



Automated cybersecurity for regulated industries and government. **All customer scan and penetration-test data is analyzed only on hardware Hudson Infosec owns in the United States, by U.S.-developed models** — no public cloud, no external AI service.

CORE COMPETENCIES

Vulnerability Scanning & Pen Testing

Continuous in-network discovery, exploitation with proof of access, and prioritized remediation reporting.

Tamper-Evident Event Ledger

Cryptographically verifiable record of security events and AI-agent actions, built for audit.

SCADA / OT Assessment

Passive, discovery, and read-only active modes for Modbus, OPC UA, Siemens S7, and BACnet.

API Security Testing

Automated OWASP API Top 10 testing across REST, GraphQL, and SOAP surfaces.

PRODUCTS & SERVICES

Ayewo — continuous vulnerability assessment and AI-assisted penetration testing from a node deployed inside the customer network (virtual or bare-metal, x86-64 / ARM64). One node per VLAN; outbound-only, no inbound ports. Scheduled and on-demand scans; branded PDF and structured reports. SCADA/OT and wireless coverage.

Sentinel — a cryptographically immutable, tamper-evident ledger of security events, AI-agent decisions, and testing activity, with full-text search and audit export. Dedicated per-customer ledgers for government and enterprise tenants.

HSEC On Prem — the full analysis stack (nodes, pipeline, U.S. models, vulnerability mirrors) running entirely on the customer's own hardware, outbound-denied and air-gap capable, for the most sensitive environments.

PAST PERFORMANCE

In active production use since **2021**, delivering recurring vulnerability scanning, AI-assisted penetration testing, and tamper-evident security-event reporting for client organizations. Client identities are held in confidence; references and engagement detail are available under NDA on request.

COMPANY OVERVIEW

Hudson Infosec, LLC is a New York-based small business and New York State-certified Minority-Owned Business Enterprise delivering automated vulnerability management, penetration testing, and tamper-evident security-event integrity for regulated industries and government. Its Ayewo and Sentinel platforms test continuously from inside the customer network and preserve a provable record of the work, while **every stage of analysis runs on hardware Hudson Infosec owns in the United States, using U.S.-developed models**. A fully on-premises, air-gap-capable option keeps all data and analysis on the customer's own hardware for contracts that require all-local processing.

DIFFERENTIATORS

- **100% U.S., on-prem analysis.** No public cloud and no external AI service ever processes customer data.
- **Verified before release.** A deterministic layer plus an independent verifier model check every report for invented CVEs, false exploit claims, and unsafe OT actions.
- **Evidence you can prove.** A tamper-evident record for audit, forensics, and AI accountability.
- **Air-gap capable.** A fully on-premises deployment for contracts that require all-local processing.
- **Deploys in minutes.** Virtual or bare-metal nodes, no inbound attack surface.

COMPLIANCE ALIGNMENT

Reporting and evidence mapped to **NIST SP 800-53 / 800-171, NIST CSF 2.0, CMMC, HIPAA, PCI DSS, NERC CIP, and NY DFS 500**. Alignment supports a customer's compliance program; it is not a certification of Hudson Infosec.

UEI
F8WESK541XW1

CAGE CODE
9YD00

PSC
7J20 — IT & Telecom

BUSINESS TYPE
LLC · Small Business

PRIMARY NAICS
541511 Custom Computer Programming · 541519 Other Computer Related Services

SOCIOECONOMIC
NYS-certified MBE

SERVICE AREA
Nationwide