Web Protection

www.link11.com

LINK11
WE PROTECT BETTER

INHALT

LINK11
WE PROTECT BETTER

WEB DDOS PROTECTION

- **Cloud-basierter DDoS-Schutz für Webanwendungen**
- **Automatisierung gewährleistet 24/7-Schutz**
- **Zero-Time-To-Mitigate für bekannte, < 10 Sekunden für neue Vektoren**

Präzise Erkennung

Keine Sorgen mehr bei komplexen Angriffen: Das System erkennt Anomalien und schützt Sie in Echtzeit vor neuen Bedrohungen.

Volle Automatisierung

Keine Arbeit für Sie: Eine manuelle Bedienung ist nicht erforderlich, das System arbeitet vollautomatisch und ohne Kompromisse.

Detaillierte Anpassung

Whitelisting, Logs, Traffic-Steuerung und mehr – hilfreiche Funktionen helfen Ihnen, den Alltag so einfach wie möglich zu machen.

ALLE MÖGLICHKEITEN MIT EINER LÖSUNG

DDoS-Angriffe nehmen weiter zu und führen heute nach wie vor zu großen Schäden. Neben der Häufigkeit sorgen vor allem die Komplexität und Dauer einer Attacke zu großen Problemen bei der Verteidigung. Daher sollte die eingesetzte Lösung präzise und schnell eingreifen, um Sie bestmöglich vor Gefahren und hohen Kosten durch Ausfälle zu schützen.

60 sek

Zeit bis zum kritischen Angriffsvolumen

1444 min

Die längste andauernde Attacke

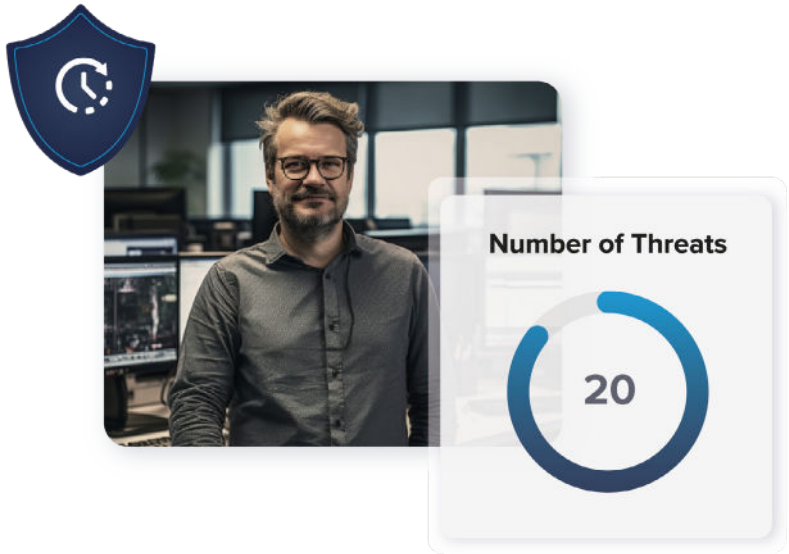
454 GBPS

Durschnittlicher Angriffsbandbreiten-Peak

Garantierter Schutz

Mit der Web DDoS Protection werden Sie von einem System geschützt, das dank künstlicher Intelligenz Angriffe auf den Layern 3, 4 und 7 effektiv stoppt. Zudem profitieren Sie von zahlreichen Algorithmen und Heuristiken, die die Ereignisse auf der Anwendungsschicht überwachen und bewerten. Durch diese Kombination können Sie sich auf eine garantierte Mitigation des Angriffs innerhalb kürzester Zeit verlassen.

Unser System analysiert die typischen Datenverkehrsmuster Ihrer Webanwendungen und identifiziert alle Anomalien, die vom „Normalen“ abweichen oder verdächtig erscheinen. Dieser proaktive Ansatz gewährleistet Ihren Schutz nicht nur vor bekannten, sondern auch vor neuen und unbekannten Bedrohungen.



Mehr Fokus auf Ihr Kerngeschäft

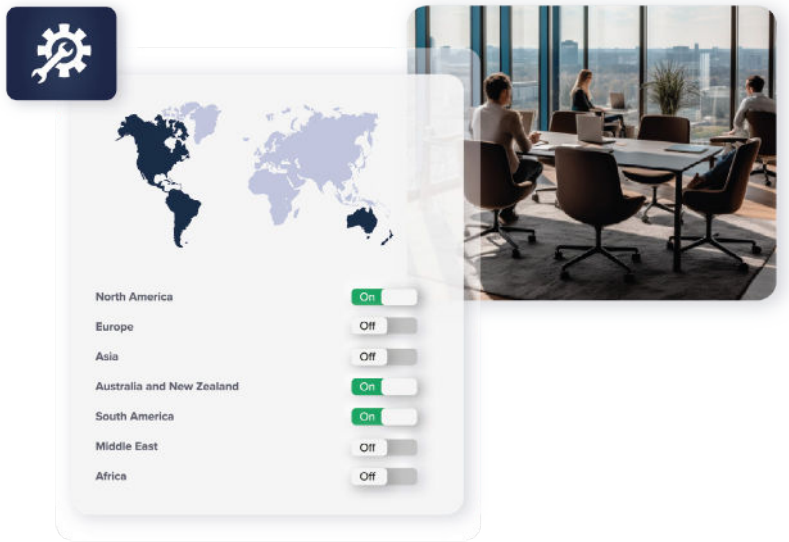
Unser DDoS-Schutz macht Ihnen den Alltag so einfach wie möglich. Daher arbeiten die Erkennungs- und Entschärfungstools der Sicherheitslösung ganz ohne manuelle Eingriffe. Angriffe werden in Echtzeit erkannt und abgewehrt, ohne dass Sie selbst mit dem Schutz interagieren müssen. Das stellt sicher, dass Sie und Ihre Anwendungen zu jeder Tageszeit rund um die Uhr geschützt sind.

