RESUMO DA SOLUÇÃO DA AKAMAI

Governança e segurança de APIs integrada para o IBM API Connect e DataPower

A promessa e o desafio das APIs

As APIs têm sido a força motriz da transformação digital, possibilitando que as organizações de todos os setores criem novos serviços e modelos de negócios para acelerar o crescimento. Contudo, à medida que as APIs se proliferam, o mesmo acontece com os riscos.

- Embora os líderes de negócios e engenharia tenham aumentado rapidamente o uso e a integração de APIs em todas as organizações, sua capacidade de gerenciar APIs com eficiência continua sendo um desafio.
- Na corrida para criar e lançar rapidamente novos aplicativos e serviços aprimorados por IA, as APIs estruturais geralmente contêm configurações incorretas, erros de codificação e problemas de lógica de negócios.
- Toda vez que um cliente, parceiro ou fornecedor interage digitalmente com uma organização, há uma API nos bastidores que facilita a troca eficaz de dados, geralmente confidenciais, e os invasores sabem disso.

Como resultado, as APIs se tornaram um dos principais vetores de ataque com altos riscos. Os ataques às APIs podem comprometer a receita, a resiliência e a conformidade regulatória de uma empresa.

Para enfrentar esse desafio, as organizações devem empregar uma abordagem de governança e segurança que abranja todo o ciclo de vida, incluindo as etapas de projeto, desenvolvimento, teste, implantação, operação e correção. Juntos, o Akamai API Security e a IBM possibilitam que as organizações desenvolvam, implantem e gerenciem APIs rapidamente e de maneira confiante, podendo responder e expandir de maneira previsível e de acordo com os negócios.

Desafios

- Manter um inventário de APIs em todo o patrimônio e encontrar APIs desconhecidas
- Identificar APIs fora de conformidade, mal configuradas ou vulneráveis
- Detectar e interromper violações ou usos indevidos de APIs, incluindo ataques de lógica de negócios
- Criar APIs seguras e consistentes sem sacrificar a velocidade ou a agilidade
- Estabelecer alinhamento e supervisão de programas de governança e segurança de APIs

Como a Akamai e a IBM ajudam os clientes

Descubra seu patrimônio de APIs

Não há como proteger o que não se pode ver. Com o Akamai API Security, você pode descobrir automaticamente APIs, domínios e problemas para criar um inventário de APIs robusto que ofereça visibilidade de todo o seu patrimônio de APIs — as empresas geralmente encontram significativamente mais APIs do que pensavam ter ou esperavam encontrar. Você também pode encontrar facilmente inteligência explorável, como informações vazadas, a fim entender os caminhos de ataque disponíveis para os adversários — e aproveitar a integração perfeita com os elementos de infraestrutura mais comuns, adjacentes aos seus gateways e plataformas de gerenciamento de APIs, para garantir o compartilhamento consistente de dados de segurança em toda a organização.

Fortaleça sua postura de segurança e governança

Dimensione suas operações e aplique as práticas recomendadas ao usar o Akamai API Security para governança de APIs:

- Entenda cada API em seu ecossistema com contexto comercial completo e alinhe às melhores práticas de gerenciamento de APIs
- Simplifique as comunicações entre as equipes de desenvolvimento e segurança
- Encontre vulnerabilidades, desde configurações incorretas a APIs que não atendem às políticas
- Proteja dados confidenciais e monitore proativamente as alterações para reduzir os riscos em suas APIs

Detenha violações e ataques a APIs usando a proteção de tempo de execução

Detecte e bloqueie ataques a APIs da edge ao núcleo — incluindo vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e mais — com análise de tráfego em tempo real, monitoramento fora de banda, opções incorporadas de correção e integrações de fluxos de trabalho para aumentar a eficácia do SOC (Centro de operações de segurança).

Forneça APIs seguras mais rapidamente com o Active Testing

Integre perfeitamente os testes de segurança de APIs a cada fase do desenvolvimento de APIs e descubra vulnerabilidades, configurações incorretas e problemas de conformidade antes que as APIs sejam colocadas em produção. Com o Active Testing, as equipes de DevSecOps podem executar um conjunto abrangente de mais de 200 testes de segurança focados em APIs sob demanda ou como parte dos processos de CI/CD da empresa. O Active Testing localiza e testa todas as APIs com base em uma compreensão da lógica de negócios subjacente do aplicativo. Isso permite que os desenvolvedores descubram vulnerabilidades complexas que podem passar despercebidas por outras ferramentas.

