Virgil PureKit

Enable post-compromise protection for stored data with Virgil Security framework and MariaDB database.

Dmitry Dain
Founder & CTO at Virgil Security

Data protection is NOT optional anymore

- Data breaches: 7.9 billion records exposed in 2019
- Acts and laws compliance: GDPR, HIPAA, PCI DSS, CCPA
- High fines: e.g. British Airways — around $230 million

Available solutions for secure data storage

Features	TDE	RDS Encryption	PureKit
Key distribution	Per database	Per database	Per user/client
Key rotation	Database re-encryption required	Database re-encryption required	In-place
Post-compromise security	No	No	Yes
SQL injection secure	No (data is still selected as plaintext)	No (data is still selected as plaintext)	Yes

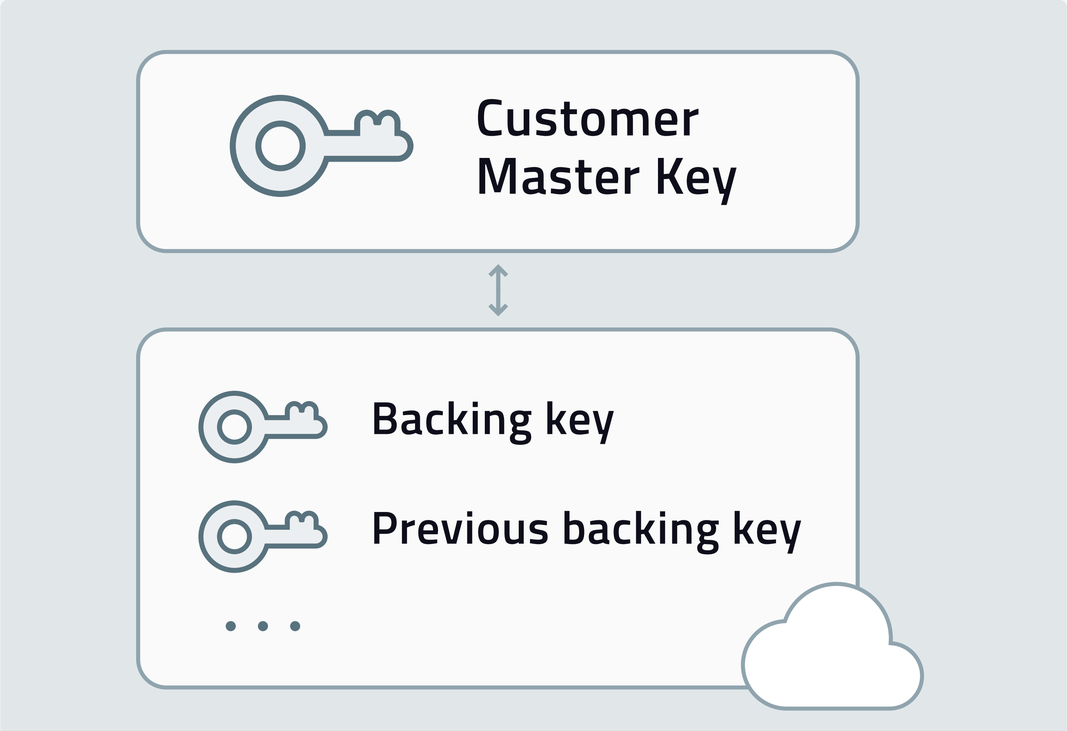
What’s post-compromise security?

Seamless key rotation	• Keys can be rotated while app is running • Proactively or in case of data breach
Data protected even if database is compromised	• Instant stolen data invalidation
Zero-knowledge proof	• Crypto service proves all operations were performed using its private key
Online and offline attacks are not possible	• Strict rate limiting per-user • Both App & Crypto service private keys required to guess password

