CLUE
CYBER SECURE

Adaptive Application Protection

Die Sicherheitslücke

Moderne Anwendungen entwickeln sich rasant: APIs vermehren sich, Deployments verändern sich laufend und die Angriffsflächen erweitern sich schneller, als Sicherheitsteams Schritt halten können. Klassische Web Application Firewalls (WAFs) setzen auf statische Signaturen, die zwar gegen bekannte Bedrohungen wirksam sind, jedoch undokumentierte APIs und Angriffe, die keinem bekannten Muster entsprechen, nicht erkennen.

Der adaptive Vorteil

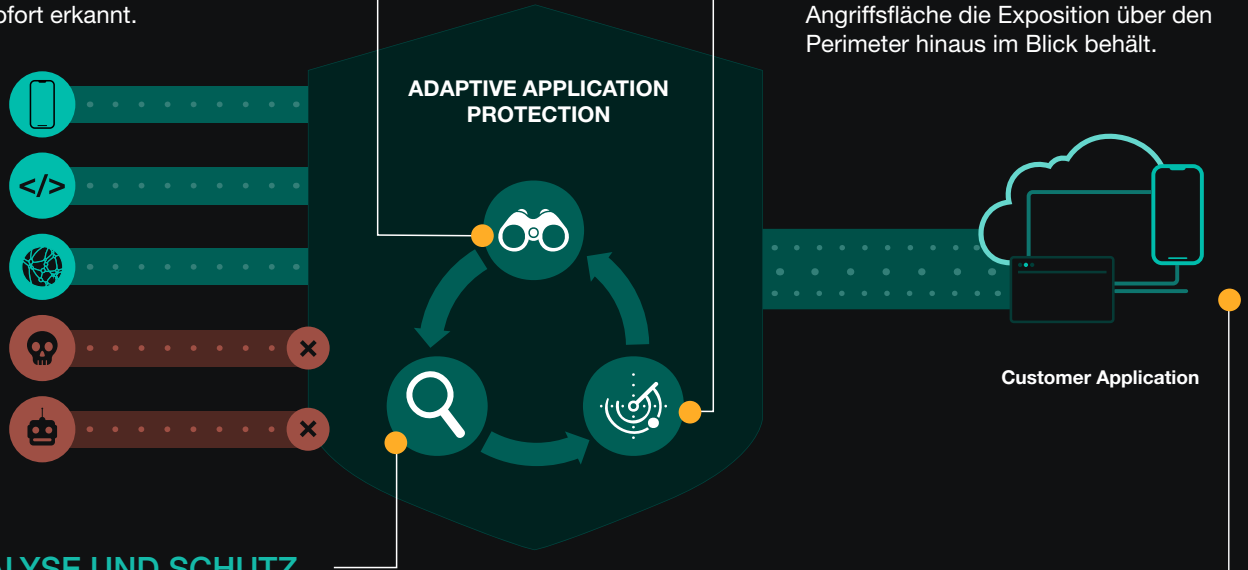
Adaptive Application Protection ist für die Funktionsweise moderner Anwendungen konzipiert. Durch die kontinuierliche Erkennung von APIs, das Verständnis Ihrer Geschäftsprozesse, die Analyse des Laufzeitverhaltens und die Überwachung der gesamten Angriffsfläche schliesst die Lösung die Lücken, die klassische Tools offen lassen. Das Ergebnis: präziser, laufend validierter Schutz, der mit Ihrer Entwicklungsgeschwindigkeit Schritt hält.

ERKENNUNG

Erfasst kontinuierlich Endpunkte, Methoden, Parameter und Auth-Mechanismen anhand des Live-Traffics, ohne manuellen Uploads. Undokumentierte, veraltete oder unautorisierte APIs werden sofort erkannt.

VALIDIERUNG

Die Wirksamkeit des Schutzes wird laufend durch Threat Replay und schemabasierte Sicherheitstests belegt, während das Monitoring der externen Angriffsfläche die Exposition über den Perimeter hinaus im Blick behält.



