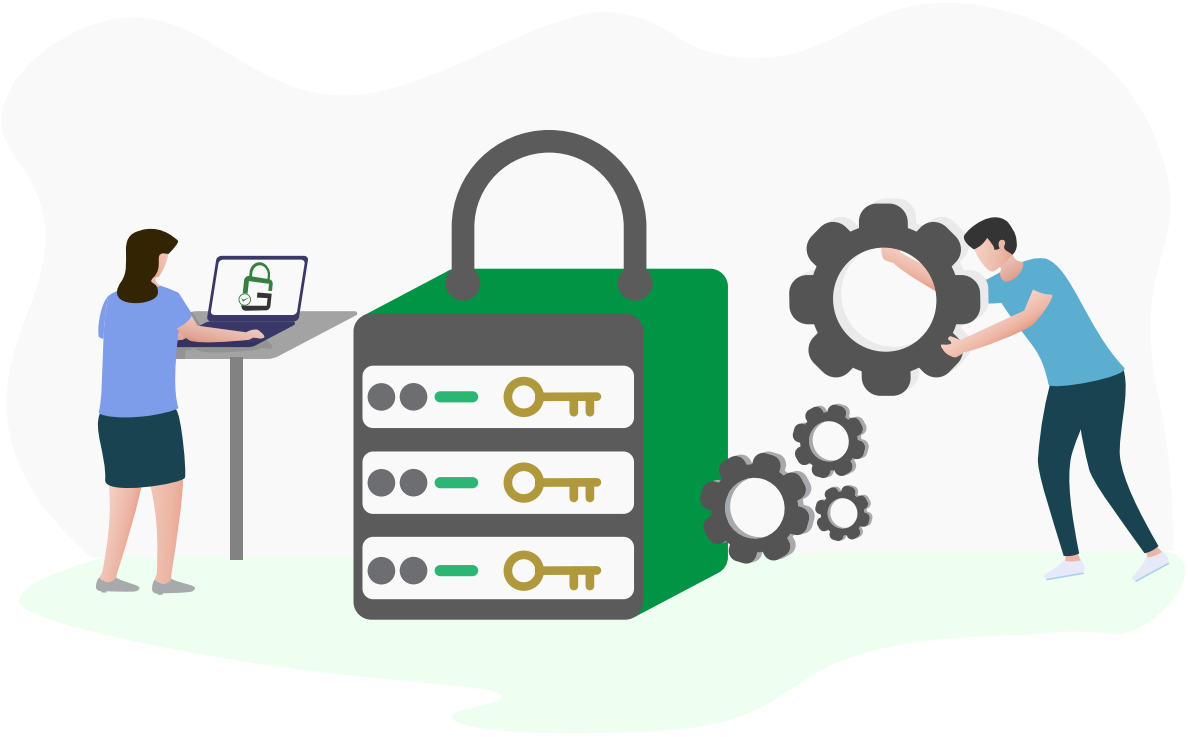
Garantir

1041 Market Street #302
San Diego, CA 92101
(858) 751 - 4865
info@garantir.io



Fast & Secure Access To Private Keys Stored In A Multi-Cloud Infrastructure

HashiCorp

Garantir

Copyright ©2020 Garantir LLC

Garantir GaraSign & HashiCorp Vault Solutions Brief

Securely Managing A Dynamic Infrastructure

As more enterprises shift from static, on-premise infrastructure to dynamic, multi-provider infrastructure, cybersecurity practices must shift, too. Whereas security in static infrastructure relies on dedicated servers, static IP addresses, and a clear network perimeter, strong security in dynamic infrastructure demands ephemeral applications and servers, trusted sources of user and application identity, and strong software-based encryption.

Enterprises with dynamic infrastructure must have the ability to secure and centrally manage secrets across multiple clouds and data centers, while also ensuring team members have secure and efficient access to the secrets they need without slowing down the speed of day-to-day operations.

Combining Garantir's GaraSign with HashiCorp Vault, enterprises can grant team members proxied access to keys stored across multiple clouds and data centers, while centrally managing those keys from a unified interface. Cryptographic operations— code signing, SSH, document signing, S/MIME, encryption/decryption, and more— remain fast and secure with GaraSign's client-side hashing architecture.

Protect Secrets Stored Across Multiple Clouds & Data Centers

HashiCorp Vault tightly controls access to secrets, such as tokens, passwords, certificates, snd encryption keys, while supporting public clouds and private data centers, as well as a host of endpoint systems like databases, cloud platforms, messaging queues, SSH, and more.

