



MSSP Guide to Earning New Business Revenue with Unbound

An Introduction to Unbound Security CORE

Partnership
Guide



About Unbound Security

At Unbound Security, we apply revolutionary breakthroughs in cryptography to empower enterprises to confidently secure and manage all their critical business transactions and information— anywhere, anytime.

Unbound leverages secure multiparty computation, as well as other advanced cryptography technologies and multilayered security architecture to eliminate single points of failure. This allows solutions that are much more secure than point solutions. We orchestrate multiple hardware and software elements in synergy, providing solutions that are secure, agile, and easy to use.

Fast Facts: Who is Unbound?

Company	Technically Validated	Analyst Validated
<ul style="list-style-type: none">• Founded 2014• Headquartered in New York; Office in Tel Aviv• 50-200 Employees• Industries• Banking• Fintech• Technology• Patents: 17	<ul style="list-style-type: none">• FIPS 140 2 Level 1 , 2 validated (first for MPC)• 17 granted patents• Rigorous testing by Fortune 100 customers• The result → Field proven in customers ' production environments	<ul style="list-style-type: none">• Unbound listed in 5 Gartner Hype Cycle Reports on data security, cloud security, digital privacy, IAM and blockchain• Selected as Gartner 'Cool Vendor'

Benefits of Working with Unbound

Built with Enterprises in Mind

As the world grows increasingly digitized and decentralized, enterprises increasingly lack the ability to manage their entire cryptographic arsenal across disparate sites and multi cloud infrastructures. With the advent of a business environment which is mostly from employees' homes, security becomes not only more complicated, but more critical.

In the meantime, businesses suffer when their key management is heavily siloed and localized:

- Refactoring applications delays the ability to migrate data to the cloud or elsewhere, lending organizations to be locked in to Cloud Service Providers (CSPs)
- Organizations are forced to use multiple key management solutions, without being able to keep track of operations in one database
- By outsourcing key management – to CSPs or external service providers – organizations abdicate control over the most critical security points for protecting their data

In short, there is a control vs. usability tradeoff – no matter what type of system organizations typically consider. This is where Unbound can help. Unbound’s key storage and protection solutions provide a unified approach to key management, enabling organizations to universally enjoy Unbound’s unique features, while maintaining the freedom to choose the key store that best suits their needs and policies – and all at the highest level of security.

Unbound Benefits

- Experience working with Fortune 500 companies and global banks
- High security – mathematically proven guarantees
- Protects from key misuse (not only key theft)
- Built for easy, detailed auditing and to meet the most rigid of compliance regulations
- Crypto agility
- Post-quantum ready
- Transparency and independent review

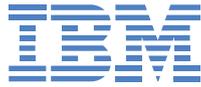
Proven Technology

Some of the world’s most successful Fortune 500 enterprises with the highest security and privacy requirements turn to Unbound for its breakthrough solutions. With Unbound, organizations are unrestricted to readily expand and evolve in today’s digital ecosystem.

Customers



Partners and Integrations



Our Technology: Unbound Security CORE

Unbound CORE – Cryptographic Orchestration Reimagined for the Enterprise – offers a single pane of glass to all of your cryptographic key management protection and services. With CORE you eliminate the single point of failure in any data protection framework, while ensuring protection of your information, identities, and crypto assets.

CORE combines both the operational efficiency aspect of a software-only platform and the complete elimination of the single point of failure in cryptographic key management and protection infrastructures. Freed from the burden of dedicated hardware, the platform offers businesses security and control at relatively low cost.

Enabled by multiparty computation (MPC), Unbound CORE splits keys into multiple random shares – never putting them together, not even while in use. Therefore, multiple parties must participate to use the key, such as to sign a transaction that is being added to the blockchain ledger – it is never a single point of failure. A compromise or loss of any one key share does not lead to a compromise of the key. Backup and recovery keys can be protected in a similar manner, split between multiple parties.

The result: Unbound's solutions eliminate the single point of failure – and your enterprise is safer, faster, and more efficient.

