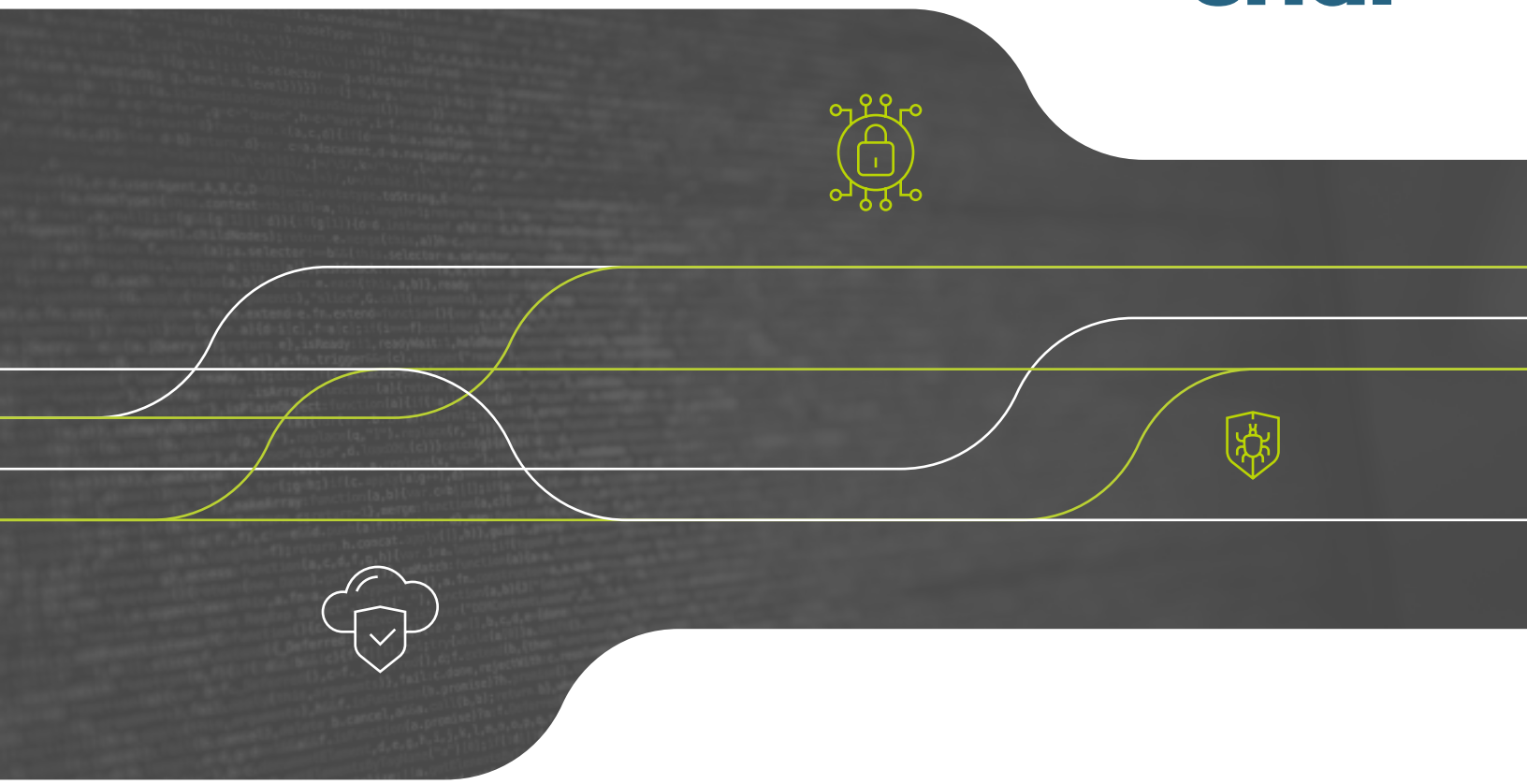

Shai™ Security

The staple of your Artificial Intelligence workforce, Shai™ is the employee that never tires and continuously improves by automating repetitive, high-volume tasks, working with the systems and tools you already have in place.

With more than 30 years of service dedicated to the federal sector, NCI offers a unique set of skills and experience to your advantage. Since two-thirds of our personnel are cleared Secret or higher, possess 800+ certifications in CISSP and CompTIA Security+, CASP, Network+ and more, we can deploy Shai™ with an unmatched level of security in highly-sensitive environments.

Shai™ has no API connection requirement or system infrastructure replacement, lowering the burden on your IT personnel. In addition, Shai™ has the same level of access to your system as a typical user to perform the same tasks.

STIG Adherence and Risk Review

Specifically designed for use in the federal sector, NCI has conducted multiple STIG audits on Shai™. The latest STIG audit on the Shai™ domain controllers was completed in May of 2018.

NCI cyber security personnel supporting NETCOM looked at 377 total factors as part of the STIG/SCAP audit. Our cyber experts performed a complete Nessus scan of the Shai architecture. If any findings have not been remediated, we have created documentation to support the decision.

Shai™ is developed in accordance with the OWASP recommended secure coding practices in JavaScript and HTML using a NodeJS-based Electron framework. As an additional security measure, access to the Internet can be disabled on the Shai™ machine, ensuring that all communication is kept internal and contained within the organization. Initially, Static Code Analysis is performed on Shai's code baseline and then during every major updated going forward, with all critical, high, and medium findings remediated or mitigated.

Flexible Infrastructure

Shai™ adapts to suit your infrastructure model, operating seamlessly in a physical, virtual, or hosted system. Made up of three software components deployed over one hardened/STIGed Windows 7 workstation, Shai™ is managed by your IT protocols and personnel, giving you control and consistency.

Physical

NCI Cortex Machine Intelligence Appliance installed at your location

Hosted

Hosted on a FedRAMP compliant system through AWS GovCloud (US) or AWS US East-West

Virtual

Hosted on a virtual machine provided by you

Security Posture includes:

- Shai™ is designed to house and safeguard sensitive information
- Shai™ currently stores and protects 70 million personal records
- FedRAMP adherence to NIST 800, HIPAA, and the HITECH Act
- ISO/IEC 27000 certified and FISMA compliant
- Sensitive data encrypted in transit and at rest using FIPS 140-2 compliant cryptography
- Shai™ does not have a user interface but instead uses the systems and tools you already have in place

Security Procedures include:

- System vulnerability and penetration scans, and Static Application Security Testing is regularly performed
- Ongoing risk assessments ensure compliance with administrative, physical, and technical safeguard responsibilities
- The Shai™ engineering team maintains secure coding practices governed by OWASP Top 10
- Code reviews, change tracking, and auditing are included in ongoing software development lifecycle
- Shai™ uses OSSEC and other intrusion detection systems
- Redundant systems are controlled through multifactor authentication