Magento Security, Privacy, and Architecture Guide

for Magento Commerce, Magento Order Management, and Magento Business Intelligence

Thank you for putting your trust in Magento. We are committed to our Customers and are sharing information around the architecture, security and privacy measures and processes undertaken with respect to our Magento Commerce (cloud) ("Magento Commerce"), Magento Order Management ("MOM") and Magento Business Intelligence ("MBI") products (collectively the "Services"). This guide does not address Magento Marketplace extensions, Magento Commerce (on-premise) or Magento Open Source.

1. Services Architecture

1.1. Magento Commerce is operated in both a single-tenant and multitenant Platform-as-a-Service ("PaaS") architecture that is designed to segregate and restrict customer data access based on business needs. The architecture provides an effective logical data separation for different customers via customer- specific unique identifiers and allows the use of customer and user role-based access privileges. Providing separate environments for different functions, especially for testing and production, provides additional data segregation.

1.2. MOM and MBI are modular web-based information systems, Software-as-a-Solution ("SaaS") platforms.

1.3. The Services leverage Amazon Web Services' ("AWS") cloud infrastructure, including, but not limited to, its Elastic Compute Cloud (or "EC2") instances, Elastic Load Balancers, ("ELBs"), and Elastic Block Storage ("EBS").

2. Audits and Certifications

2.1. The following security and privacy-related audits and certifications are applicable to the Services:

2.1.1. **PCI**: Magento Commerce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Security Standard, as formulated by The Payment Card Industry Data Security Standards Council ("PCI DSS") as a Service Provider entity or third party agent from a Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Magento's AoC is available upon request from Magento's Support organization. Customers must use Magento PaaS controls and standard configurations to benefit from Magento's PCI DSS AoC.

2.1.2. **Service Organization Control (SOC) reports**: Both Magento Commerce and MOM's information security control environment applicable to each of the Services undergoes an independent evaluation in the form of a SOC 2 (SSAE 18 / ISAE 3402) Security audit. These reports are available upon request from the Magento Support organization.

2.1.3. **EU-U.S. and Swiss-U.S. Privacy Shield Principles**: Magento continues to adhere to the Privacy Shield Principles, despite the invalidation of the EU-US Privacy Shield Program, as a way to affirm Magento's commitment to the privacy principles of the Privacy Shield framework. Magento continues to monitor the evolving legal developments in Europe and will maintain its Swiss certification unless and until Swiss authorities officially invalidate it. Details about Magento's other privacy practices can be found in Magento's Privacy Policy, located at www.magento.com/legal/terms.

3. Security Controls

3.1. The Services include a variety of configurable security controls for the Customer's authorized administrators. These controls include, but are not limited to:

3.1.1. Various user access management controls.

3.1.2. Various password complexity controls.

3.1.3. User access logs for the Customer's instance are available for review and export, where applicable.

3.1.4. Other logical controls.

4. Security Policies/Procedures

4.1. Magento Commerce is operated under a "Shared Responsibility Security Model"; documentation is available upon request from the Magento Support organization. In this model, different parties have different areas of responsibilities for maintaining the security of the system. This approach allows for both flexibility and use of best-of-breed cloud technologies.

4.2. In addition, the Services are operated in accordance with the following policies and procedures to enhance security:

4.2.1. User passwords are not transmitted unencrypted.

4.2.2. User passwords are stored using a salted hash.

4.2.3. Log files for the Customer's instance are available for review and export, where applicable.

4.2.4. Internal system accounts are reviewed on a regular basis.

4.2.5. Logs are stored securely.

4.2.6. Access is logged unless specifically disabled by Customer.

4.3. Although Customers retain the primary responsibility for security monitoring of their production instance(s), Magento, or an authorized third party, will monitor the Services for unauthorized intrusions using intrusion detection mechanisms. Magento may analyze data collected by users' web browsers (e.g. device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including for incident detection and response, to prevent fraudulent authentication, and to determine that the Services function properly.

4.4. All Magento production systems used in the Services, including firewalls, routers, operating system, log information to the respective system log facility or a centralized log collection server in order to enable security reviews and analysis.

5. Web Application Firewall

5.1. Magento has recently begun a rollout of a web application firewall ("WAF") for Magento Commerce. A WAF is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. A WAF is deployed to protect a specific web application or set of web applications. The configuration of the WAF is to block or prevent the Open Web Application Security Project's ("OWASP") top 10 most critical web application security risks.

6. Incident Management

6.1. Magento maintains a security incident management program. Upon detection of a security incident, Magento undertakes an internal investigation and where appropriate, remediation process, up to and including notification to impacted individuals, all in accordance with applicable law.

6.2. Without limiting the above, with respect to the Services, the Customer shall be responsible for any security incident relative to accounts provisioned by the Customer or their respective solutions integrator. For Magento Commerce, Customer shall remain responsible for any security incident caused by, in whole or in part, the Customer's modification or customization of Magento Commerce, any plug-in or non-Magento extension, failure to apply a security patch in a timely manner, or other negligence caused by the Customer or its solution integrator.

7. User Authentication

7.1. The Services allow Customers to customize many logical access management controls to provision and manage access. Access to the Services requires a valid user ID and password combination, which are encrypted via TLS while in transmission. Passwords are hashed and salted and only the hash is stored by the Services.

8. Physical Security

8.1. Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by remote surveillance monitoring, multi-layered access controls, badged access, and are also supported by on- site backup generators in the event of a power failure.

9. Reliability and Backup

9.1. The Services architecture is designed to be highly redundant and reliable. Should a Customer's primary data center encounter a disaster that prevents it from functioning, formal processes are in place to restore the Customer's production-level Services. Customer data submitted to the Services is stored on a primary database server with a replicated copy for high availability and performance. All Customer data submitted to the Services, up to the last committed transaction, is automatically replicated daily to another location. In the event that production facilities for the Services hosting the Customer's primary data center were to be rendered unavailable, redundant hardware, software, and equipment are in place.

10. Data Encryption

10.1. The Services enable Customers to use industry accepted encryption products to protect Customer data and communications during transmissions to the Services.

10.2. Magento offers PCI-DSS compliant encryption for supported payment field types at rest and in transit. At no time does Magento's Services store, transfer, or process cardholder data ("CHD") as defined by PCI.

11. Third Party Functionality

11.1. Magento may use third parties to protect Magento Commerce Customers from Denial of Services ("DDoS") attacks. If an attack occurs, a third party may be used to identify and block malicious online traffic. Information about website traffic and the targeted website may be accessed by the third party to enable these functions.

11.2. Magento's Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on a regular basis. Customers are responsible for conducting vulnerability assessments and/or penetration test on their respective production sites.

12. Processing

12.1. Magento has published its Data Processing Terms, affirming Magento's commitment to privacy, GDPR and to customers. In connection with providing Services to our customers, the Data Processing Terms supplement all existing commercial agreements with Customers for Magento Products and Services and sets forth our obligations around the handling of personal data. All future commercial agreements with Customers carry these same Magento obligations. Magento also shares its list of third party subprocessors that assist Magento in the provision of Magento Products and Services to Customers. Please also refer to www.magento.com/gdpr and www.magento.com/legal/terms for Magento's Privacy Policy and Privacy Shield Privacy Policy.

13. Return/Deletion of Customer Data

13.1. Following termination or expiration of the Customer's subscription to the relevant Services, the Customer has thirty (30) days to access its account and download or export Customer data. Following such thirty (30) day period, Magento will promptly deprovision the Customer environment and all Customer data in Magento systems or otherwise in its possession or under its control shall be subject to deletion.

Last Updated: October 7, 2020