ARKA
AMERGINT

INFORMATION ASSURANCE AND CYBERSECURITY

THE STRATEGY

Increasing global threats across space, air, land, and within vital information environments demand a comprehensive cybersecurity strategy. AMERGINT's responsive and proactive approach to mitigating these threats is rooted in our software architecture and our foundational software development principles. Our Information Assurance (IA) approach operates with a mission—to ensure your data is secure and protected against the latest security vulnerabilities.

AMERGINT's IA and Cybersecurity Posture

Compliance and Evaluation

Measured to adhere to industry standards and policies

Robust Security Plan

Hardened at delivery and a plan with routine updates to address vulnerabilities

Code Gen Techniques

Decreased exposure to vulnerabilities through a low code development environment

Responsive SDR Security

Resilient and continually assessed for failsafe coverage

OUR COMMITMENT

Insider threats, malicious threat actors, supply chain uncertainties, and the future dangers of tomorrow are all evaluated with:

- Comprehensive, subscription-based security plans
- Static Code Analysis (SAST) implementation, with Dynamic Code Analysis (DAST) in progess, for Continuous Integration and Continuous Deployment (CI/CD) prior to executing programs
- Resilient Cloud-based Software Defined Radio (SDR) security mitigation approaches with a minimized attack surface for a single point of contact
- Security policies aligned with industry standards
- A software and firmware development environment that limits exposure
- Zero Trust Architecture
- Regular penetration testing
- IA hardening at delivery

BEYOND BEGINS HERE

THE COMPONENTS

SECURITY HARDENING

AMERGINT systems are hardened at delivery with a secure Operating System (OS) configuration based on a Red Hat Enterprise Linux OS that leverages Common Criteria Certification. The secure configuration modifies the OS to meet the security target requested, which may include:

- Requiring more complex passwords (8 character minimum with future advancement to unique, auto-generated for hardening scripts).
- Preventing executable programs from being installed on transient storage devices.
- Securing the network against known attacks.
- Ensuring all users on the system have defined home directories that are secured.
- Mandating certain file and directory creation masks.
- Configuring immutable auditing of the OS so that all changes are logged.
- Ensuring mandatory banners are visible at access points.

SECURITY PLAN

AMERGINT's comprehensive, subscription-based security plan is robust, accommodating, and flexible. Periodic updates to the OS are provided for AMERGINT applications / services to ensure your system always operates on the most current software and protected against the latest vulnerabilities. Under a security agreement, you receive routine OS security packages, critical vulnerability updates, and full verification updates on a quarterly, biannual, or annual basis.

SDR / CLOUD SECURITY

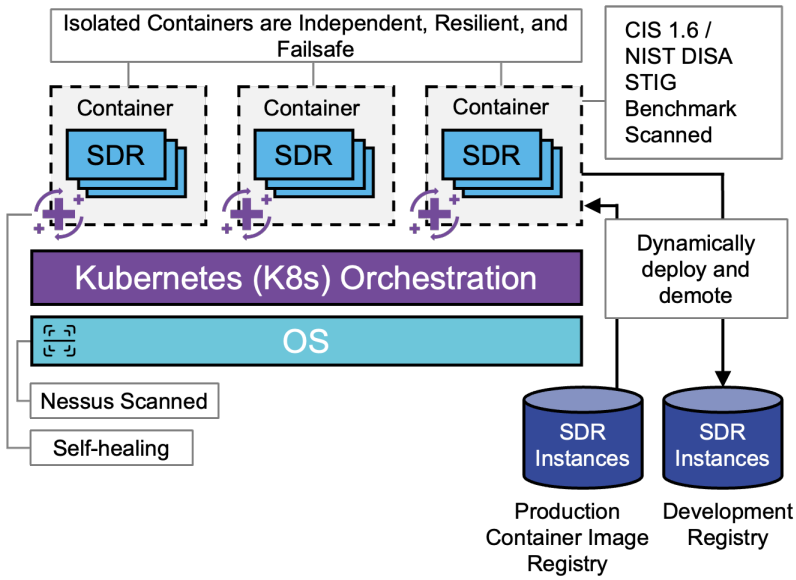
As a leader in the digital ground transformation, AMERGINT recognizes the need for systems that are not only agile and evolvable, but are also secure and resilient. Our SDRs meet this need. We test our SDR solutions against the most rigorous cybersecurity measures to provide failsafe coverage. To protect against vulnerable applications, external attacks, and misconfiguration issues in Cloud environments, AMERGINT continuously verifies the quality and security of available Cloud Services.

COMPLIANCE SERVICES

AMERGINT measures its cybersecurity posture against robust compliance frameworks and certification programs:

- Secure RHEL OS Configuration
- Hardening against DISA STIG
- Evaluation against NIST 800-53R3
- NIST.SP.800-171 Compliance
- Linux Foundation Certified Employees to adhere to CNCF best practices
- CMMC 2.0 in progress
- Alignment to NSA/CISA K8s Hardening Guide
- DoD Level II and III Certified Employess and best practices

High-Level SDR / Cloud Design for Proactive Security



www.arka.org
@AMERGINT
@AMERGINT
amergint-technologies

FOR ADDITIONAL INFORMATION:

2315 Briargate Pkwy., Suite 100
Colorado Springs, CO 80920 USA
Tel: 719-522-2800 | Fax: 719-522-2010
Email: info@amergint.com