

Europe
Community Meeting

EDINBURGH | 2026



Closing the PCI DSS v4.0.1 Gap

Continuous Visibility at the Digital Experience Layer

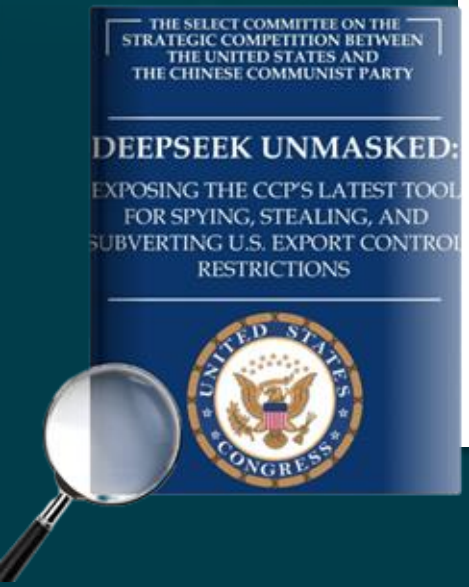
Mark Gillard

VP, Partner Alliances & Customer Success
Feroot Security



About Feroot











Feroot cited in a U.S. Congress report exposing DeepSeek's link to the Chinese Communist Party, raising concerns about potential foreign access to Americans' private information.

Moreover, cybersecurity researchers at Feroot Security uncovered hardcoded links in DeepSeek's web login page that directly connect it to China Mobile,[17] a state-owned telecommunications company also designated as a Chinese military company by the U.S. Department of Defense, as mentioned.[18] China Mobile is explicitly tasked by the CCP with supporting China's broader information control and intelligence objectives.[19] While the extent of data transmission remains unconfirmed, DeepSeek's integration with China Mobile infrastructure raises serious concerns about potential foreign access to Americans' private information.



20 YEARS OF SECURING PAYMENT DATA

The Digital Experience Has Changed



PCI DSS Changed Because the Browser Changed

The browser has become part of the payment environment.

Today's checkout pages routinely execute dozens of third-party and first-party scripts that:

- Collect payment information
- Modify page behavior
- Load additional resources
- Introduce new supply chain risk

Protecting servers alone is no longer enough.

20 YEARS OF SECURING PAYMENT DATA

The Challenge Isn't Understanding the Requirements

It's Keeping Up With **Constant Change**

Modern payment pages change continuously.

- Marketing tags
- Analytics tools
- A/B testing
- Chat widgets
- Fraud tools
- Third-party updates
- AI-powered website changes

Every change introduces new compliance and security questions.

20 YEARS OF SECURING PAYMENT DATA

CENSUSWIDE
THE SURVEY CONSULTANTS

Organizations Are Still Struggling

97% plan to evaluate additional privacy and compliance automation

64% of client-side privacy work is still performed manually

50% have experienced a regulatory inquiry related to website privacy or tracking

89% have discovered third-party technologies changing behavior without notice

The problem isn't awareness. It's maintaining continuous visibility.

20 YEARS OF SECURING PAYMENT DATA

Why Manual Compliance No Longer Works



20 YEARS OF SECURING PAYMENT DATA

Manual Monitoring Doesn't Scale

The digital experience changes every day.

Manual reviews can tell you:

✓ What existed yesterday

They cannot tell you:

✕ What changed five minutes ago

✕ Whether new scripts appeared

✕ Whether existing scripts changed behavior

✕ Whether controls remain enforced continuously

20 YEARS OF SECURING PAYMENT DATA
PCI

THE EVOLUTION OF AI-ASSISTED SECURITY & COMPLIANCE

THE AUTOCOMPLETE (Level 1)



AI serves as a reference tool or enhanced search. Humans use AI for specific answers, citations and research.

THE INTERN (Level 2)



AI writes boilerplate or low-risk reports. The privacy person prompts for specific functions, then immediately reviews and integrates output.

JUNIOR PROFESSIONAL (Level 3)



Interactive pair-assessments. Human and AI trade off control while results and conclusions are reviewed as they are generated in real time.

THE PRO (Level 4)



AI generates most of the compliance assessments. The privacy person reviews everything AI does and becomes the verification bottleneck.

SENIOR PROFESSIONAL (Level 5)



AI runs unattended for longer periods, handles complex tasks, and relies on self-checks. Humans verify final results later.

