Garantir

GaraTrust: A Security Orchestration Platform for the Enterprise

With GaraTrust, enterprise security teams can centrally set and enforce policy for a wide range of resources.

https://www.garantir.io

321 Tenth Ave #1208
San Diego, CA 92101
(858) 751-4865
info@garantir.io

Enterprise cybersecurity professionals face a number of challenges in today's digital world. First and foremost, the cyber threat landscape is more hostile than ever before. Threat actors are increasingly sophisticated, well-funded, and ruthless.

In addition, security leaders must manage a number of different aspects of cybersecurity: data security, identity and access management (IAM), secure software development, application security, network security, PKI and certificate management, email security, and more. This circumstance compels businesses to manage and maintain a number of highly complex point solutions. All too often, these tools are siloed and don't integrate to support an overarching cybersecurity strategy.

Further, cybersecurity leadership must protect enterprise data and infrastructure within the parameters of business objectives. Security systems can't disrupt existing processes and operations. At the end of the day, security solutions must enable business, not obstruct it.

Defining Objectives & Describing The Desired End-State

As the digital transformation progress and IT infrastructure becomes more complex, enterprises must design and deploy a strategy that unifies and centralizes all security operations. Ideally, an enterprise security strategy would provide the following benefits.

Security

Only authorized end-users are permitted to access enterprise services and data.

Unification

All aspects of cybersecurity are brought under one roof and centrally managed.

Centralization

Security policy is established and enforced from a single centralized interface.

Easy Deployment

A multitude of native client integrations accelerate and simplify deployment.

Business Enablement

Security systems integrate with existing processes to support business objectives.

Compliance

Access to all resources is always logged, simplifying audits and compliance.

Using Cryptography to Unify Security Administration

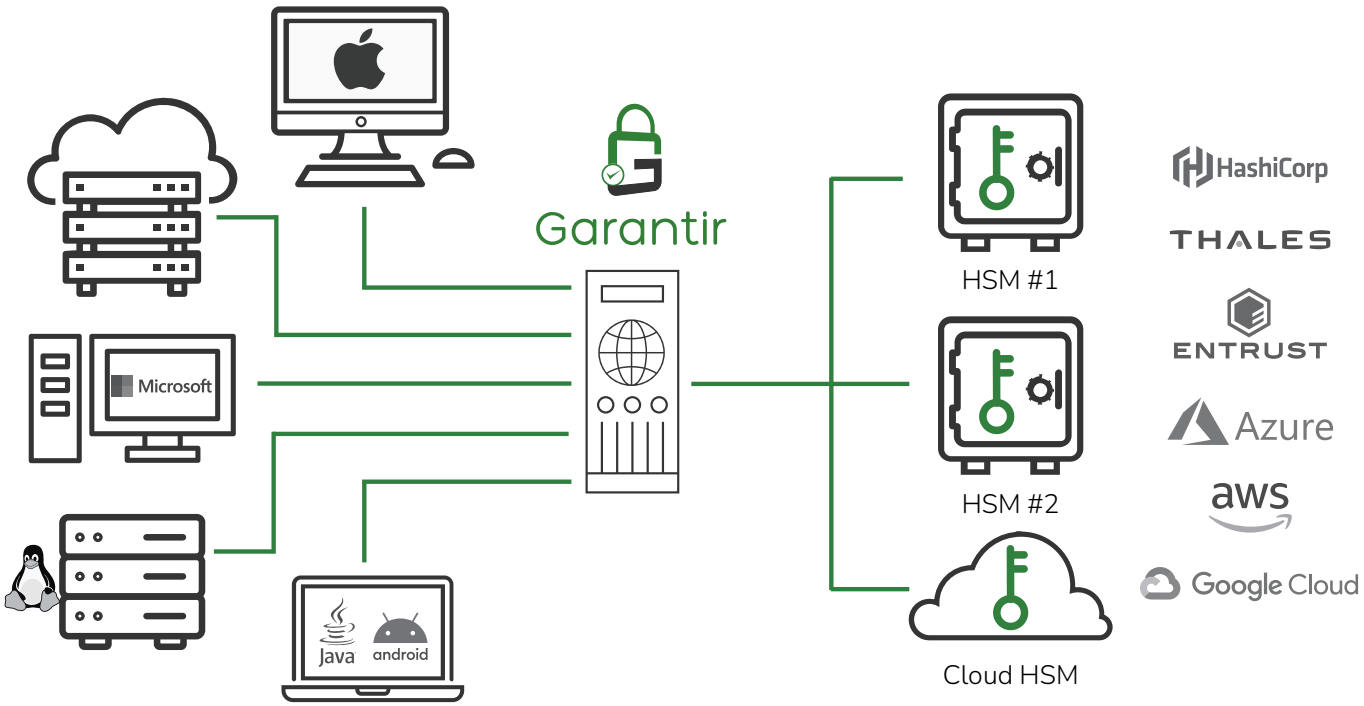
While the various dimensions of cybersecurity may seem disparate, there is one technology that unifies them: public key cryptography. Cryptography secures data in transit (TLS), authenticates users to remote servers (SSH & TLS), protects data at rest (database and file encryption), ensures the authenticity of software (code signing), safeguards email (S/MIME and PGP), and much more.

