RESUMO DO PRODUTO DA AKAMAI

Account Protector

Mantenha os fraudadores longe — e a confiança intacta — com a proteção contra violações de contas

Como saber se você está lidando com um usuário legítimo ou um impostor? Seus clientes confiam em você para fazer essa distinção.

À medida que as transações digitais e o uso de novos ativos digitais aumentam, os riscos e as consequências da violação de contas se tornam mais graves. Expandir seu negócio digital e proteger seus clientes dependem da capacidade de manter a confiança em um ambiente onde as táticas de fraude estão em constante evolução.

Violações relacionadas a contas, como a criação fraudulenta (fraude de novas contas) e a apropriação indevida de contas (ATO), representam desafios e custos significativos para empresas de todos os setores. Contas comprometidas ou falsas podem causar sérios prejuízos financeiros e danos à reputação das organizações. Quando uma conta é comprometida, os invasores podem explorá-la livremente, esgotando saldos, realizando transações fraudulentas, desativando recursos de segurança como MFA ou roubando informações pessoais confidenciais. Contas falsas, por outro lado, podem ser usadas para tirar proveito de promoções, como testes e créditos gratuitos, realizar fraudes por SMS ou inundar plataformas com spam ou conteúdo inadequado. O impacto desses ataques é significativo, e as empresas correm o risco de perder a confiança dos clientes e sofrer prejuízos milionários com fraudes, além de enfrentar multas regulatórias e danos à imagem.

Akamai Account Protector

O Account Protector é uma solução de segurança projetada para prevenir violações durante todo o ciclo de vida de uma conta, utilizando aprendizado de máquina e uma vasta base de indicadores de risco e confiança para determinar a legitimidade de uma solicitação de usuário. Ele analisa o comportamento em tempo real para identificar sinais sutis de atividades fraudulentas, desde a criação da conta até o login e além. Se comportamentos suspeitos ou anômalos forem detectados, o Account Protector oferecerá opções imediatas de mitigação para garantir uma experiência de usuário fluida, como bloqueio e ações na edge, desafios criptográficos e comportamentais, exibição de conteúdo alternativo e mais.

Benefícios para os seus negócios

Aumente a confiança, a sua e a dos clientes:
Saiba quais interações são legítimas, reduza atritos para os usuários e proteja-os de atividades fraudulentas.

Desenvolva proteções adaptadas às necessidades específicas do seu negócio:
Aproveite a detecção automática de bots e entenda os perfis de usuários com base em como eles interagem com seu website.

Obtenha insights detalhados e maior visibilidade:
Aja com confiança, guiado por sinais e indicadores transparentes.

Reduza os custos de remediação:
Minimize o impacto financeiro e de recursos necessários para investigar contas comprometidas, substituir ativos roubados, entre outros.

Tome decisões mais informadas e baseadas em dados:
Integre com ferramentas de combate a fraudes, SIEM e outras soluções de segurança para permitir o consumo dos sinais de risco e confiança do Account Protector, aumentando a precisão e otimizando o investimento nessas ferramentas.

