Commercial Value:

- Firmware is 50% of the code in your organization and it is not being monitored.
- Today organizations have “Zero Visibility” into firmware vulnerabilities.
- Vulnerabilities Below the OS (VBOS) are increasing and are a clear and present danger to all organizations.
- Firmware monitoring is a requirement of every major risk-based Cyber Security Framework but until now has been ignored. Patching does not solve the problem.
- Enterprise-wide, device integrity monitoring solution.
- Best in Class Vulnerability Research – OEM Databases, National Vulnerability Database, Independent Research Firms & Custom Research.
- Cybersecurity Maturity Model Certification (CMMC) – allows government contractors the ability to meet all levels of CMMC compliance.

Technology:

- Firmware Compromise/Vulnerability management – Monitors / Alerts to any critical vulnerabilities and firmware compromises any IT, IoT & OT device in real time.
- Able to connect to ANY device – Connector’s can access ANY IT, IoT & OT devices via either REST APIs or SDK or basic SSH CLI sessions.
- Supply Chain Integrity & Compliance Tool.
- Device “Evidence Record” is extracted and saved in an “insert only” database.
- “Evidence Record” is compared to the last record and all changes in device state are identified and logged for the forensic lifecycle of the device.
- Device state changes are run through an Analysis layer to identify anomalies based upon the 4 quadrants of integrity.
- Resulting Events and Critical Alerts are sent to organization’s security tools as well as are available in T5 User Interface for further deep dive analysis.

Federal Government Value:

- DOD Certified COTS solution – Commercial Item Designation.
- DHS-CISA CDM – Only authorized enterprise firmware monitoring solution.
- Vendor Agnostic – Monitors any infrastructure, network or virtual device (IT, OT, IoT).
- Compliance Reporting – NIST 800-53, FEDRAMP, FISMA, HIPAA, HITRUST CSF, PCI, 20 CIS Controls and GDPR.
- Big Data Analysis – Runs data science tools directly; no ETL required.
- Single Pane of Glass – Alerts sent to your SEIM or logging tool or drill down into built in UI for investigation.
- Lightweight and agentless – Avoids invasive code distribution by polling systems on user defined frequency without degrading performance.
- Flexible Deployment – On Prem, in the Cloud, or as a Managed Security Service.

Company Background:

- Founded 2015 – HQ Denver Colorado with multiple offices across the USA.
- CAGE CODE – 7EYS9 – Certified Woman / Minority Owned Small Business.
- Core Competencies – Cybersecurity, Managed IT Services, IT Consulting & IT Recruiting.
- Clients Include – we have work with Airforce, Army, Navy, CBP, FBI, VA, SOCOM, NETCOM and Army Corps of Engineers.