Synack

SOLUTION BRIEF

Continuous Penetration Testing that's FedRAMP Authorized at the Moderate Level

Moderate impact level gives government agencies ability to perform dedicated application security testing to meet M-22-09

Agencies enabled to conduct pentests in a FedRAMP Moderate Authorized Environment

Continuous penetration testing is a vital offensive security practice for federal agencies to reduce vulnerabilities and cyber risk. By achieving the FedRAMP Moderate Authorized status, Synack is empowering agencies to address the cyber talent gap by easily leveraging its continuous security testing SaaS platform powered by a network of elite and vetted security researchers to uncover and remediate the vulnerabilities that matter most.

The designation of choice for federal agencies

Synack's FedRAMP Moderate designation sets a new bar for security, data privacy and compliance in the continuous security testing market. FedRAMP offers four impact levels with different kinds of risk. As shown below, the difference in requirements between a LI-SaaS and Moderate level designation are significant.

LEVEL	LI-SAAS	MODERATE
Stated purpose	LI-SaaS is for low-risk, low-cost services (i.e. collaboration tools)	Moderate Impact systems are for services handling low to moderately risky government data, including PII or non public information
Number of controls	<= 150 NIST 800-53 controls	325 NIST 800-53 controls
Types of authorized systems	Limited PII: Authentication only	For Official Use Only (FOUO) Controlled Unclassified Information (CUI)
Network access for government applications	External only	External and Internal

Synack & the FedRAMP Moderate Authorized Level: Highest designation achieved

FedRAMP provides a standardized process for security assessment, authorization and monitoring of cloud service offerings. Organizations are granted authorizations at four impact levels: Low-Impact Software-as-a-Service (LI-SaaS), Low, Moderate and High.[1] Synack has achieved the highest FedRAMP baseline level of any continuous security testing provider. The rigorous nature of the Moderate level FedRAMP security assessment speaks for itself.

Synack takes pride in having met the required 325 NIST 800-53 controls aligned with the Moderate impact level, as this has empowered numerous federal agencies to procure continuous penetration testing in a cloud-first environment with greater confidence and ease. Additionally, Synack's designation can aid government orgs in saving 30-40%[2] of government cost, time and effort. Agencies can now leverage Synack's security assessment through the FedRAMP Marketplace and reduce duplicative risk management efforts.

[1] Synack achieved the Moderate Authorized designation on December 19, 2023, enabling operation as a FedRAMP-certified provider.
[2] https://olao.od.nih.gov/content/fedramp

COMMON USE CASES FOR THE SYNACK PLATFORM	
Penetration testing	On-demand and continuous pentesting that scales with you. Powered by the elite expertise of the SRT and the Synack Testing Platform
Compliance-driven testing	Check for common and critical vulnerabilities and deliver proof-of-work reports to compliance auditors for frameworks like PCI, HIPAA, FISMA and more
Zero day response	Activate researchers for urgent vulnerabilities like Log4Shell and Spring4Shell. Receive detailed reports on your susceptibility to specific zero days and CVEs
API security testing	Synack provides an adversarial perspective on your API attack surface
Cloud security	Tests for external misconfigurations and dynamic changes to your public and private assets with rigorous assessments by skilled cloud researchers
Application security	Receive actionable feedback on vulnerabilities throughout the development cycle with testing that adapts to your developers' cadence and needs
Vulnerability management	End-to-end vulnerability management with Synack pentesting enabled by platform features and third-party integrations

Five ways federal agencies save costs and time with a FedRAMP Authorized Provider

1. FISMA and NIST compliance
Agencies are required to maintain FISMA compliance, and for those working with Cloud Service Providers, FedRAMP provides a highly efficient path to reaching compliance. Many of the NIST 800-53 controls in FedRAMP overlap with those required by FISMA, which means you don't have to spend extra resources implementing these controls with vendors.

2. Data security
Unlike FedRAMP LI-SaaS, FedRAMP Moderate is built for companies handling both external and internal government applications. If an agency is testing assets with sensitive data, they should be working with providers at the Moderate level.

3. Risk mitigation
A security assessment at the Moderate level contains 3x the security controls than those covered by the ISO 27001 certification and SOC 2 compliance. These steps provide assurance that Synack is handling your data and the penetration testing process with extra care.

4. Quick procurement for federal agencies
By leveraging Synack's Moderate Authorized designation under the FedRAMP program, agencies may reduce costs, time and staff needed to activate and deploy critical security testing technology.

5. Continuous monitoring
In order to comply with FedRAMP, software providers must continuously monitor certain controls and go through an annual assessment, which ensures you are always working with a fully-compliant testing provider.

Steps to getting started with Synack's FedRAMP Moderate Authorized environment

- **Step 1:** Locate Synack's Authorized listing in the FedRAMP Marketplace.

  Submit the FedRAMP Package Access Request Form.

- **Step 2:** Conduct a package review and risk analysis.

  Federal agencies can leverage the security authorization packages to grant a security authorization at their own agency.

To learn more about Synack's FedRAMP environment or security testing solutions for your cybersecurity team, contact your Synack representative or reach out to **federal@synack.com**.