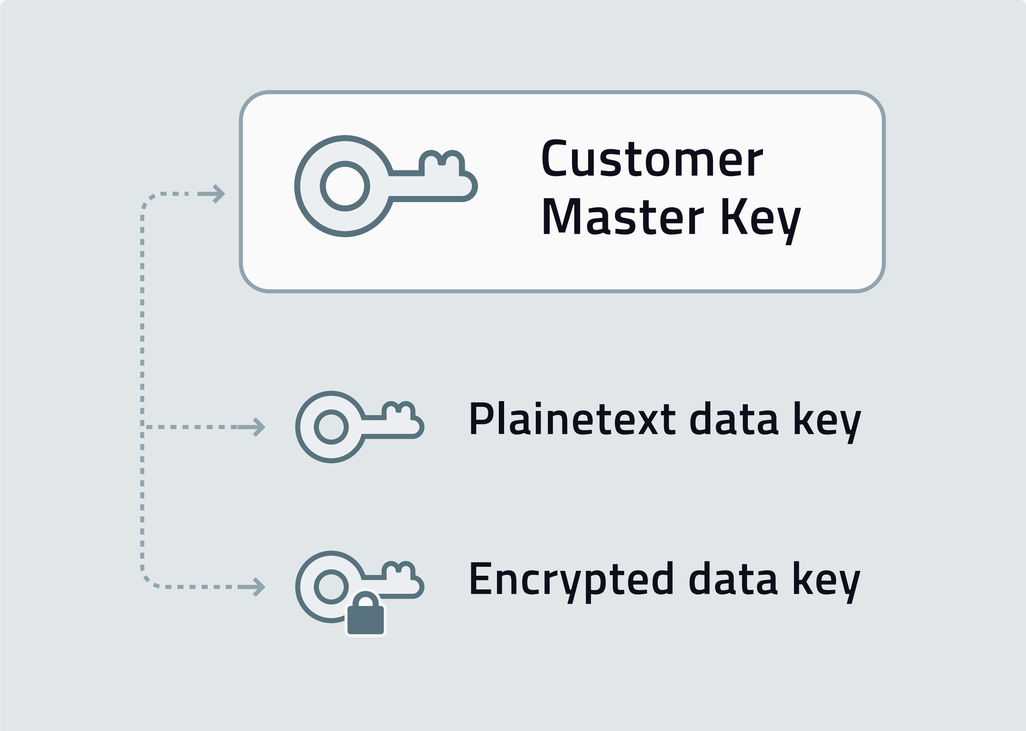
How about AWS KMS?

Key Management System

Key Management System (KMS)



AWS KMS saves the CMK's older cryptographic material in perpetuity



Single master symmetric key for all crypto operations

Key Management System (KMS)

Features	AWS	Virgil Security
GDPR/HIPAA compliance	×	+
Single point of failure	Yes	No
User controls data access	×	+
Post-compromise secure	×	+
Insider-secure	×	+
Price	1 CloudHSM is over $1K/month	Cloud KMS Pricing

Understanding Virgil PureKit and ZKP

PureKit

Open-source security framework for developers to enable post-compromise protection for stored data

Functions:

