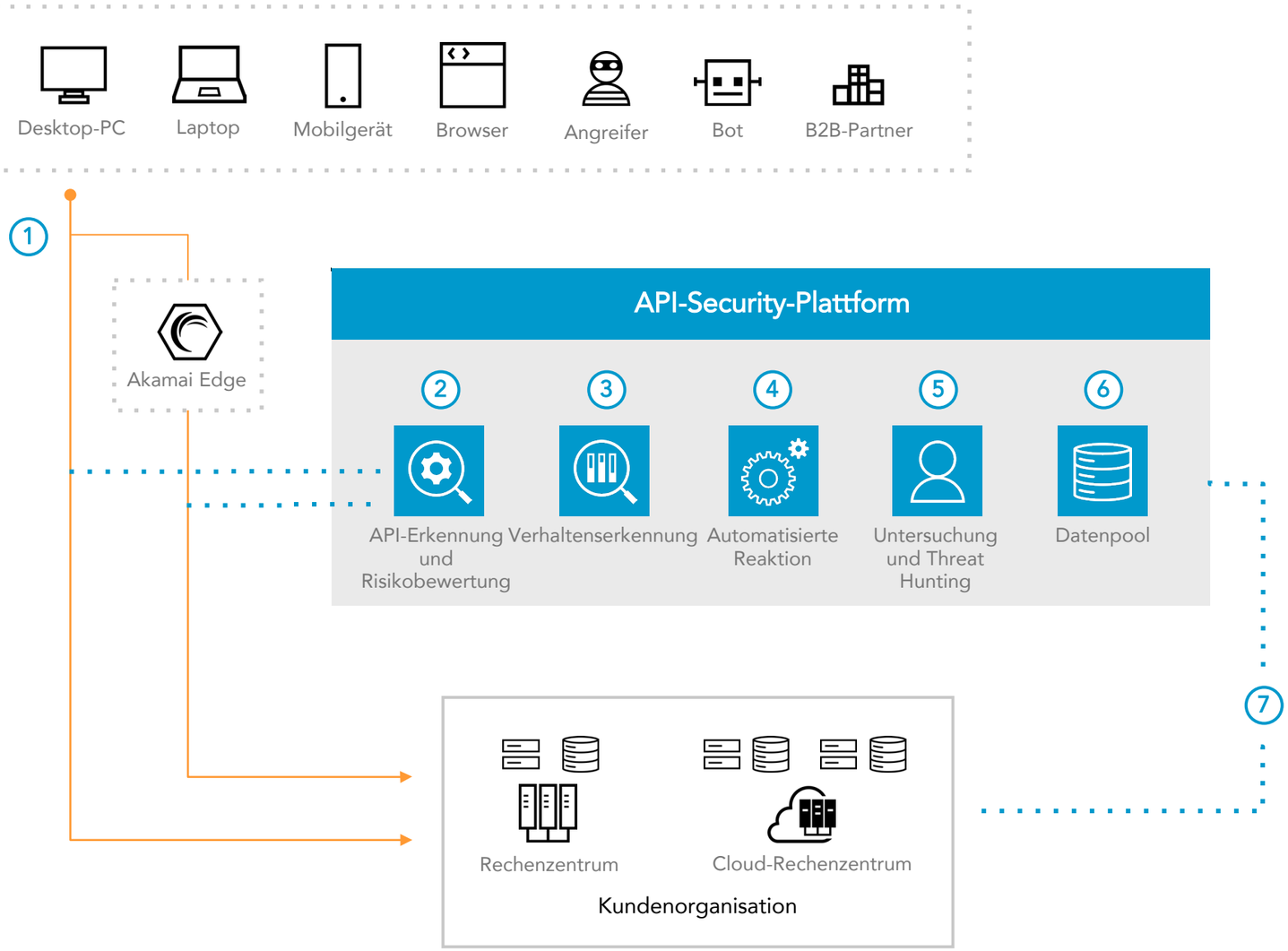
API SECURITY

Funktionsweise



OVERVIEW

Akamai API Security erkennt und prüft alle APIs und überwacht deren Aktivitäten mithilfe von Verhaltensanalysen, um Bedrohungen und Missbrauch zu erkennen und darauf zu reagieren. Es bietet kontextbasierte Erkennungen, um Missbrauch von Geschäftslogik und API-Angriffe zu verhindern, mit denen sich signaturbasierte Lösungen oft schwertun.

1. Der Traffic fließt vom Kundenunternehmen und/oder über die Edge-Plattform von Akamai.
2. Eine Kopie dieses Traffics wird in die API Security-Plattform eingespeist, auf der alle APIs erkannt werden.
3. Über Verhaltenserkennung wird ein normales Verhaltensmuster festgelegt, um Anomalien und Missbrauch von Geschäftslogik zu erkennen.
4. Automatisierte Reaktionen leiten entweder wichtige Informationen an Sicherheitsteams weiter oder blockieren den Traffic direkt an der Akamai Edge.
5. Sicherheitsteams können den Verhaltenskontext oder einen Managed Threat Hunting Service verwenden, um Bedrohungen im API-Traffic zu finden und zu untersuchen.
6. Der API-Aktivitätsverlauf wird in unserem Datenpool gespeichert und unterstützt Untersuchungen und Threat Hunting.
7. API Security bietet außerdem vollständige Transparenz in die APIs und API-Aktivitäten des Kundenunternehmens.

HAUPTPRODUKTE

API-Schutz ► Akamai API Security

Managed Threat Hunting ► Akamai API Security ShadowHunt

Weitere Informationen auf akamai.com/products/api-security

Veröffentlicht: 04/24