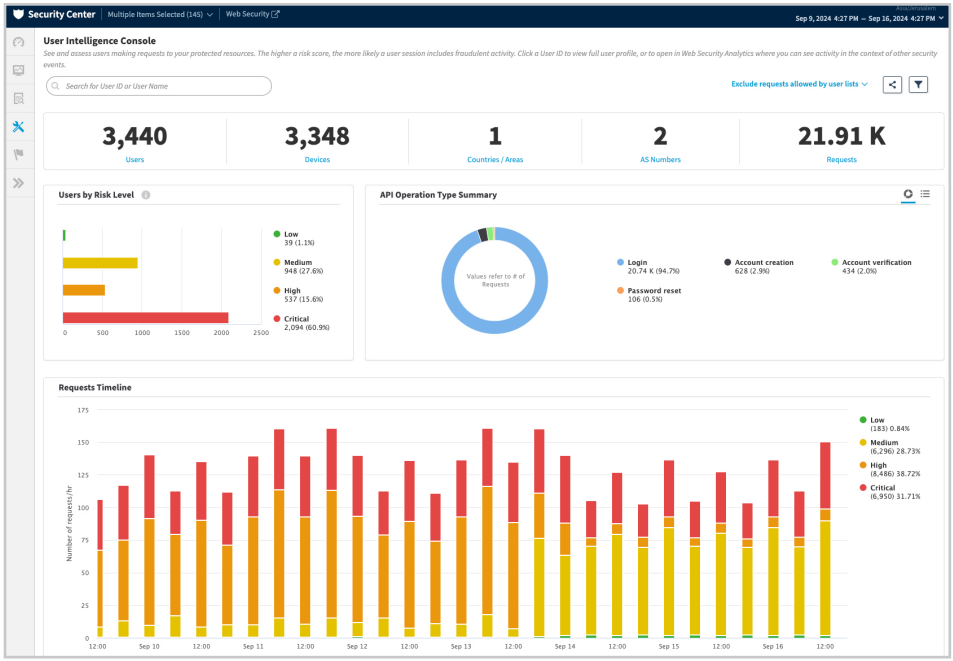
Garanta uma defesa completa contra violações de contas

Proteja as contas de usuários contra violações durante todo o seu ciclo de vida — oferecendo proteção avançada contra fraudes de abertura de contas, ataques de apropriação indevida de contas e os esquemas de ataque associados.

Violação de abertura de contas — Reduza a criação de contas falsas usadas para explorar promoções, realizar fraudes por SMS, testar cartões de crédito roubados, acumular inventário e mais.

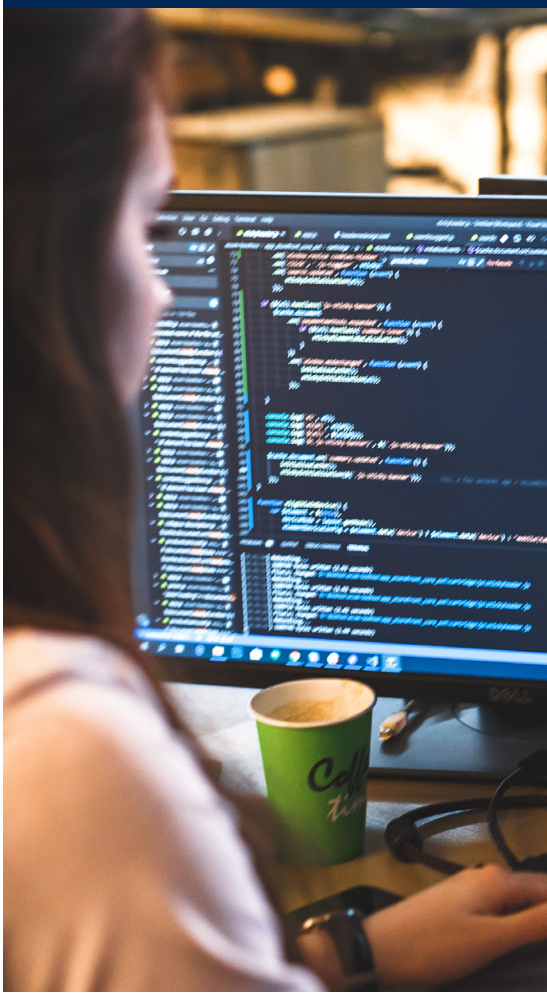
Apropriação indevida de contas — Proteja-se contra impostores que acessam contas legítimas de clientes para sacar valores, roubar dados confidenciais e realizar transações fraudulentas.

Ataques sofisticados de bots invasores — Proteja as contas de usuários contra ataques automatizados, como preenchimento de credencial, manipulação de inventário e outros ataques frequentemente realizados em conjunto com fraudes de abertura ou apropriação indevida de contas (ATO) para roubar produtos valiosos, dinheiro ou outros ativos importantes.



