CEQUENCE

FOLHA DE DADOS

Segurança de API Cequence

Gerenciamento, Teste e Remediação da Postura de Segurança de API

O mundo atual, movido por software, funciona com aplicações conectadas por APIs. Essas APIs oferecem acesso às aplicações e aos dados sensíveis de uma organização e se tornaram um dos principais alvos dos atacantes. As organizações precisam de visibilidade e controle sobre sua pegada de APIs como parte de um programa de segurança robusto. A rápida proliferação de APIs expôs uma ampla gama de desafios de segurança que podem levar à perda de dados, violações de conformidade e fraudes:

- APIs shadow, ocultas, obsoletas e de terceiros
- Exposição de dados confidenciais ou sensíveis
- Erros de codificação que levam à elevação de privilégios
- Abuso da lógica de negócios

Esses desafios exigem uma solução especializada que seja capaz de descobrir e inventariar APIs novas e existentes, avaliá-las quanto à conformidade com especificações e regulamentos aplicáveis e protege-las ao longo de todo o seu ciclo de vida – desde o desenvolvimento até a produção.

Visão Geral da Segurança de API da Cequence

- **Descoberta completo de APIs** por meio de integração com a infraestrutura e/ou sensores inline e varredura de domínios.
- **Mascaramento de dados sensíveis** detecção de exposição e prevenção de vazamento.
- **Visibilidade contínua de riscos,** identificando erros de codificação e configurações incorretas.
- **Teste de segurança de APIs integrado,** cobrindo APIs em pré-produção e em tempo de execução.
- **Proteção de aplicações e APIs** para prevenir a perda de dados, o roubo e a fraude.

Visão Geral da Segurança de API

A Cequence descobre, monitora e testa APIs, avaliando uma ampla gama de riscos que frequentemente resultam em problemas de conformidade ou governança, perda de dados e interrupção dos negócios. Ao fornecer visibilidade completa e monitoramento de APIs internas, externas e de terceiros, a Cequence ajuda as organizações a acompanhar as mudanças em APIs e serviços, revela exposições de dados sensíveis e identifica vulnerabilidades e riscos de segurança do OWASP API Security Top 10. O teste de segurança de APIs é um componente essencial do API Security, permitindo que as organizações testem suas APIs de pré-produção e em tempo de execução em conformidade com as especificações — e as gerem automaticamente quando não estiverem disponíveis. O API Security pode ser implantado como SaaS, on-premises ou em um modelo híbrido.

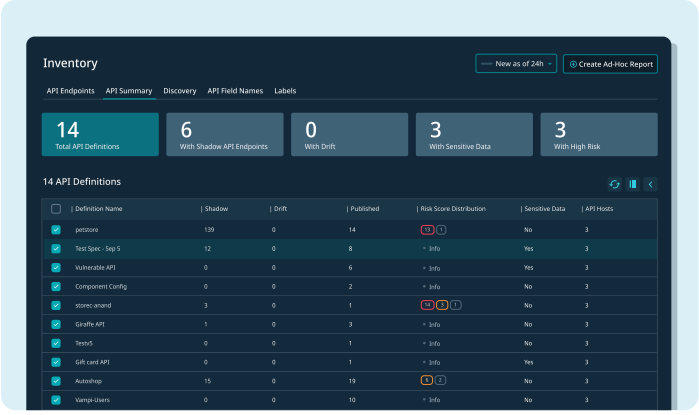
A Cequence Permite que as Organizações:

- **Descubra todas as APIs em uso,** incluindo APIs shadow e zombie, sem a necessidade de especificações de API.
- **Obtenha insights sobre o uso das APIs,** incluindo localização geográfica, cabeçalhos, parâmetros de consulta e elementos do corpo.
- **Gere automaticamente especificações** OpenAPI a partir das APIs descobertas e garanta a conformidade.
- **Avalie dinamicamente os riscos** com base em categorias de risco predefinidas e personalizáveis, como OWASP API Security Top 10 e Automated Top 10.
- **Teste APIs em ambientes de pré-produção** com tráfego sintético para identificar riscos do OWASP e outras vulnerabilidades.
- **Proteja as APIs contra ataques** por meio da integração com infraestrutura de terceiros, como WAFs e gateways de API.

