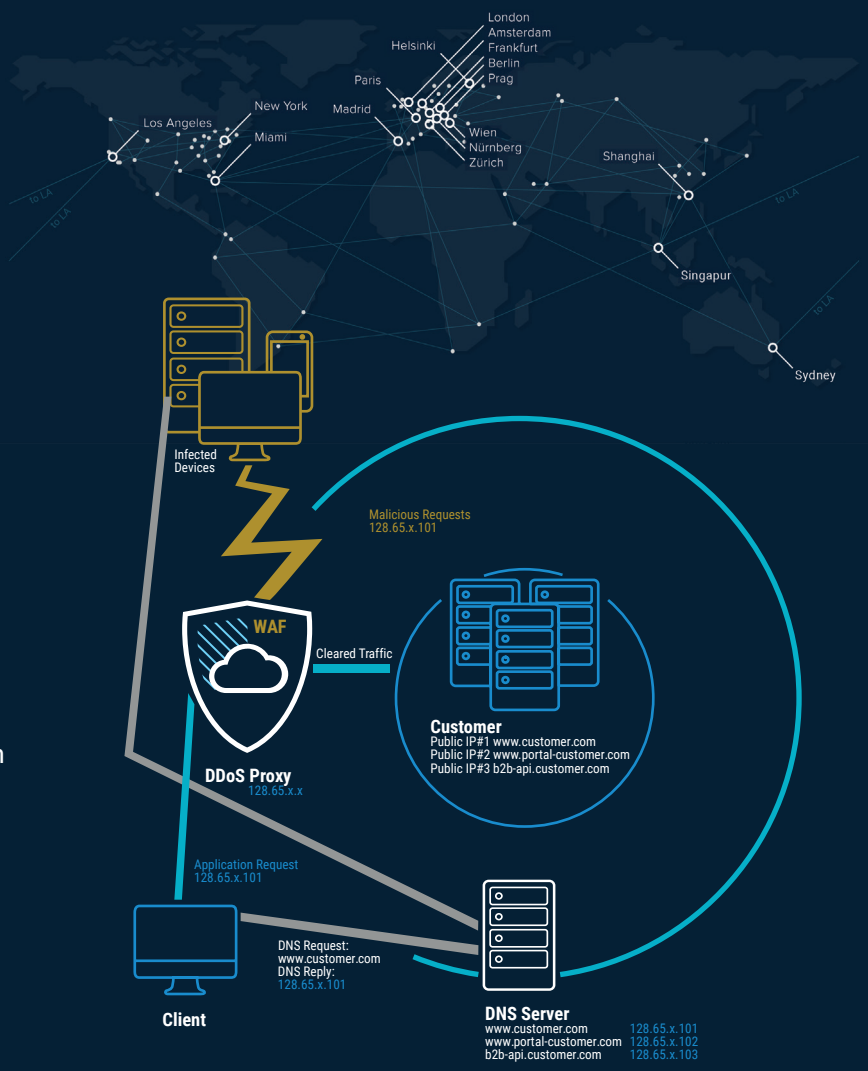
METAWAYS

ZERO TOUCH WEB APPLICATION FIREWALL (WAF)

Serviceübersicht

Die Zero Touch Web Application Firewall (WAF) ist Teil der Link11 Cloud Security Platform, die auf einer innovativen, patentierten Technologie basiert. Dank des vollständig cloudnativen Ansatzes und dem Einsatz Künstlicher Intelligenz (KI) bietet die Lösung einen vollautomatischen Schutz.

Die Lösung erkennt bösartigen Datenverkehr in Millisekunden und filtert ihn heraus, ohne den echten Benutzer zu stören. Sie schützt Webanwendungen und APIs gegen alle gängigen Bedrohungen, einschließlich der Top10-Liste des Open Web Application Security Projects (OWASP Top10). Unternehmenskritische Webanwendungen erhalten mit einer einzigen Lösung umfassenden Schutz vor allen gängigen Bedrohungen und Angriffsformen. So können Sie sich auf ihr Kerngeschäft konzentrieren. Für seine innovativen Schutzlösungen wie die Zero Touch WAF wurde Link11 mehrfach ausgezeichnet. Sie stellen sicher, dass die Link11 geschützten Kunden den Angreifern immer einen Schritt voraus sind.



Intelligente Regelwerkerstellung

Cloudnativer Schutz-Ansatz

Implementierung

Die Zero Touch WAF ist Teil der Web Security Suite und kann pro Instanz in der WebGUI des Kunden aktiviert werden. Der Service verwendet das Zero Touch WAF Ruleset, um Kunden gegen alle Arten von üblichen Anwendungsangriffen, wie z. B. SQL-Injektion, XSS und CSRF, zu schützen. Die Lösung startet im Lernmodus, in dem Regeln getriggert werden, aber keine direkte Blockierung von Anfragen stattfindet. Administratoren können dann das standardmäßige WAF-Regelwerk überprüfen und False-Positive-Regeln pro Web-DDoS-Instanz deaktivieren. Am Ende der Evaluierungsphase können Kunden den WAF-Sperrmodus aktivieren.

METAWAYS

FEATURES

Hauptmerkmale

- Automatischer Schutz für kritische Webanwendungen, APIs und Services
- One-Click-Deployment zusätzlich zur Web DDoS Protection
- Globale Abdeckung durch die Cloud Security Plattform
- Echtzeit-Zugriff auf Link11 WebGUI
- Detaillierte Angriffs-Reports
- Hochmoderne Verschlüsselung (SSL/TLS)
- Spezielle SSL-/TLS-Frontend-Einstellungen
- Spezielle SSL-/TLS-Backend-Einstellungen (erneute Verschlüsselung)
- Out-of-the-box-Schutz vor OWASP Top10-Bedrohungen
- GeoIP Country Blocking

Schutz vor

- OWASP Top10 Schwachstellen
- SQL Injections
- Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- Remote Code Execution
- Metadata / Error Leakages
- Scanner Detection
- Session Fixation

Fundierte Erfahrung bei der Bereitstellung von Sicherheit

Unser Partner Link11 ist der im Bereich Cyber-Resilienz führende europäische IT-Sicherheitsanbieter. Die globalen Schutzlösungen der Cloud Security Plattform sind vollständig automatisiert, reagieren in Echtzeit und wehren alle Angriffe, so auch unbekannte und neue Muster, in unter 10 Sekunden ab. Link11 bietet laut einhelliger Analysten-Meinung (Gartner, Frost & Sullivan u. a.) die schnellste Mitigation (TTM), die auf dem Markt verfügbar ist. Um Cyber-Resilienz zu gewährleisten, sorgen u. a. Web- und Infrastruktur-DDoS-Schutz, Bot-Mitigation, API-Schutz, Secure DNS, Zero Touch WAF, Secure CDN bis hin zu Threat-Intelligence-Services für eine ganzheitliche und Plattform-übergreifende Härtung der Netzwerke und kritischer Anwendungen von Unternehmen. Die internationalen Kunden können sich so auf ihr Geschäft und digitales Wachstum konzentrieren. Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovativen Lösungen ausgezeichnet.

Als offizieller Partner nationaler und internationaler Fachverbände wie dem G4C, einer Kooperation der Privatwirtschaft mit dem BSI und dem BKA, engagiert sich Link11 aktiv im Bereich IT-Security und bei der Aufklärung von Cybercrime.