

RESUMO DA SOLUÇÃO DA AKAMAI

Deloitte aprimora ofertas de resposta a incidentes e mitigação de ransomware com a Akamai Guardicore Segmentation

Desafios do cliente

As categorias de produtos de segurança firmemente estabelecidas prometem níveis superiores de proteção contra as ameaças mais recentes às redes corporativas. No entanto, poucas soluções têm sido capazes de oferecer um método abrangente e único para reduzir a superfície de ataque protegendo contra movimentos laterais mal-intencionados: seja para ou de hardware local, cargas de trabalho hospedadas na nuvem, dispositivos de usuário final ou contêineres. Além disso, as primeiras iniciativas de segmentação Zero Trust costumavam levar meses, até mesmo anos, para serem concluídas pelos clientes empresariais. Isso acontecia devido às restrições tecnológicas e à limitada experiência humana para executar projetos que visam interromper ataques caso eles consigam passar por produtos de segurança estabelecidos, como firewalls herdados, EDRs e outros.

Ao abordar projetos de segmentação, os clientes corporativos normalmente enfrentam os seguintes desafios:

- Falta de visibilidade de todos os ativos, fluxos de rede, usuários e conexões em todos os ambientes
- Controles de segurança limitados sobre tecnologias e infraestrutura diferentes, como infraestrutura de nuvem híbrida, sistemas operacionais legados e OT/Internet das coisas
- A necessidade de garantir a continuidade dos negócios evitando o tempo de inatividade que muitas vezes acompanha as técnicas tradicionais de segmentação
- Falta de recursos de segurança e talento para criar, implantar e gerenciar iniciativas que ofereçam suporte à tecnologia Zero Trust

Destaques da solução

A Akamai Guardicore Segmentation é uma solução de microssegmentação baseada em host que oferece a maneira mais simples, rápida e intuitiva de aplicar os princípios Zero Trust à rede. Usando uma combinação de sensores baseados em agentes, coletores de dados baseados em rede e registros virtuais de fluxos de nuvem privada para mapear sua rede, a Akamai Guardicore Segmentation foi projetada para fornecer uma visão única de todos os seus ativos e infraestrutura, incluindo sistemas operacionais legados e modernos, tecnologia operacional e dispositivos de Internet das coisas. A partir daí, é possível criar e aplicar com facilidade políticas que limitarão comunicações indesejadas, reduzindo a superfície de ataque e garantindo a continuidade dos negócios.

Principais casos de uso

- **Controle de tráfego leste-oeste**
Separe ambientes, aplicações, usuários e infraestrutura que não precisam se comunicar
- **Mitigação de ransomware**
Implante modelos de políticas com IA/ML para bloquear caminhos de ataque que sabidamente são usados por vários tipos de ataques de ransomware
- **Isolamento de aplicações**
Concentre-se nas dependências específicas das suas aplicações essenciais aos negócios para criar controles de segurança rígidos



- **Segmentação baseada no usuário**
Impeça que os usuários acessem aplicações, ambientes e dispositivos que não sejam essenciais para o trabalho
- **Isolamento de dispositivos infectados**
Contenha a disseminação de uma violação se um ou mais dispositivos estiverem comprometidos
- **Conformidade**
Esteja pronto para demonstrar conformidade rapidamente com profundo conhecimento contextual de sua rede, dispositivos e possíveis caminhos de ataque

Benefícios para o cliente

- Resolva desafios de visibilidade com um painel único que mostra toda a sua rede e conexões, incluindo servidores, pontos de extremidade, nuvens, contêineres, usuários e muito mais
- Aplique políticas Zero Trust para reduzir a possibilidade de um ataque de ransomware bem-sucedido
- Reduza o tempo de resposta a incidentes usando inteligência de ameaças e recursos abrangentes de detecção de violações e tecnologia deception
- Simplifique a análise de rede e os projetos de conformidade usando recursos tanto históricos como em tempo real

Experiência da Deloitte

1. Aconselhamento

A experiência da Deloitte no suporte a decisões de cibersegurança, na análise de lacunas de segurança e na criação de roteiros de implementação de maneira impactante garante que os clientes empresariais tomem decisões acertadas durante violações, bem como no planejamento para o futuro

2. Serviços profissionais

Experimente serviços de implementação totalmente gerenciados, bem como integrações personalizadas em suas soluções existentes de segurança, ITSM e nuvem

3. Serviços gerenciados de resposta a incidentes

Receba assistência qualificada instantânea dos técnicos de resposta a incidentes da Deloitte para conter a violação e ajudar a evitar incidentes futuros

