Case study

INFOVISION
#AccelerateDigital

Enabling FedRAMP compliance with infrastructure security solutions

InfoVision successfully transformed a leading US-based multinational cloud communications provider's security infrastructure to achieve FedRAMP compliance. By implementing a suite of Qualys Cloud solutions, including VMDR (Vulnerability Management Detection & Response), Policy Compliance, File Integrity Monitoring (FIM), and Container Security, the project not only met stringent federal requirements but also significantly enhanced the client's overall security posture.

About the customer

The customer is a leading multinational technology company specializing in cloud communications and workstream collaboration solutions. Their core offerings include Unified Communications as a Service (UCaaS), Contact Center as a Service (CCaaS), and Communications Platform as a Service (CPaaS). The company serves global enterprises with cutting-edge cloud communication solutions and is known for its innovation in workstream collaboration and customer engagement.

Why is FedRAMP compliance important?

- Enhanced security posture
- Government contract opportunities
- Customer trust
- Competitive advantage
- Streamlined compliance
- Data protection

Business need

The client faced a challenge in meeting FedRAMP (Federal Risk and Authorization Management Program) compliance requirements. To achieve this, they needed to migrate from their existing tenable solution to a more robust security infrastructure.

Key drivers for this transition included:

- Ensuring compliance with stringent federal security standards.
- Enhancing overall security posture to protect sensitive data.
- Maintaining customer trust and stakeholder confidence.
- Enabling the provision of secure and compliant services to government and enterprise customers.

Solution delivered

InfoVision implemented a comprehensive Infrastructure Security Services solution, leveraging Qualys cloud technologies.

Advanced Vulnerability Management

Deployed Qualys VMDR (Vulnerability Management, Detection, and Response) for real-time threat detection and response across the client's infrastructure.

File integrity assurance

Integrated Qualys File Integrity Monitoring (FIM) to detect unauthorized changes to critical system files and configurations.

Continuous Compliance Monitoring

Implemented Qualys Policy Compliance (PC) to ensure ongoing adherence to FedRAMP standards.

Container security enhancement

Utilized Qualys Container Security (CS) to secure containerized environments, crucial for the client's cloud-based services.

Implementation strategy

Infrastructure assessment
Conducted a thorough evaluation of the existing infrastructure to identify security gaps.

Security hardening
Implemented best practices to strengthen the overall infrastructure security.

Custom deployment
Tailored the Qualys solutions to the client's unique cloud environment.

Automation integration
Set up automated scanning and reporting processes to streamline security operations.

Agent installation
Deployed Qualys agents across Windows and Linux servers for comprehensive coverage.

Tech stack

Security platform:
Qualys Cloud Solutions – VMDR, FIM, PC, CS

Cloud security:
Secure agents for both Windows and Linux environments

Compliance framework:
FedRAMP, ISO 27001

Key outcomes

- Achieved **FedRAMP compliance.**
- Enhanced real-time visibility into infrastructure vulnerabilities, **reducing the average time to detect threats.**
- Implemented continuous monitoring, resulting in a **reduction in security incidents.**
- Streamlined compliance reporting, **cutting audit preparation time.**