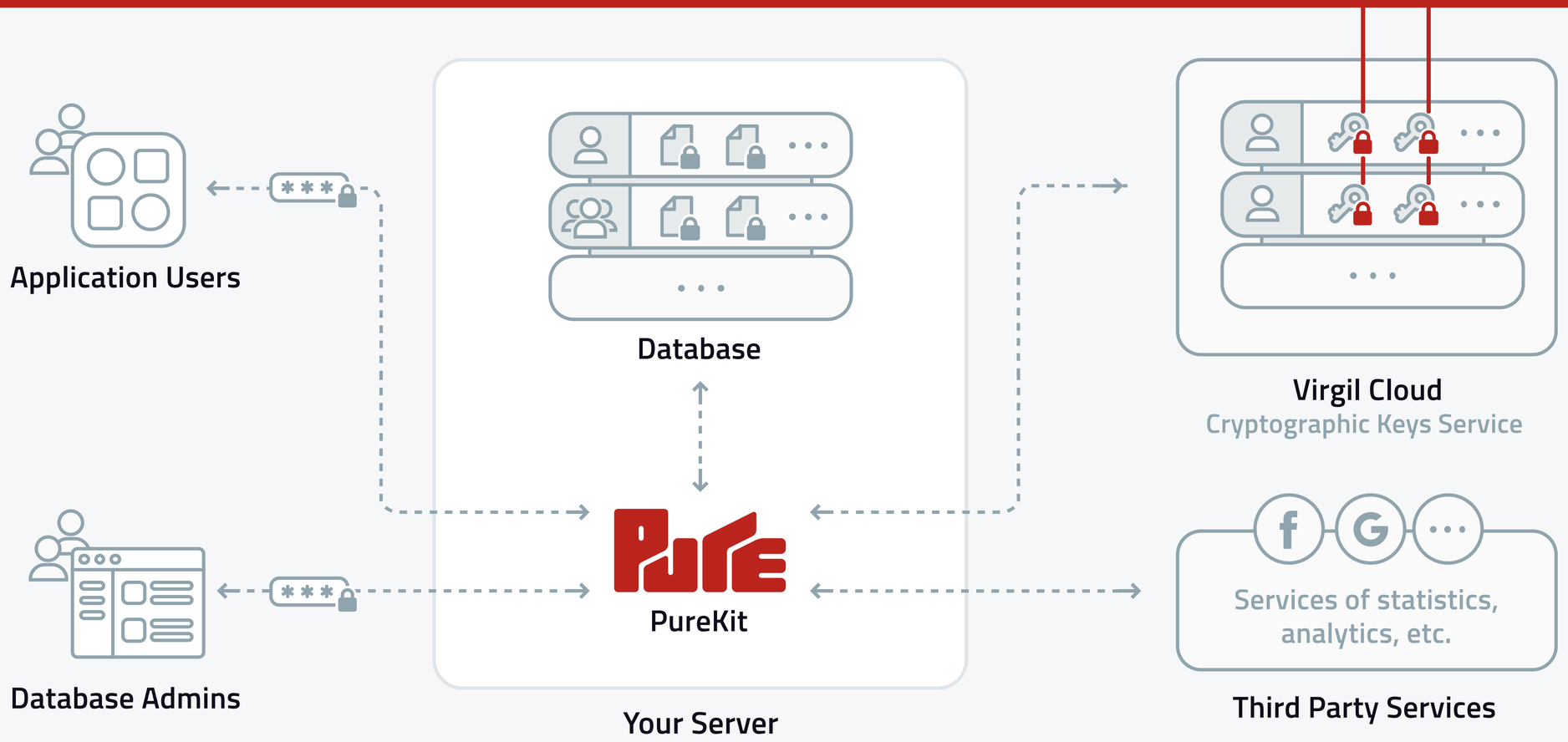
- Per-user data and files encryption
- Role-based data encryption
- Secure data sharing
- Key rotation
- Password-hardened encryption
- Data access recovery

Benefits:

- User controls data access
- Post-compromise security
- GDPR/HIPAA compliance
- Works with any database
- Low overhead, instant “re-encryption”

How PureKit works

All user's keys are protected with a unique user's PURE Record



VirgilSecurity.com
github.com/VirgilSecurity

How PureKit Works

Phase #1. The App Backend asks PHE Service for an Enrollment

App Backend:

1. Sends empty request to the PHE service.

PHE Service:

1. Generates 32-byte random salt.
2. Hashes salt with two different domains into two curve points HS0 and HS1.
3. Performs scalar multiplication of HS0 and HS1 by its Private Key (Y) to get points C0 and C1.
4. Calculates Zero Knowledge Proof which proves that C0 and C1 were indeed calculated using app server's Private Key (Y).
5. PHE Service replies with the following data:
   a. 32-byte random salt
   b. Points C0 and C1
   c. ZKP

Pure Record

A unique data that is associated with a specific user’s password,
1 password = 1 record

Pure Record composition:

- User's Pure Record version
- App & PHE service random salts
- Two values obtained during the execution of the PHE protocol
- User's PHE Encryption key

PURE Record Enrollment

Create unique Record for each user on PHE service

PUBLIC KEY

BACKEND

PRIVATE KEY (x)

Enroll? →

← sNonce, C0, C1, Proof

C0, C1 — points

C0 = y · (sNonce, "0")

C1 = y · (sNonce, "1")

PRIVATE KEY (y)

PHE SERVICE

HC0 = x · (cNonce, password, "0")

HC1 = x · (cNonce, password, "1")

