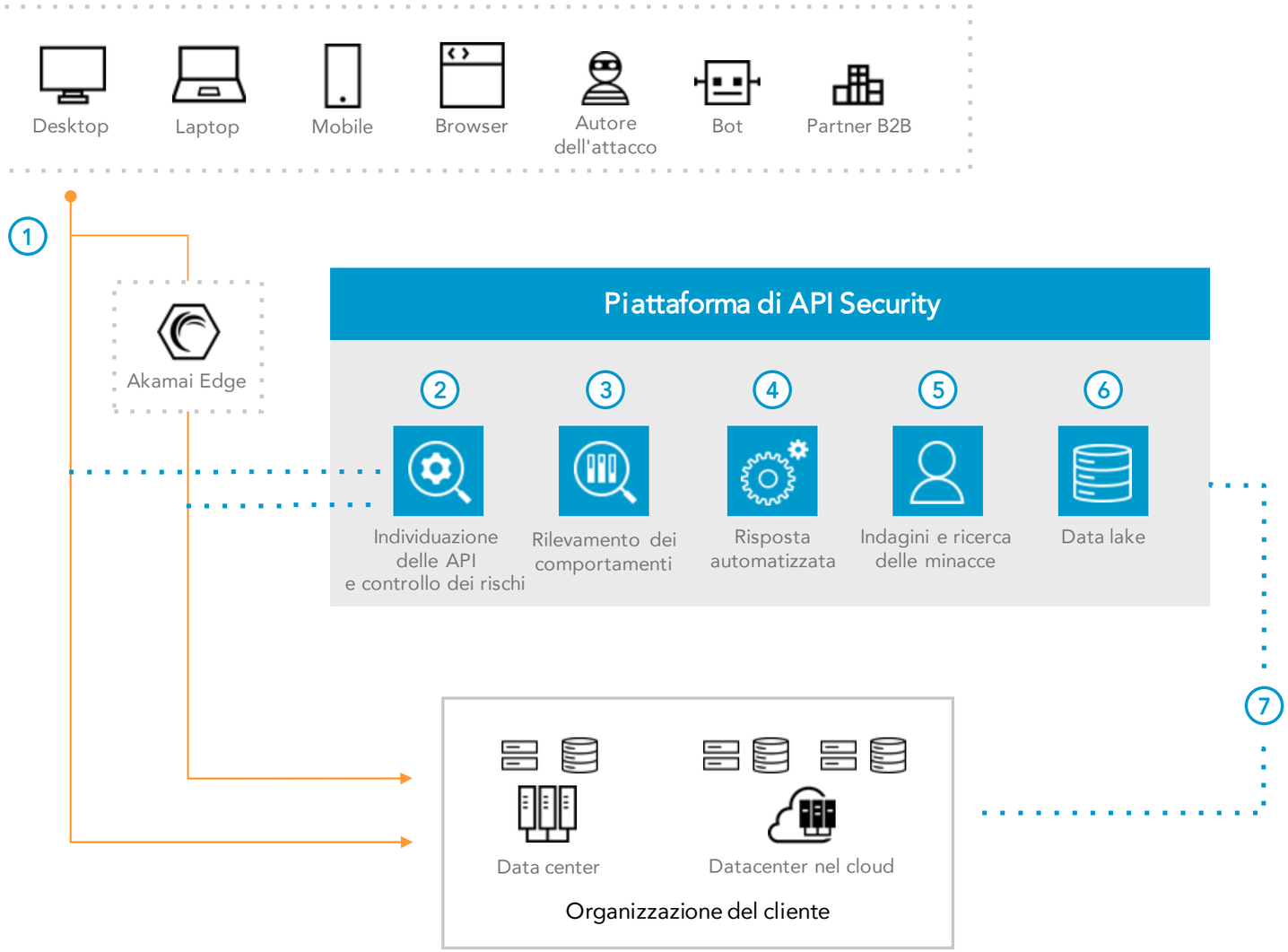
API SECURITY

Come funziona



PANORAMICA

Akamai API Security consente di identificare e verificare tutte le API, oltre a monitorare la loro attività, mediante l'analisi comportamentale per rilevare e rispondere ad eventuali minacce e violazioni. La soluzione fornisce sistemi di rilevamento del contesto per proteggere dagli abusi della logica aziendale e dagli attacchi alle API che altre soluzioni basate sulle firme non riescono ad individuare.

1. Il traffico viene trasmesso dall'organizzazione del cliente e/o tramite la piattaforma edge di Akamai
2. Una copia del traffico viene distribuita nella piattaforma di API Security in cui vengono individuate tutte le API
3. I sistemi di rilevamento dei comportamenti stabiliscono un modello di comportamento normale al fine di rilevare eventuali anomalie e abusi della logica aziendale
4. Le risposte automatizzate possono inviare informazioni critiche ai team addetti alla sicurezza o bloccare il traffico sull'edge di Akamai
5. I team addetti alla sicurezza possono utilizzare il contesto comportamentale per indagare e cercare le minacce all'interno del traffico delle API o utilizzare un servizio di ricerca delle minacce gestito
6. L'attività cronologica delle API viene archiviata nel nostro data lake e supporta le operazioni di indagine e ricerca delle minacce
7. API Security offre, inoltre, piena visibilità sulle API e sulle loro attività nell'organizzazione del cliente

PRODOTTI PRINCIPALI

Protezione delle API ► Akamai API Security

Ricerca delle minacce gestita ► Akamai API Security ShadowHunt

Visitate la pagina akamai.com/products/api-security

Data di pubblicazione: 04/24