Diese automatisierte Sicherheit spart Zeit und Geld und macht es noch einfacher für Sie, sich auf das Wesentliche zu konzentrieren. Ebenfalls von Vorteil: Sie brauchen uns im Angriffsfall nicht zu kontaktieren. Unser System weiß es bereits und hat alle benötigten Schritte eingeleitet, um die Gefahr zu mitigieren. Ihr Business-Alltag kann daher weitergehen, als wäre nichts passiert.

Genau so, wie es sein soll

Individuelle Einstellungen helfen Ihnen, das System ideal auf Ihre Bedürfnisse zuzuschneiden – unsere Web DDoS Protection bietet genau das. Stellen Sie der Lösung Ihr eigenes Zertifikat zur Verfügung oder nutzen Sie eines von uns, richten Sie TCP-Port-Weiterleitungen ein oder modifizieren Sie die Geoblocking-Funktion. Die Wahl liegt ganz bei Ihnen.

Durch die Auswahlmöglichkeiten müssen Sie mit keinem starren System arbeiten, dass Ihnen vorschreibt, was Sie tun können und was nicht. Profitieren Sie von der Flexibilität und passen Sie Ihre Einstellungen immer genau auf die Situation an.



Funktionen, die den Unterschied machen

Access Logs & Analyse

Gewinnen Sie mit den umfassenden Zugriffsprotokollen und interaktiven Dashboard-Visualisierungen maximale Transparenz und wichtige Einblicke in die Verkehrsmuster Ihres Netzwerks. Unsere Zugriffsprotokolle zeichnen akribisch jede Verbindung auf und bieten einen detaillierten Überblick über die Aktivitäten der Anfragenden, sowohl im regulären Betrieb als auch in Angriffsszenarien.

Aber das ist noch nicht alles: Unsere benutzerfreundlichen Dashboards wandeln diese Daten in visuelle Darstellungen um, so dass Sie Ihre Verteidigung mühelos überwachen, analysieren und strategisch ausrichten können. Vertrauen beruht auf Transparenz, und unsere Zugriffsprotokolle und Dashboards geben Ihnen das nötige Wissen an die Hand, um in Zukunft noch sicherer zu sein.

Flexible IP & Geo-Blocking

Gestalten Sie Ihre Verteidigungsstrategie perfekt mit unseren anpassbaren IP-, Geo und ASN-Blockalgorithmen, die Ihnen die volle Kontrolle über Ihre Sicherheitsmaßnahmen bieten. Diese dynamischen Algorithmen ermöglichen Ihnen eine Feinabstimmung Ihres Schutzes und gewährleisten einen idealen Mittelweg zwischen robuster Sicherheit und der Reduzierung von Fehlalarmen auf ein Minimum.

Ganz gleich, ob Sie bestimmte IPs, Regionen oder ASNs (Autonomous System Numbers) blockieren müssen – unsere umfassenden Blockoptionen bietet Ihnen dank Whitelisting die Flexibilität, eine maßgeschneiderte Sicherheitslösung zu erstellen, die perfekt auf die individuellen Anforderungen Ihres Unternehmens abgestimmt ist.

Captcha-Schutz vor verdächtigen IPs

Schützen Sie Ihr Netzwerk vor verdächtigen IPs mit unserem robusten Captcha-Verifizierungssystem, das automatisierten und Bot-Verkehr effektiv herausfiltert und gleichzeitig legitimen Nutzern den nahtlosen Zugriff auf Ihre Dienste ermöglicht. Was uns auszeichnet, ist unser Engagement für den Schutz der Privatsphäre und den Datenschutz.

Mit dieser zusätzlichen Sicherheitsebene können Sie Ihr Netzwerk nicht nur schützen, sondern auch alle rechtlichen Regularien garantieren.

Erweitertes Traffic-Management

Verbessern Sie die Leistung Ihres Netzwerks mit einer Reihe Funktionen, darunter Umleitungen, Origin Load Balancing und Origin Timeouts. Umleitungen leiten unverschlüsselten HTTP-Datenverkehr effizient auf HTTPS-Verbindungen um und erhöhen so die Datensicherheit. Origin Load Balancing verteilt den eingehenden Datenverkehr auf intelligente Weise auf mehrere Server, um eine optimale Ressourcennutzung und minimale Latenzzeiten zu gewährleisten.

Mit Origin Timeouts können Sie präzise Werte für Verbindungs- und Lesezeitüberschreitungen festlegen, um zu verhindern, dass Anfragen festgelegte Grenzen überschreiten, und um die Gesamteffizienz des Netzwerks zu verbessern. Diese Hilfsmittel optimieren die Verteilung des Datenverkehrs und helfen Ihnen, die Performance Ihrer Online-Dienste zu optimieren.