4. Assinaturas de licença

A Deloitte pode oferecer uma ampla variedade de assinaturas de licenças para aquisição

Estudo de caso de cliente: como a Akamai e a Deloitte solucionam os desafios de ransomware de clientes

Grandes eventos de ransomware fizeram com que os clientes buscassem orientação e soluções que pudessem ajudar de modo imediato em um momento crítico. Os recursos combinados das equipes de resposta a incidentes e segurança da Deloitte, aproveitando a visibilidade da rede, a análise de violações e as medidas subsequentes para redução significativa da superfície de ataque fornecidas pela Akamai Guardicore Segmentation, produziram uma combinação de alto nível para esses clientes.

Histórico

No caso de uma organização empresarial, o cliente estava enfrentando um evento de ransomware significativo que interrompeu suas operações comerciais principais, e não sabia como começar a resolver a situação. Todo o data center, que consiste em milhares de servidores, foi tomado, e a violação precisava ser contida imediatamente de maneira segura. Confiando na orientação da Deloitte, o cliente ligou e perguntou o que fazer. Com a equipe da Deloitte já preparada para oferecer e implantar a Akamai Guardicore Segmentation, o cliente conseguiu obter rapidamente visibilidade da escala do ataque, entender quais ativos e aplicações foram afetados e identificar quais eram todas as dependências de aplicações relacionadas.

Solução

Ao mapear todo o ambiente do cliente no nível de processo individual, a solução Akamai Guardicore Segmentation conseguiu revelar todas as possíveis rotas que o malware pôde ter traçado na infraestrutura que estava comprometida, permitindo que a equipe da Deloitte focasse em partes específicas da rede para análise forense adicional. Isso garantiu que, depois que o cliente restaurasse as operações comerciais e o acesso ao data center, não houvesse mais nenhum dispositivo comprometido.

Resultado

Com a resolução do ataque de ransomware, a reativação do data center e a retomada das operações comerciais, foram realizadas ações para reduzir a chance de um ataque desse tipo acontecer novamente. Como muitos clientes empresariais, esse cliente usa uma abordagem de segurança em camadas com várias soluções líderes para proteger dispositivos, aplicações, usuários e muito mais. No entanto, como algo tão simples quanto um e-mail de phishing pode ser a porta de entrada para um invasor, essas soluções não foram suficientes para interromper o ataque. Com a visibilidade completa da rede, de dependências de aplicações e dos usuários que tinham acesso ao data center, o cliente pôde implementar controles precisos de microsegmentação para reduzir consideravelmente as possíveis rotas de uma futura violação de ransomware.

Ao ver de perto o valor da solução da Deloitte, o cliente reforçou sua confiança na empresa e decidiu manter a solução em vigor para continuar fornecendo segmentação Zero Trust, além de ter solicitado que a Deloitte se encarregasse do gerenciamento diário da sua tecnologia.

Em resumo

A profunda experiência técnica e o conhecimento da Deloitte na execução de projetos Zero Trust para clientes fazem dela um parceiro ideal para implantar e gerenciar a Akamai Guardicore Segmentation para clientes. Os clientes podem contar com a Deloitte para usar essa tecnologia em qualquer iniciativa de segurança que inclua redução da superfície de ataque, controles de movimento lateral, isolamento de aplicações ou mitigação de ransomware.

Sobre a Deloitte

A Deloitte fornece serviços de auditoria, consultoria, tributação e assessoramento líderes do setor para muitas das marcas mais admiradas do mundo, incluindo quase 90% das empresas da Fortune 500® e mais de 7.000 empresas privadas. Nossos funcionários visam o bem maior e trabalham em todos os setores da indústria que impulsionam e moldam o mercado atual, proporcionando resultados mensuráveis e duradouros que ajudam a reforçar a confiança pública em nossos mercados mais importantes, inspirar os clientes a ver desafios como oportunidades de transformar e prosperar e ajudar a liderar o caminho para uma economia mais forte e uma sociedade mais saudável. A Deloitte tem orgulho de fazer parte da maior rede global de serviços profissionais que atende nossos clientes nos mercados mais importantes para eles. Com um histórico de mais de 175 anos de serviço, nossa rede de empresas afiliadas abrange mais de 150 países e territórios. Saiba como aproximadamente 415 mil colaboradores da Deloitte se conectam no mundo todo para promover um impacto positivo em deloitte.com.

Contatos

Ola Sergatchov

Diretora de Alianças estratégicas globais, Akamai

osergatc@akamai.com