



# Product Brief

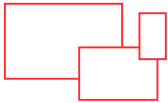
DevOps und die Cloud sind entscheidende Treiber unserer softwaregesteuerten Welt. Neue Apps und Services werden schneller denn je und in immer größerem Maßstab bereitgestellt. Für den Schutz dieser wachsenden und sich ständig verändernden Infrastruktur wird ein einheitlicher Ansatz benötigt.

## Fastly + Signal Sciences: Gemeinsam transformieren wir die Security-Landschaft

Um unseren Kunden ein noch solideres Angebot an Sicherheitslösungen für Webanwendungen und APIs bieten zu können, hat Fastly Ende 2020 Signal Sciences übernommen. Egal wie, wo und in welchem Maßstab Sie Ihre Anwendungen bereitstellen, wir können sie schützen. Unsere [Sicherheitsexperten](#) helfen Ihnen gerne, wenn Sie Ihr Nutzererlebnis durch eine führende Next-Gen Lösung sicherer gestalten möchten.

## Effektiverer Schutz für Ihre Anwendungen, APIs und Microservices

Signal Sciences bietet Schutz vor komplexen Web-Layer-Angriffen und lässt sich leicht in DevOps-Tools integrieren, damit Ihre Teams Sicherheitsdaten teilen können, wann und wie sie diese benötigen. So können Dev, Sec und Ops alle an einem Strang ziehen, um für erhöhten Schutz und gleichbleibende Zuverlässigkeit zu sorgen, ohne dabei Abstriche bei der Geschwindigkeit machen zu müssen. Mit flexiblen Bereitstellungsoptionen, höherem Schutz und Transparenz, die über die [OWASP-Top-10](#)-Angriffe hinausgehen, sowie erweiterten Integrationsmöglichkeiten in Ihre bestehenden Tools, lässt sich Signal Sciences problemlos in jeder Infrastruktur installieren und sorgt für eine kurze Time-to-Value ohne Regelanpassung.



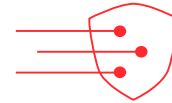
### Flexible Implementierung

Installieren Sie unsere Software auf Ihrem Webserver, in Ihrer Anwendung, Ihrem PaaS oder auf Ihrem Gateway – On-Prem oder in der Cloud.



### Fortschrittlicher Schutz vor Angriffen

Stoppen Sie OWASP Top 10-Angriffe, bösartige Bots, Account-Takeover-Versuche, DoS und Missbrauch von Anwendungen.



### Einfache Integration in DevOps-Tools

Erhalten Sie Warnmeldungen und wichtige Daten über genau die Tools, die Operations- und Entwicklerteams bereits im Einsatz haben.

Signal Sciences (jetzt Teil von Fastly) ist der einzige Anbieter, der für seine Web Application Firewall (WAF) drei Jahre in Folge mit dem Gartner Peer Insights Customers' Choice ausgezeichnet wurde und eine der am besten bewerteten WAF-Lösungen auf dem Markt (Gesamtbewertung: 4,9/5; Stand: 31. Januar 2021) bietet.

## Entscheidende Vorteile

- Über 90 % der Kunden nutzen unsere Lösung komplett im Blocking Mode
- Über 75.000 App-Bereitstellungen werden bereits geschützt
- Flexibel einsetzbar auf über 100 cloudnativen und Datacenter-Plattformen



### Transparenz

Detaillierte Einblicke in den Sicherheitsstatus

Benachrichtigen Sie Dev und Ops über Sicherheitsvorfälle, damit diese schnell behoben werden können. Unsere Sicherheitslösung ist für agile Teams konzipiert, die häufig Änderungen vornehmen. Mit intuitiven Dashboards und Workflow-Integrationen können alle Teams selbstständig auf relevante Daten und Sicherheitsinformationen zugreifen, um sich einen Überblick über den aktuellen Status zu verschaffen.



### Verbesserter Schutz

Verbringen Sie weniger Zeit mit Logging und mehr Zeit mit Blocking

Gehören auch Sie zu den mehr als 90 % unserer Kunden, die unsere WAF im Blocking Mode betreiben. So werden OWASP Top 10, aber auch Anwendungs-DoS bis hin zu Bots und Missbrauch abgewehrt. Ersparen Sie sich das Durchforsten von Logs oder die Feinabstimmung von Regex-Regeln, nur um Fehlalarme zu vermeiden. Verwenden Sie stattdessen die intuitive Nutzeroberfläche des Rule Builders, um Regeln für sämtliche Transaktionen Ihrer Web-Apps und APIs festzulegen, zu überwachen und entsprechende Maßnahmen zu ergreifen.



