RUNSAFE SECURITY

RunSafe Security's Protect:

NIST 800-53

Technical Briefing

RunSafeSecurity.com

Table of Contents

Addressing NIST 800-53

The Department of Defense's Cyber Risk Management Framework (RMF) is meant to ensure that deployed mission capability is able to perform the mission without malicious cyber interference in the workings of the system. A program's objective is to achieve authority to operate (ATO) at the lowest possible cost with the lowest possible time delay, because safe cyber operation isn't the mission objective, but instead a mission requirement.

Systems running firmware, apps, and OS protected by RunSafe Security's Protect solution are better able to document their compliance with RMF (DoDI 8510.01) which incorporates NIST 800-53. Consequently, programs accelerate time to ATO at lower cost. For High Impact systems, Protect enhances compliance with more than 20% of the controls. For many of the Protect affected controls, the only alternative is thousands of hours of testing.

Even though 800-53 and RMF have been the acquisition guidelines for years, systems achieving ATO have still been compromised.

PROTECT RESETS THE SECURITY BASELINE TO THE DEFENDER'S BENEFIT FOR THE FOLLOWING REASONS:

- Last-mile integrity, down to the running memory. Existing processes have done a reasonably good job ensuring that system design intent translates into developed code. Processes and configuration management have also helped ensure that properly developed code is what is actually deployed to the target system. The breakdown though is limited tooling to guarantee that the running code in memory corresponds exactly to the code that was deployed.
- Zero-days and root kits are able to hijack running code and divert execution in unintended ways. This risk is especially prevalent for systems that are "outside the perimeter" and can't support traditional virus scanning, such as embedded systems (e.g. CM-2(7) CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS, SA-10(6) TRUSTED DISTRIBUTION)
- Protect mitigates the risk of an entire class of vulnerabilities (memory corruption), providing advanced heretofore impossible incident response resilience (e.g. IR-4 INCIDENT HANDLING, IR-9 INFORMATION SPILLAGE RESPONSE)
- Protect can be applied to the system firmware, operating system, and applications, providing a totality of protection, from the processor to the top of the stack that would previously have cost orders of magnitude more (SI-2 (5) AUTOMATIC SOFTWARE / FIRMWARE UPDATES, SI-7 (10) PROTECTION OF BOOT FIRMWARE, SI-3a TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS)

The Solution

With its roots in a DARPA project, RunSafe Protect confronts the previously unaddressed risks of zero-day vulnerabilities. Protect brings a new advantage to the cyber defense toolkits for organizations and addresses multiple NIST 800-53 controls across numerous control families. By filling the current void of zero-day vulnerability mitigation entities can leverage Protect to proactively address NIST 800-53 controls from a revolutionary and disruptive standpoint.

Addressing the multitude of vulnerabilities is a constant challenge for organizations. An even greater risk resides in the identification and remediation of unknown (zero-day) vulnerabilities. In many cases, compliance does not equate to security. However, zero days are numbered with Protect.

RunSafe Protect introduces an innovative and revolutionary solution to this challenge.

Current vulnerability and patch management techniques rely on a static process of scanning for flaws and addressing vulnerabilities. By the time that vulnerabilities are publicly released, attackers have leveraged such flaws to exploit organizations.

A recent report by the United States Government Accountability Office demonstrated the paramount concerns over the vulnerabilities that are plaguing the Department of Defense's weapon systems. This problem is one that requires automated methodologies to ensure systems are properly secured. Such organizations have implemented the NIST 800-53 standards, but this is simply insufficient in combatting the advanced threats of today.

RunSafe Protect technology hardens software binaries against memory corruption errors and buffer overflow exploits — the techniques attackers typically use to gain control of embedded systems and devices.

Protect processes can be accessed through a web client or RestAPI and applied to new build or systems already fielded. It covers applications down to bare metal, whether in IT or OT; Windows, Linux, or no OS; AMD, ARM, Intel and PowerPC platforms. Protect defends software, devices, and systems in minutes and requires no new software, services or hardware; no access to source code, compiler or operating system; no alerts that consume scarce resources to monitor.