Wichtige Zertifizierungen & Partnerschaften

Einfach in der Nutzung, leistungsstark im Ergebnis

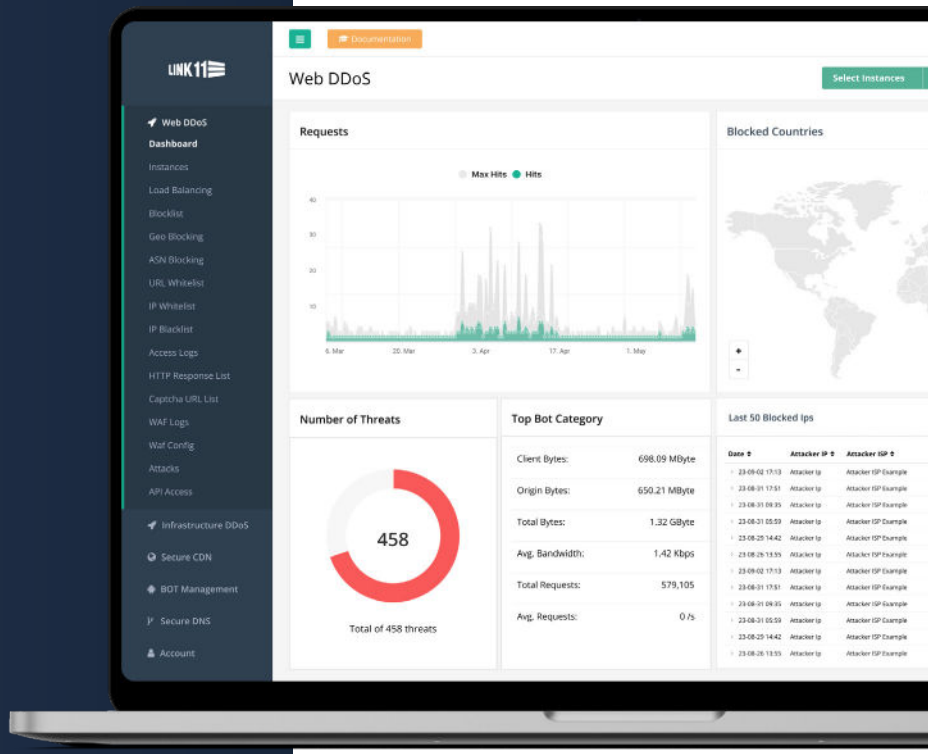
- **Alles auf einen Blick:** Das Dashboard zeigt wichtige Metriken, Bedrohungsdaten, abgewehrte Angriffe und Daten über die eingesparte Bandbreite oder den verbrauchten Datenverkehr.

- **Reporting:** Erstellen Sie individuelle oder geplante Berichte, die zudem in PDF-Form exportiert und auf Wunsch zu einem gewählten Zeitpunkt automatisch verschickt werden können.

- **Benutzerverwaltung:** Details, wie die letzten Passwortänderungen, Nutzerrechte oder die Aktivierung der 2-Faktor-Authentisierung können hier eingesehen und angepasst werden.

- **Alarming:** Legen Sie hier genau fest, in welcher Frequenz ausgewählte Mitarbeiter Benachrichtigungen erhalten. Die Anpassungsmöglichkeiten sind dabei hochgradig individuell.

- **Passwortverwaltung:** Alphanumerischen Passwörter, konfigurierbare Passwortlängen oder die Einstellung von Passwortlebensdauern garantieren, dass der Zugang sicher ist und bleibt.



Warum Sie sich auf Link11 verlassen können

Schneller & präziser Schutz

Wir schützen über zwei Millionen Assets von führenden Unternehmen auf der Welt. Dabei hat sich unsere patentierte Technologie mehr als bewährt.

Einfache Integration & Bedienung

Unsere Lösungen sind einfach in jedes Set-Up zu integrieren. Dabei ist uns wichtig, dass der Aufwand für Sie auf ein absolutes Minimum reduziert wird.

24/7 Kundenservice

Für uns ist es wichtig, jederzeit für Sie da zu sein. Von daher bieten wir Ihnen einen 24/7 Kundenservice in deutsch und englisch an, der Ihnen zur Seite steht.

Zertifiziert & qualifiziert

Vollständig konform mit den strengen EU-Datenschutzgesetzen. Außerdem ISO 27001-zertifiziert und offiziell vom BSI für den KRITIS-Sektor qualifiziert.

Einfach erweiterbar

Obwohl der Web DDoS-Schutz bereits ein großes Sicherheitsspektrum abdeckt, können Sie ganz den Schutzstandard ganz unkompliziert mit weiteren Services erweitern.

LINK 11
WE PROTECT BETTER

BOT MANAGEMENT

- **Effektive Erkennung, Klassifizierung und Verwaltung von Bot-Traffic**
- **Wertvolle Einblicke in alle Bot-Aktionen**
- **Erkennung von bösartigen Aktivitäten, ohne hilfreiche Bots zu blockieren**

Erhöhte Sichtbarkeit

Das Bot Management bietet Ihnen einen unvergleichlichen Überblick, der Ihnen jeden Bot detailliert aufzeigt, der Ihre Website besucht.

Schutz nach Maß

Passen Sie existierende Richtlinien an, um im System exakt festzulegen, welche Bots erwünscht und welche blockiert werden sollen.

Effizientes Profiling

Unterscheiden Sie nahtlos zwischen menschlichem Verkehr und Bots, um so zwischen echten Besuchern und Bedrohungen zu unterscheiden.

ALLE MÖGLICHKEITEN MIT EINER LÖSUNG

Ein Großteil des weltweiten Internetverkehrs ist automatisiert und wird Bots zugeschrieben. Mit unserem Bot Management verwalten Sie den automatisierten Traffic auf Ihrer Webseite: Effektive Erkennung, Klassifizierung und das Erkennen und Blockieren bösartige Aktivitäten, ohne hilfreiche Bots zu auszuschließen.