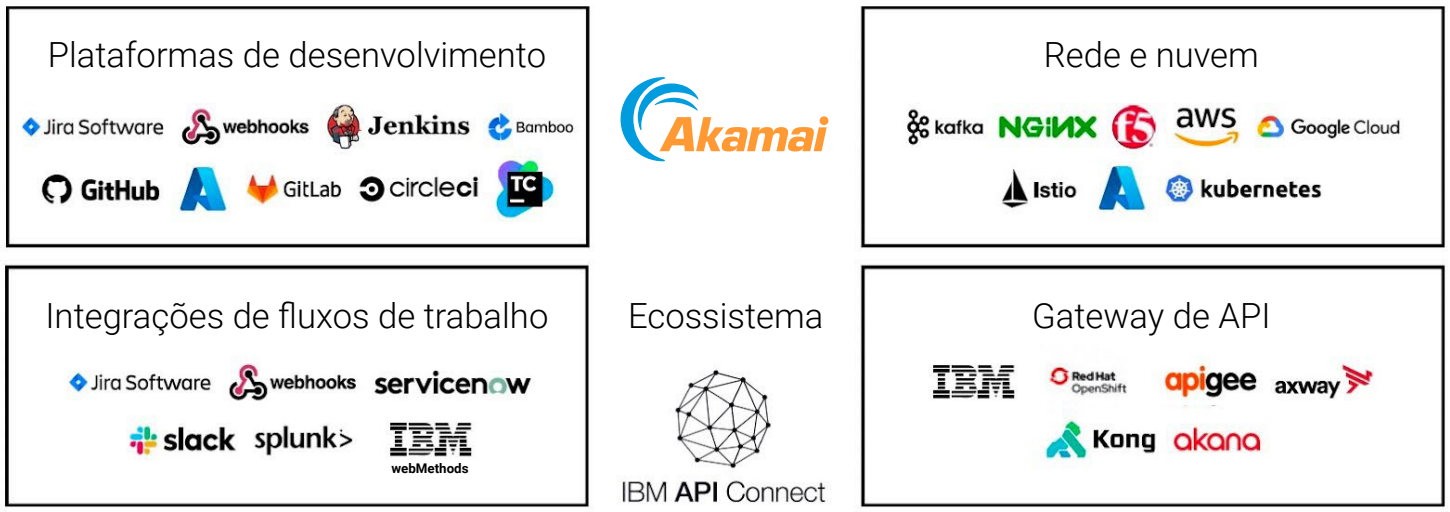
Como a Akamai permite que os usuários da IBM obtenham visibilidade e proteção com integração que impulsiona a eficiência

O Akamai API Security integra-se ao API Connect e ao DataPower em várias plataformas de nuvem e opções de implantação. Além disso, quando o API Connect gerencia o DataPower, são feitas alterações de configuração unilaterais em todos os sistemas, o que aumenta a eficiência operacional e reduz o risco de atividades de desenvolvimento não autorizadas e fora de conformidade.