By the Numbers

NIST 800-53 offers three categories of impact boundaries; High, Moderate, and Low. These categories apply more controls to the information system for higher levels and less controls to that of lower levels. This classification is predicated upon the Federal Information Processing Standard Publication 199 (FIPS-199). FIPS-199 defines system boundaries under the following criteria:

The potential impact is high if:

the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- **AMPLIFICATION:** A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The potential impact is moderate if:

the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- **AMPLIFICATION:** A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is low if:

the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

- **AMPLIFICATION:** A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced: (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The Protect Impact

RunSafe Protect can drastically reduce the complexity of achieving compliance with the NIST 800-53 controls. The figures below demonstrate the breadth of controls that are addressed by Protect across the three FIPS-199 security categories. For a full listing of the 800-53 Controls and Sub-Controls, see page 12.

FIPS-199 CATEGORY	TOTAL CONTROLS (TOP LEVEL)	CONTROLS ADDRESSED BY PROTECT	PERCENTAGE ADDRESSED BY PROTECT
HIGH	170	35	21%
MODERATE	159	30	19%
LOW	115	16	14%

MULTIPLE CONTROL FAMILIES ARE ADDRESSED FROM A UNIQUE AND REVOLUTIONARY PERSPECTIVE WITH PROTECT.

- Security Assessment and Authorization (CA)
  Configuration Management (CM)
- Incident Response (IR)
- Maintenance (MA)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Sample Control Response

Below is a comparison of a standard NIST 800-53 rev. 4 control response leveraging traditional methodologies and the advanced response using Protect.

- Control Family: System and Information Integrity
- Control Number: S|-3a
- Control Title: Time to Remediate Flaws/ Benchmarks for Corrective Action

Control Requirement: Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

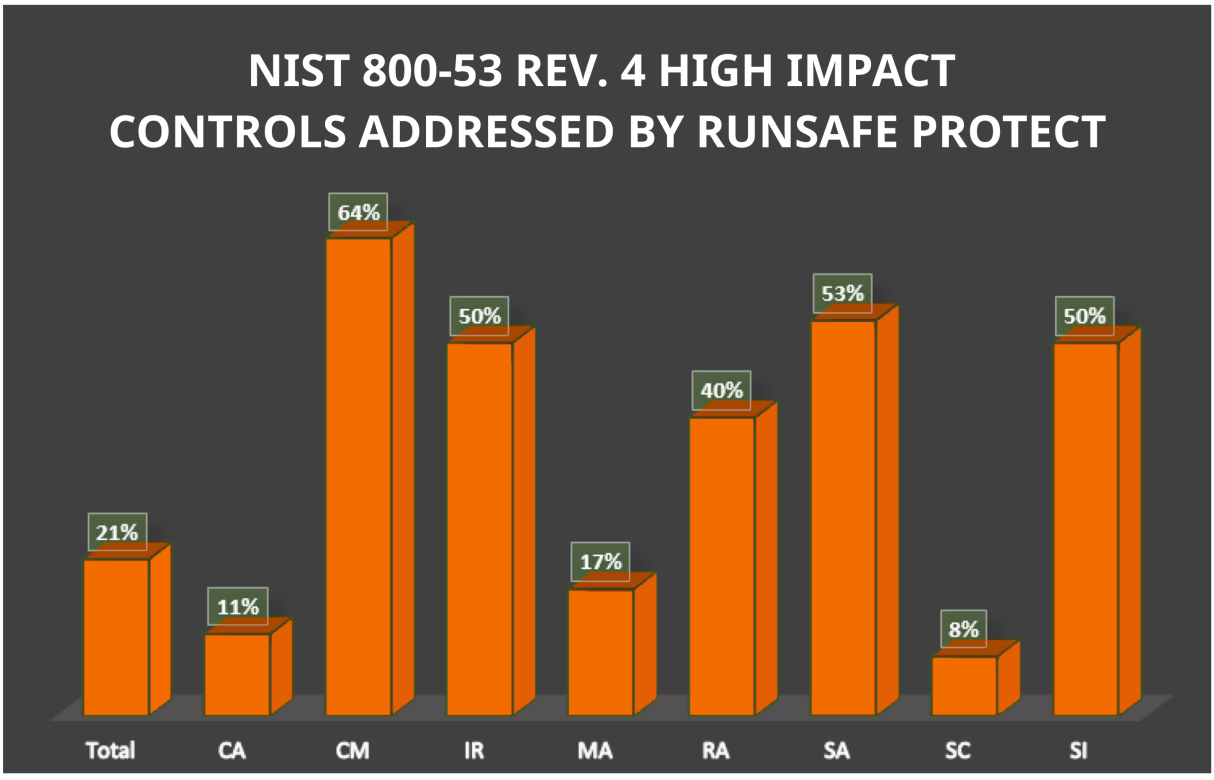
Traditional Response: The organization employs the use of ***[Organization-Defined Intrusion Prevention Systems (IPS)]*** at various ingress and egress points within the network to detect and eradicate malicious code. The ***[Organization-Defined Intrusion Prevention Systems (IPS)]*** are signature-based and detect/ eradicate malicious code that has been previously identified as threats by ***[vendor/threat analysis source].***