Proteção, confiança e experiência do usuário

Analise riscos e interrompa violações em tempo real, monitorando continuamente as contas durante todo o ciclo de vida quanto a comportamentos suspeitos à medida que se manifestam.



Principais recursos

Proteção abrangente ao longo do ciclo de vida da conta — Identifica e analisa riscos do usuário em qualquer etapa, desde a criação da conta até atividades pós-login, como atualizações de conta, alterações de senha e pagamentos.

Pontuação de risco da sessão do usuário em tempo real — Avalia o risco e a confiança em toda a sessão do usuário para avaliar se uma solicitação é proveniente de um usuário legítimo ou de um impostor.

Inteligência de endereços de e-mail — Analisa a sintaxe de um endereço de e-mail e o uso anormal de um e-mail para detectar padrões maliciosos.

Inteligência de domínios de e-mail — Avalia o padrão de atividade proveniente de domínios de e-mail individuais, incluindo domínios descartáveis e o uso excessivo de um domínio.

Reconhecimento global de usuários confiáveis — Fornece visibilidade do comportamento do usuário em toda a rede da Akamai para a tomada de decisões mais informadas sobre a confiabilidade de um login.

Perfis comportamentais do usuário — Desenvolve um perfil comportamental do usuário com base em localizações, redes, dispositivos, endereços de IP e tempo de atividade previamente observados, a fim de identificar usuários recorrentes.

Perfis de população — Agrega os perfis de usuário da sua organização em um superconjunto, por meio do qual as variações no comportamento também podem ser comparadas com toda a população de usuários para detecção de anomalias.

Reputação da fonte — Avalia a reputação da fonte com base em atividades maliciosas anteriores observadas em todos os clientes da Akamai, incluindo muitos dos maiores websites do mundo, mais frequentemente atacados e com tráfego mais intenso.

Indicadores — Alimenta a avaliação de cada solicitação com indicadores de risco, confiança e gerais para avaliar o risco de violação de contas. Os indicadores são fornecidos junto com a pontuação de risco do usuário final e podem ser usados para análise.

Detecções sofisticadas de bots — Detecta bots desconhecidos desde a primeira interação usando uma variedade de modelos e técnicas de inteligência artificial e aprendizado de máquina. Isso inclui análise de comportamento/telemetria do usuário, impressões digitais do navegador, detecção automática de navegadores, detecção de anomalias em HTTP, alta taxa de solicitação e mais.

Análise e geração de relatórios — Fornece relatórios históricos e em tempo real. Analise a atividade em terminais individuais, investigue um usuário específico, revise os usuários por nível de risco e obtenha insights detalhados.

Ações avançadas de resposta — Oferece uma ampla variedade de ações para combater violações, incluindo alertas, bloqueios, atrasos, desafios criptográficos e comportamentais, exibição de conteúdo alternativo, entre outros. Além disso, as organizações podem atribuir diferentes ações com base no URL, na hora do dia, na geolocalização, na rede ou no percentual de tráfego.

Injeção de cabeçalho — Envia informações de risco do usuário para análise e mitigação em tempo real. Um cabeçalho de solicitação adicional é injetado na solicitação encaminhada com informações sobre a pontuação de risco do usuário e os indicadores gerais, de risco e de confiança que contribuíram para a pontuação para análise posterior e mitigação em tempo real.

Automatização com aprendizado de máquina — Atualiza automaticamente as características e os comportamentos usados para identificar bots e atividades humanas fraudulentas, desde padrões de comportamento até as mais recentes pontuações de reputação na plataforma da Akamai.

Integração SIEM (opcional) — Integra informações de risco do usuário a ferramentas SIEM para clientes que desejam visibilidade de segurança mais integrada. Você pode enriquecer o valor de suas ferramentas existentes com os insights do Account Protector.

Entre em contato com seu representante da Akamai ou acesse Akamai.com para saber mais.