APPLICATION SECURITY

# Protect Client-Side Scripts & Meet PCI DSS 4.0 Compliance

Stop online skimming, protect cardholder data, & demonstrate PCI-DSS 4.0 compliance with a joint solution

## Client-side script attacks are prevalent

Protecting customer data and payment information from threats like skimming and fraud is critical. Businesses using AWS infrastructure rely on client-side scripts in end-user browsers and apps to enhance e-commerce experiences. However, these scripts are often targeted by cybercriminals, putting cardholder data at risk Some of these risks include:

- **Skimming attacks** – Cybercriminals steal payment details from compromised scripts.
- **Fraud exploitation** – Malicious actors manipulate scripts to intercept sensitive information.
- **Data exposure** – Unsecured scripts can leave customer cardholder data vulnerable.

## Meet new PCI DSS 4.0 compliance mandates

Starting **Q1 2025**, **PCI DSS 4.0** mandates stricter client-side security:

- **Requirement 6.4.3**: Scripts must be documented, tested, reviewed, and approved with justification.
- **Requirement 11.6.1**: Scripts must be monitored for tampering and malicious activity.

The challenge? Finding a cost-effective, easily integrated solution.

## Joint solution: DataDome Page Protect & AWS WAF

Page Protect is a turnkey security solution from DataDome, available on AWS Marketplace and integrated with AWS WAF. It automates client-side protections, securing scripts across all domains while ensuring PCI DSS 4.0 compliance—without added complexity or extra tools. Designed for seamless AWS integration, it helps businesses save time, reduce costs, and enhance security.

In collaboration with

DataDome

## DataDome on AWS key benefits

- <0.01% false positive rate
- Scales protection resources by 200 times (or more) in 90 seconds
- Analyzes 5 trillion data signals per day
- 30+ worldwide PoPs
- Zero latency
- Stops 350+ billion attacks annually

