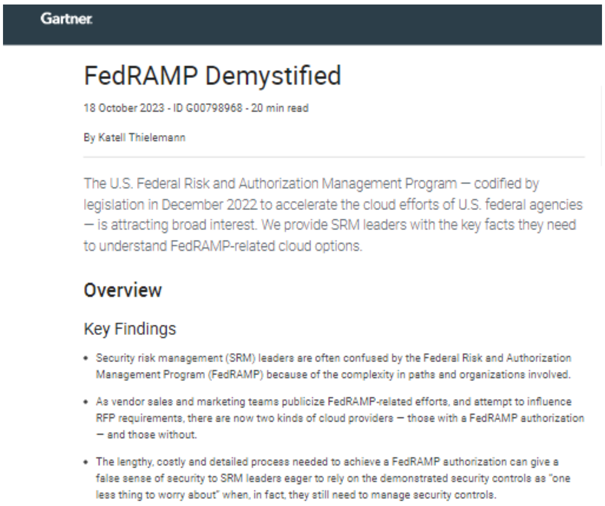
Gartner® Report: FedRAMP Demystified



FedRAMP Demystified

18 October 2023 - ID G00798968 - 20 min read

By Katell Thielemann

The U.S. Federal Risk and Authorization Management Program — codified by legislation in December 2022 to accelerate the cloud efforts of U.S. federal agencies — is attracting broad interest. We provide SRM leaders with the key facts they need to understand FedRAMP-related cloud options.

Overview

Key Findings

- Security risk management (SRM) leaders are often confused by the Federal Risk and Authorization Management Program (FedRAMP) because of the complexity in paths and organizations involved.
- As vendor sales and marketing teams publicize FedRAMP-related efforts, and attempt to influence RFP requirements, there are now two kinds of cloud providers — those with a FedRAMP authorization — and those without.
- The lengthy, costly and detailed process needed to achieve a FedRAMP authorization can give a false sense of security to SRM leaders eager to rely on the demonstrated security controls as "one less thing to worry about" when, in fact, they still need to manage security controls.

How can government agencies, leveraging cloud transformation and hybrid work scenarios for efficiency, engage in their digital transformation without sacrificing security? The answer is Federal Risk and Authorization Management Program (FedRAMP) – an independent review process based on security standards and controls. FedRAMP is complex, and so is cybersecurity. As per Gartner, to make educated strategic decisions on how to proceed as a security risk management leader, it's important to understand the FedRAMP process and a few key concepts: the players, the available cloud security levels and controls, the Authority to Operate (ATO) paths, and the pros and cons. This Gartner® report lays out the key facts that security risk management (SRM) leaders need to understand FedRAMP-related cloud options.