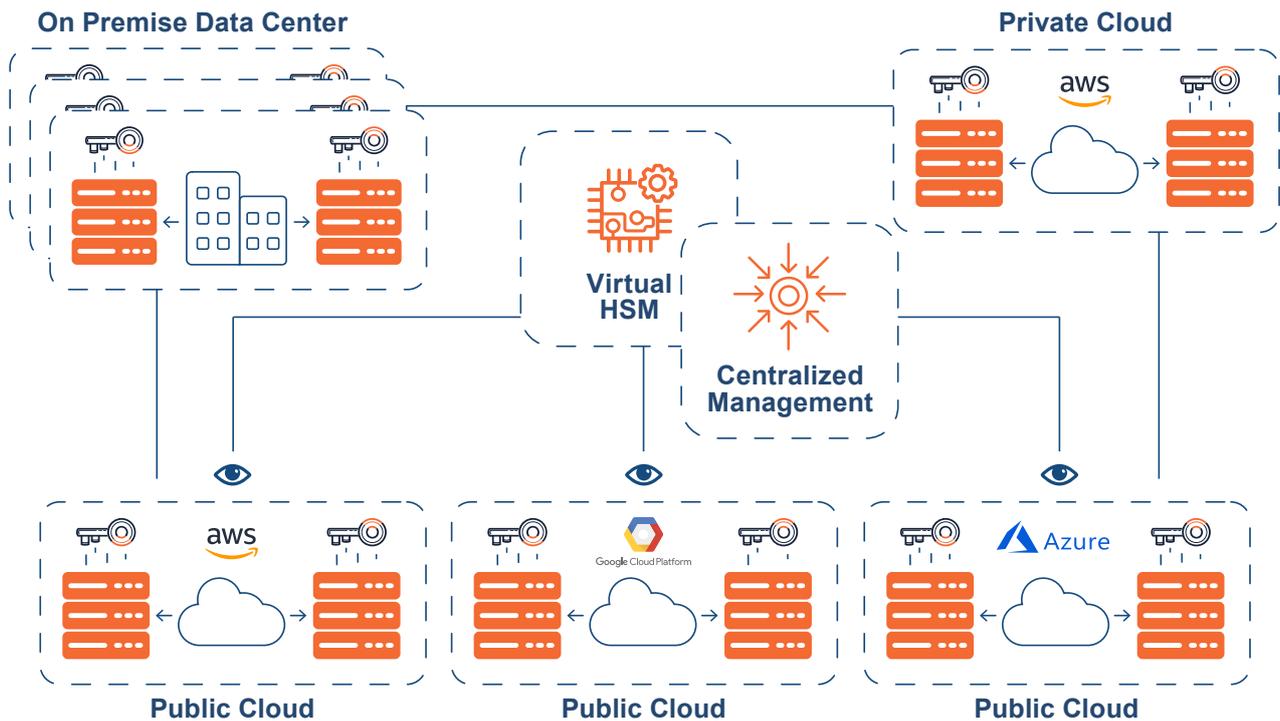
Splitting Keys with MPC

- Each private key is split into random shares stored on separate locations and continually refreshed
- Key shares are never united, from generation through usage
- Key material never exists in its entirety at any point of its lifecycle

Key Management

Unbound CORE for key management uses a virtual MPC key store to secure, store, and manage all of your critical cryptographic keys in one place. It provides easy integration to existing solutions, and includes native support for all standard libraries, including KMIP.

CORE can be deployed uniformly across different geo-locations and environments, creating a powerful mesh, without disrupting existing application workflows. It removes the single point of failure of cryptography, supports company-wide policies for key usage, provides comprehensive tamper-resistant audit logging, and enables flexible and fast deployment.