Direcionamento e resposta consistentes contra ataques

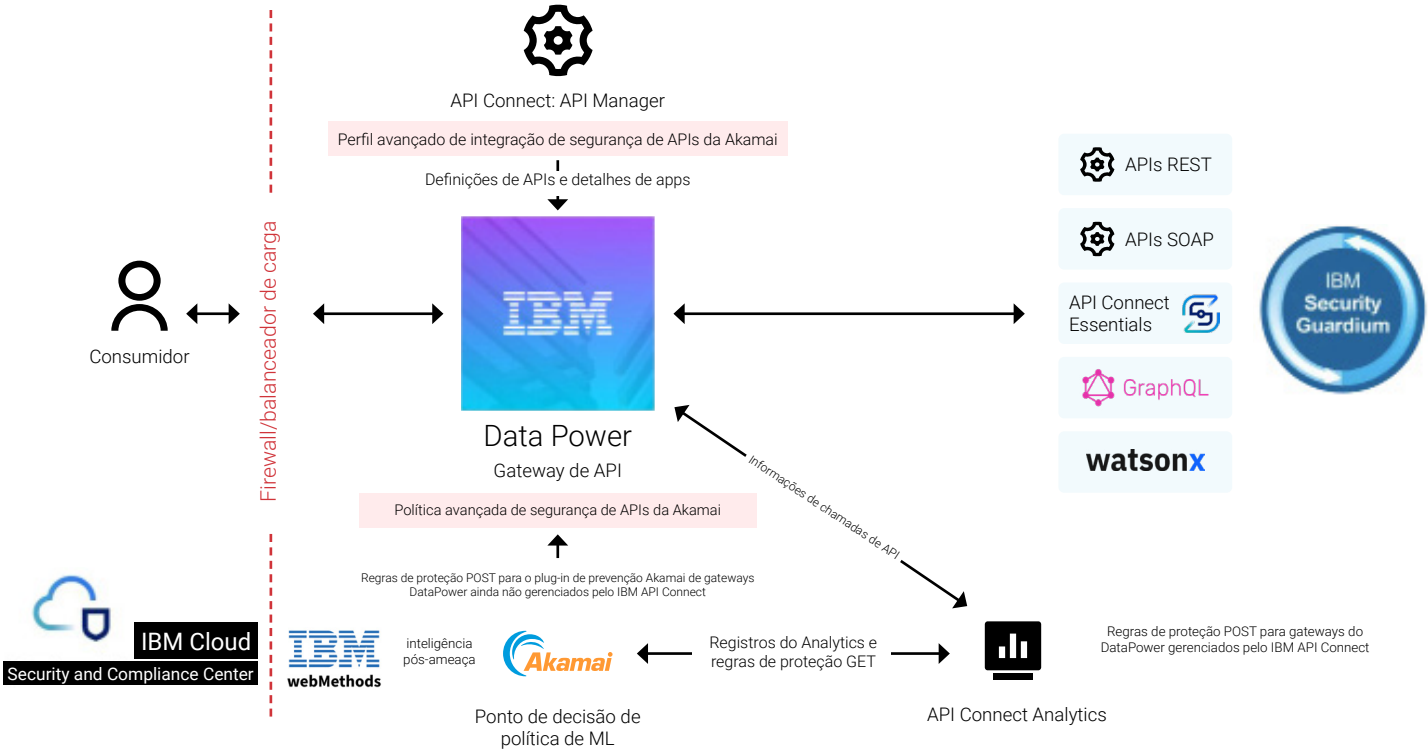
Além disso, os clientes do IBM DataPower podem obter detecção e bloqueio de ameaças quase em tempo real sem impacto no desempenho e na latência e sem a necessidade de instalar plug-ins adicionais nos gateways do DataPower: basta realizar a integração à solução Akamai API Security.

O IBM API Connect pode avaliar solicitações de acesso a recursos com base nas políticas de autorização do Akamai API Security, além de aplicar regras de bloqueio em clusters do IBM DataPower, reduzindo o tempo de correção de dias para minutos ou segundos.



Combine o poder do IBM webMethods e do Akamai API Security para gerenciamento e proteção de APIs sem precedentes. Essa parceria oferece uma solução completa que une a descoberta avançada de APIs da Akamai à governança robusta e à integração de dados em tempo real do IBM webMethods. Obtenha visibilidade total e controle sobre suas APIs para garantir a segurança e a conformidade. Essa integração não só fortalece as defesas, mas também aumenta a eficiência, permitindo que sua empresa responda de forma rápida e segura às demandas dinâmicas do mercado.

Os clientes do IBM DataPower podem aproveitar a integração Akamai eBPF Red Hat OpenShift para descobrir APIs que ainda não são gerenciadas pelo API Connect ou com proxy pelo DataPower, o que permite a descoberta e proteção de APIs que processam dados confidenciais e transações de alto risco. Esses recursos se estendem a configurações de nuvem e híbridas, para além de arquiteturas locais, com suporte para Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).



Próximas etapas

As APIs são uma força motriz por trás da capacidade das organizações de atender às necessidades dos clientes, gerar receita e competir em uma economia digital em rápida evolução. No entanto, seu crescimento contínuo, a proximidade com dados confidenciais e as diversas vulnerabilidades fazem delas alvos atraentes para os invasores. Com o aumento constante dos incidentes de segurança de APIs, é essencial ter recursos para ver, proteger e testar todas as APIs de sua organização. A união de forças entre a IBM e a Akamai pode dar às empresas confiança para criar, manter e usar APIs de forma segura e em escala.

Saiba como podemos ajudar agendando uma demonstração personalizada do Akamai API Security. Você também pode recorrer a seu contato na IBM para saber mais.