Red River

aws PARTNER

CYBERSECURITY

CASE STUDY

CMMC Compliance Case Study

Red River Enables CMMC Compliance for CPA Firm Supporting Federal Agencies

CHALLENGE

Kearney & Company is a financial firm dedicated to assisting the federal government with improving its overall financial operations while increasing accountability and transparency. As a CPA firm for several large federal agencies, Kearney needed to meet the requirements set by the Cybersecurity Maturity Model Certification (CMMC). Managed by the Department of Defense, CMMC compliance is a tiered system of compliance measures, which are ultimately intended to evaluate the maturity of the organization's cybersecurity systems, processes, and contingencies. It was introduced in 2020, refined in late 2021 and will be fully required by 2026. Kearney & Company turned to Red River, their long-term managed services provider, for designing a solution and strategy for CMMC compliance.

As a trusted MS partner with experience in CMMC compliance and adoption, Red River designed a solution leveraging AWS GovCloud and stackArmor.

SOLUTION

With a deep understanding of Kearney's infrastructure, Red River was already managing the Kearney environment with CMMC compliant platforms and toolsets. This provided a secure foundation toward complete CMMC compliance.

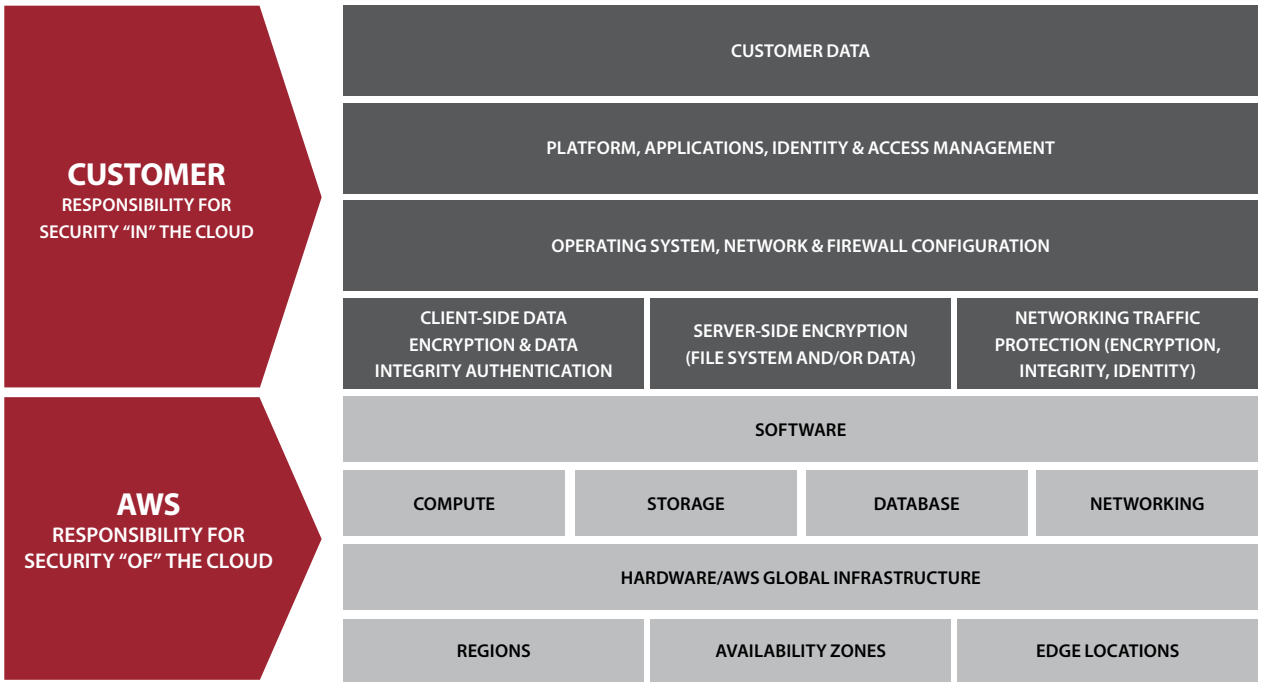
Red River was quickly able to build an enclave in AWS GovCloud to meet CMMC requirements. This isolated any access to their environment by limiting it to only US Regions (East and West). This enclave also ensured that any workloads handling Controlled Unclassified Information (CUI) would be managed with physical access controls that are isolated to US citizens and that the data would be stored on FIPS 140-2 compliant storage.

Red River also leveraged stackArmor's compliance accelerator ThreatAlert within the CMMC solution. ThreatAlert enables continuous monitoring and ensures that all the customer data stays within the Kearney environment.

Finally, a management enclave was created that is used for the management and monitoring of the Kearney infrastructure. This toolset includes DUO, Kaseya, Science Logic, Delinea, and the FedRAMP'd version of ServiceNow. This platform is weighed against the same compliance requirements to ensure that it is CMMC compliant. Significant training is required by the Red River Managed Services teams to even gain access to this management platform. AWS Workspace instances are created and locked down for each person supporting our customers. All personnel that have access, are US citizens.

RESULTS

Through the Red River solution, the environment now has a clear delineation when it comes to inherited, shared and customer specific controls. This shared responsibility model means that aspects such as physical or environmental controls (inherited) are now clearly the responsibility of AWS. Items such as patch management, configuration management, or awareness and training fall under shared controls. This shared responsibility model (see model below) relieves Kearney of tedious operational obligations by allowing AWS to operate and control many of the security components from the host operating system. The inclusion of ThreatAlert added even more visibility and monitoring controls over their environment.



By leveraging Red River's cyber and managed services expertise, Kearney & Company was able to seamlessly deploy a solution that leveraged compliant cloud technology with minimal operational interruption and an accelerated onboarding timeline.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, cybersecurity, infrastructure, collaboration and cloud solutions. Learn more at **redriver.com**.