CAPSULE8'S FEDRAMP CAPABILITIES

Supporting your Federal Risk and Authorization Program (FedRAMP) projects with enterprise Linux infrastructure protection in any environment at any scale

- Malicious code protection via non-signature detection mechanisms, memory protection, and detection of unwanted code execution
- Integrity verification to detect unauthorized changes to critical system files that helps power incident response
- Automated response against unwanted activity, including remote access, programs, and file execution, with the ability to define allowlists

NIST 800-53's Control Families C8 Covers


Access Control (AC)


Configuration Management (CM)


Risk Assessment (RA)


Systems & Information Integrity (SI)

Capsule8 aligns with the controls laid out in NIST SP 800-53 R4 for Access Control, Configuration Management, Risk Assessment, and Systems and Information Integrity. Meeting these strict requirements demonstrates Capsule8's mission of supporting our customers in any environment by detecting unwanted activity and upholding systems resilience. For customers subject to FedRAMP, you can gain confidence that your Linux infrastructure is protected as part of your FedRAMP projects.

Capsule8 helps you meet the following FedRAMP requirements in your Linux infrastructure pertaining to Access Control (AC), Configuration Management (CM), and Risk Assessment (RA):

- **Session Termination – AC-13:** Capsule8 can automatically kill processes associated with user sessions exhibiting unwanted or unauthorized activity.
- **Remote Access – AC-17 (1, 4, 9):** Capsule8 detects remote interactive shells and execution of privileged commands, with the ability to shut down either activity automatically.
- **Least Functionality – CM-7 (2, 4, 5):** Capsule8 detects the execution of unwanted or programs and enables program allowlists and denylists.
- **Vulnerability Scanning – RA-5:** Capsule detects kernel and userland exploitation of vulnerabilities, and monitors critical system, configuration, and content files.

Talk to your Capsule8 representative to learn more about our FedRAMP support, or reach out via support@capsule8.com

For more information:
info@capsule8.com
capsule8.com
@capsule8

CAPSULE8

COMPLIANCE OVERVIEW

Capsule8 detects unwanted activity in enterprise Linux infrastructure, including activity that can compromise the integrity of the systems that underpin your organization's operations. Our distributed host agent collects system telemetry to trigger detection policies and automated response actions, as well as to enforce allowlists and denylists.

As a result, Capsule8 helps you meet the following FedRAMP requirements for Systems and Information Integrity (SI) in your Linux infrastructure:

- **Malicious Code Protection – SI-3:** Capsule8 detects unwanted system activity and can automatically respond to malicious behavior. Capsule8's detection policies can be configured based on your unique environment to minimize false positives and incorporate new threat intelligence.
- **Nonsignature-based Detection – SI-3 (7):** Capsule8's default detection provides nonsignature-based malicious code detection mechanisms, analyzing host telemetry to identify system behaviors indicative of unwanted activity.
- **System-generated Alerts – SI-4 (7):** Capsule8 generates alerts about incidents and security-relevant events that can be consumed through the optional Capsule8 UI.
- **Host-based Devices – SI-4 (23):** All of Capsule8's components report their health status, including telemetry reception, analytics processing, and control message reception status.
- **Software, Firmware, and Information Integrity – SI-7:** Capsule8's file-based policies can be used to detect unauthorized changes to /boot/, /lib/, and binary directories.
- **Integration of Detection and Response – SI-7 (7):** Capsule8 detects unauthorized privilege escalation, as well as modification to files in /etc/ as per NIST's supplemental guidance.
- **Code Execution in Protected Environments – SI-7 (13):** Capsule8 detects execution of new files, along with malicious code execution such as system exploitation. Capsule8 can also enforce allowlists and denylists on programs and other behavior.
- **Memory Protection – SI-16:** Capsule8 protects system memory against exploitation or other unauthorized code execution, including detection of memory corruption, kernel exploitation, disabling of processor-level protections, container escapes, and more.

CAPSULE8

Ask your Capsule8 representative for more information about our FedRAMP capabilities.

For more information: info@capsule8.com
https://capsule8.com
@capsule8