Securing Your Data with MariaDB Enterprise

mariadb.com

Comprehensive Protection for Your Data

Arming Against the Growing Threat

The wave of large-scale cyber attacks across industries has CIOs worried for good reason. Cyber criminals continuously innovate to craft increasingly sophisticated attacks on businesses, governments and non-profit organizations around the world. The potential damage and liability associated with database infiltration is staggering. A recent Forrester survey that the majority of consumers will not conduct business with an organization that they do not believe adequately protects their data, or has a history of compromising customer information. Executives must be on alert.

The sheer volume of sensitive data that organizations need to manage across distributed environments on premises and in the cloud renders perimeter data security safeguards inadequate. Effectively securing data requires protection at every level, including network access, firewalls, disk-level encryption, identity management, and anti-phishing education.

Ultimately, hackers are after the data because it's the data that holds real value. This is why multi-layered database security measures that include access and authentication controls, attack protection, encryption, auditing, and ongoing innovation to address evolving threats must be a core component of the organizational security regimen.

MariaDB Enterprise Security

MariaDB Enterprise, based on the MariaDB Server open source relational database, is a complete data management solution for online transactional processing (OLTP). Given the central role that the database plays in safeguarding sensitive information, MariaDB Enterprise incorporate security into the very fabric of the database. With our MariaDB Security Audit service, we also offer the advice and expertise you need to make the best possible use of those capabilities.

MariaDB leverages a true community contribution model and open source distribution to build security capabilities that makes it among the most secure databases in the world. MariaDB is engineered to protect data without sacrificing great usability or breaking the bank. Because of the vast ecosystem supporting MariaDB combined with the ability to perpetually incorporate new community open source innovations, an investment in MariaDB is future-proof.

MariaDB Enterprise
Data Security Components

Attack Protection and Access Control

MariaDB provides multiple authentication and access control features to protect sensitive data from unauthorized access, and detect and prevent attacks.

PAM Authentication Plugin

The PAM Authentication Plugin provides an authentication framework used by Linux, FreeBSD, Solaris, and other operating systems. PAM enables implementation of various authentication schemes of different complexities, providing the flexibility required to fit database authentication into the existing infrastructure in your organization – for example, authentication using LDAP, SSH passphrases, one-time passwords with SMS confirmation, and system authentication. PAM also allows for combining different authentication models, where either one or all of them are required to succeed in addition to password expiration.

Role-Based Access Control (RBAC)

In larger organizations where a group of users should have the same access privileges based on their role, RBAC empowers IT administrators to manage the privileges of these individuals as a group. Prior to RBAC, the only way to change privileges for a group of users was to make the changes at an individual level. This introduced opportunity for errors and required a time-consuming process to manage a large set of users. Additionally, multiple external users could have been assigned the same database user ID, making it impossible to audit which actual user was responsible for a specific action.

RBAC simplifies managing user privileges. For example, there could be a number of users assigned to a journalist role. Changing the privileges for all the journalists is as simple as changing the role's privileges while ensuring that access control and auditing are still tied to individual user accounts. Most importantly, RBAC ensures that the right roles are accessing the data allowed to them.

Password Management and Validation Plugin

MariaDB's Password Management and Validation Plugins ensure that user passwords meet pre-specified minimal security requirements. The Password Validation Plugin API allows for the creation of password validation plugins customized to special needs and automatically checks user passwords based on these parameters to either accept or reject them. The Simple Password Check Plugin enforces a minimum password length and guarantees that a password contains at least a specified number of uppercase and lowercase letter, digits, and punctuation characters. The CrackLib Password Check Plugin only allows passwords that are strong enough to pass the CrackLib test.

Protection from Application Level Attacks

SQL injections have been a leading cause of data breaches through web application attacks, and MariaDB MaxScale's database firewall filter creates an additional barrier against these kinds of attacks. This filter prevents data damage and unauthorized data access by matching and blocking certain query patterns. The solution also provides the ability to configure patterns to block, including date and time, WHERE clauses, wildcards, regular expression, column matches, or types of queries.

Persistent Connections and Protection from Denial of Service Attacks

MariaDB's MaxScale caches the connections to the database server so that when clients connect to MaxScale, there is minimal latency associated with server side connectivity. Caching connections creates persistent connections. This also throttles the connection to backend servers to avoid too many connections creating an artificial denial of service attack (DDoS) to the database server while sending a flood of connection errors to applications.

Secure Connectors

MariaDB connectors empower customers to successfully integrate MariaDB Enterprise into their organization's broader data management processes. MariaDB provides connectors for JAVA, C/C++ and ODBC. These connectors deliver important security benefits, including SSL, MTM attack prevention, transport layer security, and password protected

Encryption

MariaDB provides encryption for data-at-rest, data in motion, and data-in-use. There are a variety of encryption options, so organizations can tailor encryption measures to best protect their data. Encryption options include:

Native Encryption of Data at Rest

Encrypting tables and logs prevents hackers from accessing sensitive data if they obtain either privileged or physical access to storage media. Security standards also require that System Administrators cannot access sensitive information when accessing the server and storage layer. MariaDB encryption is fully supported for XtraDB and InnoDB, and the Aria storage engine is also supported using default settings. MariaDB affords the database administrator the flexibility to configure encryption for all tablespace and tables, individual tables (capability donated by eperi®), XtraDB and InnoDB log files, and the binary log. MariaDB encryption supports multiple encryption keys as well as automatic key rotation. XtraDB and InnoDB can automatically re-encrypt data from an older to a newer version of the same key.

