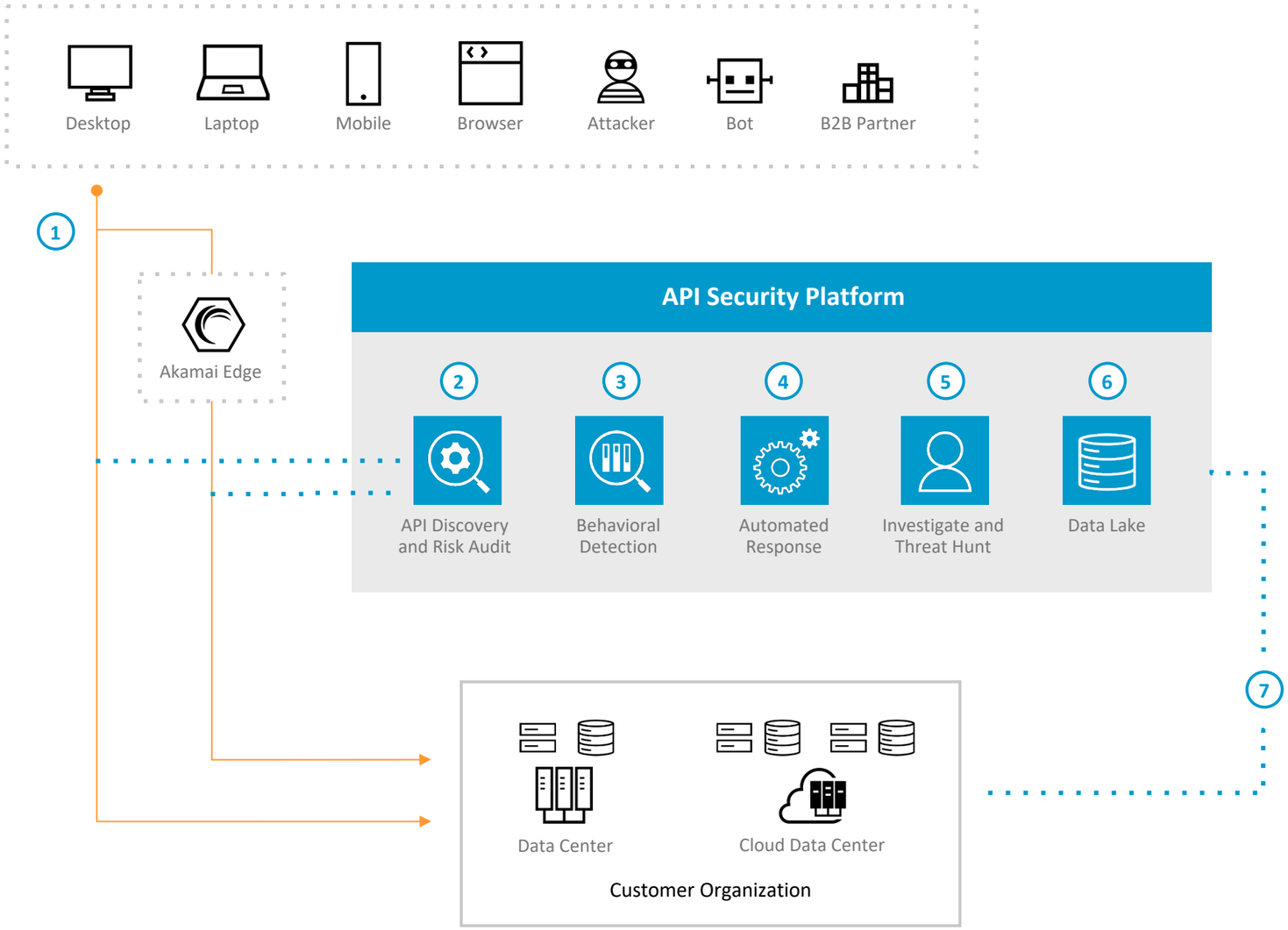
# API SECURITY

## How It Works




## OVERVIEW

Akamai API Security discovers and audits all APIs and monitors API activity, using behavioral analytics to detect and respond to threats and abuse. It provides contextual detections to protect against logic abuse and API attacks that signature-based solutions cannot detect.

1. Traffic flows from the customer organization and/or through the Akamai edge platform
2. A copy of that traffic feeds into the API Security platform where all APIs are discovered
3. Behavioral detections establish a normal pattern of behavior in order to detect anomalies and logic abuse
4. Automated responses can send critical information to security teams or block traffic at the Akamai edge
5. Security teams can use behavioral context to investigate and hunt for threats within API traffic or use a managed threat hunting service
6. Historic API activity is stored in our data lake and supports investigation and threat hunting initiatives
7. API Security also has full visibility into the customer organization's APIs and API activity

## KEY PRODUCTS

API protection ▶ Akamai API Security

Managed threat hunting ▶ Akamai API Security ShadowHunt

Visit akamai.com/products/api-security

Published 04/24