

Page Integrity Manager

Verbesserung der Webseitenintegrität durch Erkennung und Abwehr von verdächtigem Skriptverhalten



Moderne Webseiten verwenden in großem Umfang Skripte, die Angreifer als neuen Angriffsvektor nutzen, um vertrauliche Kundendaten zu stehlen. Aktuelle skriptbasierte Angriffe wie Magecart haben einen hohen Grad an Komplexität erreicht. Sie sind schwer zu erkennen und noch schwerer abzuwehren. Diese Web-Skimming-Angriffe konzentrieren sich zunehmend auf den Diebstahl von Kreditkarteninformationen und Kontoanmeldedaten. Sie schaden Ihrer Marke und gefährden Ihr Unternehmen, weil erhebliche Geldstrafen drohen.

Page Integrity Manager

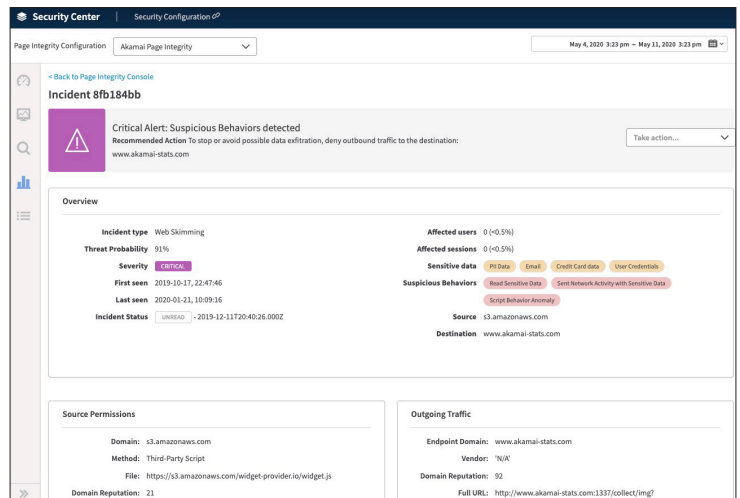
Der Page Integrity Manager von Akamai schützt Websites vor JavaScript-Bedrohungen wie Web Skimming, Formjacking und Magecart-Angriffen, indem er anfällige Ressourcen identifiziert, verdächtiges Verhalten erkennt und schädliche Aktivitäten blockiert. Durch die Erkennung von kompromittiertem JavaScript-Verhalten werden der Diebstahl von Nutzerdaten und die Beeinträchtigung des Nutzererlebnisses minimiert. Sofort umsetzbare Erkenntnisse versetzen Sicherheitsteams in die Lage, skriptbasierte Bedrohungen schnell zu verstehen und entsprechend zu reagieren.

Wie funktioniert das?

Page Integrity Manager wird im Browser des Nutzers ausgeführt und überwacht alle Skriptausführungen auf einer geschützten Seite. Wenn sich das Verhalten von Skripten ändert, werden Techniken des maschinellen Lernens eingesetzt, mit denen das Risiko nicht autorisierter oder unangemessener Aktionen bewertet wird. Bei Hochrisiko-Ereignissen werden Sicherheitsteams hinzugezogen und ausreichend Informationen zur Verfügung gestellt, um effektive Abwehrentscheidungen zu treffen.

Vorteile

- **Schützen Sie sich vor unerwünschtem Code**, der aus vielen kundenseitigen Quellen stammen und sowohl eigene als auch Drittanbieterskripte kompromittieren kann. Page Integrity Manager bietet genaue und gezielte Erkenntnisse, damit Sie kompromittierte Skripte schnell unschädlich machen und Richtlinieneinstellungen so aktualisieren können, dass Zero-Day-Angriffe und wiederkehrende Angriffe abgewehrt werden.
- **Erhalten Sie Einblicke in Schwachstellen und Skript-Angriffe**. Schädlicher Code bleibt oft Tage, Wochen oder sogar Monate lang unentdeckt, während weiterhin vertrauliche Nutzerdaten gestohlen werden. Page Integrity Manager bietet Ihnen unübertroffene Einblicke in die toten Winkel Ihrer Webseiten, sowohl für Ihre eigenen Skripte als auch für Drittanbieterskripte, von denen Sie vielleicht gar nicht wissen.



Page Integrity Manager bietet umsetzbare Warnungen in Echtzeit zu verdächtigem Verhalten mit echten Nutzerdaten.

Page Integrity Manager

Stärkung der Webseitenintegrität durch Erkennung und Abwehr von verdächtigem Skriptverhalten

- **Einfachere Bereitstellung und Verwaltung.** Page Integrity Manager wird innerhalb von Minuten bereitgestellt und beginnt sofort mit der Analyse des Skriptverhaltens. Wenn fragwürdiges Verhalten erkannt wird, erhalten Sie sofort eine Benachrichtigung zu kritischen Warnungen und können den Angriff mit einem einzigen Klick abwehren.

Wichtige Funktionen

- **Verfahren zur Verhaltenserkennung** – Die effektivste Methode zur Abwehr von Angriffen in Browsern ist das Erkennen von verdächtigem und schädlichem Skriptverhalten. Page Integrity Manager nutzt Sitzungen echter Nutzer zur Überwachung des Skriptverhaltens in Echtzeit, einschließlich Quelle, Ausführungsverhalten und aller ausgehender Netzwerkziele.
- **Priorisierte Warnungen in Echtzeit** – Die verhaltensbezogene Heuristik weist jedem Skript Risikobewertungen zu, die auf Faktoren wie Anzahl der betroffenen Nutzer, Daten, auf die zugegriffen wurde, und Exportzielen basieren. Page Integrity Manager gibt dann Warnungen in Echtzeit aus. Dabei werden Ereignisse mit dem höchsten Risiko priorisiert und detaillierte Informationen zur Verfügung gestellt, die zur Abwehr erforderlich sind.
- **Intuitive Dashboards und Berichte** – Dashboards bieten einen intuitiven Einblick in jedes Skript, das auf Ihren Webseiten ausgeführt wird. So erhalten Sicherheitsteams einen Überblick über alle wichtigen Details wie Skriptkategorien und -anzahl sowie Vorfallstypen und -anzahl. Berichte enthalten Zusammenfassungen von Vorfällen, Richtlinienverletzungen und CVE-Erkennung.
- **Richtlinienverwaltung** – Überwachen Sie das Skriptverhalten und steuern Sie die Laufzeit der JavaScript-Ausführung durch die Erstellung von Richtlinien für das Skriptverhalten. So können Sie den Zugriff auf Cookies, Netzwerkziele, lokale Speicher oder vertrauliche Dateneingaben nach Ursprungsdomäne überwachen und/oder einschränken.
- **Erkennung von Schwachstellen** – Analysieren Sie kontinuierlich eigene und Drittanbieter-URLs auf häufige Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVE). So lassen sich riskante Skriptquellen identifizieren, die entweder mit böartigem Skriptverhalten in Bezug gesetzt oder mit einer einzigen Schaltfläche blockiert werden können.
- **Flexible Bereitstellungsoptionen** – Page Integrity Manager bietet Bereitstellungsmodelle für Edge- und Ursprungs-Injection, sodass alle Websites geschützt sind – auch solche, die sich nicht auf der Akamai-Plattform befinden. Aktivieren Sie Page Integrity Manager an der Edge für eine schnelle und nahtlose Bereitstellung, ohne dass Anwendungsänderungen erforderlich sind.

Weitere Informationen erhalten Sie [auf dieser Seite](#) oder vom Vertriebsteam von Akamai.



Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter [@Akamai](https://twitter.com/Akamai). Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: Mai 2020