Problem: The traditional control response is relying on intelligence from previously detected malicious code and signatures. Essentially, this represents a similar gap to that of stagnant antivirus methodologies. Furthermore, this control response is not addressing potentially harmful code in running-memory. From an attacker's perspective, such control responses and implemented procedures are the inherent gaps required to mount successful malicious campaigns against entities, exploiting the stale methodologies and widely known gaps. While such traditional methodologies are still recommended, supplemental protections must be implemented to provide adequate protections to the more advanced layers of the technology stack.

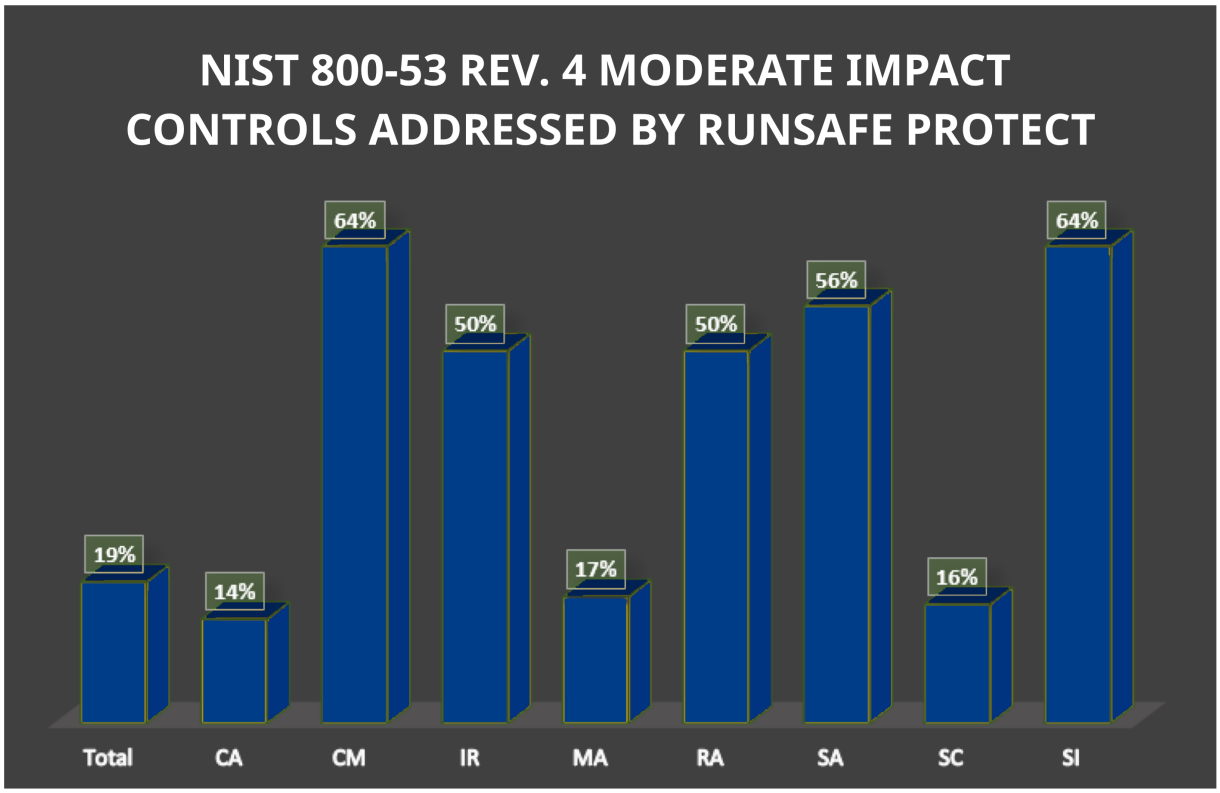
RunSafe's Response: RunSafe Protect is used to harden code on ***[organizationdefined systems]*** and at strategic entry/exit points. The application of RunSafe Protect defends against malicious code execution by hardening binaries to perform only the desired function(s). When used in conjunction with IPS/IDS, the organization protects key ingress and egress points from a multitude of attacks including those beyond the previously detected malicious code from intelligence gathered by threat sources. Additionally, flaws that are identified that do not have current fixes or patches may be addressed by the cyberhardening of the binaries.

