Tenable FedRAMP FAQ

Frequently Asked Questions about FedRAMP in Tenable Products

Last Revised: April 15, 2024

Tenable FedRAMP FAQ

Q: *What is FedRAMP?*

- **A**: The Federal Risk and Authorization Management Program (FedRAMP) is a program the U.S. federal government uses to determine whether cloud products and services are secure enough to be used by federal agencies. It provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. For more information, see the *Tenable Vulnerability Management User Guide*.

Q: *Is Tenable FedRAMP Authorized?*

- **A**: Yes, Tenable is **Authorized** on FedRAMP Marketplace.

Q: *Why is FedRAMP important?*

- **A**: Cloud computing continues to evolve and revolutionize the way businesses operate. As U.S. federal agencies focus on modernizing their IT infrastructure with the adoption of cloud computing, security is a top priority. FedRAMP was established to minimize the risk federal agencies face when adopting cloud computing. FedRAMP is the first government-wide security authorization program and it is important for several reasons, including:
    - It offers a standardized framework to save federal agencies time, effort and money when assessing security.
    - It increases consistency and confidence in the security of cloud solutions using NIST and FISMA defined standards.
    - It promotes transparency between US government and cloud providers.
    - It accelerates the adoption of secure cloud solutions through reuse of assessments and authorizations.
    - It ensures consistent application of existing security practice.
    - It increases confidence in security assessments.
    - It increases automation and near real-time data for continuous monitoring.

Q: *Is FedRAMP mandatory?*

- **A**: FedRAMP is mandatory for all Executive Agency cloud deployments and service models at the low, moderate, and high risk impact levels. Many federal, state, and local agencies seek FedRAMP authorized cloud providers in an effort to reduce risk in cloud adoption. Commercial/Enterprise customers seeking their own FedRAMP authorization also require the use of FedRAMP solutions within their own technology stacks. For more information, see the FedRAMP Policy Memo.

Q: *What are the types of FedRAMP compliance?*

- **A**: CSPs can become FedRAMP compliant in two ways:
    - **JAB Authorization**: To receive FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO), a CSP is reviewed by the FedRAMP Program Management Office (PMO), assessed by a FedRAMP-accredited 3PAO, and receives a P-ATO from the JAB. The JAB is made up of the Chief Information Officers (CIOs) from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA).
    - **Agency Authorization**: To receive FedRAMP Agency Authority to Operate (ATO), a CSP is reviewed by a customer Agency CIO or Delegated Authorizing Official(s) to achieve a FedRAMP-compliant ATO that is verified by the FedRAMP Program Management Office (PMO).

Q: *What does Agency Authorization to Operate (ATO) mean? How do other agencies become authorized?*

- **A**: An ATO is a type of FedRAMP authorization where a cloud service provider works directly with an agency partner to complete the security assessment and authorization. Each Agency must undergo their own ATO.

  Once FedRAMP Authorization is achieved with one agency, the security package is available for other agencies to reuse. Each agency deploying Tenable cloud products must undergo their own ATO. However, because we have already achieved the FedRAMP Authorized designation, the process is greatly simplified for new agencies. New agencies can simply request access to our security package, review the package and issue their own ATO for our products.

It is important to note that some agencies may have specific requirements above the requirements in our existing FedRAMP security package.

Q: *What is the FedRAMP boundary?*

- A: The FedRAMP authorization boundary encompasses all technologies, external and internal services and leveraged systems and accounts for all federal information data and metadata that a CSO is responsible for. The FedRAMP boundary can include a Cloud Service Provider's CSP core services as well as surrounding solutions that support the core solution.