M — random, MC = x · M

T0 = C0 + HC0

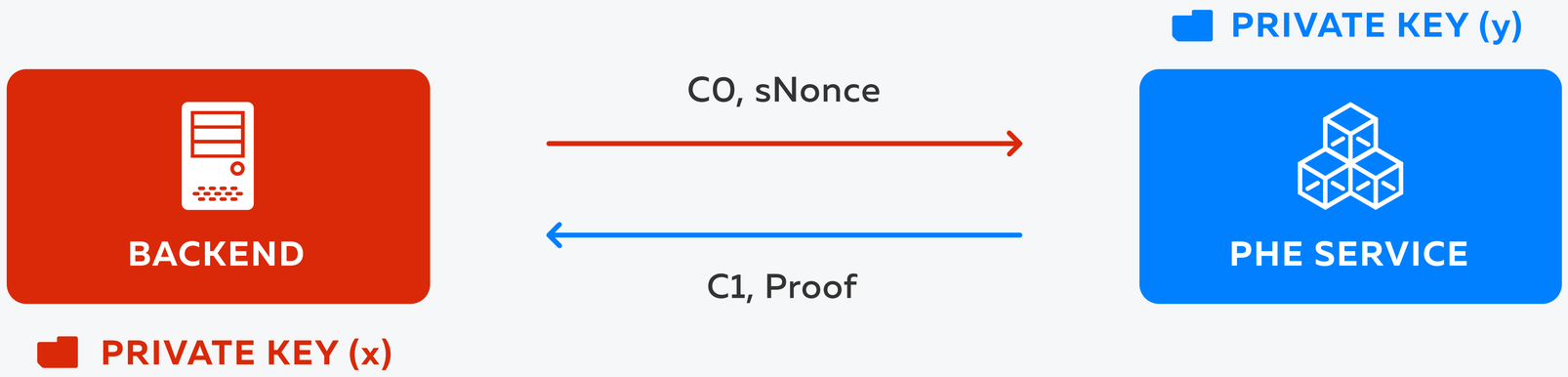
T1 = C1 + HC1 + MC

DATABASE:

T0, T1, sNonce, cNonce

PURE Record Verification

Verifies user's Record in the database during login step



HC0 = x · (cNonce, password, "0")

C0 = T0 − HC0

HC1 = x · (cNonce, password, "1")

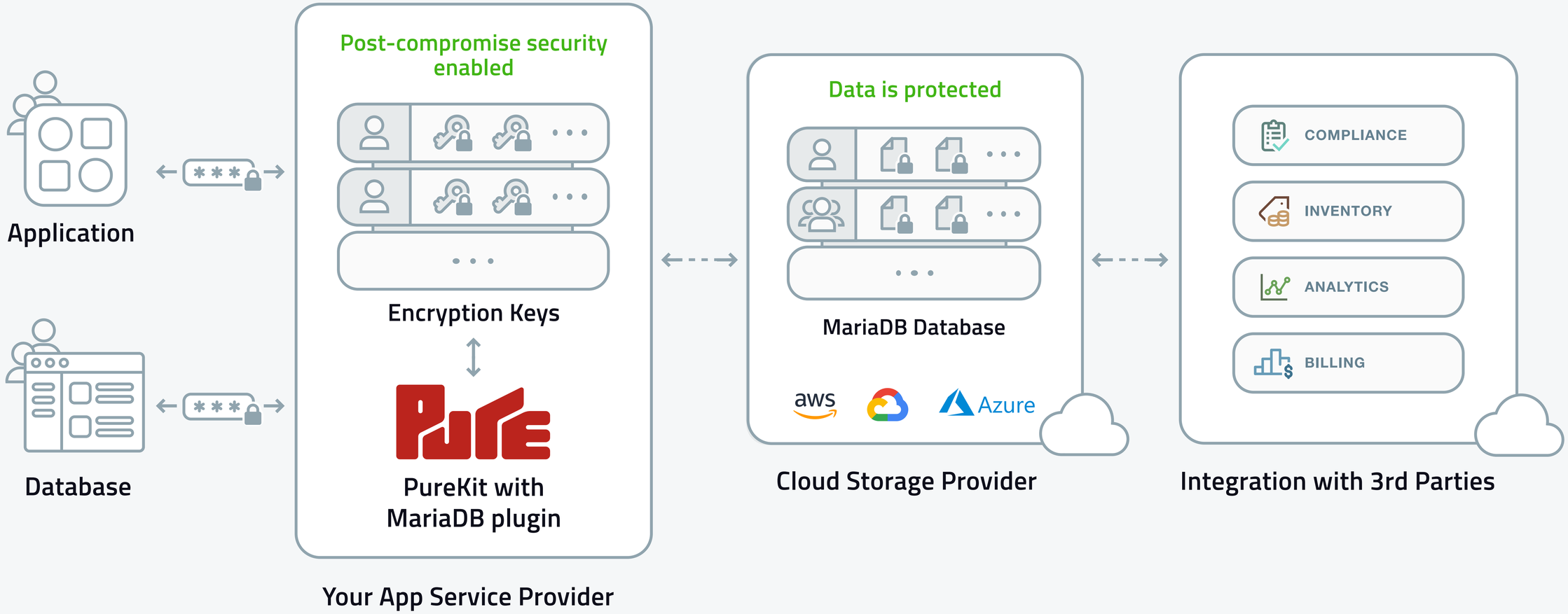
MC = T1 − C1 − HC1

C0 == y · (sNonce, "0") ?

