Page Integrity Manager

Strengthening web page integrity by detecting and mitigating suspicious script behaviors

With modern web pages relying heavily on scripts, bad actors are exploiting scripts as a new attack vector to steal sensitive customer information. Recent script-based attacks such as Magecart have increased in sophistication and are difficult to detect, let alone stop. Increasingly, these web-skimming attacks focus on stealing credit card information and account credentials, damaging your brand and subjecting your organization to substantial fines.

Page Integrity Manager

Akamai's Page Integrity Manager protects websites from JavaScript threats – such as web skimming, formjacking, and Magecart attacks – by identifying vulnerable resources, detecting suspicious behavior, and blocking malicious activity. By detecting compromised JavaScript behavior, it minimizes user data theft and defacing of the user experience. Immediate, actionable insights empower security teams to rapidly understand and act on script-based threats.

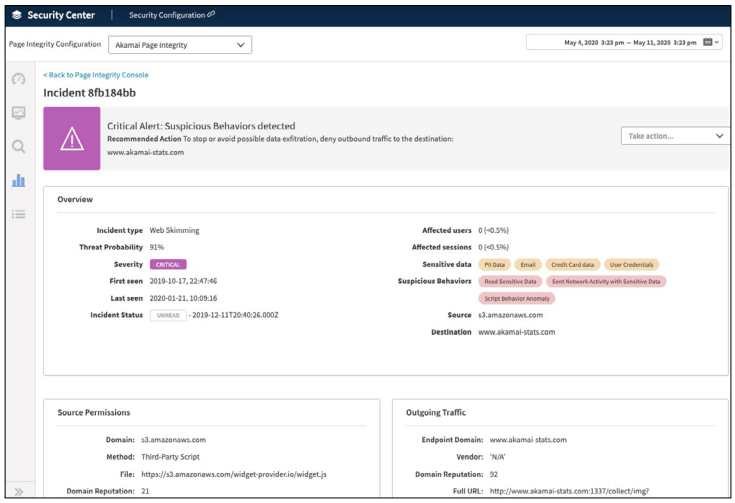
How Does It Work?

Page Integrity Manager runs in the user's browser to monitor all script executions for a protected page. When scripts exhibit changes in behaviors, machine learning techniques are employed to assess risk of unauthorized or inappropriate action. High-risk events alert security teams with sufficient information to make effective mitigation decisions.

Benefits

- **Get protection from malicious code** that can come from many client-side sources and compromise both first- and third-party scripts. Page Integrity Manager provides specific, targeted insight so that you can quickly mitigate compromised scripts and update policy controls to stop both zero-day and recurring attacks.

- **Gain visibility** into vulnerabilities and script attacks. Harmful code can go undetected for days, weeks, or even months while continuing to steal sensitive user information. Page Integrity Manager provides unmatched visibility into your web page blind spots for your own scripts as well as third-party scripts you might not even know about.



Page Integrity Manager provides real-time, actionable alerts of suspicious behavior using real user data.

Page Integrity Manager

Strengthening web page integrity by detecting and mitigating suspicious script behaviors

- **Simplify deployment and administration.** Page Integrity Manager deploys in minutes and immediately starts analyzing script behavior. When questionable behavior is detected, you get immediate, critical alert notifications that can be mitigated with a single click.

Key Capabilities

- **Behavioral detection technology** – Detecting suspicious and malicious script behavior is the most effective way to mitigate in-browser attacks. Page Integrity Manager instruments real-user sessions to monitor script behavior in real time, including the source, execution behavior, and any outgoing network destinations.

- **Prioritized real-time alerting** – Behavioral heuristics assign risk scores for every script based on factors such as the number of users affected, data accessed, and export destinations. Page Integrity Manager then provides real-time alerting to prioritize the highest-risk events with detailed information needed to mitigate.

- **Intuitive dashboards and reports** – Dashboards offer an intuitive view into every script running on your web pages to provide security teams with details at a glance, including script categories and counts, and incident types and counts. Reports show incident, policy violation, and CVE detection summaries.

- **Policy management** – Govern script behavior and control runtime JavaScript execution by creating script behavior policies that monitor and/or restrict access to cookies, network destinations, local storage, or sensitive data inputs per originating domains.

- **Vulnerability detection** – Continuously analyze first- and third-party URLs for Common Vulnerabilities and Exposures (CVE) to identify risky script sources that can be either correlated with malicious script behavior or blocked outright with a single button.

- **Flexible deployment options** – Page Integrity Manager offers both edge and origin injection deployment models to protect every website, including those not on the Akamai platform. Enable Page Integrity Manager at the edge for fast and seamless deployment without requiring application changes.

To learn more, visit this page or contact your Akamai sales team.