ANALYSE UND SCHUTZ

Der Live-Traffic wird laufend mit erlernten Verhaltensbaselines abgeglichen, die auf Ihren tatsächlichen Workflows und Geschäftsabläufen basieren. So werden Abweichungen, Missbrauchsmuster und Business-Logic-Angriffe wie BOLA (Broken Object Level Authorization) in Echtzeit erkannt.

KONTINUIERLICHER SCHUTZ

Nur validierter, legitimer Traffic erreicht Ihre Anwendungen. Bösartige Anfragen und bekannte Bedrohungen werden gestoppt, bevor sie ankommen, während sich der Schutz laufend an die Weiterentwicklung Ihrer APIs anpasst.

CLUE
CYBER SECURE

Benefits

Was uns als Security-Partner auszeichnet.

HUMAN EDGE

CLUE kombiniert adaptive Technologie mit direktem Analysten-Zugang. So treffen Sie schnelle, fundierte Entscheidungen, statt in der Alarmflut unterzugehen.

- Kontinuierliche, verhaltensbasierte Erkennung für höhere Präzision
- Automatisierte Workflows beschleunigen Triage und Reaktion
- Flexible Integration in Security- und CI/CD-Tools
- Transparente Lizenzierung auf Basis von Requests per Month (RPM)

API-NATIVE EXPERTISE

Speziell für verteilte, cloud-native, API-getriebene Architekturen entwickelt, nicht auf Basis klassischer WAF-Technologie nachgerüstet.

- Expertise in API-Discovery, Verhaltensanalyse und Lifecycle Governance
- Native Unterstützung für REST/JSON, GraphQL, XML-RPC, JSON-RPC, OData, gRPC, WebSocket, SOAP
- Kontinuierliche Validierung durch aktive Sicherheitstests statt statischer Regeln allein

EFFIZIENZ UND TRANSPARENZ

Statt überwältigender Alarmflut liefert CLUE klar strukturierte und jederzeit nachvollziehbare Informationen.

- Reduktion von Fehlalarmen durch verhaltensbasiertes Baselining
- Risikobasierte Priorisierung durch endpunktspezifisches Security Scoring
- Lösungsdesigns, die Schutzwirkung und Kosten ausbalancieren
- Detaillierte Einblicke und Reports über das CLUE Portal

Features

Die technischen Elemente unseres Ansatzes.

Kontinuierliche API-Erkennung

Erfasst automatisch Endpunkte, Parameter, Methoden und Authentifizierungsmechanismen aus dem Live-Datenverkehr und kennzeichnet neue oder undokumentierte APIs, sobald sie auftreten.

“Rogue & Shadow“ API Erkennung

Korreliert die Erkennung zur Laufzeit mit genehmigten Baselines, um nicht autorisierte, veraltete oder falsch konfigurierte APIs aufzudecken – einschliesslich „Shadow“-APIs und extern erreichbarer APIs.

Erkennung sensibler Daten

Untersucht Request- und Response-Payloads auf Zugangsdaten, Tokens und personenbezogene Daten und erkennt übermässige Datenexposition, bevor daraus ein Sicherheitsvorfall wird.

API Security Testing

Validiert den Schutz laufend durch Threat Replay und schemabasierte Tests gegen OpenAPI-Definitionen und deckt Sicherheitslücken auf, bevor Angreifer sie finden.

Application Attack Surface Management

Erfasst kontinuierlich öffentlich exponierte APIs und Endpunkte, inklusive Assets hinter CDNs, IaaS- und PaaS-Providern, und bewertet deren Risiko.

Erkennung externer API-Leaks

Durchsucht öffentliche Repositories und exponierte Assets nach geleakten API-Keys, Tokens und Zugangsdaten und ermöglicht so eine Behebung, bevor die Secrets ausgenutzt werden.

Jede Applikation ist eine Zielscheibe.

Adaptive Security hält Schritt.

Erleben Sie Adaptive Application Protection live. Jetzt Demo vereinbaren.

+41 44 667 77 66 | info@clue.ch | clue.ch

07.2026