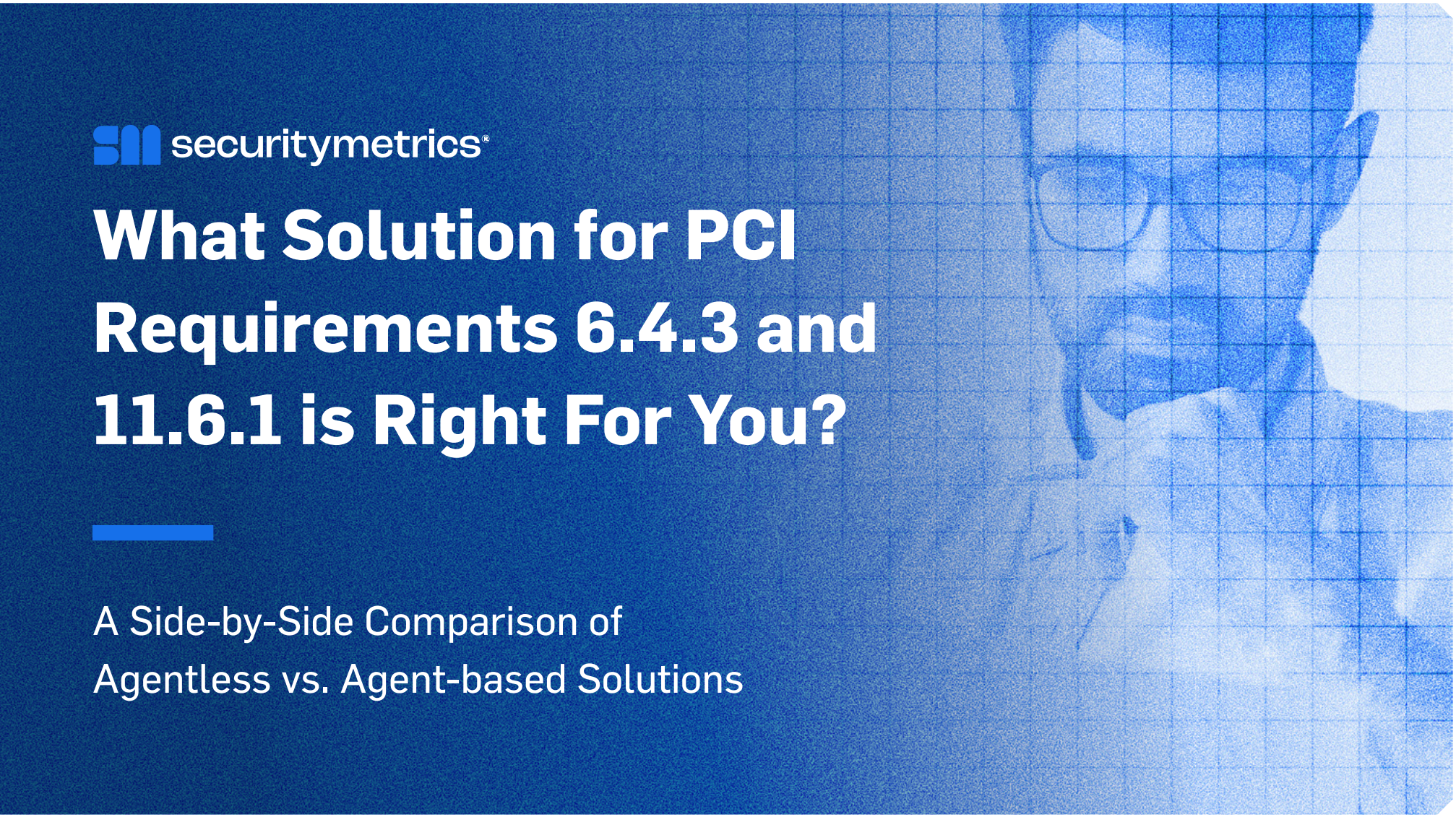
securitymetrics®

What Solution for PCI Requirements 6.4.3 and 11.6.1 is Right For You?



A Side-by-Side Comparison of Agentless vs. Agent-based Solutions

© 2025 SecurityMetrics

Ecommerce Websites Are Under Attack

As countless new ecommerce websites pop up each day, the number of cyber attacks is also massively on the rise. Hackers no longer only attack servers; they are injecting malicious Javascript (e.g., Magecart, eskimming attacks) directly into a checkout page to steal credit card data from customers in real time without businesses even being aware that it's happening.

To combat this, the PCI Council introduced two new critical requirements:

- PCI requirement 6.4.3: Maintain an inventory for all payment page scripts, with justification on why each one is needed
- PCI requirement 11.6.1: Tamper-detection mechanism for HTTP headers and payment page content as received by the consumer browser.

