Page Integrity Manager Beta
Protect your website from Magecart and other in-browser threats

Modern web applications are heavily reliant on external code, services and vendors, executing JavaScript code in the browser. Those scripts come from a myriad of sources, massively increase the attack surface and resulting risk for website operators, with no practical way for website operators to detect and mitigate. Injecting malicious code into web pages via first, third, and fourth party JavaScripts is an increasingly popular attack surface for credit card and credential skimming. Currently, detection of third party JavaScript vulnerabilities and threats, is outside of common security visibility. This leaves web protectors susceptible and blind to attacks on their real users.

Introducing Akamai Page Integrity Manager

Akamai Page Integrity Manager is a real-user behavioral detection technology for web apps that catalogs JavaScript resources, and identifies suspicious and malicious script behaviors. Seeing unexpected behavior is critical to prevent credit card-skimming by first, and third-party scripts and can be deployed and operated immediately without requiring impactful changes.

Akamai Page Integrity Manager is a detection-first solution that revolutionizes current Content Security Policy approaches by detecting changed, malicious, and compromised JavaScript resources that could be used to steal user data or defacing the user experience. Page integrity Manager then notifies security teams with actionable insight, empowering them to rapidly understand, and act on the threats.

Attacks Using First and Third-party Scripts Are Accelerating

Significant, persistent and effective attack activity within the browser increased throughout 2019 via malicious JavaScript code, there have been meaningful data breaches and substantial fines for privacy regulation violations. Most notably are form-jacking attacks, such as Magecart, that steal credit card, user credential, or personally identifiable information via malicious or compromised Javascript resources. These attacks damage brand and subject companies to substantial fines to web operators who suffer from such breaches e.g., British Airways, Macy’s and Newegg. Form-jacking attacks will continue to evolve and will require flexible and comprehensive solutions.

More than 57% of website client-side code consists an external scripts*

Compromised or outright malicious scripts are an active attack vector allowing threat actors to steal customer PII, credentials, payment information resulting in regulatory violations, eroding user trust, and negatively affecting brand perception.
Page Integrity Manager Beta

How does this work:

Akamai Page Integrity Manager is designed to discover and assess the risk of new or modified JavaScript, control third-party access to sensitive forms or data fields and enable automated mitigation. The solution fully monitors the behavior of each JavaScript workload in the session, through a series of detection layer, using machine learning model, heuristics, signatures and risk score model. This advanced approach identifies suspicious and malicious behavior, enable automated mitigation using policy-based controls, and block bad actors using Akamai threat intelligence to improve accuracy.

Capabilities

- Behavioral detection technology: constantly analyses the behavior of script execution, in real-user sessions, to identify suspicious, or outright malicious behavior and notify security teams with timely and actionable insights.
- Outgoing network monitoring and script Intelligence: monitor network requests and know what real-users are downloading and executing when they interact with your brand to detect potential malicious threats.
- CVEs detection: continuously check all web resources, seen on the web application against open Common Vulnerabilities and Exposures database, to identify existing known vulnerabilities in runtime Javascript code.
- Edge Injection for rapid enablement: Page Integrity Manager is injected at the CDN level, easy to deploy, no code needed.
- Policy management: control your runtime Javascript execution by optionally craft policies that monitor and/or restrict access to cookies, network destinations, local storage, sensitive data inputs, or DOM events per originating domains.

BENEFITS TO YOUR BUSINESS:

- Unmatched visibility into your web assets’ blind-spots.
- Protect your web application from Magecart and other zero-days and tailored client-side attacks.
- Get notified immediately on data breaches and suspicious activity.
- Easily mitigate attacks surfacing in browsers.
- From initial install through constant change, Page Integrity is always on, always in the right location, always protecting.

Over 80% of pages contain at least one known third-party library security vulnerability (Common Vulnerabilities and Exposures (CVE))

Akamai will be launching Page Integrity Manager in 2020, but we are inviting customers to participate in a valuable beta project with a working product to help you be protected from malicious scripts.

Join our beta program today by contacting your Akamai sales team.

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 12/19.