

Client-Side Defense

Safely benefit from browser scripts

Protect Trusted Digital Experiences without Sacrificing Script Value

Unlike tools that rely on static scans or periodic checks, Client-Side Defense observes script behavior in real user sessions—where digital skimming, data leakage, and risky changes actually occur. Client-Side Defense gives security and digital teams full visibility and surgical controls over the browser scripts running in every user session, creating a client-side trust layer in the browser. Automated zero-trust policies put invisible guardrails around scripts so teams can block risky or malicious actions, like reading payment or login data, without disabling or disrupting business-critical experiences. The result is safer customer data, lower breach and compliance risk, and simple adherence to standards such as PCI DSS 4.0, NIST CSF, GDPR, and HIPAA.

Client-side Defense Addresses:

- Client-side supply chain attacks, including digital skimming, Magecart, formjacking, and malicious redirects.
- Data leakage and privacy risk from unauthorized script access to login data, PII, payment data, cookies, and other sensitive fields.
- Compliance complexity tied to browser-focused requirements, including PCI DSS 4.0 inventory, authorization, integrity checks, and change detection for scripts and headers.

“We wanted to find the anomalies and changes in our client-side scripts. HUMAN’s behavioral analysis solution greatly simplifies this process. It helps us identify the known risks to our website and enables us to mitigate those risks.”

*Senior Manager of Information Security Architecture and Engineering,
Sally Beauty*

Benefits



GET COMPLETE VISIBILITY

Gain a clear view of the scripts running in real user sessions, what they access, and where they introduce security, privacy, or compliance risk.



PROTECT AND ENABLE YOUR BUSINESS

Put precise guardrails around script behavior so trusted tools keep working while risky actions are blocked.



SIMPLIFY AND MAINTAIN COMPLIANCE

Replace manual reviews and fragmented evidence gathering with continuous oversight and audit-ready reporting.

How It Works



COLLECTS

real-time script activity through a lightweight JavaScript sensor in real users' browsers, continuously inventorying first- and nth-party scripts, sensitive fields, script actions, domains, cookies, and more.



DETECTS

risky and anomalous behavior, including suspicious data access, malicious redirects, header changes, and other high-priority security and privacy incidents that warrant investigation.



BLOCKS

risky or malicious script actions protecting login data, payment data, and other sensitive information without disrupting legitimate scripts or user experience.

Key Capabilities



Comprehensive script visibility:

Automatically maps and inventories first- and Nth-party scripts in real user sessions and shows what data they access and where they send it.



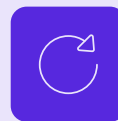
Compliance support and reporting:

Simplifies browser-focused security and privacy requirements with automated evidence collection, change monitoring, and audit-ready reporting.



Risk-based detection and alerting:

Surface high-priority incidents with behavioral analysis and risk scoring so teams can quickly identify the script activity that matters most.



Frictionless operational impact:

Connect with existing AppSec and DevSecOps workflows through APIs and out-of-the-box integrations for tools like SIEM, ticketing, and messaging.



Granular policy enforcement:

Apply precise controls that restrict unauthorized script behavior at the action level, without disabling legitimate, business-critical scripts.

The Human Advantage

Detection without Blindspots

We verify over 20 trillion interactions weekly across 3 billion devices, connecting global dots to reveal threats others miss across the customer journey.

Intelligence at the Core

Satori isn't just threat intel, it's a team on the front lines. From uncovering global fraud rings to surfacing new attack patterns, every HUMAN decision is powered by real-time insights.

Precision that Performs

>2,500+ signals per interaction. 400+ adaptive models. Decisions in milliseconds. HUMAN turns massive telemetry into high-fidelity decisions you can trust.

HUMAN Security is the global leader in Agentic Trust, the emerging discipline that informs and governs how humans, bots, and AI agents operate online. For more than a decade we help enterprises, platforms, and digital ecosystems verify digital interactions and establish trust across the entire customer journey - from first ad impression to final transaction. Powered by one of the world's largest behavioral signal networks, HUMAN analyzes over a quadrillion digital interactions each year to distinguish legitimate activity from fraud, abuse, and automated manipulation. Learn more at www.humansecurity.com