

A melhor defesa é o ataque: Detecção baseada em políticas com a Akamai Guardicore Segmentation

A detecção baseada em políticas pode ajudar as equipes de segurança a detectar, confirmar e conter ameaças mais rapidamente para evitar danos e minimizar perdas. Esses controles de segurança granulares têm dupla função: impedir que um invasor obtenha acesso mal-intencionado a uma aplicação ou a um processo e alertar simultaneamente os administradores sobre a presença do invasor.

Os recursos das políticas de segmentação na Akamai Guardicore Segmentation permitem que os profissionais de segurança:

- Gerem um mapa visual abrangente de todas as aplicações e atividades dentro do data center, permitindo a visibilidade de todas as cargas de trabalho e uma compreensão completa das comunicações na camada de aplicações

Vários métodos de detecção identificam violações mais rapidamente

Fraude dinâmica

Uma arquitetura de redirecionamento e ambientes ativos gerados dinamicamente atacam os invasores e identificam seus métodos sem interromper o desempenho do data center

Detecção baseada em políticas

As políticas de segurança nos níveis de rede da Camada 4 e de processo da Camada 7 permitem o reconhecimento instantâneo de comunicações não autorizadas e tráfego não compatível

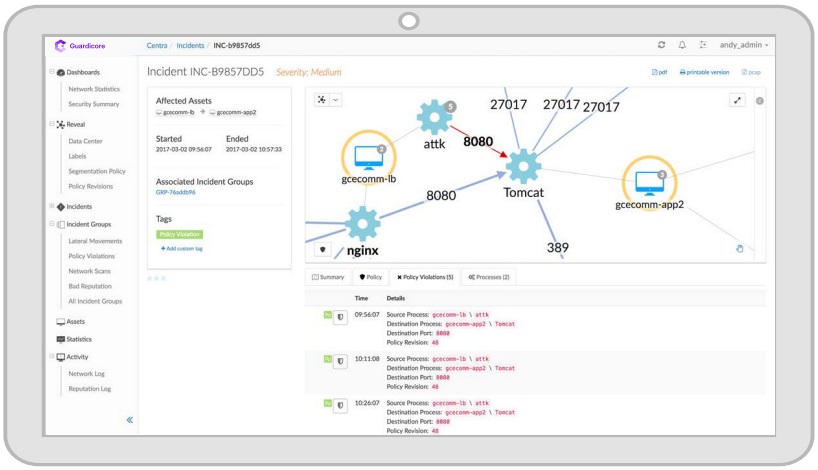
Análise de reputação

Detecta nomes de domínio suspeitos, endereços IP e hashes de arquivo nos fluxos de tráfego, fornecendo detecção abrangente de violações

Akamai

- Filtrem e organizem aplicações em grupos e as rotulem com o objetivo de definir políticas de segurança comuns, por exemplo, todas as aplicações relacionadas a um fluxo de trabalho ou função comercial em particular
- Definam e criem regras que regem as comunicações autorizadas entre aplicações
- Testem e refinem essas regras para garantir que elas não interrompam o tráfego normal autorizado

Qualquer tráfego fora de conformidade, comunicação não autorizada ou outra violação de política aciona automaticamente um alerta indicando que um invasor pode estar presente. Isso, por sua vez, inicia o processo investigativo para confirmar e conter a ameaça.



A Akamai Guardicore Segmentation detecta uma possível violação ao reconhecer e alertar sobre violações da política de segmentação que envolvem processos não autorizados que tentam se comunicar em portas autorizadas entre dois hosts permitidos.

Encurrale seus adversários com vários métodos de detecção

A detecção baseada em políticas é apenas um dos vários métodos que nossa solução usa para melhorar a detecção de violações em tempo real e a resposta a essas violações. Trabalhando em conjunto, esses métodos complementares também incluem:

- **Fraude dinâmica**, que emprega servidores de data center reais, endereços IP, sistemas operacionais e serviços como iscas que buscam ativamente atividades suspeitas na primeira indicação, interagem com elas e as redirecionam para uma área de contenção para confirmação e investigação de ameaças
- **Análise de reputação**, que aproveita a rede global de sensores de ameaças e feeds de inteligência da Akamai para identificar processos negativos e endereços IP suspeitos, nomes de domínio ou hashes de arquivos associados a ameaças

A implantação desses três métodos simultaneamente forma uma rede de segurança forte, praticamente garantindo que qualquer violação ativa no data center seja detectada, mitigada e contida para uma investigação aprofundada.

Saiba mais sobre os recursos abrangentes de detecção de violação da Akamai Guardicore Segmentation em akamai.com/guardicore.