WHITEPAPER

MuleSoft™

Anypoint Platform Cloud Security & Compliance

Overview

Security is a top concern when evaluating cloud services, whether it be physical, network, infrastructure, platform or data security. MuleSoft's Anypoint platform is designed to be a secure platform for our customers. The Anypoint platform spans SOA, SaaS Integration and APIs. This whitepaper covers the security and compliance of MuleSoft's cloud services, namely CloudHub and API Manager.

Our approach to cloud security is two-pronged: (a) we do not inspect, permanently store, or otherwise interact directly with sensitive customer data; (b) we provide a highly secure environment in which customers can perform sensitive data manipulations. MuleSoft's dedicated security team ensures our ongoing cloud security and compliance by following industry best practices, running internal security audits and establishing policies that span operations, data security, passwords and credentials, facilities and network security and secure connectivity.

Operations

Our goal is to provide a secure platform where customers can operate, while giving customers the freedom and confidence to do so without our examination or intervention. In order to do this, MuleSoft follows industry best practices for operational processes to provide a secure environment for customers. These include, but are not limited to:

- Comprehensive security policies
- Least privilege access
- Secure virtual private cloud environments
- Regular application and network penetration testing and vulnerability scanning
- Regular external reviews of our security program and audits of adherence to security compliance standards
- Logging and alerting of platform-level security events
- Strong authentication for administrative sessions
- Secure software development lifecycle (SLDC) methodology and standards
- Security incident response and disaster recovery procedures
- Tight controls and restrictions on administrative rights

Data Security

When the Anypoint platform is run as a cloud service, MuleSoft transmits data for customers, though we are data agnostic. MuleSoft does not inspect, permanently store, or otherwise interact directly with customer payload data. MuleSoft understands that the data our customers are transmitting should be treated carefully to mitigate any security risks. To this end, our customers maintain control over their data, configuration and workers.

MuleSoft may collect monitoring, analytics or log data from Mule instances. A Mule instance here refers to both CloudHub workers and Mule ESB cores, as both CloudHub and API Manager have connectivity to Mule instances for monitoring. Customers may initiate actions on Mule instances from the cloud. All communication between MuleSoft's cloud and Mule instances is secured using SSL with client certificate authentication. This ensures unauthorized parties cannot read data and that they cannot initiate unauthorized actions.

CloudHub workers provide a secure facility for transmitting and processing data by giving each application their own virtual machine. This ensures complete isolation between tenants for payload security and isolation from other tenant's code.

Passwords and Credentials

All account passwords and credentials are stored in a non-reversible secure format in the database. Data encryption as a feature of the platform can also be enabled. Customers can store credentials for their own services inside the Mule Credential Vault. CloudHub customers can also use the Secure Environment Variables feature to ensure that sensitive configuration, such as passwords or keys, are stored in encrypted form on our servers.

Facilities & Network

Amazon is our cloud provider and the Amazon Web Service (AWS) cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures.

AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). AWS undergoes annual SOC 1 audits and has been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems. AWS infrastructure is in alignment with the following SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC2, PCI DSS Level 1, ISO 27001, and ITAR.

More detail on AWS security can be found here.

Secure Connectivity

MuleSoft's platform includes support for secure protocols and provides tools to build secure services on our platform. MuleSoft recommends that customers use these protocols and tools to secure their services to secure their business. These include, but are not limited to:

- SSL
- PGP payload encryption/decryption
- OAuth2
- WS-Security
- SAML

CloudHub also provides built in security for communication from the cloud to on-premises application, databases, and services using the Secure Data Gateway (SDG) and Virtual Private Cloud (VPC) offerings. SDG makes is possible to connect securely to on-premise applications from the cloud without the need to change firewall policies or proxy servers. VPC is designed to securely handle high-throughput use cases, bringing network level security, increased redundancy and higher availability. CloudHub makes is possible to manage integrations to SaaS and on-premise applications securely, as a part of customers' compliant network.

EU Data Protection Directive

The EU Data Protection Directive places constraints on companies that may transmit data with personally identifiable information (PII), specifying that PII may not leave the EU unless a company is safe harbor certified. Since CloudHub may transmit customer's payload data, these regulations may apply to usage of the CloudHub service.

CloudHub addresses these regulations by providing customers with an EU worker cloud. By using the EU worker cloud, data will never be transmitted outside the EU, ensuring that customers can be compliant with the Data Protection Directive.

For EU users who are transferring PII through CloudHub, they must adhere to adhere to to use the platform in a compliant way:

- Applications must be deployed in the EU worker cloud
- Message replay must not be enabled
- No PII should be logged or used in CloudHub Insight
- All HTTP traffic should be transferred over the eu.cloudhub.io load balancing service. For example, if you created the application "myapp", then its full domain would be "myapp.eu.cloudhub.io." This will ensure that payload data will never be transferred outside the EU when invoking HTTP services.

On-Premise Security

The Anypoint platform can be deployed in the cloud (CloudHub) or on-premise (MuleESB). When you choose to run the Anypoint platform on-premise, MuleSoft does not interact with customers' data at all. Customers configure and run the software themselves and handle all storing, processing and transmitting of data directly, without interference from MuleSoft. As we do not process, store or transmit your data, information security standards are dictated by how the customer's environment is managed. The Anypoint Platform on-premise is a solid part of our customers secure and compliant environments.

More Information

MuleSoft is dedicated to ensuring that customers can meet their security and compliance goals with our platform. For more information or answers to questions about MuleSoft security and compliance, please contact info@mulesoft.com.