Solution Explained: In contrast to the sole antiquated control response, the incorporation of RunSafe Protect into this section addresses an area that has been left as a window of opportunity to attackers. Adversaries are aware that defenses are limited to the current solutions offered in the marketplace. Signature-based and even heuristic protection mechanisms have wide gaps that are often exploited. With traditional mechanisms, organizations are left with a strictly reactive defense, rather than a proactive defense with RunSafe Protect. Additionally, addressing zero-day vulnerabilities and running memory exploitation is a challenge. Attackers are studying these gaps and succeeding in exploiting organizations due to the lack of proactive solutions currently offered.

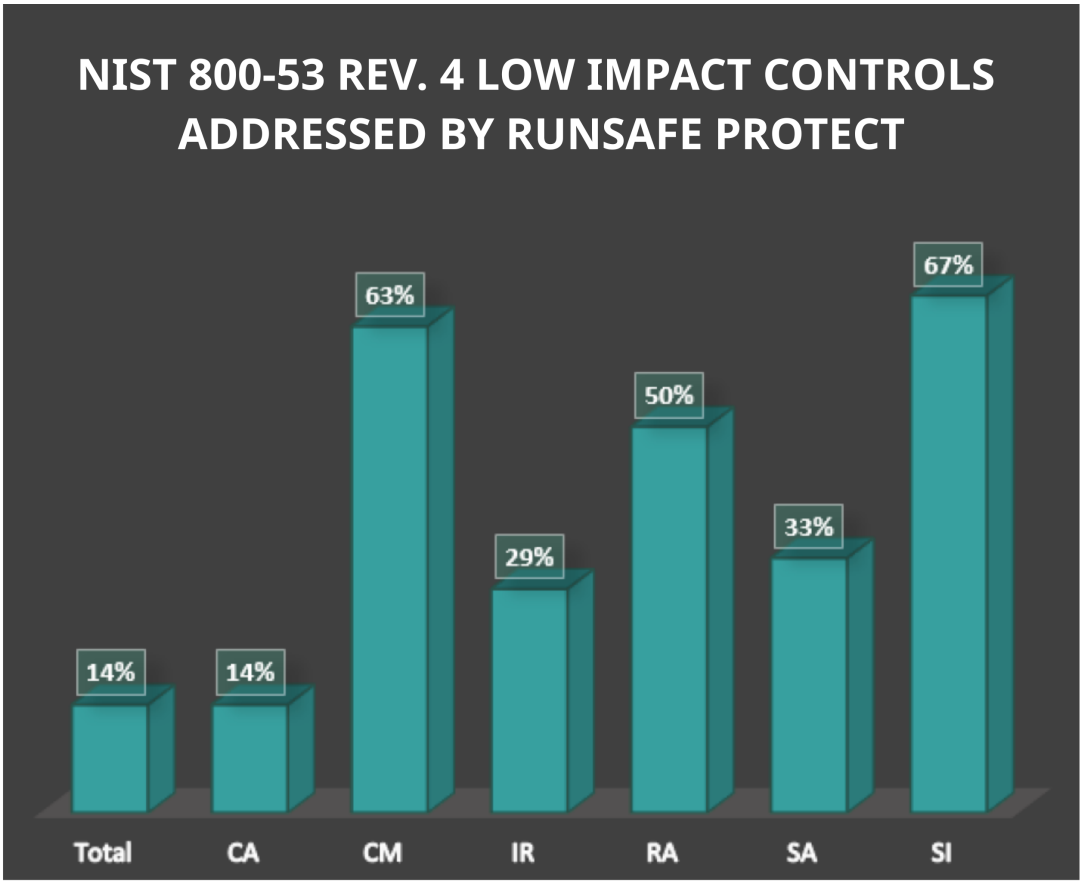
Within the High Impact NIST 800-53 Rev. 4 Boundary, RunSafe Protect addresses 35 out of the 170 controls across the following families.



