

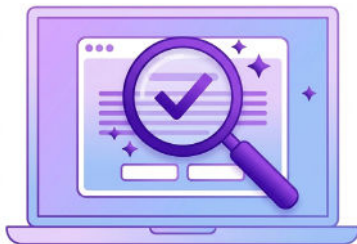
Ferooot Digital User Experience Security and Compliance Platform

AI-powered security and compliance for every website and mobile app.

Security threats and privacy regulations constantly evolve across every industry, creating a complex and growing web of obligations for organizations operating websites and mobile applications. To stay secure and compliant, organizations need more than point-in-time audits and manual controls. They need AI-powered agents that continuously discover, monitor, enforce, and remediate risk at the digital experience layer, across every user session, every regulation, and every jurisdiction.

Three critical problems at the digital experience layer

Websites and mobile apps rely on dozens of third-party scripts, pixels, and tracking technologies that can introduce privacy, security, and payment compliance risks invisible to traditional tools. Malicious scripts operate silently at the browser layer. Consent controls drift without detection. Payment pages are left exposed to unauthorized script behavior while regulators demand continuous proof of control.



Global privacy regulations such as GDPR, CCPA/CPRA, HIPAA, LGPD, PDPA, and POPIA — combined with security frameworks including NIST CSF, OWASP Top 10, and PCI DSS v4.0.1 — require organizations to continuously enforce controls, prove consent, protect sensitive data flows, and secure payment pages in real time. Managing these obligations manually across multiple websites and mobile apps is unsustainable. Organizations need AI-powered agents that never stop working.

How Ferooot's AI agents solve compliance, security, and PCI challenges

Automate privacy & security compliance

Continuously discover all pages and scripts processing user data across your websites and mobile apps, inspect data in motion, automate cookie consent audit, and enforce policies aligned to GDPR, CCPA, HIPAA, LGPD, PDPA, POPIA, and 50+ global regulations — proving controls are working every day, not just at audit time.

Stop malicious scripts & data exfiltration

Monitor and block malicious scripts at the browser and mobile app layer — including data skimming, formjacking, script injection, and unauthorized script execution — across every website and mobile app, aligned to NIST CSF, OWASP Top 10, PCI DSS, and 50+ global security frameworks.

Automate PCI DSS v4.0.1 compliance

Automatically manage and authorize scripts on payment pages (PCI DSS 6.4.3), detect unauthorized changes in real time (PCI DSS 11.6.1), and block cardholder data exfiltration across websites and mobile apps — generating continuous QSA-ready evidence every session.

Three products. One unified platform.

DXComply

Automate Compliance & Consent Audit at Scale: AI agents continuously discover, inventory, and enforce privacy and security policies — including automated consent audits and cookie consent tracking — across your websites and mobile applications. Native support for GDPR, CCPA, HIPAA, LGPD, PDPA, POPIA, PIPEDA, and 50+ global regulations.

DXSecure

Always-On AI Protection for Your Digital Experience Layer: AI agents continuously discover, inventory, monitor, and block threats at the browser and mobile app layer — detecting data skimming, formjacking, script injection, and unauthorized script execution in real time. Aligned to NIST CSF, OWASP Top 10, PCI DSS, and 50+ global security frameworks.

PaymentGuard

Automate PCI DSS 6.4.3 & 11.6.1 Across Every Payment Channel: AI agents auto-discover and inventory all scripts on payment pages, enforce PCI DSS v4.0.1 requirements 6.4.3 and 11.6.1 continuously, block cardholder data exfiltration in real time, and generate QSA-ready audit evidence automatically — across websites and mobile apps.

Operational benefits

- **AI agents that never stop working:** Continuously discover, inventory, enforce policy, detect threats, and remediate risk across every website and mobile app — 24x7, without manual intervention.
- **50+ regulations and frameworks natively enforced:** Privacy regulations, security frameworks, and industry standards enforced out of the box — with AI-generated audit evidence always ready.
- **Proven every day, not just at audit time:** Controls are continuously operating and evidence is continuously generated, so compliance is always demonstrable, not scrambled for.
- **Connected to your enterprise security & GRC stack:** AI-generated telemetry, risk signals, and compliance evidence extend directly into your existing SIEM and GRC platforms — no rip-and-replace.

Beyond point-in-time compliance

The Feroot Digital User Experience Security and Compliance Platform goes far beyond periodic audits and manual controls. It is an AI-powered platform that continuously secures and automates compliance across the digital experience layer — discovering data flows, enforcing privacy and security policies, protecting payment pages, and delivering real-time evidence to SecOps and GRC teams. With more than a billion web pages scanned across some of the world's most recognizable brands, Feroot is the platform enterprises trust to keep every user experience secure and compliant at scale.

AI-powered compliance built from
100+ global implementations.

Schedule a Demo

Feroot ensures secure and compliant user experiences by protecting sensitive data across websites and mobile applications. Supporting more than 50 global regulations, frameworks, and standards, Feroot automates compliance at the digital experience layer by providing continuous visibility into the inventory and runtime behavior of third-party and potentially malicious scripts. The platform delivers real-time alerting and reporting to SecOps and GRC teams and integrates with native security and compliance tools to accelerate remediation and enforce user-tracking consent policies at scale. Feroot has scanned more than one billion web pages for leading brands including Instacart, Reddit, and Gusto, and was named G2's Best Data Privacy Software Product of 2026 based on customer reviews. Learn more at www.feroot.com.