"FSD" COMPLIANCE FACTORY (Level 6)



Privacy people manage goals and constraints, not software. AI defines implementation, performs discovery, runs tests, writes reports, fixes gaps, enforces policies, and ships.

AI Is Accelerating Website Change

AI isn't just creating code.

It's creating more change.

Organizations are increasingly using AI to:

- Generate website code
- Deploy new experiences
- Personalize content
- Introduce new third-party integrations
- Build AI agents into customer journeys

The pace of change now exceeds what humans can realistically monitor manually.

20 YEARS OF SECURING PAYMENT DATA
PCI

PCI DSS v4.0.1 Raised the Bar

The standard now expects organizations to understand and monitor what executes inside the browser.

The focus is no longer simply:

> "Was the page secure?"

It's now:

> "Can you continuously demonstrate that only authorized code is executing?"

20 YEARS OF SECURING PAYMENT DATA

Understanding PCI DSS v4.0.1



Two Requirements Changed Everything

Requirement 6.4.3

Maintain an inventory of payment page scripts and ensure their integrity and authorization.

Requirement 11.6.1

Detect unauthorized changes to payment pages and respond appropriately.

These requirements introduce continuous operational responsibility—not one-time validation.

20 YEARS OF SECURING PAYMENT DATA

The Compliance Gap

Many organizations believe they're compliant because they:

- ✓ Performed a script inventory
- ✓ Completed an assessment
- ✓ Documented controls

But...

- New scripts appear
- Existing scripts change
- Vendors update code
- Configurations drift

20 YEARS OF SECURING PAYMENT DATA

Continuous Compliance Requires Continuous Visibility

Think of payment pages like cloud infrastructure.

Nobody scans cloud environments once a year.

Nobody checks endpoint security quarterly.

Payment pages deserve the same continuous monitoring approach.

Compliance can disappear without anyone noticing.

20 YEARS OF SECURING PAYMENT DATA
PCI

Continuous Visibility in Action



This Is a Job Built for Automation

Automation continuously:

- Discovers every script
- Detects behavior changes
- identifies unauthorized code
- Validates policy enforcement
- Produces audit-ready evidence
- Alerts on new risk

Humans investigate.

Machines monitor.

20 YEARS OF SECURING PAYMENT DATA
PCI

B2B | LARGE-SCALE PAYMENT PROCESSOR

PCI Compliance at Scale

CHALLENGE

Managing PCI requirements across a complex, growing payment ecosystem.

NEEDED

Simple, centralized oversight across 100+ payment pages.

PAYMENTGUARD

One script tag. One pane of glass.
Seamless PCI compliance.

100+ Payment Pages | 1 Script Tag | 3-Year Renewal



B2C | LARGE CONSUMER PLATFORM

Beyond the PCI Checkbox

CHALLENGE

Protecting high-volume payment pages with complete visibility.

NEEDED

Deeper context into what's happening across every payment page.

PAYMENTGUARD

Continuous monitoring with actionable, security-grade insight.

43 Payment Pages | 250K+ Daily Visitors | 20K Payments/Day



What Continuous Monitoring Looks Like

Continuous visibility includes:

- Real-time script inventory
- Behavior monitoring
- Change detection
- Authorization validation
- Evidence collection
- Historical reporting

Instead of asking:

"Were we compliant?"

You can answer:

”Here’s proof we remained compliant.”

20 YEARS OF SECURING PAYMENT DATA
PCI

Audit-Ready Evidence

QSAs increasingly expect evidence—not assumptions.

Continuous monitoring provides:

- Historical script inventories
- Change history
- Alerts
- Control validation
- Policy enforcement records

Making assessments faster and easier.

20 YEARS OF SECURING PAYMENT DATA

Closing the Gap



Key Takeaways

PCI DSS v4.0.1 shifted security into the browser.

Manual monitoring cannot keep pace with modern websites.

Continuous visibility closes the gap between policy and reality.

Automation provides the evidence needed to remain compliant as environments continuously evolve.

20 YEARS OF SECURING PAYMENT DATA

Always-on GRC and AppSec Protection for merchants and payment service providers keeps payment webpages and iFrames PCI DSS v4.0.1 compliant.

Schedule a demo



20 YEARS OF SECURING PAYMENT DATA