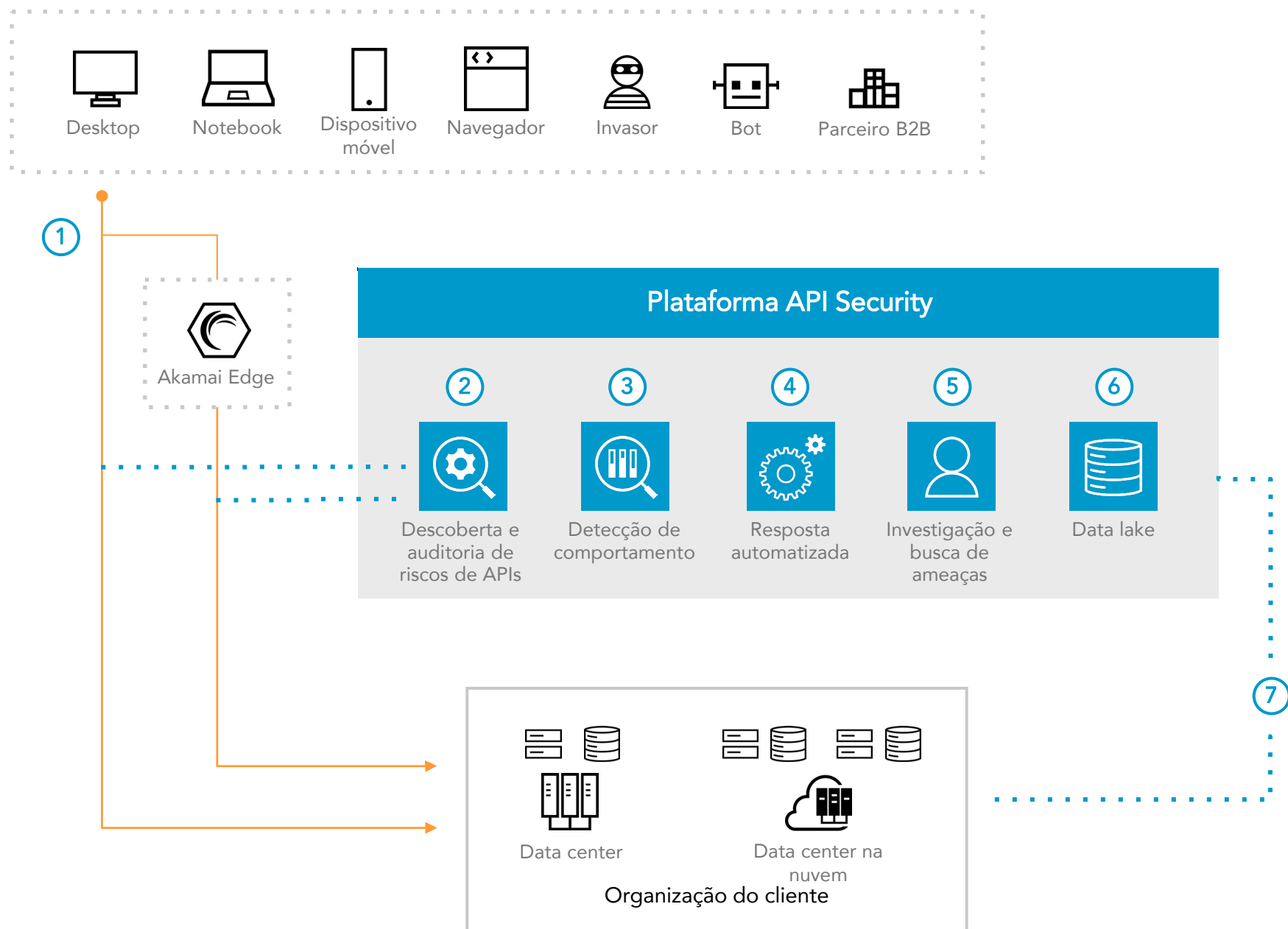


API SECURITY

Como funciona



OVERVIEW

O Akamai API Security descobre e audita todas as APIs e monitora as suas atividades, usando análises comportamentais para detectar e responder a ameaças e violações. Ele fornece detecções contextuais para proteger contra violação de lógica e ataques a APIs que as soluções baseadas em assinatura não conseguem detectar.

- 1** O tráfego flui da organização do cliente e/ou através da plataforma de edge da Akamai
- 2** Uma cópia desse tráfego é alimentada na plataforma API Security, onde todas as APIs são descobertas
- 3** As detecções comportamentais estabelecem um padrão normal de comportamento para detectar anomalias e violação de lógica
- 4** As respostas automatizadas podem enviar informações críticas para as equipes de segurança ou bloquear o tráfego na edge da Akamai
- 5** As equipes de segurança podem usar o contexto comportamental para investigar e procurar ameaças no tráfego de APIs ou usar um serviço gerenciado de busca de ameaças
- 6** A atividade histórica de APIs é armazenada em nosso data lake e oferece suporte a iniciativas de investigação e busca de ameaças
- 7** O API Security também tem visibilidade total das APIs e da atividade das APIs da organização do cliente

PRINCIPAIS PRODUTOS

Proteção de APIs ► [Akamai API Security](#)

Busca gerenciada de ameaças ► [Akamai API Security ShadowHunt](#)

Visite akamai.com/products/api-security