The Challenge: How do you meet these requirements without disrupting your website performance and user experience?

Contents

Ecommerce Websites Are Under Attack ____ 2

The Agent-Based Solution ____ 3

The Agentless Solution ____ 4

Side-by-Side Comparison ____ 5

Agentless: the Superior Choice for PCI v4 ____ 5

Shopping Cart Monitor from SecurityMetrics ____ 6



Option 1:

The Agent-Based Solution

An agent-based solution involves injecting a piece of code (e.g., JavaScript or "Agent") directly into the header of your payment pages. It sits between your customer and your shop.

The primary selling point of an agent is **real-time detection**. If an attack happens, the agent may stop it instantly.

However, the reality of an agent is a double-edged sword.

Agent solutions often require businesses to make complex, ongoing adjustments and updates to their checkout pages and Content Security Policy (CSP) to ensure the agent plays nice with existing code. This leads to huge dev involvement and creates ongoing **IT management nightmares** with constant maintenance and redeployment needs.

And because the agent is code installed on the browser, it's **completely visible to hackers**. If they can see it, they can study it. And if they can study it, they can bypass it.

The Hidden Costs of Agents

- **False Positives:** While agentless solutions cannot block active attacks in real-time, the agent's ability to do so introduces a critical business risk of getting false positives.
  - If the agent misidentifies a legitimate marketing script or analytics tool as a threat, it blocks it, which leads to broken checkout pages, failed transactions, and lost revenue.

Option 2:

The Agentless Solution

An agentless solution approaches the problem from a completely different mindset. It doesn't reside on the customer's browser at all. Instead, it scans and monitors the payment environment from the outside, replicating user behavior to detect changes.

The Stealth Advantage

- **Zero Footprint:** Because there is no code injected into the user's browser, the solution is invisible to threat actors.
- **Un-bypassable:** Hackers have no idea they are being watched. They can't reverse-engineer a defense mechanism they can't find, and they can't tamper with it in any way.

Zero-Friction Installation

- **Agentless:** Simply enter your website's domain. There's no code to inject, no developer involvement required, and onboarding is instant.
- **Agent-Based:** Requires you to get developers involved to install code at the top of each of your payment page headers.

Revenue Safety

Agentless solutions detect and alert rather than auto-block scripts. You never risk accidentally blocking a legitimate customer or a critical sales tool. You maintain 100% uptime and revenue flow while maintaining complete situational awareness of your shopping cart experience.



Side-by-Side Comparison

Feature	Agent-Based Solution	Agentless Solution
Installation	**Complex:** Code injection required on all payment headers.	**Simple:** Just enter the URL.
Visibility to Hackers	**High:** Visible in the DOM, vulnerable to subversion and bypass.	**None:** Completely invisible footprint, tamper-proof.
Scope Limitations	**Limited:** Can only see what a single javascript can see within its own context.	**Unlimited:** Can see many additional elements beyond a single javascript
IT Maintenance	**High Maintenance:** Requires constant IT management, adjustment of CSP, and regular testing.	**None:** No testing necessary, zero internal changes or management required.
Actions & Process	**Active Blocking:** Runs exhaustively, risks breaking valid scripts and checkouts.	**Monitoring:** Runs at desired frequency, sends alerts without breaking the site.
Performance Impact	**Variable:** Can slow down page load times.	**None:** Zero performance issues, no code runs on the client's website.

Agentless: the Superior Choice for PCI v4

While agent-based solutions offer the allure of immediate blocking, the operational risks (e.g., breaking payment pages, high maintenance, visibility to attackers) often outweigh the benefits.

Secure your checkout without slowing it down.



Shopping Cart Monitor from SecurityMetrics

SecurityMetrics launched its agentless solution to meet PCI requirements 6.4.3 and 11.6.1 called **Shopping Cart Monitor**.

Shopping Cart Monitor doesn't require software downloads or configuration, instead, only a URL is needed to get started. For organizations that rely on transactions from their ecommerce website, this tool improves security without being subverted. It gives merchants a complete picture of what's happening behind the scenes, so their customers don't have their personal information stolen.

