Assessing the security of mission-critical systems in the cloud

FedRAMP Assessment Services

AT A GLANCE

Virtustream, an enterprise-class cloud software and service provider, was supporting the U.S. Department of the Interior (DOI) Financial and Business Management Systems (FBMS) as it migrated its mission-critical application systems to its high-performance federal cloud.

virtustream

CLIENT CHALLENGE

The goal of the migration was to provide significant flexibility while meeting the department's stringent requirements for high availability of data and applications. To assure the highest level of security was met, Virtustream selected Coalfire, a leading FedRAMP Third Party Assessment Organization (3PAO), as the assessor for this DOI FedRAMP Agency Authority to Operate (ATO).

Through the course of the relationship, Virtustream identified a need to upgrade from the FedRAMP Agency ATO to the FedRamp Joint Authorization Board (JAB) Provisional ATO (P-ATO).

APPROACH

With the NIST Special Publication 800-53 Revision 3 (FedRAMP v1) as a guide, Coalfire used recent versions of documentation (system security plan [SSP], policies, procedures, and asset list) to develop a customized Security Assessment Plan (SAP), which included:

- Test processes
- Scope (databases, websites, IP addresses)
- Automated/manual tests to be performed
- Physical locations
- Types of roles/accounts to be tested
- Changes required for the network (virtual LAN, IP addresses, intrusion detection systems, firewalls)
- Where credentials would be used
- Privileges to be used and assessed
- Type of sampling needed

Prior to beginning the assessment, Coalfire submitted the SAP to the FedRAMP Project Management Office (PMO). Once validation for readiness was received from the FedRAMP PMO, Coalfire:

- Conducted technical tests and vulnerability scans – specifically network/OS, database, and web scans – across the enterprise infrastructure.
- Led penetration tests (external-to-target, tenant-to-tenant, and portal-to-management) to ensure that the solution was properly protected, areas with possible operational or security impacts were carefully planned, and risks were appropriately mitigated and documented.
- Prepared documents for submission for review by the DOI's certified information systems security officer (CISSO).

To manage the project, Coalfire implemented an integrated set of tools through proven methodologies and industry best practices, including Project Management Institute's Project Management Body of Knowledge (PMBoK) principles inclusive of project charter, schedule, and projected percent-completed metrics. Coalfire's project management approach enabled the project to meet deadlines and mitigate risks. Throughout the engagement, Coalfire provided status reports that summarized the activities performed, planned activities, issues/concerns, and expended labor hours.

Following the successful DOI implementation, Virtustream upgraded their system to meet the assessment criteria of the FedRAMP JAB, which Coalfire assessed as the 3PAO, and achieved a P-ATO. As part of JAB acceptance, the test results were reviewed by security officers from the General Services Administration (GSA), Department of Defense (DoD), and Department of Homeland Security (DHS). JAB reviews are known to be rigorous and require a briefing of the cloud service provider's security posture.

In subsequent years, Coalfire assured that Virtustream met continuous monitoring obligations and assisted with the transition from the NIST 800-53 Rev. 3 to Rev. 4 (FedRAMP v2) baseline. For continuous monitoring Coalfire examined changes to the SSP, baseline configurations, and the Plan of Actions and Milestones (POA&M) from earlier assessment efforts.

CS_FedRAMP-Virtustream_011917

RESULTS

Through Coalfire's efforts, the DOI cloud system achieved the initial internal DOI FedRAMP ATO. To upgrade to the FedRAMP P-ATO, Virtustream completed remediation of high vulnerabilities and performed continuous monitoring activities. Coalfire performed the continuous monitoring assessment for the transition to the FedRAMP v2 baseline that upgraded Virtustream to the latest compliance guidelines and FedRAMP PMO requirements.

In 2015, EMC acquired Virtustream to expand its presence and range of offerings (under the Virtustream brand) in the growing cloud computing domain.

About Coalfire

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe.
www.coalfire.com

COALFIRE