Unfortunately, sensitive cryptographic keys, like decryption keys, SSH keys, code signing keys, and TLS keys, are often left in software on endpoint devices. This creates major security risks, visibility and auditing complications, and compliance challenges.

If all of the enterprise's private keys are stored in a centralized hardware security module (HSM) or key management system (KMS), security is dramatically improved and the enterprise can centrally manage multiple aspects of their cybersecurity operations. Since use of a private key is needed to access a wide range of resources, properly securing the cryptographic keys enables the enterprise to centrally grant, manage, revoke, and monitor access to data and services.

GaraTrust: A Security Orchestration Platform

GaraTrust is a security orchestration platform that enables centralized management of enterprise infrastructure, services, and data. With native client integrations to all major operating systems, platforms, and tools, GaraTrust ensures that existing processes and workflows can continue to operate without interruption or impediment, while simultaneously improving their overall security posture and compliance.



Common Use Cases

GaraTrust can be deployed for many use cases. Below is a brief overview of the most common use cases.

Supply Chain Security – Protect your code signing keys, seamlessly enable MFA on source code repositories, and integrate verified reproducible builds and code scanning into the CI/CD pipeline.

Identity and Access Management – Centrally manage your digital identities and apply granular controls on a variety of resources and services without needing to manually modify applications or reconfigure servers.

Data Security & Ransomware Protection – Protect files, email, databases, and backups in motion and at rest. Ensure the integrity of data with digital signatures and cryptographic timestamping.

Certificate & Key Management – Manage all keys and certificates across a complex infrastructure from one interface. Avoid costly outages with centralized auditing, automated renewal, and simplified administration.

Centralized Policy Settings & Auditing

With GaraTrust, security policy is set and enforced from a single interface. The enterprise can centrally grant, revoke, manage, and monitor access to an array of resources, from encrypted databases, files, and email, to enterprise services, applications, DevOps tools, and more. The keys are never exported from the HSM and all key usage is logged, making it easy to conduct audits and comply with all relevant regulations.

Granular Security Controls

End-users authenticate to GaraTrust every time they request to use a key. GaraTrust supports a host of granular controls, such as MFA, device authentication, approval workflows, just-in-time access, notifications, and more. These controls can be enforced on a per-key or per-user basis without needing to manually reconfigure servers or make modifications to applications.

Native Client Integrations

GaraTrust provides a multitude of native client integrations so you can continue using the same tools and platforms that you do today without any noticeable impact on performance. Existing processes do not need to be adjusted and there's no need for custom development work. This simplifies deployment and ensures that you can make the most out of GaraTrust without any heavy lifting.

Support For All Infrastructures

GaraTrust can be deployed on-premises, in the cloud, or in a hybrid environment. GaraTrust supports multiple HSMs and key managers simultaneously, so the enterprise can manage a plethora of keys stored across a complex, multi-cloud infrastructure and on-premise environment with a single solution. GaraTrust is typically licensed in three-year agreements and deployed on customer-managed infrastructure.

Garantir

About 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 GaraTrust, Garantir's flagship product, private keys remain secured at all times, while a client-side hashing architecture ensures high performance for all cryptographic operations, including code signing, SSH, S/MIME, document signing, TLS, secure backup, and more.

https://www.garantir.io

321 Tenth Ave #1208
San Diego, CA 92101
(858) 751-4865
info@garantir.io