SYNACK BRINGS SCALABLE, CONTINUOUS PENTESTING TO FEDRAMP

IN PROCESS MODERATE IMPACT LEVEL DESIGNATION ENABLES FEDERAL AGENCIES TO IMPROVE SECURITY POSTURE

Synack for Federal Agencies

Continuous pentesting is a vital offensive security practice for federal agencies to reduce vulnerabilities and cyber risk. By achieving the FedRAMP In Process status, Synack empowers agencies to address the cyber talent gap by easily leveraging its on-demand security testing platform powered by a network of elite and vetted security researchers to uncover and remediate the vulnerabilities that matter.

The FedRAMP Moderate Level & Synack

FedRAMP is a U.S. Government-wide program that 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 level of security of any crowdsourced security testing provider. The rigorous nature of the Moderate level FedRAMP security assessment speaks for itself. Additionally, Synack's designation can save 30–40 percent[2] of government cost, time and effort. Agencies can now leverage Synack's single security assessment through FedRAMP and avoid duplicative risk management efforts.

Five Ways Federal Agencies Save Costs and Time with a FedRAMP In Process Provider

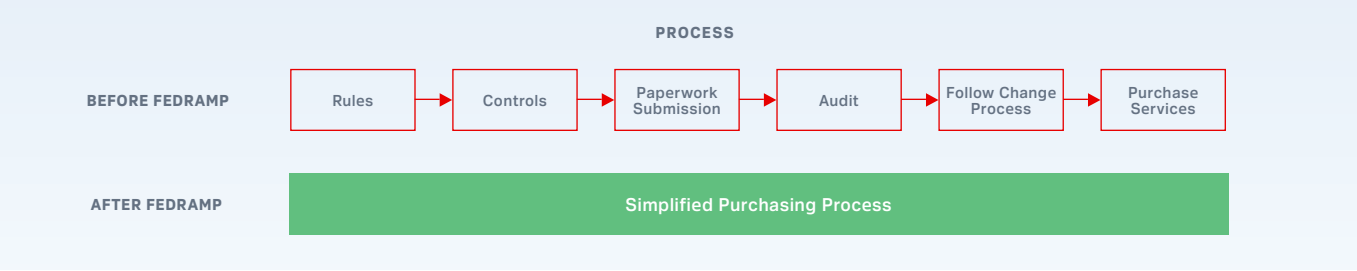
1. FISMA Compliance
Agencies are required to maintain FISMA compliance, and for those working with Cloud Service Providers, FedRAMP provides a highly efficient path to reaching compliance. Many of the NIST 800-53 controls in FedRAMP overlap with those required by FISMA, which means you don't have to 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 in an ISO 27001 certification. These steps provide assurance that Synack is handling your data and the pentesting process with extra care.

4. Easy and Quick Procurement for Federal Agencies
By leveraging Synack's In Process Moderate 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.

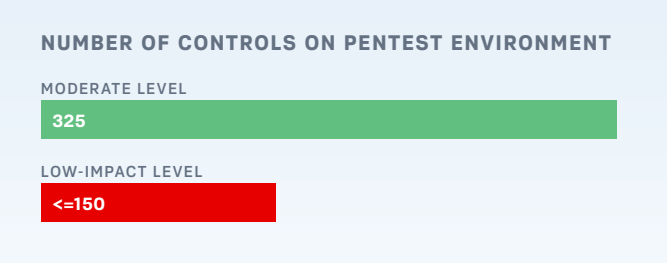


1. As of February 2022, Synack achieved the In-Process designation, which allows full operation as a FedRAMP-certified provider.
2. https://olao.od.nih.gov/content/fedramp

The Designation of Choice for Federal Agencies

Synack's FedRAMP Moderate designation sets a new bar for security, data privacy and compliance in the crowdsourced security testing market (CST). 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)	MI-SaaS is 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 Data	Limited PII: Authentication only	For Official Use Only (FOUO) Controlled Unclassified Information (CUI)
Network Access for Government applications	External only	External and Internal



Not all penetration testing solutions offer the same level of data security

Get Started with Synack FedRAMP Moderate Environment[1]

As an agency purchaser, please adhere to the following steps:

Step 1: Locate Synack's "In Process" listing in the FedRAMP Marketplace
Synack completed the security assessment process with a 3PAO using a standardized set of requirements in accordance with FISMA, using a baseline set of NIST 800-53 controls.

Step 2: Conduct a package review and risk analysis
Federal agencies can view security authorization packages in the FedRAMP Marketplace[2] and leverage the security authorization packages to grant a security authorization at their own agency.

Step 3: Issue an ATO, enabling agency access to Synack for ongoing, continuous monitoring
All the federal agency's data is held in a FedRAMP environment to ensure compliance with FISMA and proper handling of external and internal information.

Step 4: Federal agency oversees Synack's continuous monitoring activities
Once an Authority to Operate (ATO) has been granted, the agency will oversee security artifacts submitted by Synack. This includes any major system changes that could affect security controls as well as an annual risk assessment, penetration testing and vulnerability scanning results.

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

1. https://www.fedramp.gov/assets/resources/documents/Reusing_Authorizations_for_Cloud_Products_Quick_Guide.pdf
2. https://marketplace.fedramp.gov/#!/products?sort=productName

Synack, Inc.
855.796.2251 | www.synack.com | info@synack.com