Within the Moderate Impact NIST 800-53 Rev. 4 Boundary, RunSafe Protect addresses 30 out of the 159 controls across the following families.



Within the Low Impact NIST 800-53 Rev. 4 Boundary RunSafe Protect addresses 16 out of the 115 controls across the following families.



Last-Mile Integrity with Protect

Bringing NIST 800-53 control compliance to organizations is an achievable task. The controls address a wide array of factors that can raise the cyber security postures when properly implemented.

However, the grey spaces in security are the areas in which solutions such as Protect fill the void. Last-mile integrity and running memory are currently under attack and must be protected. Minimal solutions are currently offered in the marketplace that offer proactive options to defend these critical areas.

Protect is quickly becoming a trusted solution in combatting the complex security flaws in running memory. Protect works by ensuring that protected binaries cannot be misused to grant entry ways and attack paths for cyber-threats. In doing so, unauthorized code or execution manipulation of a protected system is blocked. Addressing these inherent system problems has caused organizations to invest significant amounts of time and resources into mitigating bug fixes and vulnerabilities on a one-for-one basis. Turning to automation with Protect can drastically reduce the Mean Time to Response (MTTR). By leveraging Protect within your information security stack, your organization can streamline control satisfaction in multiple families of NIST 800-53.

Protect introduces the capability to defend against exploitation of runtime level code. This solution protects against various exploitation tactics that seek to interrupt and/ or compromise running code in memory. Therefore, unauthorized code or execution manipulation of a protected system is blocked. This effectively ensures that the protected code only performs the desired effects and only executes as the developer intended.

RunSafe Security is the pioneer of a patented cyberhardening transformation process designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the critical infrastructure, IoT, automotive, medical, and national security industries.