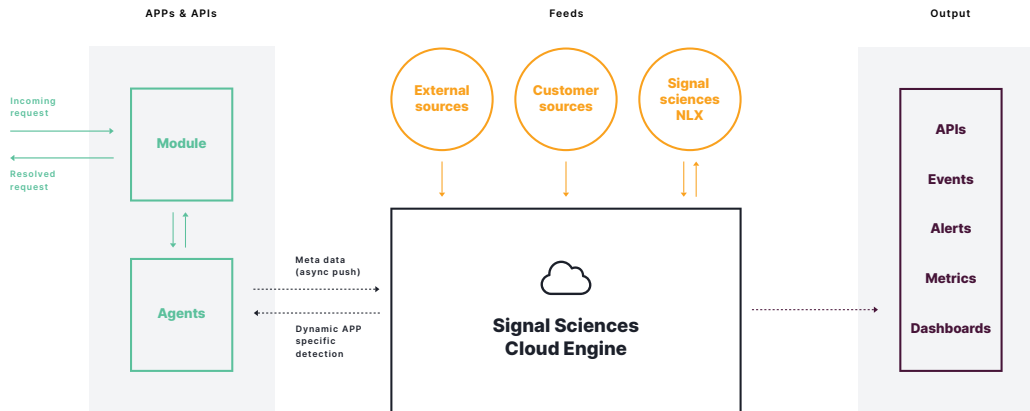
### Skalierbarkeit

Entdecken Sie ganz neue Möglichkeiten mit einer Next-Gen WAF

Finden und beheben Sie Schwachstellen schneller – durch App Monitoring vom Server über den Code bis hin zum Container. Unsere Next-Gen WAF und Runtime Application Self-Protection (RASP) lassen sich überall ausführen – mit niedriger TCO (Total Cost of Ownership), ohne Verwaltung von Signaturen und ohne spürbare Auswirkungen auf die Performance.

## • Unser patentierter Ansatz

Mithilfe von schlanken Softwaremodulen, sowie Agents auf Ihren Webservern und in Ihren Anwendungen sammeln wir Informationen über Ihren Sicherheitsstatus. Die Signal Sciences Cloud Engine liefert dabei Echtzeit-Informationen zu Sicherheitsvorfällen über Self-Service Dashboards sowie intelligente Warnmeldungen und leistungsstarke Berichte.



Unsere Bereitstellungsoptionen bieten Dev-, Sec- und Ops-Teams die nötige Flexibilität, um unsere Web-Defense-Technologie an verschiedenen Stellen in ihrem Stack zu installieren. Die Kommunikation mit der Signal Sciences Cloud Engine erfolgt asynchron und unabhängig von der gewählten Bereitstellungsoption. Außerdem lassen sich für komplexe Anwendungen, die von unterschiedlichen Teams verwaltet werden, mehrere Bereitstellungsoptionen nutzen.

Im Gegensatz zu vielen herkömmlichen WAFs, bei denen Sie sich in mehrere Tools einloggen müssen, um den Überblick zu behalten, liefert die einheitliche Managementkonsole von Signal Sciences im Handumdrehen umsetzbare Informationen und wichtige Sicherheitsdaten über eine einzige zentrale Oberfläche.

## Mehr als eine WAF

	Herkömmliche WAFs	Signal Sciences Next-Gen WAF
Bereitstellung	91 % werden im Logging oder Monitoring Mode betrieben oder aufgrund von Fehlalarmen (False Positives) sogar vollständig abgeschaltet <sup>1</sup>	Über 90 % der Kunden nutzen unsere Lösung komplett im Blocking Mode
Kompatibilität	Physikalische oder virtuelle Anwendung Wenig geeignet für die Nutzung in der Cloud  CDN Keine einheitliche Verwaltung verschiedener CDN-WAF-Produkte	Selbe Architektur und UI für eine einheitliche Verwaltung aller App-Bereitstellungen: Webserver, App-Server, PaaS, native, Hybrid- und Multi-Cloud-, On-Premise- und Serverless-Umgebungen sowie Container
Angriffstypen	Nur OWASP Top 10	OWASP-Top-10-, DoS-, Brute-Force-/ATO-Angriffe, App-Missbrauch, bösartige Bots
DevOps-Tauglichkeit	Fast ausschließlich von Sec-Teams genutzt; schlechte Toolchain-Integrationen	Vollständige Transparenz über Warnmeldungen für DevOps und Sec über Slack, Jira, Pagerduty, Splunk und Dutzende weitere Tools

<sup>1</sup> Ergebnisse einer von Fastly in Auftrag gegebenen Studie der Enterprise Strategy Group, Juni 2021

### Über Signal Sciences (jetzt Teil von Fastly)

Wir machen Webanwendungen sicherer. So einfach ist das. Wir bieten Webschutz, den Sicherheits-, Operations- und Entwicklerteams tatsächlich nutzen wollen.

Erfahren Sie mehr unter [signalsciences.com](https://signalsciences.com).