Key Benefits of Garantir GaraSign & HashiCorp Vault

- **Easy Administration** - All of your enterprise's private keys are centrally managed from a unified interface that makes it easy to grant, revoke, and audit access to those keys

- **Security** - All signing clients are restricted to proxied key access, so the private keys remain secured in HashiCorp Vault, HSMs, or key managers at all times

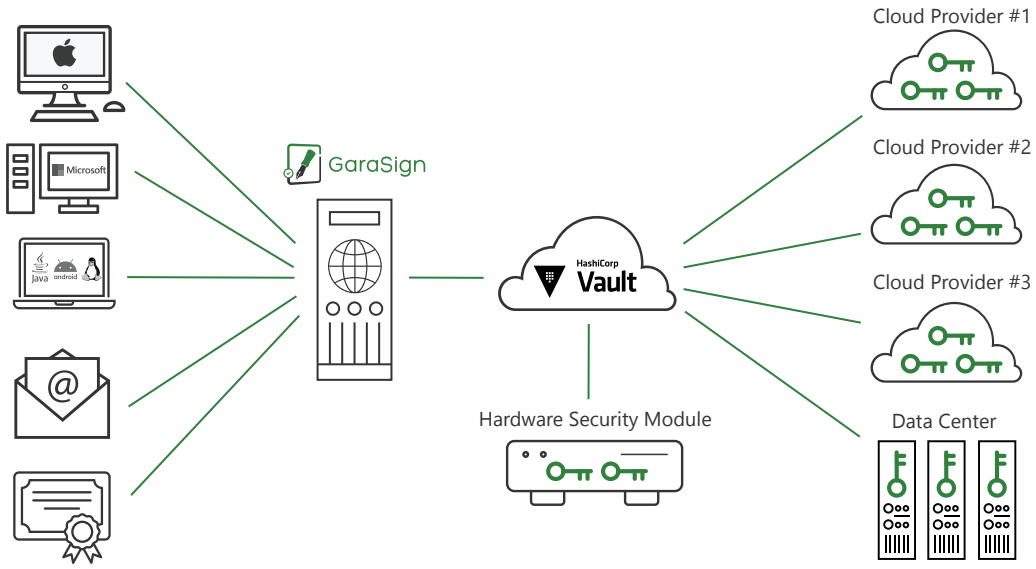
- **Performance** - The performance of cryptographic operations remains high with a client-side hashing architecture

- **All Use Cases** - End-users can efficiently access keys to perform cryptographic operations of all kinds, including code signing, SSH, S/MIME, document signing, & more

- **Easy Adoption** - With native client integrations to Apple, Microsoft, Android, GPG, Debian, RPM, and more, the joint solution is easily deployed in any enterprise environment

- **Highly Scalable** - GaraSign and Vault can scale up to support the largest of enterprises, regardless of the number of users or cryptographic operations

Copyright ©2020 Garantir LLC



Centrally Manage Distributed Keys From A Unified Interface

With Vault and GaraSign, you are able to centrally manage your enterprise's private keys and minimize the exposure of those keys by limiting their lifespan with time-based tokens that enable automatic or manual revocation. Vault also enables granular authorization of which users and applications are granted access to secrets.

Accelerated Performance For All Private Key Use Cases

End-user signing clients hash the data they need to sign before sending it over the network to create the signature. This keeps the signing process fast and efficient for all use cases, from code signing and document signing to SSH, S/MIME, TLS, and more.

Record A Detailed Audit Log Of Private Key Usage

Detailed audit logs provide detailed history of client interaction— authentication, token creation, secret access & revocation— which can be used to detect security breaches and attempted access to systems.

Maximize Security By Restricting Clients To Proxied Key Access

GaraSign is deployed on customer-managed infrastructure between clients and HashiCorp Vault. The clients are restricted to proxied key access so that private keys can remain in Vault at all times, providing maximum security, while team members can still gain access to the keys they need to perform cryptographic operations, like code signing or SSH.

Integrate With All Of Your Environment's Tools & Platforms

Microsoft Java android debian GnuPG rpm npm XML git OpenSSL PCKS #11

Copyright ©2020 Garantir LLC

HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp's open source tools VagrantTM, PackerTM, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco, though 85 percent of HashiCorp employees work remotely, strategically distributed around the globe. HashiCorp is backed by Bessemer Venture Partners, Franklin Templeton, Geodesic Capital, GGV Capital, IVP, Mayfield, Redpoint Ventures, T. Rowe Price funds and accounts, and True Ventures. Visit https://www.hashicorp.com/ to learn more.

Garantir

Garantir is a cybersecurity company that provides advanced cryptographic solutions to the enterprise. The Garantir team has worked on the security needs of businesses of all sizes, from startups to Fortune 500 companies. At the core of Garantir's philosophy is the belief that securing business infrastructure and data should not hinder performance or interrupt day-to-day operations. With GaraSign, Garantir's flagship product, private keys remain secured at all times, without limiting the performance of cryptographic operations, including code signing, SSH, S/MIME, document signing, TLS, secure backup, and more.

Garantir

1041 Market Street #302
San Diego, CA 92101
(858) 751 - 4865
info@garantir.io