Recursos da Segurança de API da Cequence

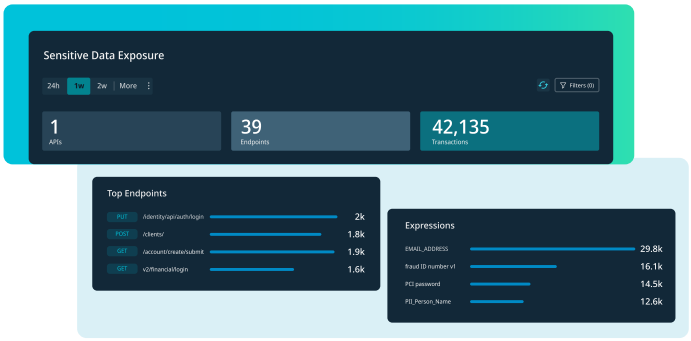
Obtenha Visibilidade Completa e Contínua do Ecossistema de APIs

Um dos maiores desafios de segurança de API enfrentados pelas organizações é saber quais APIs elas possuem, onde estão localizadas e quem tem acesso. A Cequence adota uma abordagem única para fornecer visibilidade completa e contínua da pegada de APIs em tempo de execução de uma organização, implantando sensores projetados especificamente no nível da rede, além de se integrar à infraestrutura existente, incluindo CDNs e gateways de API. O Cequence API Security também oferece uma perspectiva externa, escaneando seus domínios e subdomínios para identificar hosts e endpoints de APIs públicas, mesmo que não estejam em uso. Essa técnica de "visão do atacante" também descobre provedores de edge, infraestrutura e hospedagem.



A descoberta contínua, o rastreamento de inventário e a categorização de riscos ajudam você a controlar sua pegada de APIs.

O API Security não requer agentes no lado do servidor ou cliente, nem integração com JavaScript ou SDKs, garantindo que a descoberta de APIs não fique limitada a softwares instrumentados, além de eliminar penalidades posteriores como ciclos de desenvolvimento prolongados, carregamento lento de páginas e aumento dos custos em nuvem. A solução cria um catálogo de APIs em tempo de execução e gera automaticamente especificações de APIs caso não existam, reduzindo drasticamente os esforços manuais. Os painéis exibem APIs categorizadas por nível de risco, com métricas detalhadas que incluem a distribuição geográfica do uso de APIs por país, endereço IP e organização.



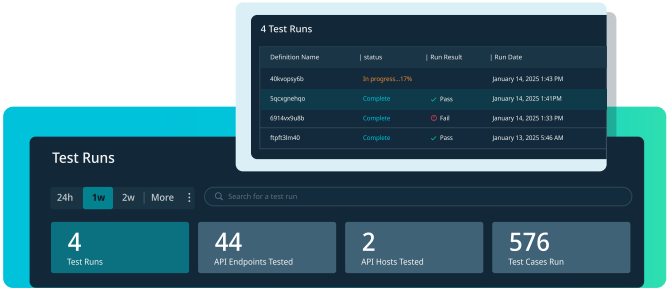
Prevenção da Exposição de Dados Sensíveis

A Cequence inclui recursos avançados para evitar a exposição de dados sensíveis. Sua capacidade de baselining descobre as APIs e compreende seu contexto de negócios em poucas horas após a implantação, identificando APIs que processam informações sensíveis. A Cequence detecta automaticamente dados sensíveis com base em padrões predefinidos (como números de cartão de crédito ou de seguridade social) e padrões personalizáveis. Os padrões de dados sensíveis têm suporte global — por exemplo, a Cequence pode diferenciar automaticamente um número de carteira de motorista dos EUA de um número de identificação nacional da Arábia Saudita.

O machine learning com Processamento de Linguagem Natural (NLP) complementa os padrões predefinidos e reduz falsos positivos ao identificar dados sensíveis por meio de indícios contextuais, como a presença de palavras-chave próximas ao valor detectado. O painel de Exposição de Dados Sensíveis apresenta os resultados de forma gráfica, com detalhes como a API de origem e os códigos de resposta que estão vazando os dados, o padrão identificado e informações detalhadas do endereço IP subjacente. Notificações podem ser enviadas às equipes de desenvolvimento para correção rápida por meio de alertas predefinidos para ferramentas como Slack, PagerDuty e e-mail. A Cequence também oferece mascaramento de dados sensíveis com criptografia que preserva o formato (FPE), aplicada antes que o produto "veja" os dados, garantindo que as informações sensíveis permaneçam privadas.

