Garantir

Case Study

MongoDB Secures and Scales Global Code Signing with Garantir's GaraTrust Platform

THE CHALLENGE

Securing the Software Supply Chain at Scale

As MongoDB's product portfolio and global engineering teams expanded, so did the complexity—and risk—of ensuring the integrity of every distributed artifact: binaries, drivers, container images, and Linux repository packages. Code signing became non-negotiable, providing users with confidence that downloads were authentic and untampered.

MongoDB's existing, home-grown signing solution was functional, but as requirements grew, it faced three major pressures:

1. SECURITY HARDENING & KEY CONTROL

To strengthen cryptographic assurance, MongoDB's security team required that all signing keys be protected in hardware security modules (HSMs)—ensuring private keys are never exposed in software or accessible to unauthorized systems. The legacy solution lacked native HSM support, leaving a potential path for key compromise.

2. NATIVE ECOSYSTEM SUPPORT & FLEXIBILITY

MongoDB ships across diverse ecosystems (C++, Python, Node.js, Rust, and more), each with its own native package managers and signature formats. The in-house service used a standalone client and it was a challenge to integrate natively with a variety of tools.

MongoDB

CHALLENGE

MongoDB's expanding product line outgrew its home-grown code signing system, which lacked HSM key protection, struggled with diverse ecosystem integration, and created a high operational maintenance load.

SOLUTION

Adopted Garantir's GaraTrust platform to secure signing keys in customer-controlled HSMs (Azure), providing native support across all ecosystems, and integrating seamlessly into CI/CD pipelines.

OUTCOMES

Elevated security (keys in HSMs), standardized workflows, and operational savings (reclaimed ~1 engineering week per month) by retiring the legacy system and scaling effortlessly.

Case Study

3. OPERATIONAL LOAD & COMPLIANCE

Maintaining and evolving the internal service was consuming engineering time and risked lagging behind evolving security standards. Supporting new use cases and ecosystems meant increasing complexity and fragmentation.

MongoDB.

> ***If you're not moving forward, you're moving backward. Security changes fast. Leaving an internal tool alone for a year or two can mean you miss something important.***
>
> - Zakhar Kleyman, Lead, DevProdRelease Infrastructure

THE SOLUTION: THE GARATRUST PLATFORM

High Assurance, High Flexibility Code Signing

MongoDB evaluated multiple vendors and selected Garantir's GaraTrust for its combination of robust security, developer fit, and operational flexibility. **Why GaraTrust?**

1 HSM KEY PROTECTION

GaraTrust enabled MongoDB to store signing keys in customer-controlled Azure HSMs, ensuring keys are never exportable and always under MongoDB's control—even if the vendor relationship changes.

2 SEAMLESS AUTOMATION

Integrated directly into MongoDB's global, 24/7 CI/CD workflow, GaraTrust ensures artifacts are signed automatically as part of releases—without slowing the pace of development. Behind the scenes, Garantir's automated certificate lifecycle management seamlessly authenticates each signing request against MongoDB's trusted public certificates, eliminating manual verification steps and reducing administrative overhead.

> ***With GaraTrust, we could keep control of what matters — our keys, our clouds, our HSMs — while still getting a reliable, supported platform.***
>
> - Zakhar Kleyman

3 GRANULAR KEY MANAGEMENT

Different internal teams could use unique signing keys within CI/CD pipelines—no more sharing a single key across the company.

4 COMPREHENSIVE PLATFORM SUPPORT

GaraTrust's robust signing engine supports PGP/GPG detached signatures for Linux repositories, diverse ecosystems (C++, Python, Node.js, Rust, and more), and native code signing for major and less common platforms (Windows, macOS, Java, and more). This flexibility gives MongoDB the assurance that its signing infrastructure can adapt seamlessly as new products and ecosystems evolve.

5 EXPERT PARTNERSHIP

Beyond the product, Garantir provided MongoDB with ongoing expertise, helping navigate implementation choices and stay current with industry best practices.

Case Study

THE RESULTS

Security, Standardization, and Savings

IMMEDIATE SCALE AND STREAMLINED ADOPTION

MongoDB's transition to GaraTrust was seamless—scaling its signing volume, user onboarding, and key / certificate management right away, with no need to rearchitect pipelines. GaraTrust "worked out of the box," and MongoDB was able to retire its legacy system without slowing release cycles.

STANDARDIZED DEVELOPER WORKFLOWS

The migration was an opportunity to align internal teams on best practices, standardizing processes across a diverse developer ecosystem. GaraTrust's native support lets each team use familiar tools and signature formats, reducing friction and ad-hoc requests.

ELEVATED SECURITY AND TRUST

Private keys are now protected in HSMs that MongoDB's cloud vendor controls, eliminating the risk of accidental key leaks and ensuring continuity even if vendor relationships change. This gives both internal teams and external customers confidence in the security and authenticity of MongoDB's software.

As Zakhar stated, "We still own the keys... If something happens to Garantir tomorrow, we can still have the keys. That gives confidence to our internal users... and mitigates the risk of having to issue a note to the client saying, 'Hey, you got to change the keys that you trust.'"

IMPROVED OPERATIONAL EFFICIENCY

By deprecating the in-house signing service, MongoDB reclaimed about one engineering week per month previously spent on maintenance and security updates—a significant resource now applied to higher-value work.

MongoDB.

"We reclaimed ~1 engineering week per month by retiring our in-house service."

ELASTIC SCALE

As the volume of signing, keys, users, and pipelines grew, GaraTrust absorbed the increase with no effort required from MongoDB's side.

AUDITABILITY AND COMPLIANCE

Built-in audit logs and traceability features streamlined compliance reviews and internal audits, improving overall readiness.

ADVICE TO OTHER ENTERPRISES

Define what you must control: keep ownership of your keys and HSMs if they're mission-critical. Insist on native ecosystem support so users and package managers can validate signatures without custom workarounds. Plan for scale and per-team flexibility from day one. And always "trust, but verify" - choose a partner who listens and provides both reliability and technical levers for control.

> *"Trust but verify. With GaraTrust we kept control of the important parts while benefiting from a reliable partner."*
>
> *— Zakhar Kleyman*

LOOKING AHEAD

With Garantir's GaraTrust platform in place, MongoDB now has a cryptographic services foundation capable of rapidly supporting new use cases such as SSH, application-level encryption, private PKI, and more. The platform positions MongoDB to meet future demands—whether scaling signature volume, expanding products, or adapting to emerging security and compliance requirements. By partnering with Garantir, MongoDB has made security a force multiplier, not a bottleneck, for its global, high-velocity development operation.

Learn more about Garantir and GaraTrust at garantir.io.