47%

des Internetverkehrs im Jahr 2022 war automatisiert

30%

des Internetverkehrs im Jahr 2022 stammte von bösartigen Bots

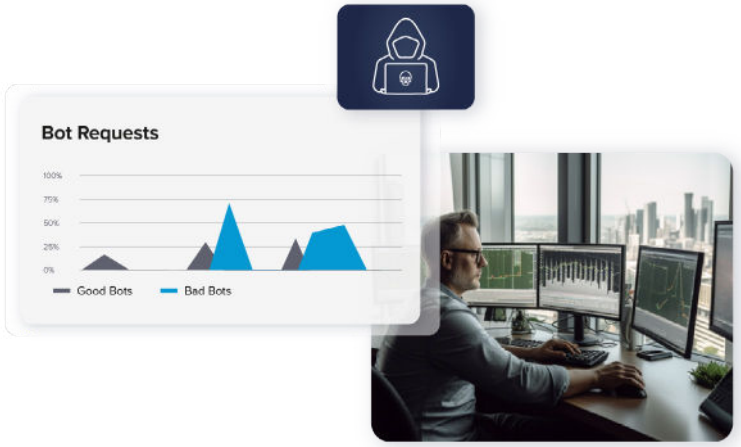
60%

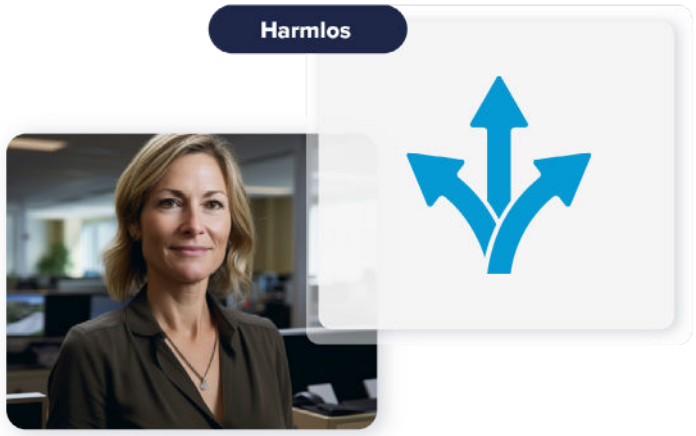
des deutschen Datenverkehrs stammte von bösen Bots

Leistungsstarke Klassifizierung

Mit unserem Bot Management profitieren Sie von Klassifizierungsprotokollen, die alle Informationen über die Art der besuchenden Bots anzeigen. Dadurch können Sie die Protokolle überprüfen und erkennen, welche Anfragen vom System als Bots markiert wurden.

Das System legt bereits im Voraus fest, welche Bots als gut oder schlecht eingestuft sind und welche Zwecke diese verfolgen. Dank der vorhandenen Klassifizierungsregeln können Sie diese Annahmen aktualisieren, um den einkommenden Datenverkehr besser auf Ihre Bedürfnisse zuzuschneiden. Sie haben zudem die alternative Option, ein Captcha einzublenden, statt einen gewissen Teil des Bot-Traffics direkt zu blockieren.





Zugangsverbot für schlechten Traffic

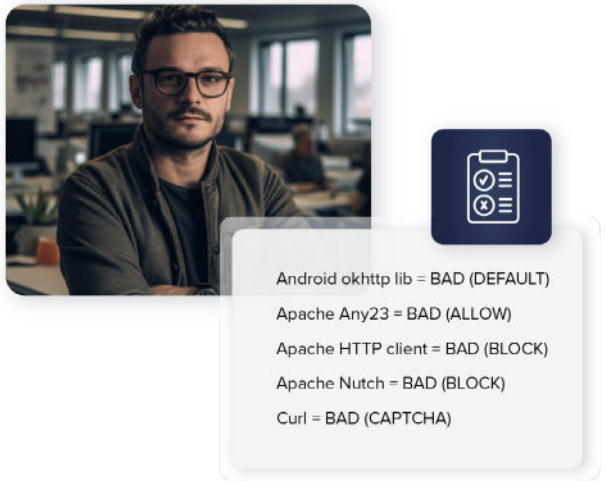
Der einkommende Traffic wird für Sie in drei Kategorien eingeteilt: Menschlicher Traffic, der nicht von einem Bot erzeugt wird. Schädliche Bots, die etwas Bösartiges oder zumindest Verdächtiges im Sinn haben. Und zu guter Letzt hilfreiche Bots, die entweder als ungefährlich oder sogar als förderlich markiert wurden. Der Google Web-Crawler wäre ein Beispiel, eines sogenannten guten Bots.

Mit der Einteilung dieser Kategorien sehen Sie auf einen Blick, wie sich der Bot-Traffic auf Ihrer Webseite verteilt und wie Sie am besten vorgehen, um mit diesen gewünschten oder ungewünschten Besuchern umzugehen.

Riesige Regelvielfalt

Ein Bot Management bietet Ihnen die größten Vorteile, wenn es die passenden Einstellmöglichkeiten gibt, um das System ideal auf Ihre Vorstellungen anzupassen. Nur mit Hilfe zahlreicher Anpassungsoptionen können Sie bis ins kleinste Detail sicherstellen, welchen Traffic Sie auch wirklich wollen.

Von daher bieten wir Ihnen eine Vielzahl von Einstellungen an, die über die simple Traffic-Organisation, über das Whitelisting spezieller IPs bis hin zu Kategorisierungen einzelner Bot-Typen reicht. Lassen Sie das System so arbeiten, wie Sie es wünschen.



Verlässliche mobile Erkennung

Mobiler Traffic verhält sich etwas anders als der klassische Traffic, da sich viele verschiedene Geräte oft hinter einer einzigen öffentlichen IP befinden. Manche Systeme haben damit ihre Probleme, da die Aktionen eines einzigen böswilligen Akteurs sich dann oft auf alle Nutzer hinter dieser IP-Adresse auswirken.