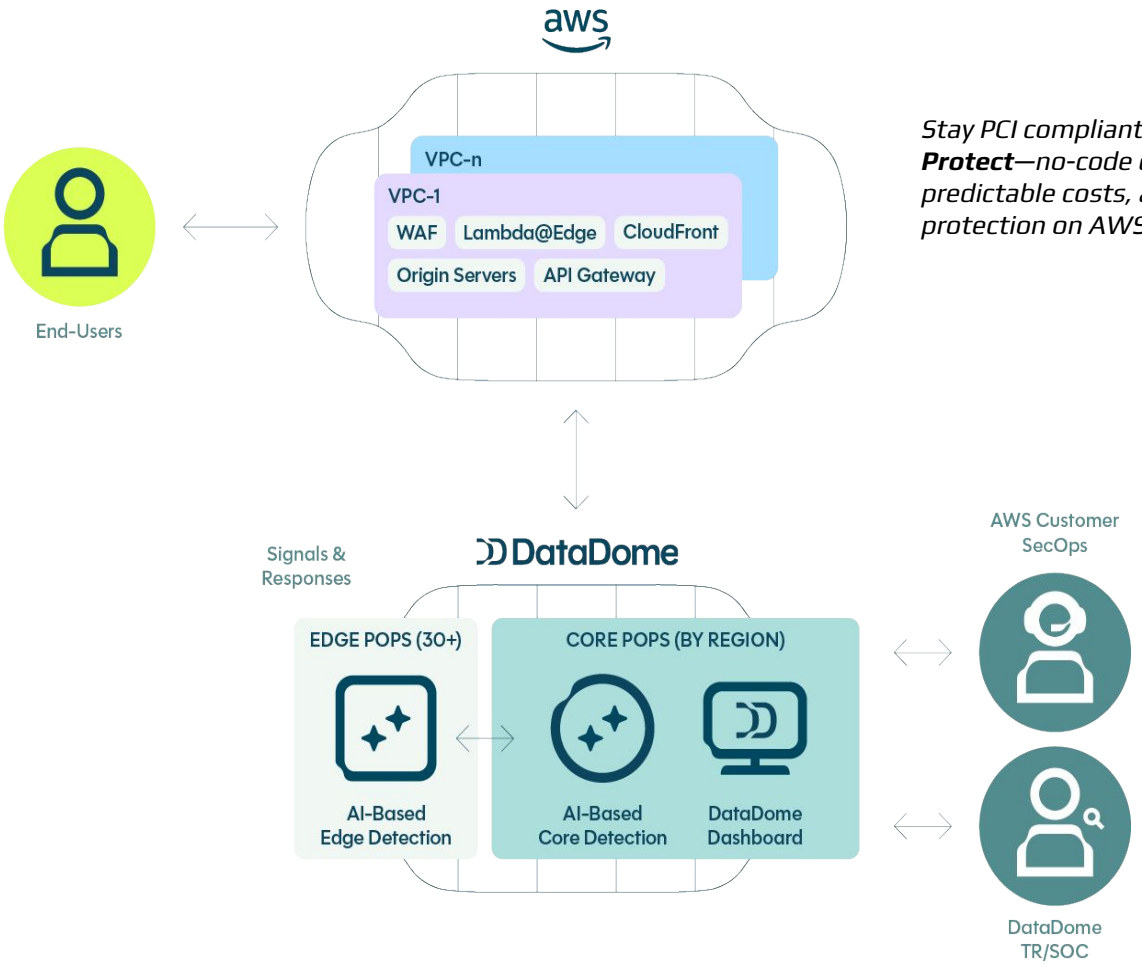
aws PARTNER

- AWS WAF Ready
- Amazon CloudFront Ready
- Retail Software Competency
- Security Software Competency
- Consumer Goods Software Competency
- Travel & Hospitality Software Competency
- Media & Entertainment Software Competency

FORRESTER WAVE LEADER 2024 Bot Management Software

G2 Top 50 Security Products BEST SOFTWARE AWARDS 2024

## DataDome x AWS architecture & workflow




*Stay PCI compliant with **Page Protect**—no-code deployment, predictable costs, and fast bot protection on AWS.*

## The power of Page Protect & AWS WAF

**Meet PCI DSS 4.0 compliance**
Get a turnkey solution to address PCI DSS 4.0 client-side requirements 6.4.3 & 11.6.1.

**Safeguard brand reputation**
Limit the impact of fraud to ensure a trusted user experience, protect your brand, and reduce financial penalties.

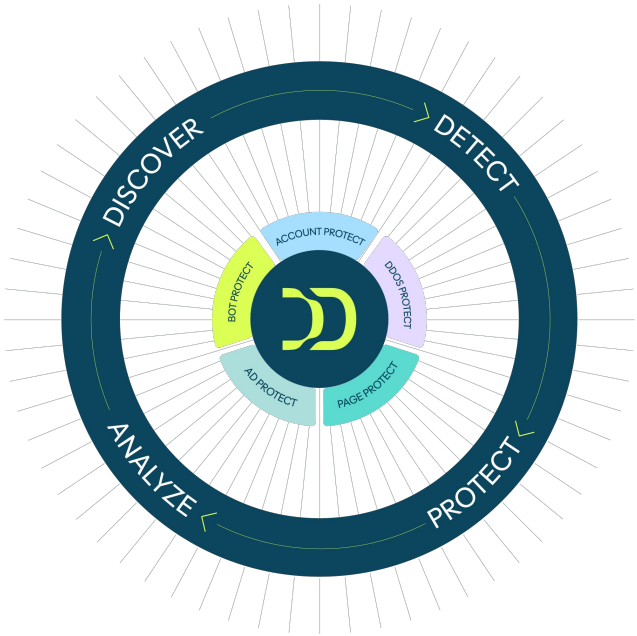
**Protect cardholder data**
Safeguard payment & personal information from theft and exfiltration.

**Streamline operations**
Ease resource constraints with automation, visibility, and on-demand reporting.

## How Page Protect works with AWS WAF

Enjoy seamless integration to secure cardholder data, address client-side PCI DSS 4.0 compliance, & increase operational efficiency.

Page Protect can be easily provisioned from the AWS WAF console. Unlike alternatives, users deploy without having to add new code to their payment pages and applications. As a result, users can secure their cardholder data from skimming, theft, and fraud while simplifying compliance. Seamlessly integrating into existing AWS infrastructure, it provides dashboard visibility, continuous monitoring, and one-click reporting to meet PCI DSS 4.0 requirements 6.4.3 and 11.6.1.




*DataDome Cyberfraud Protection Platform*

## Key benefits:

- **Seamless integration with AWS WAF:** Deploy protection directly from the AWS console for your websites and apps.
- **Continuous discovery & automation**: Automates inventory & simplifies documentation of client-side scripts. Tracks script activity, enabling rapid detection and response to threats.
- **Streamline script authorization & policy management:** Dashboard-level script visibility and approval with automated code generation of web page content security policy (CSP) updates.
- **On-demand reporting:** Streamlines PCI DSS compliance audits with detailed client-side script reports.
- **Integrity assurance:** Safeguards authorized scripts, flagging unauthorized changes and indicators of compromise (IoCs).

**Get your free Bot Vulnerability Assessment**

**Find DataDome in AWS Marketplace**

### About DataDome

DataDome protects businesses from cyberfraud and bots in real time, securing websites, mobile apps, ads, and APIs. Named a Leader in The Forrester Wave™ Bot Management 2024, DataDome is trusted by leading brands like Tripadvisor, Zocdoc, and SoundCloud. Its AI-powered Cyberfraud Protection Platform processes 5 trillion signals daily—without compromising performance. Backed by DataDome Advanced Threat Research, the platform stays ahead of emerging threats and autonomously stops over 350 billion attacks annually. With 50+ integrations, 30+ global PoPs, and 24/7 SOC coverage, DataDome has record-fast time to value. Recognized as a G2 Leader and one of G2's Best Security Products of 2024, DataDome delivers protection that outperforms.