RESUMO DA SOLUÇÃO DA AKAMAI

Computação confidencial: Proteção de dados em uso

Como as ameaças continuam a crescer em escopo, escala e sofisticação, as equipes de segurança geralmente estão conseguindo enfrentar o desafio, principalmente ao criptografar os dados à medida que são movidos e limitar o acesso quando estão armazenados. No entanto, está se tornando cada vez mais evidente que as equipes também precisam proteger os dados enquanto eles estão sendo ativamente editados, lidos ou processados, comumente chamados de *dados em uso*.

Essa lacuna na proteção de dados em uso está se tornando cada vez mais importante em meio à evolução da computação e da IA. A prevalência da computação híbrida e multinuvem expandiu as maneiras pelas quais as organizações coletam e armazenam dados. Enquanto isso, à medida que as organizações buscam tirar proveito da IA, elas estão colocando enormes conjuntos de dados, muitas vezes os dados mais importantes e confidenciais, em uso sem criptografia e sem proteção.

Esses riscos estão alimentando o interesse pela computação confidencial, uma abordagem de segurança que garante que todos os dados confidenciais usados por aplicações, processos ou serviços permaneçam criptografados e protegidos.

As APIs adicionam complexidade

As APIs estão se proliferando porque desempenham funções essenciais em duas áreas nas quais as empresas estão investindo recursos de forma consistente: ambientes e serviços em nuvem e modelos de IA. Na nuvem, as APIs são essenciais para permitir que as tecnologias se comuniquem e compartilhem dados. Com a IA, os modelos de linguagem grandes (LLMs) usam APIs para acessar e combinar dados para realizar tarefas complexas, como compreensão de linguagem e geração de texto.

Infelizmente, as APIs não recebem a mesma atenção das equipes de segurança que as aplicações e a infraestrutura. Os invasores estão aproveitando essa lacuna de segurança, sendo que 84% das organizações sofreram incidentes de segurança de APIs nos últimos 12 meses.[1] Para proteger os dados confidenciais que cada uma das APIs relacionadas à nuvem e à IA toca, as empresas precisam de recursos completos de segurança de APIs em execução nos ambientes de computação confidenciais.

Trancar as três portas

Bloquear os dados em trânsito e no armazenamento ainda pode deixar uma porta aberta, a dos dados em uso, expondo as empresas a riscos.

Na computação confidencial, esses dados são processados em um ambiente considerado confiável no nível do hardware. Com as APIs, as organizações podem implementar as próprias instâncias privadas de machine learning, criadas especificamente para proteger o tráfego da API, em vez de utilizar um serviço de API em nuvem pública, reduzindo drasticamente a superfície de ataque. A execução de uma solução de segurança de APIs em um ambiente de computação confidencial cria uma camada extra de segurança. Mesmo que parte do sistema seja comprometida, os dados dentro do ambiente protegido permanecem seguros. A execução da análise de API nesses dados em um ambiente confiável é mais segura e elimina o risco presente nos ambientes tradicionais.

Essa combinação de IA, segurança de APIs e computação confidencial ajuda a impedir que entidades não autorizadas, como o hipervisor, o proprietário da infraestrutura do sistema do operador de host ou qualquer pessoa com acesso físico, visualizem ou alterem o código ou os dados durante a execução, protegendo contra ameaças internas

Benefícios para os negócios

Segurança de dados aprimorada
Limite o acesso aos dados em uso com controles rígidos, reduzindo a superfície de ataque e protegendo os processos confidenciais orientados por API contra acesso não autorizado

Proteção para APIs
Execute uma análise detalhada do tráfego de API e mantenha os dados confidenciais criptografados em uso, reduzindo o risco de exposição durante o monitoramento

Maior conformidade
Atenda às normas de proteção de dados globais rigorosas e em constante evolução, garantindo a conformidade com os padrões governamentais e do setor

1. Akamai, Estudo sobre o impacto da segurança de APIs, 2024

(por exemplo, administradores de sistema desonestos ou cargas de trabalho executadas em infraestrutura não confiável) e ameaças externas (por exemplo, invasores que se aproveitam de vulnerabilidades).

Os benefícios

À medida que as ameaças à API se proliferam, e com os dados em uso se tornando um alvo atraente, os invasores não ficarão muito atrás. As organizações com visão de futuro estão começando a adotar a computação confidencial por vários motivos:

- Limitar o acesso aos dados em uso, em primeiro lugar, por meio de controles rígidos
- Analisar com segurança o crescente número de APIs
- Atender aos novos e rigorosos requisitos de conformidade de proteção de dados em todo o mundo com os controles que a computação confidencial disponibiliza

A computação confidencial tem o maior benefício para empresas altamente regulamentadas, seja uma empresa de serviços financeiros que busca proteger transações online ou uma empresa de ciências biológicas que protege dados de pacientes. Essa abordagem também pode ajudar um fornecedor de software independente a proteger um modelo de IA que ele distribui aos clientes em vários locais, desde a edge até a nuvem. De fato, qualquer organização de TI empresarial que execute processamento analítico em tempo real nos dados vitais precisa pensar em computação confidencial.

Como nós e nossos parceiros podemos ajudar

A computação confidencial eficaz exige um conjunto integrado de soluções que trabalhem em conjunto para oferecer controle e proteção completos. A Akamai, juntamente com nossos parceiros Intel e IBM, oferece segurança para os dados em uso, desde o nível do hardware até a nuvem e as APIs.

Primeiro, o Intel® Trust Domain Extensions (TDX) fornece ambientes de execução confiáveis que:

- Protegem contra intrusões externas originadas de agentes de ameaças e/ou entidades não maliciosas que não deveriam ter acesso
- Melhoram a segurança do software que controla a tecnologia usada para criar recursos virtuais na nuvem, como redes, servidores e armazenamento
- Adicionam uma camada muito necessária de segurança em torno das pessoas que administram qualquer um desses sistemas distribuídos, reduzindo o risco de erros honestos e possíveis instâncias de atividades maliciosas internas

Além disso, a verificação e os tokens da Intel Tiber™ Trust Authority permitem que as organizações limitem e controlem o acesso a dados não criptografados em uso.

A solução Akamai API Security fornece um inventário das APIs usadas na empresa e depois monitora e detecta como essas APIs são usadas. Ele detecta e impede automaticamente as solicitações de API mal-intencionadas por meio da análise de padrões e comportamentos de tráfego, bloqueando efetivamente as ameaças na edge da rede sem intervenção manual. Isso permite a proteção em tempo real contra ataques à API, como violações de dados, acesso não autorizado e abuso de lógica.

Juntos, os mecanismos remotos de machine learning da Akamai, combinados com os processadores Intel Xeon® nos IBM Cloud Virtual Servers, que são protegidos com o Intel TDX e atestados com a Intel Tiber Trust Authority, oferecem um ambiente privado e hiperescalável projetado para impedir que qualquer ameaça externa acesse dados não criptografados no estágio final dos dados em uso, seja por ataques de bots alimentados por IA ou por invasores humanos.

Chegou a hora de proteger os dados em uso

As organizações precisam de um ambiente bastante confiável para proteger os dados corporativos mais valiosos, não apenas quando estão sendo armazenados ou acessados, mas também quando estão realmente em uso. Elas estão recorrendo à Akamai e aos nossos parceiros para fornecer segurança completa. Juntos, esses nomes confiáveis da computação estão garantindo a segurança à medida que ela passa por todas as camadas do ciclo de vida dos dados.

Saiba mais sobre como nossa parceria para computação confidencial pode ajudar a proteger os dados confidenciais.
Saiba mais sobre a solução Akamai API Security.