Mit unserem Bot Management passiert Ihnen das nicht. Das System erkennt die schädliche Quelle und nutzt weitere Faktoren als nur die Quell-IP, um Anfragen unterschiedlich zu identifizieren und bei Bedarf zu blockieren. Die Technologie erkennt selbst Bots, die über NAT-geschützte IP-Adressen kommen oder sich per verschleierter oder gefälschter Quelle Zugang verschaffen möchten.

Funktionen, die den Unterschied machen

Klassifizierungsprotokolle

Mit den Klassifizierungsprotokollen erhalten Sie einen tiefen Einblick in den Bot-Erkennungsprozess. Diese Protokolle bieten einen umfassenden Überblick über die Anfragen, die zur Klassifizierung einer Quell-IP als Bot beigetragen haben.

Nutzen Sie diese Protokolle, um besser zu verstehen, wie Bots erkannt werden, und werfen Sie einen Blick hinter den Vorhang, wie das System im Detail funktioniert.

Klassifizierungsregeln

Flexibilität ist das Herzstück eines effektiven Bot Managements. Mit speziellen Klassifizierungsregeln können Sie unsere vordefinierten Annahmen so anpassen, so dass diese perfekt auf Ihre individuellen Anforderungen abgestimmt sind.

Durch diese Anpassung werden Fehlalarme reduziert, was einen reibungslosen und problemlosen Betrieb gewährleistet und Ihnen die Kontrolle darüber gibt, wie Bots in Ihrer Webanwendung behandelt werden.

Bot-Profiling

Überprüfen Sie die Aufschlüsselung des Datenverkehrs, der Ihre Webanwendungen erreicht. Der Datenverkehr wird in menschlichen Datenverkehr, Datenverkehr von zugelassenen Bots und Datenverkehr von bösartigen oder unbekannten Bots unterteilt.

Das Verständnis des Gleichgewichts zwischen diesen drei Arten von Datenverkehr hilft bei der Effektivität des Bot Managements und gibt einen guten Einblick in die Arten von Benutzern, die auf Ihre Webanwendung zugreifen.

Organisationsregeln

Übernehmen Sie eine noch direktere Kontrolle mit den Organisationsregeln. Definieren Sie Standardaktionen für „böse“ Bots, um eine Basisreaktion festzulegen, und passen Sie dann spezifische Aktionen für einzelne Bots an.

Bei bösartigen Bots können Sie wählen, ob Sie den Datenverkehr komplett blockieren oder ein Captcha anzeigen möchten – je nach Ihren individuellen Präferenzen und Sicherheitsanforderungen.

Whitelisting

Stellen Sie mit Whitelisting den reibungslosen Betrieb Ihrer eigenen automatisierten Tools sicher. Egal, ob es sich um Administrator-IPs oder um eine Überwachungslösung handelt – Sie haben die Möglichkeit, bestimmten Datenverkehr zu erlauben, das Bot Management zu umgehen, sodass Ihre vertrauenswürdigen Systeme ohne Unterbrechung funktionieren.

Fingerprinting

Die Funktion verwendet fortschrittliches TLS-Verbindungs-Fingerprinting, das auf der JA3-Technologie basiert. Sie wandelt eindeutige Verbindungsattribute in kryptografische Hashes um, die es uns ermöglichen, bestimmte Verbindungsmuster zu identifizieren.

Auf diese Weise können wir potenzielle Bedrohungen und böswillige Quellen präzise erkennen und eine zusätzliche Sicherheitsebene über die Quell-IPs hinaus einrichten. Dieser Ansatz reduziert Fehlalarme und gewährleistet eine effiziente und genaue Identifizierung von Sicherheitsbedrohungen in Ihrem Netzwerk.

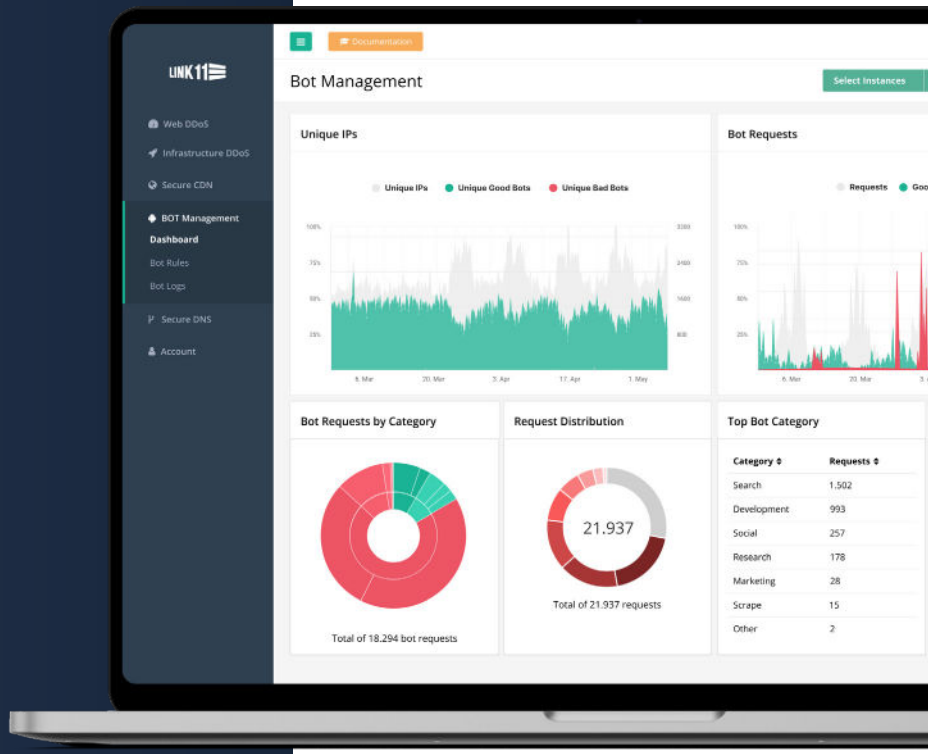
Mobile Erkennung

Überwinden Sie Herausforderungen im Zusammenhang mit NAT (Network Address Translation) mit der „Mobile Endpoint Detection“. Diese Funktion nutzt Faktoren, die über die Quell-IP hinausgehen, um Anfragen zu identifizieren, die blockiert werden sollten, und gewährleistet so ein präzises und effektives Bot Management für Ihr Netzwerk.

