DXSecure

Always-on AI protection against malicious scripts and data exfiltration at the digital experience layer

Threats targeting your users don't attack your backend, they operate silently inside your websites and mobile apps, at the exact layer where users interact with your brand and enter sensitive data. Malicious scripts, formjackers, and data skimmers bypass traditional WAFs, SIEMs, and endpoint tools entirely. Organizations need AI agents that continuously discover, inventory, monitor, and block threats at the digital experience layer — across every website and mobile app, every session, 24x7.

The security gap at the digital experience layer

Websites and mobile apps execute dozens of first-party and third-party scripts — any one of which can be compromised, injected, or repurposed to exfiltrate sensitive user data. These threats operate inside the browser, invisible to network-layer tools. OWASP identifies client-side attacks as among the most critical web application risks, and NIST CSF requires continuous monitoring of exactly these threats.

Data skimming, formjacking, malicious script injection, and unauthorized third-party script execution are invisible to traditional security stacks, yet they are among the most prevalent and damaging threats facing organizations with web and mobile presences. Without continuous, session-level monitoring at the digital experience layer, organizations cannot detect these threats in time to prevent exfiltration of sensitive user data, PII, and cardholder information.

How DXSecure's AI agents provide always-on digital experience layer protection

AI-powered script discovery and inventory

Automatically discover and continuously inventory every first-party and third-party script, tag, and data flow across your entire web and mobile footprint — auto-generating an always-current, always-accurate inventory without manual tagging, code changes, or agent installation on websites or mobile apps.

Real-time threat detection and blocking

Detect and block data skimming, formjacking, malicious script injection, and unauthorized script execution in real time across websites and mobile applications before sensitive user data can be exfiltrated. Behavioral analysis identifies known threats and novel zero-day client-side attack patterns the moment they activate.

Sensitive data flow protection

Continuously monitor and protect sensitive user interactions and regulated data flows across websites and mobile apps — tied to PCI DSS, HIPAA, NIST CSF, OWASP Top 10, GDPR, CCPA, and 50+ global security and privacy frameworks — at the moment of user interaction, every session.

Continuous behavioral monitoring and third-party risk

Perform persistent, session-level behavioral monitoring across every website and mobile app — detecting anomalies, behavioral drift, unauthorized data collection, and supply chain risks from third-party scripts across every user session, every day, with no sampling and no gaps.

Security Frameworks & Standards

NIST CSF · NIST SP 800-53 · OWASP Top 10 · OWASP ASVS · PCI DSS · SOC 2 · ISO 27001 · CIS Controls

Privacy & Compliance Regulations

HIPAA · GDPR · CCPA · LGPD · PDPA · POPIA · PIPEDA · + more

Operational benefits

- **Always-on, AI-driven threat protection:** 24x7 detection and blocking of malicious scripts, data skimming, and exfiltration across all websites and mobile apps — continuously, without manual intervention.
- **Complete script visibility:** Auto-generate and continuously maintain a real-time inventory of every script across your digital footprint — always current, never manually maintained.
- **NIST CSF, OWASP, and PCI DSS aligned:** Controls are continuously enforced and evidenced against leading security frameworks and global compliance mandates — natively, without code changes.
- **Integrated with your SecOps and GRC stack:** AI-generated threat telemetry and prioritized risk signals extend directly into your existing SIEM and GRC tools for fast investigation and remediation.

Beyond cookie compliance

DXSecure goes far beyond WAFs and network-layer tools. It is an AI-powered digital experience security platform that continuously discovers, monitors, and blocks threats at the exact layer where users are most vulnerable — inside the browser, on your websites and mobile apps. By combining AI agents, real-time behavioral monitoring, and continuous script inventory, DXSecure helps organizations prevent data exfiltration, meet OWASP and NIST requirements, and protect sensitive user interactions 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.

feroot