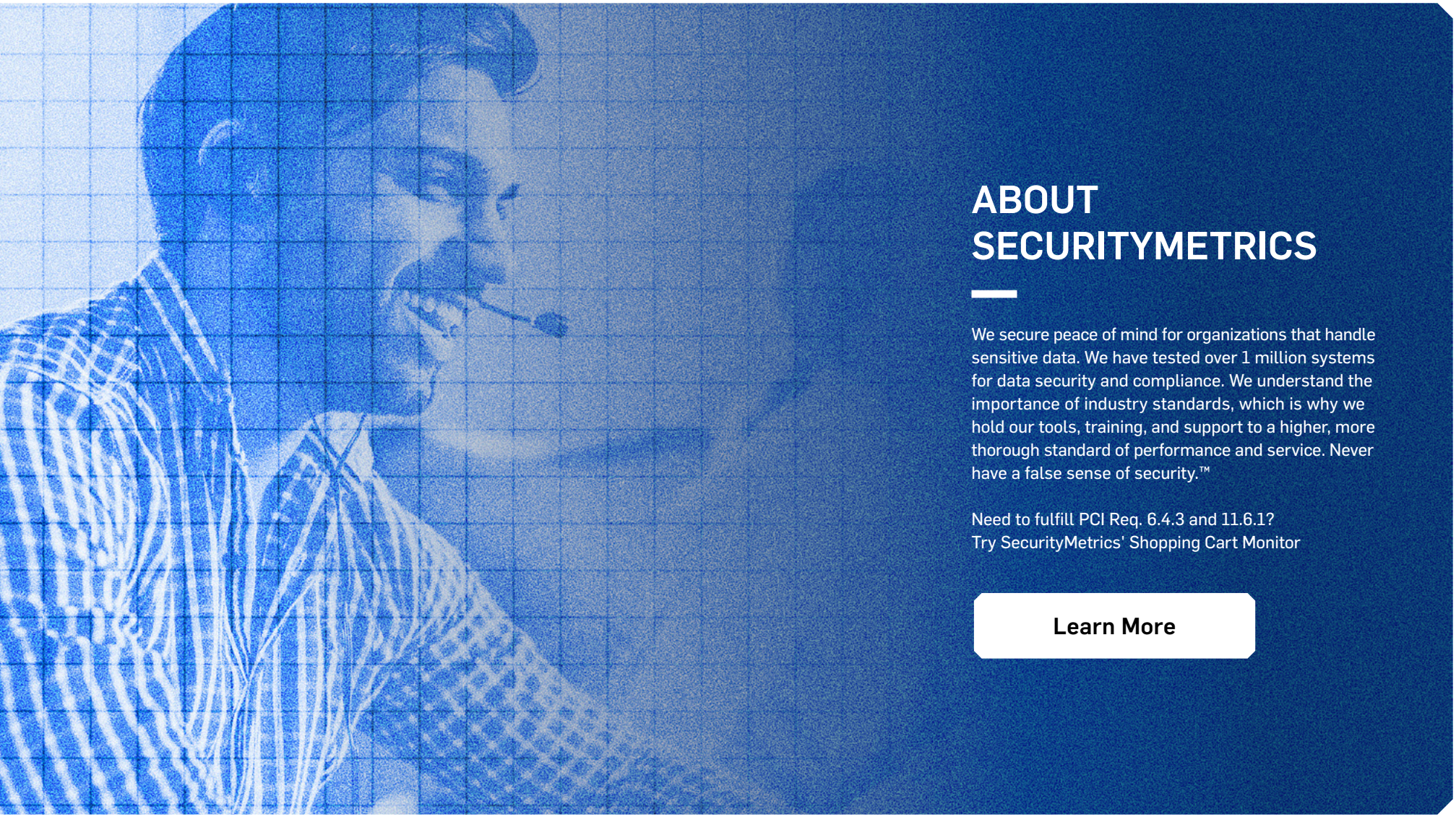
For users looking to avoid a complex installation, this cloud-based product provides a seamless setup for PCI compliance and ecommerce security.

SecurityMetrics has been actively developing and updating this technology since 2019, ensuring that advances in cyberattacks are matched by advances in Shopping Cart Monitor's technology like their **patented-Web Integrity Monitoring**.

For businesses looking for even more website protection, SecurityMetrics offers different packages that each meet requirements 6.4.3 and 11.6.1 to ensure every organization can achieve ecommerce security and PCI Compliance, no matter the size.

Shopping Cart Monitor offers unique, watchful protection against eskimming and takes the pressure off organizations to navigate ecommerce-focused PCI requirements, all at a cost-effective price.

To learn more about Shopping Cart Monitor and get started, **visit our website** and secure your business and your customers' personal information today.



ABOUT SECURITYMETRICS

We secure peace of mind for organizations that handle sensitive data. We have tested over 1 million systems for data security and compliance. We understand the importance of industry standards, which is why we hold our tools, training, and support to a higher, more thorough standard of performance and service. Never have a false sense of security.™

Need to fulfill PCI Req. 6.4.3 and 11.6.1?
Try SecurityMetrics' Shopping Cart Monitor

Learn More