Wichtige Zertifizierungen & Partnerschaften

Smartes Bot Management mit einer Vielzahl von Anpassungsoptionen

- **Zeitreihen-Diagramm:** Überprüfen Sie die Bot-Aktivität im Zeitverlauf. Sehen Sie im Detail die Aktivität von Bots auf Ihrer Webanwendung in Echtzeit.
- **Bot-Kategorien:** Schlüsseln Sie die Arten von Bots auf, sowohl gute als auch schlechte, die mit Ihrer Webanwendung interagieren.
- **Anfragenverteilung:** Bewerten Sie den prozentualen Anteil des von guten und schlechten Bots generierten Datenverkehrs im Vergleich zu Nicht-Bots.
- **Zusatzinformationen:** Erhalten Sie Statistiken über Bot-Arten, Organisationen, die den automatisierten Datenverkehr verursachen, und Daten zur Captcha-Lösungsrate.
- **Passwortverwaltung:** Alphanumerischen Passwörter, konfigurierbare Passwortlängen oder die Einstellung von Passwortlebensdauern garantieren, dass der Zugang sicher ist und bleibt.



Warum Sie sich auf Link11 verlassen können

Maßgeschneiderte Lösungen

Unser Anspruch ist es, mit Ihnen zusammen die ideale Lösung für Sie zu erkennen und umzusetzen. Nur wenn Sie zufrieden sind, sind wir es auch.

24/7 Kundenservice

Unsere Experten sind rund um die Uhr in englisch und deutsch für Sie da und stehen Ihnen mit Rat und Tat zur Seite, wenn es von Ihrer Seite aus etwas zu besprechen gibt.

Markterfahrung

Wir bieten spezialisierte Schutzlösungen seit über 18 Jahren an und schützen über 2 Millionen Assets von nationalen und internationalen Unternehmen weltweit.

Zertifiziert & qualifiziert

Vollständig konform mit den strengen EU-Datenschutzgesetzen. Außerdem ISO 27001-zertifiziert und offiziell vom BSI für den KRITIS-Sektor qualifiziert.

Einfache Implementierung

Unsere Schutzlösungen können unkompliziert und in kürzester Zeit aufgesetzt werden, damit Sie mehr Zeit mit der tatsächlichen Nutzung statt der Umsetzung einplanen können.

LINK 11
WE PROTECT BETTER

ZERO TOUCH WAF

- **Wirksamer Schutz vor Zero-Day-Schwachstellen**
- **Whitelisting-Regeln zur Anpassung persönlicher Präferenzen**
- **Automatisierter Schutz, der direkt zur Verfügung steht**

Automatisierter Schutz

Das System schützt Sie jederzeit automatisch vor allen bekannten Bedrohungen und das ganz ohne menschliche Interaktion.

Detaillierte Einstellungen

Nutzen Sie maßgeschneiderten WAF-Regeln, die den Anforderungen Ihrer Website oder Anwendung entsprechen.

Hohe Flexibilität

Passen Sie Ihren Schutz durch flexible Whitelisting-Regeln nach Bedarf an das Design Ihrer Website oder Anwendung an.

ALLE MÖGLICHKEITEN MIT EINER LÖSUNG

Nicht gepatchte Software gilt auch in der heutigen Zeit als gefährliches Einfalltor für Cyberkriminelle. Die Nutzung von weltweiten Exploits sinkt nicht etwa, die Zahlen steigen immer weiter an. Um sich nicht auf den Software-Support zu verlassen, sollten Sie daher auf unsere Zero Touch WAF setzen, die solche ungewünschten Events entdeckt und einen Riegel vorschiebt.

180k

Abgeschwächte WAF-Ereignisse pro Tag durch Link11

4135

Kritische CVEs, die im Jahr 2022 gemeldet wurden

93

CVE-2022-Einträge wurden im Jahr 2022 ausgenutzt

Umfassender & automatisierter Schutz

Im Falle einer Bedrohung sollten Sie auf eine WAF setzen, die regelmäßig geupdatet wird und Sie vor aktuellen Gefahren effektiv schützt. Daher wird unsere Zero Touch WAF ständig aktualisiert und aktiv mit neuen Regeln zur Absicherung geupdatet. Diese Flexibilität bedeutet für Sie eine erhöhte und stetig modernisierte Sicherheit vor Zero-Day-Gefahren, die aufgrund der Agilität vielen größeren WAF-Anbietern einen Schritt voraus ist.

Das virtuelle Zero-Day-Patching und die Abdeckung der OWASP Top 10 Regeln garantiert Ihnen eine hohe Schutzleistung, die immer auf dem neusten Stand bleibt. Wichtig für Sie: Das übernehmen alles wir. Sie genießen immer ein hohes Schutzlevel und müssen sich um nichts Weiteres kümmern.

