

SECURITY HARDENING AND MAINTENANCE PLAN

Security hardening

Custom audit and remediation tools

Security and operating system updates

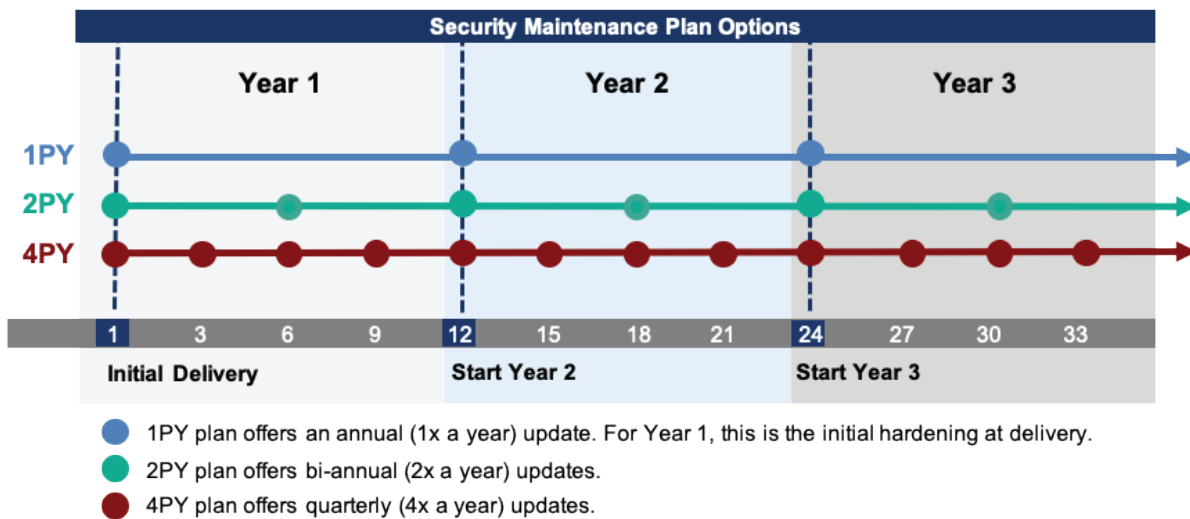
OVERVIEW

- » **Security Hardening:** AMERGINT offers Security Hardening on delivered systems to help meet your Information Assurance (IA) needs. We measure against the following benchmarks: DISA Red Hat® Enterprise Linux (RHEL7 and RHEL8) Security Technical Implementation Guide (STIG), DISA Apache Server STIG, and DISA Firefox STIG.
- » **Security Hardening Deliverables:** With each hardened system, AMERGINT delivers: a document describing our hardening process; STIG audit results files; our custom audit tool (to use onsite for future audits); the input STIGs used for auditing; and a Hardening Report that lists findings and any site-specific items not remediated during hardening.
- » **Custom Audit and Remediation Tools:** AMERGINT employs custom audit and remediation tools to ensure thorough and consistent audit testing against DISA STIGs. TestExec™ (our custom, automated testing framework) generates an output STIG .xml file that can be viewed directly within the DISA STIG Viewer application. We also provide our audit tool that can be run onsite to audit any local changes made to the system after delivery.
- » **Security Hardening Maintenance Plan:** AMERGINT offers a robust Security Hardening Maintenance Plan that provides OS security patches, critical vulnerability updates, and full verification testing at flexible intervals (annually (1PY), bi-annually (2PY), or quarterly (4PY)).
- » **Functional Compatibility Verified With Every Update:** As part of the AMERGINT Security Hardening Maintenance Plan, the software/hardware configuration for your system is kept updated, and then re-tested using the same production tests and Factory Acceptance Tests to ensure the software functions to the level that was initially provided.
- » **Certification Support:** For complex certification scenarios, our security experts can provide detailed reports on the configuration as well as detailed explanations of any exceptions to security standards required for the software to run.
- » **Top Notch Security Expertise:** Our security staff consists of CISSP™ Certified individuals, focused on delivering solid security value in a timely manner. If our standard hardening offering does not meet your needs, please discuss other options (e.g., integration with site LDAP and NTP servers, multi-factor authentication, etc.) with your AMERGINT representative.

SECURITY HARDENING MAINTENANCE PLAN OPTIONS

Today’s computing environment requires a constant update approach to minimize security risks. This modern approach can be time-consuming and logistically difficult. AMERGINT’s Security Hardening Maintenance Plan provides the necessary updates, in an easy to consume format, to keep your systems up and running with minimal operational impact.

Security Hardening Maintenance is offered in yearly increments—starting at initial delivery—and at flexible intervals, either annually (1PY), bi-annually (2PY), or quarterly (4PY) to meet individual security requirements and schedules. For example, if you are seeking only initial hardening, you can purchase the 1-year/1PY plan. If you desire regular OS and security updates, you can purchase the 2PY or 4PY plan, or continue to purchase the 1PY plan, annually. Regular updates improve functionality and protect your system from ever emerging security threats.



*Operating systems are updated to the most recent minor revision of RHEL that AMERGINT fully supports.

MORE SECURITY HARDENING OPTIONS

Hardening options include:

- » SCAP scans
- » Nessus scans
- » CIS benchmarks

Delivery options include:

- » DVD
- » Cloud based repository
- » On-Premise repository

WE ARE THE LINK

2315 Briargate Pkwy, Suite 100
 Colorado Springs, CO 80920
www.amergint.com | info@amergint.com
 719-522-2800

www.amergint.com

AMERGINT

amergint-technologies

