Axonius Federal SaaS Architecture

Overview

The architecture depicted illustrates the secure deployment model for the Axonius Federal Software-as-a-Service (SaaS) platform, hosted within an AWS customer environment. This model ensures alignment with **FedRAMP security baselines** and applicable compliance frameworks, providing secure, centralized asset management capabilities across both on-premises and cloud-based environments.

Organizational Internal Network

- **Internal Systems:** The organization's internal infrastructure, including servers, applications, and network devices, is depicted within the internal network boundary.
- **Axonius Gateway:** A dedicated gateway node resides within the organization's boundary to securely facilitate communication between on-premises systems and the Axonius SaaS platform.
- **Transport Security:** All communications between the internal environment and Axonius are conducted over **TCP port 443 (HTTPS)** utilizing TLS encryption, ensuring confidentiality and integrity of transmitted data in accordance with FedRAMP requirements.

Cloud Solutions

- **External Cloud Integrations:** The architecture supports integration with external cloud service providers (e.g., IaaS, PaaS, SaaS). These integrations are achieved via approved APIs and are represented in the architecture as "Cloud Solutions."
- **Axonius Gateway:** A dedicated gateway node resides within the organization's boundary to securely facilitate communication between cloud environments and the Axonius SaaS platform.
- **Data Flow:** All communications between the cloud environments and Axonius are conducted over **TCP port 443 (HTTPS)** utilizing TLS encryption, ensuring confidentiality and integrity of transmitted data in accordance with FedRAMP requirements.

Axonius Federal SaaS Instance

- **Hosting Environment:** The Axonius Federal SaaS instance is hosted within **AWS GovCloud (U.S.)**, ensuring compliance with FedRAMP boundary requirements.
- **Axonius GUI:** The user-facing web interface provides authorized personnel with access to dashboards, reporting, and asset correlation functions.

- **Adapters:** Multiple integration adapters are deployed within the Axonius SaaS instance. These adapters interface with various security and IT systems (e.g., vulnerability scanners, endpoint detection tools, identity management systems) to aggregate and normalize asset data.
- **Assets Database:** A centralized, secure database stores all collected and correlated asset data. Data at rest is encrypted in compliance with **FIPS 140-2 validated cryptographic modules**, ensuring confidentiality and integrity.
- **Customer Environment Boundary:** The SaaS instance resides within the customer-designated environment boundary, protected by AWS security controls, Axonius application-level controls, and organizational access management policies.

Security and Compliance Considerations

- **Encryption in Transit:** All data exchanges (internal, cloud, and SaaS) utilize TLS 1.2/1.3 to maintain compliance with FedRAMP and NIST SP 800-53 control requirements (SC-12, SC-13, SC-28).
- **Authentication and Authorization:** Access to the Axonius GUI and adapters requires multi-factor authentication (MFA) and role-based access control (RBAC) in compliance with FedRAMP identity management controls (IA family).
- **Boundary Protection:** The architecture enforces strict separation of customer data, with inbound and outbound connections restricted to approved endpoints and services.
- **Audit and Monitoring:** All system activity is logged, monitored, and stored in compliance with **FedRAMP audit requirements (AU family)**.