Encryption Key Management

To maximize encryption effectiveness, encryption keys should reside on a separate system from the data. With MariaDB Enterprise, there are three plugin options for managing encryption keys: 1) MariaDB encryption plugin (file_key_management) available with all MariaDB servers; 2) Amazon Key Management System plugin; and 3) Eperi Key Management System plugin.

SSL Encryption of Data in Motion

SSL Encryption protects data traveling between clients and the MariaDB Enterprise Server as well as between multiple servers connected in a replication topology. Both the MariaDB Enterprise Server and MariaDB MaxScale accept SSL connections. MariaDB Connectors allow applications to connect to databases over an SSL connection as well.

Auditing

MariaDB Enterprise offers features to audit server activity to enable security and compliance monitoring and attack forensics. The MariaDB Audit Plugin logs user activity data on the server. The information logged includes who connected from where to the server, what queries were executed, and what tables were touched.

MariaDB MaxScale includes the Query Log All (QLA) filter, which logs all query content sent through the filter on a per-session basis. MaxScale's extensible plugin interfaces also allow for constructing customized filters to meet a variety of business requirements.

On-Going Innovation to Meet Evolving Threats

Ongoing enhancements, innovations, and testing are conducted by MariaDB and draw from the MariaDB open source ecosystem. Together, these factors make MariaDB Enterprise the most secure database in the world. You'll benefit from:

Community Contribution of New Security Features
The MariaDB development community directly contributes to the innovation of the MariaDB feature set. Some of the largest Internet users in the world contribute to MariaDB, making functionality and benefits highly relevant to the needs of a global client base.

Rigorous Community Testing and Feedback
The software development process for MariaDB also involves extensive testing and feedback from the MariaDB user community. The software installed from MariaDB has been community tested and as a result, hardened against both common and uncommon security threats found in the real world.

Enterprise Monitoring and Query Analysis
Webyog's MONyog Ultimate Monitor delivers monitoring capabilities to MariaDB Enterprise. MONyog is a "DBA in a box" that helps DBAs monitor, manage, tune, and correct problems on their MariaDB based database applications and issues alerts on potential problems before they impact the system. As a result, the productivity of developers, DBAs, and System Administrators improves significantly. MONyog also includes a Query Analyzer that identifies problematic queries.

Patches, Fixes and Security Updates
With MariaDB Enterprise, you have access to security updates for the MariaDB Enterprise Server to ensure that you're always deploying the most stable and secure MariaDB version. We also provide maintenance releases, patches,
and bug fixes.

MariaDB Security Audit Service

The MariaDB Security Audit is a service performed by MariaDB data security experts to examine the security practices on your MariaDB deployment, and identify and correct gaps and weaknesses in database protection. The detailed audit starts with a review of your database security needs and requirements. The team then evaluates access control, automated attack protection, encryption tools and practices, and your forensic capabilities to produce a Database Security Report Card. The team then provides a Compliance and Security plan with actionable recommendations for changes and improvements to ensure the ongoing security of your data.

Speak with a MariaDB Expert about Securing Your Data

Through contribution by a global community and development and support of multiple layers of database security features, MariaDB offers a level of data protection that is unsurpassed in the industry. You can feel confident that MariaDB has and will continue to bring relevant innovation in security to your business and enterprise-grade features and functionality supported by the global team of MariaDB and MySQL experts.

Hackers will be sorely disappointed.

Request to speak to an expert about how MariaDB can protect your critical business data, now and in the future at https://mariadb.com/about/contact

About MariaDB Corporation

MariaDB Corporation is a leader in open-source database solutions for SaaS, cloud, and on-premises applications that require high availability, scalability, and performance. Built by the founder and core engineering team behind MySQL, MariaDB is the database that powers millions of users on sites like Booking.com and Wikipedia. Moreover, MariaDB is the "M" in LAMP, having displaced MySQL as the default database in the Red Hat and SUSE Linux distributions. MariaDB is also included in Pivotal Cloud Foundry, Rackspace and other cloud stacks, and it is the database of choice for IBM POWER8. MariaDB has over 9 million users and customers in more than 45 countries, including global brands such as HP, Virgin Mobile, Booking.com, and Orange.

www.mariadb.com

Americas
sales-AMER@mariadb.com
+1.303.638.3577

Asia Pacific
sales-APAC@mariadb.com
+33.6.80.59.53.51

Europe, Middle East, Africa
sales-EMEA@mariadb.com

Benelux: +358.50.5710528
D.A.CH.: +49.89.220.61124
Denmark: +45.69.918 495
Finland: +358 9.42597815
France: +33.1.82.88.37.38
Italy: +39.02.40.70.82.17
Norway: +47.2.1018944
Sweden: +46.840.838.825
UK & Ireland: +44.20.3355.2937
ME & Africa: +46.72.22.33.444

DS-ENT SEC-031416 – A4