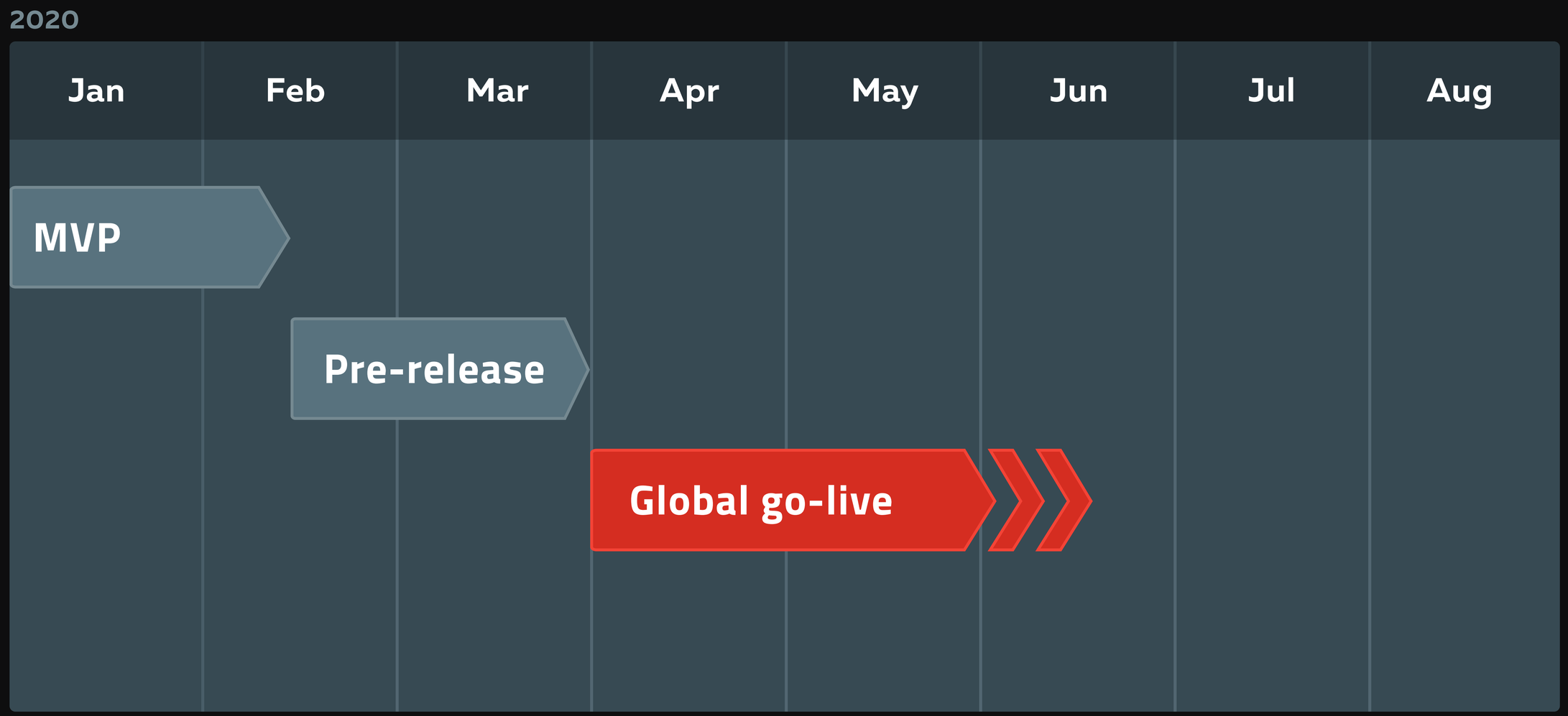
MC — encryption key

Virgil PureKit + MariaDB

How PureKit + MariaDB plugin works



PureKit Plugin for MariaDB: Timeline



Pre-release version includes

Password protection	• Password hashing is replaced in a way that it's impossible to run offline and online attacks
Per-user data encryption	• Each user owns personal data encryption key

Getting started with PureKit

Ask anything about MariaDB plugin based on PureKit

support@VirgilSecurity.com

PureKit documentation

Developer.VirgilSecurity.com