Auf Ihre Bedürfnisse zugeschnitten

Entwerfen Sie auf Wunsch Ihre eigenen WAF-Regeln, um die Schutzlösung so genau wie nur möglich auf Ihre Bedürfnisse abzustimmen. Hinzu kommt das von uns hinterlegte Regelwerk, in das unsere Erfahrung sowie die Übersicht der aktuellen Sicherheitssituation mit einfließen. Die Flexibilität in Kombination mit jahrelanger Branchenerfahrung eröffnet für Sie ganz neue Möglichkeiten.

Hier spielen auch die Whitelisting-Regeln eine wichtige Rolle: Mit diesen können Sie den Schutz selbst anpassen, der ideal auf das Design Ihrer Webseite oder Anwendung abgestimmt ist. Stellen Sie so sicher, dass Ihre einzigartigen Elemente erhalten bleiben, ohne die Sicherheit zu beeinträchtigen.

Funktionen, die den Unterschied machen

0

Zero-Day-Schutz

Eine risikoreiche Schwachstelle, die dem Softwarehersteller bisher nicht bekannt war und für die es zum Zeitpunkt ihrer Entdeckung keinen Schutz oder Patch gab, wird als Zero-Day-Exploit bezeichnet.

Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts werden in der Regel erst dann auf die Schwachstelle aufmerksam, wenn Angriffe auf Basis dieser Schwachstelle entdeckt werden. Die Zero Touch WAF schützt Sie effektiv vor solchen Gefahren.

Whitelisting

Sollten Sie ein einzigartiges oder komplexes Website-Design haben, ist die Option der Deaktivierung von WAF-Regeln von großem Vorteil. Obwohl unsere WAF so implementiert ist, dass sie ohne Ihr Eingreifen funktioniert und Sicherheit vor bekannten bösartigen Aktionen bietet, müssen Sie möglicherweise Regeln deaktivieren, die ihre spezifischen erwarteten Aktivitäten beeinträchtigen.

Zero Touch

Hier ist der Name tatsächlich Programm: Das System arbeitet völlig autonom, es ist keine Hilfe oder Überwachung von Ihrer Seite aus notwendig. Das System wird in kürzester Zeit eingerichtet und danach erfolgen alle Prozesse automatisiert. Das ist für Sie äußerst unkompliziert und schont wichtige Ressourcen.

Selbst die Sicherheitsupdates erfolgen ohne menschliches Zutun. Die Technologie aktualisiert sich nach der Veröffentlichung von Updates von selbst und ist somit immer auf dem neuesten Stand, um Sie vor Bedrohungen zu schützen. Sie können auf Wunsch die Aktualisierungen allerdings verzögern, wenn Sie das wünschen.

Zero Touch WAF mit DDoS-Schutz kombinieren

Cyberkriminelle können DDoS-Attacken als Ablenkungsmanöver nutzen, um sich beispielsweise Zugang zu Ihren persönlichen Daten zu verschaffen. Die Zero Touch WAF erkennt Angriffe auf Web-Applikationen wie SQLinjection, XSS und CSRF, sofern sie Teil der OWASP Top 10 sind, blockiert die bösartigen Anfragen und stellt so die Verfügbarkeit Ihrer Web-Ressourcen jederzeit sicher. Als optionales Add-on zu unserem DDoS-Schutz wird die Performance der WAF maximiert und die Sicherheit um eine zusätzliche Instanz erweitert.

- ✓ **Geringer Konfigurations- und Wartungsaufwand**
- ✓ **Integrierte und skalierbare Lösung**
- ✓ **Schutz vor den OWASP Top 10 Bedrohungen**
- ✓ **Zentrale Verwaltung aller Anwendungen (On-Premise und Cloud)**

Warum Sie sich auf Link11 verlassen können

Ständige Weiterentwicklung

Unsere Sicherheitslösungen entwickeln sich stetig weiter und passen sich immer an die Gegebenheiten des Marktes an. Neue Gefahren werden so schnell identifiziert und in das Regelset mit aufgenommen.

Langjährige Markterfahrung

Seit über 18 Jahren kümmern wir uns bereits um die Cybersicherheit von Kunden weltweit und haben dadurch wertvolle Erfahrungen sammeln können.

Automatisierte Lösungen

Unsere Sicherheitslösungen arbeiten alle automatisiert und benötigen keinerlei menschliche Interaktion, um Sie rund um die Uhr verlässlich zu schützen.

Unkomplizierte Implementierung

Mit Hilfe unserer Experten werden die Sicherheitslösungen für Sie unkompliziert und ohne großen Zeitaufwand in das bestehende Set-up implementiert.

24/7 Kundenservice

Unsere Experten stehen Ihnen rund um die Uhr mit Rat und Tat zur Seite. Wir nehmen uns so viel Zeit für Sie, wie Sie brauchen, in deutscher oder englischer Sprache.

LINK 11
WE PROTECT BETTER

API PROTECTION

- **Verbesserter Schutz für Ihre APIs**
- **Zuverlässige Erkennung von verdächtigen Aktivitäten**
- **Maximale Verfügbarkeit bei Angriffen**

Optimale Verfügbarkeit

Stellen Sie sicher, dass Ihre APIs immer verfügbar und reaktionsschnell sind, selbst bei hohem Datenverkehr oder starker Angriffslast.

Präzise Erkennung

Identifizieren und blockieren Sie automatisierte schädliche Aktivitäten, die auf Ihre APIs abzielen, um Ihre Daten und Dienste zu schützen.

Verbesserter Schutz

Schützen Sie Ihre APIs vor gängigen Web-Sicherheitsrisiken und lassen Sie keine Schwachstellen zu, die ausgenutzt werden könnten.