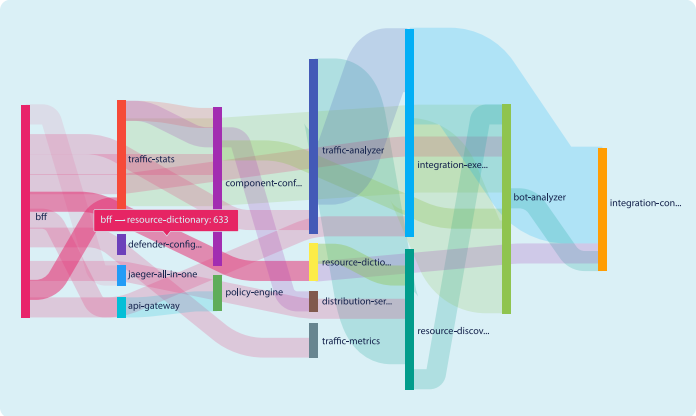
Teste Inteligente de Segurança de API

A Cequence permite que as equipes de TI e desenvolvimento testem exaustivamente suas APIs em pré-produção e em tempo de execução, identificando erros de codificação, vulnerabilidades e outras divergências em relação às especificações. Se não houver especificações disponíveis, a criação autônoma de testes gera especificações de API sem envolvimento humano, eliminando potencialmente horas ou semanas de trabalho manual. Essas capacidades de teste de segurança podem ser integradas ao pipeline de CI/CD e aos IDEs, ou executadas de forma independente conforme necessário em tempo de execução.



Visualize os Fluxos de Tráfego de API

O Cequence Flow Graph permite visualizar as interações entre APIs, oferecendo uma visão clara dos fluxos de comunicação entre elas. A solução possibilita a identificação de APIs internas e de terceiros, além de suas dependências, permitindo validar interações aprovadas, detectar anomalias e lacunas na postura de segurança e descobrir APIs shadow e APIs não autorizadas (rogue APIs).



Proteja APIs Contra Ameaças e Ataques

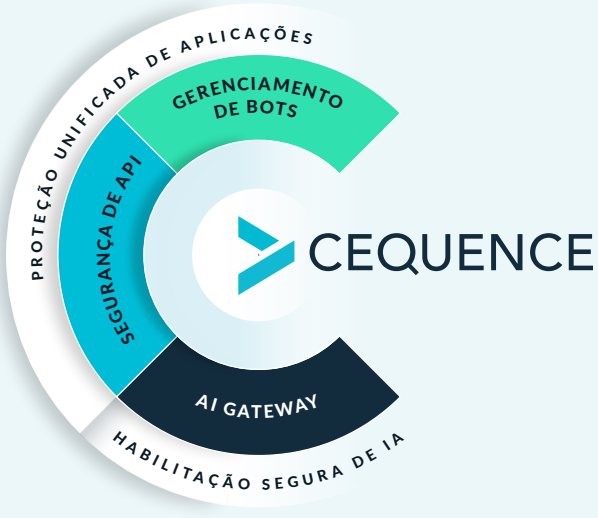
A Cequence protege aplicações web, móveis e APIs contra ataques, prevenindo perda de dados, roubo e fraude. Com um mecanismo de detecção de ameaças impulsionado por aprendizado de máquina (ML) e integração com soluções defensivas de terceiros, como WAFs e gateways de API, a Cequence garante proteção contra até os ataques mais sofisticados. O Cequence Bot Management oferece mitigação nativa, incluindo bloqueio, limitação de taxa, injeção de cabeçalhos e dissuasão, garantindo defesa proativa contra ameaças automatizadas.

Funciona com o Cequence AI Gateway

O Cequence AI Gateway habilita o acesso de IA baseada em agentes (agentic) a qualquer aplicação interna, externa ou SaaS, em minutos e sem necessidade de código. O API Security pode criar automaticamente especificações de API que o AI Gateway usa para criar servidores MCP, eliminando um esforço manual significativo.

Segurança de API é Parte da Plataforma Cequence Unified Application Protection

A plataforma Cequence Unified Application Protection une descoberta, conformidade e proteção para defender as aplicações e APIs de uma organização contra ataques, abuso de lógica de negócios e fraudes. Demonstrando valor em minutos — e não em dias ou semanas —, a Cequence oferece um modelo de implantação flexível que não exige instrumentação ou modificação dos aplicativos. Confiada pelas maiores e mais exigentes organizações dos setores público e privado, a Cequence protege mais de 10 bilhões de interações de API por dia e 4 bilhões de contas de usuários.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai