NeoSecure Suite

NeoSystems®

Innovate. Evolve. Transform.

NeoSecure Suite

As a trusted, ground-breaking innovator and thought leader in professional services for industry and the government, NeoSystems is a leader in managed security who understands and implements compliance requirements that impact business and security operations. As NIST and DoD-mandated Cybersecurity Maturity Model Certification (CMMC) compliance frameworks driving the Defense Industrial Base's (DIB) security footprint, Neosystems harnesses a comprehensive approach and foundational first milestone into securing businesses both large and small.

NEOSECURE SUITE: MANAGED SECURITY SOLUTION

The NeoSecure Suite is a managed security product designed from a superior technology stack combined with professional services, that adhere to the latest compliance requirements from the Department of Defense (DoD), such as the Cybersecurity Maturity Model Certification (CMMC), and government organizations such as the National Institute of Standards and Technology (NIST). NeoSecure can also be implemented and rolled out to other agencies and government organizations, and those that align with global compliance requirements.

NEOSECURE SUITE

The NeoSecure Suite is composed of 3 product solutions designed to fully manage a holistic group of business operations: security, compliance, and Information Technology: NeoSec, NeoTech and NeoEnclave. The products can be combined for maximized operational and regulatory success or can be implemented individually to enhance existing IT and Security operations.

(888) 676-6367 | growahead@neosystemscorp.com | www.neosystemscorp.com

NeoSecure Suite

NeoSec

NeoTec

NeoEnclave

NeoSec

NeoSec is a Managed Security Program Compliance Solution. It is a combination of compliance driven services that fulfill NIST SP 800-171 and DFARS 252.204- 7012. These services, readjusted for CMMC 2.0 delivery include:

- Security Program Management
- Boundary Protection
- Endpoint Protection
- Vulnerability and Configuration Management
- Managed Detection and Response (MDR)

TRANSLATION: NeoSec is best suited for small and medium enterprises with no, little or partial security program management, resources or staff in place. It's end-to-end, comprehensive delivery, which includes monthly and annual reporting for compliance purposes, takes the burden of CMMC preparation and readiness, or general security maturity, off of the client in order for the client to focus on its mission or business growth.

WHAT NEOSEC INCLUDES:

Comprehensive End-to-End Security Program Management

- Data and data flow assessments to define and document a CMMC Assessment Scope
- System review through a System Development Lifecycle (SDLC) framework
- Security control assessment and maintenance
- Security program roadmap development aligned with NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC) compliance matrix, and proposed solution for all applicable control
- Risk Assessment and security controls review
- CMMC audit support
- Output Documents for Audit include:
  - System Security Plan
  - Plan of Actions and Milestones
  - Information Security Policy and Procedures
  - Security Awareness Training
  - Security Role-based Training
  - Continuous Monitoring Plan
  - Incident Response Plan

Incident Response Management

- Incident investigation, analysis, and response activities
- Case management, response coordination, communications, and required reporting for security incidents

Vulnerability Scanning

- Monthly vulnerability scanning of all external and internal Client IP addresses
- Reporting on scan metrics such as systems scanned, vulnerability counts, and vulnerability aging

Endpoint Protection

- Advanced anti-malware protection for user workstationsand servers
- Automated detection, blocking of threats, and alerting of suspicious events
- Alert response and management to support event resolution and incident declaration

Log Management

- Log collection to meet CMMC requirements
- Alert configuration for known malicious events

NeoTec

NeoTec is a Managed Security and IT Program Compliance Solution. It is an enhancement to NeoSec and works holistically to complete necessary IT functions that are essential to running a robust IT and Security shop. The NeoSec + NeoTech combination fully runs, manages, reviews, audits, updates all necessary aspects compliance and operational IT security Security Program Management

WHAT NEOTEC INCLUDES:

CMMC Workstation Compliance Management

- Machine health and status monitoring with client systems/networks, and data reporting
- Client systems maintenance including patching and vulnerability scanning and reporting
- Issue resolution
- Remote patch installation including software updates within a unified dashboard
- Scheduled maintenance automation (remote and on-prem)

Microsoft 365 Management

- M365 Tenant implementation: GCC, GCC High
- Security Baseline, Accounts, MFA
- Continuous Automated monitoring and Security Baseline Controls maintenance
- Client configuration (workstations, devices)
- Audit Logging (Log Management)
- Email and Data Migration
- SharePoint and Teams set up
- Monitor and maintain configuration and compliance status
- Security alerts configuration and Management
- Monthly Security Control Reporting

CMMC Network Compliance

- Firewall Management
  - Firewall configuration and maintenance and adherence to compliance requirements
  - Firewall continuous monitoring
  - Firewall rules and configuration updates and adherence network security compliance
- Network Management
  - Network device configuration and maintenance and adherence to compliance requirementsand maintenance and adherence to compliance requirements

NeoEnclave

The Neo Secure Enclave Solution is a virtual compliant environment to run your applications. This solution addresses and complies with all security controls specified in NIST SP 800-171 and DFARS 252.204-7012 standards relating to the protection of Federal and DoD controlled unclassified information (CUI).

WHAT NEOENCLAVE DOES:

- Sequesters CUI and ITAR data
- Allows authorized End Users to receive, store, process, edit, and share (internally and externally) CUI
- Provides the processing power (CPU and memory) needed to support End User workload
- Supports required End User applications

  Supports NIST 800-171, DFARS 252.204-7012, and CMMC requirements
- Minimizes the responsibilities, actions, and business operation timing for the organization and their employees

  Supports the users' business requirements while handling CUI
- Is affordable and easy to use
- Can be turned on and turned off on a contract-by-contract basis

  Takes the corporate network out of CMMC scope
- Pairing with the NeoSec solution provides a holistic, complete CMMC solution that includes a full set of documented securitypractices and processes aligned with the CMMC 2.0 standard

What NeoEnclave Includes:

- Setup and configuration of the Secure Enclave environment compliant with NIST SP 800-171 and DFARS 252.204-7012
- Operation and maintenance including installation of software patches and upgrades issued by the Neo TechStack software application vendors

  Setup Organizations in a Secure Enclave Environment

  Setup User Accounts in a Secure Enclave Environment

  Enroll End User laptops for access to digital workspace in a Secure Enclave Environment

  CMMC compliant security documentation for desktop application software and

  cloud access

WHO WE ARE

AWARDS

Inc. 5000 List for 7 Consecutive Years | SAP Concur Distinguished Partner Award
Adaptive Insights (Workday) Partner Momentum Award - Americas
Deltek Premier Partner Award: GovCon Consulting | E&Y Entrepreneur of the Year Finalist: Michael Tinsley