ALLE MÖGLICHKEITEN MIT EINER LÖSUNG

Viele Unternehmen erleben API-Angriffe in Regelmäßigkeit und viele davon hätten bei einer besseren Vorbereitung verhindert oder zumindest besser eingedämmt werden können. Mit unserer API Protection lösen Sie das Problem in kürzester Zeit und sorgen für eine maximale Verfügbarkeit Ihrer Services, ohne großen Implementationsaufwand.

91%

des Webverkehrs entfallen auf API-Verkehr

41%

der befragten Unternehmen gaben an, dass sie im Jahr 2022 einen API-Sicherheitsvorfall erlebt haben

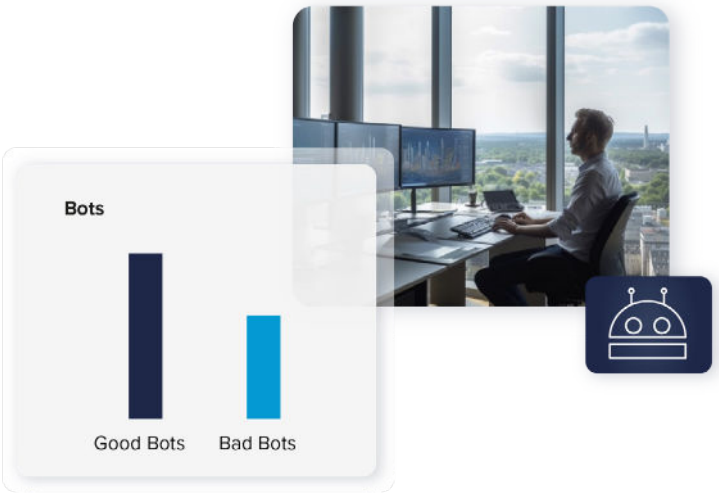
40%

der Befragten gaben an, dass Schatten APIs das größte Problem darstellen

DDoS Protection

Schützen Sie Ihre API-Endpunkte vor DDoS-Angriffen, die zu einer Unterbrechung der Dienste führen können, und sorgen Sie so für ununterbrochene Verfügbarkeit und Leistung.

Unser Schutzdienst ist so konzipiert, dass er selbst den aggressivsten DDoS-Angriffen standhält und die ununterbrochene Verfügbarkeit von APIs gewährleistet. Mit fortschrittlichen Verkehrsanalysen und Heuristiken sorgen wir für eine optimale Leistung selbst bei hoher Belastung. Unsere robuste Infrastruktur, zu der auch ein globales Content Delivery Network (CDN) gehört, verarbeitet eingehende Anfragen effizient und schützt Sie so vor Serviceunterbrechungen.



Bot Management

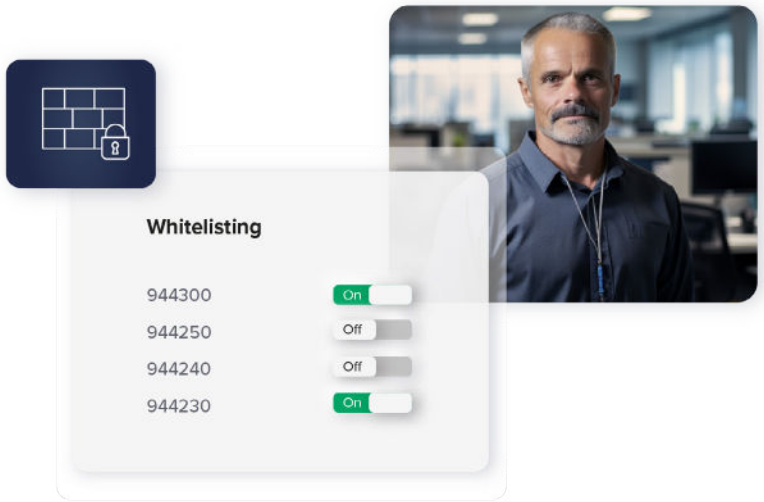
Identifizieren und verwalten Sie den automatisierten Bot-Verkehr zu Ihren APIs und unterscheiden Sie dabei zwischen guten und bösartigen Bots, um API-Ressourcen und Sicherheit zu optimieren.

Mithilfe ausgefeilter Bot-Erkennungs- und Verwaltungstechniken identifiziert und neutralisiert unser Bot-Management bösartigen Bot-Traffic in Echtzeit. Durch Verhaltensanalysen und Mustererkennung identifizieren und blockieren wir schädliche Bots, die versuchen, Schwachstellen auszunutzen. Dieser proaktive Ansatz garantiert die Sicherheit Ihres Datenverkehrs, den Schutz sensibler Daten und die Aufrechterhaltung der Integrität Ihrer Dienste.

Zero Touch WAF

Profitieren Sie von verlässlichen Schutz gegen die zehn kritischsten Schwachstellen der OWASP Top 10 und stärken Sie die Sicherheit Ihrer APIs gegen gängige Angriffsvektoren wie SQL-Injection, Cross-Site Scripting (XSS) und mehr.

Unser WAF-Service enthält eine umfassende OWASP Top 10 sowie von uns bereitgestellte Regelsätze, die vor gängigen Web-Sicherheitsbedrohungen wie SQL-Injection und Cross-Site Scripting (XSS) schützen. Durch kontinuierliche Überwachung und Anomalie-Analyse stellen wir sicher, dass Ihre APIs sowohl vor bekannten als auch vor neuen Angriffsvektoren geschützt sind.



Link11 GmbH
Lindleystraße 12
60314 Frankfurt am Main

www.link11.com