800-53 Controls and Sub-Controls

Control	Sub-Control	Title
SECURITY ASSESSMENT AND AUTHORIZATION		
CA-7	CA-7e	CONTINUOUS MONITORING
CONFIGURATION MANAGEMENT		
CM-2	CM-2 (2)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY
CM-2	CM-2 (6)	DEVELOPMENT AND TEST ENVIRONMENTS
CM-2	CM-2 (7)(a)	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS
CM-2	CM-2 (7)(b)	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS
CM-3	CM-3a	CONFIGURATION CHANGE CONTROL
CM-3	CM-3d	CONFIGURATION CHANGE CONTROL
CM-3	CM-3 (1)(d)	AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES
CM-3	CM-3 (3)	AUTOMATED CHANGE IMPLEMENTATION
CM-5	CM-5 (3)	SIGNED COMPONENTS
CM-6	CM-6a	CONFIGURATION SETTINGS
CM-6	CM-6c	CONFIGURATION SETTINGS
CM-6	CM-6 (1)	AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION
CM-6	CM-6 (2)	RESPOND TO UNAUTHORIZED CHANGES
CM-7	CM-7a	LEAST FUNCTIONALITY
CM-7	CM-7 (2)	PREVENT PROGRAM EXECUTION
CM-8	CM-8 (3)(a)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION
CM-10	CM-10 (1)	OPEN SOURCE SOFTWARE
INCIDENT RESPONSE		
IR-1	IR-1a.2	INCIDENT RESPONSE POLICY AND PROCEDURES
IR-3	IR-3 (1)	AUTOMATED TESTING
IR-4	IR-4a	INCIDENT HANDLING
IR-4	IR-4 (1)	AUTOMATED INCIDENT HANDLING PROCESSES
IR-4	IR-4 (2)	DYNAMIC RECONFIGURATION
IR-4	IR-4 (10)	SUPPLY CHAIN COORDINATION
IR-9	IR-9f	INFORMATION SPILLAGE RESPONSE
MAINTENANCE		
MA-6 (2)	MA-6 (2)	PREDICTIVE MAINTENANCE
RISK ASSESSMENT		
RA-1	RA-1a.2	RISK ASSESSMENT POLICY AND PROCEDURES
RA-5	RA-5a	VULNERABILITY SCANNING
RA-5	RA-5b.1	VULNERABILITY SCANNING
RA-5	RA-5b.3	VULNERABILITY SCANNING
RA-5	RA-5d	VULNERABILITY SCANNING
RA-5	RA-5 (4)	DISCOVERABLE INFORMATION
SYSTEM AND SERVICES ACQUISITION		
SA-3	SA-3a	SYSTEM DEVELOPMENT LIFE CYCLE
SA-3	SA-3d	SYSTEM DEVELOPMENT LIFE CYCLE
SA-4	SA-4 (3)	DEVELOPMENT METHODS / TECHNIQUES / PRACTICES
SA-4	SA-4 (5)(a)	SYSTEM / COMPONENT / SERVICE CONFIGURATIONS
SA-4	SA-4 (5)(b)	SYSTEM / COMPONENT / SERVICE CONFIGURATIONS
SA-8	SA-8	SECURITY ENGINEERING PRINCIPLES
SA-10	SA-10e	DEVELOPER CONFIGURATION MANAGEMENT
SA-10	SA-10 (4)	TRUSTED GENERATION
SA-10	SA-10 (6)	TRUSTED DISTRIBUTION
SA-11	SA-11e	DEVELOPER SECURITY TESTING AND EVALUATION
SA-11	SA-11 (2)	THREAT AND VULNERABILITY ANALYSES
SA-11	SA-11 (6)	ATTACK SURFACE REVIEWS
SA-12	SA-12	SUPPLY CHAIN PROTECTION
SA-12	SA-12 (5)	LIMITATION OF HARM
SA-12	SA-12 (15	PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES
SA-15	SA-15a.2	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
SA-15	SA-15 (4)	THREAT MODELING / VULNERABILITY ANALYSIS
SA-15	SA-15 (4)(	THREAT MODELING / VULNERABILITY ANALYSIS
SA-15	SA-15 (5)	ATTACK SURFACE REDUCTION
SA-15	SA-15 (6)	CONTINUOUS IMPROVEMENT
SA-15	SA-15 (7)(	AUTOMATED VULNERABILITY ANALYSIS
SA-15	SA-15 (7)(	AUTOMATED VULNERABILITY ANALYSIS
SA-18	SA-18	TAMPER RESISTANCE AND DETECTION
SA-18	SA-18 (1)	MULTIPLE PHASES OF SDLC
SA-20	SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS
SYSTEM AND COMMUNICATION PROTECTION		
SC-4	SC-4	INFORMATION IN SHARED RESOURCES
SC-8	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
SC-18	SC-18 (2)	ACQUISITION / DEVELOPMENT / USE
SC-1	SI-1a.2	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SYSTEM AND INFORMATION INTEGRITY		
SI-2	SI-2a	FLAW REMEDIATION
SI-2	SI-2d	FLAW REMEDIATION
SI-2	SI-2 (1)	CENTRAL MANAGEMENT
SI-2	SI-2 (2)	AUTOMATED FLAW REMEDIATION STATUS
SI-2	SI-2 (3)(a)	TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS
SI-2	SI-2 (5)	AUTOMATIC SOFTWARE / FIRMWARE UPDATES
SI-3	SI-3a	TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS
SI-3	SI-3c.2	TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS
SI-3	SI-3 (1)	CENTRAL MANAGEMENT
SI-3	SI-3 (2)	AUTOMATIC UPDATES
SI-3	SI-3 (8)	DETECT UNAUTHORIZED COMMANDS
SI-4	SI-4 (3)	AUTOMATED TOOL INTEGRATION
SI-7	SI-7 (5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS
SI-7	SI-7 (10)	PROTECTION OF BOOT FIRMWARE
SI-7	SI-7 (15)	CODE AUTHENTICATION
SI-10	SI-10	INFORMATION INPUT VALIDATION
SI-10 (3)	SI-10 (3)	PREDICTABLE BEHAVIOR
SI-10 (5)	SI-10 (5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS
SI-16	SI-16	MEMORY PROTECTION
SI-17	SI-17	FAIL-SAFE PROCEDURES

RUNSAFE SECURITY

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security is the pioneer of a unique cyberhardening technology designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Based in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the Industrial Internet of Things (IIoT), critical infrastructure, automotive, and national security industries.

RunSafeSecurity.com

571.441.5076

Sales@RunSafeSecurity.com