CORE Key Management includes three different types of use cases:

- Information Security – to protect information across all environments
- Identity Security – for authenticating transactions and identifications of users and machines
- Crypto Asset security – blockchain security built with risk-based approval policy support and workflows with a financial industry focus

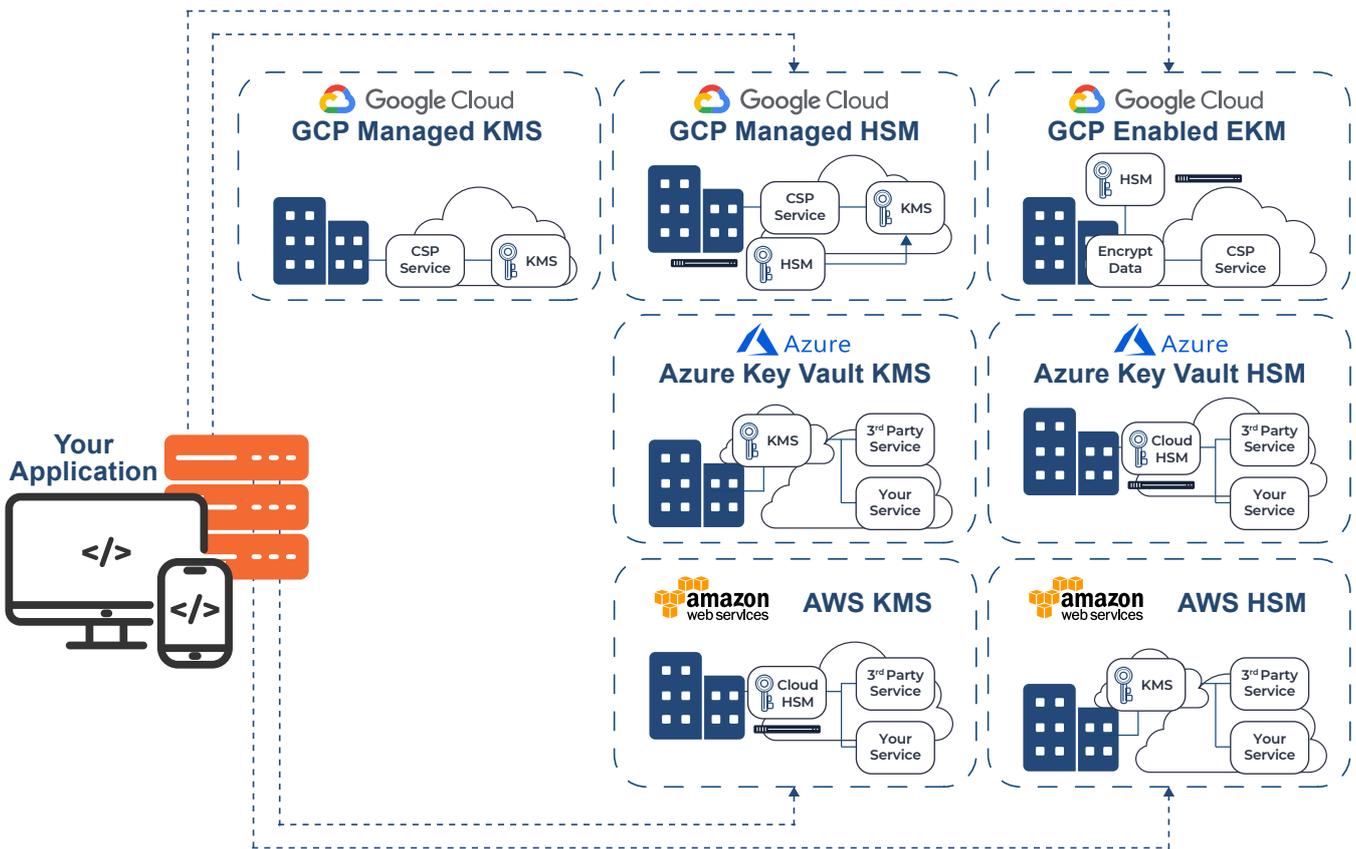
Unbound Security currently offers information and identity security services to MSSPs and their clients. We will elaborate on these services below.

Use Case: Cloud Agnostic Key Management

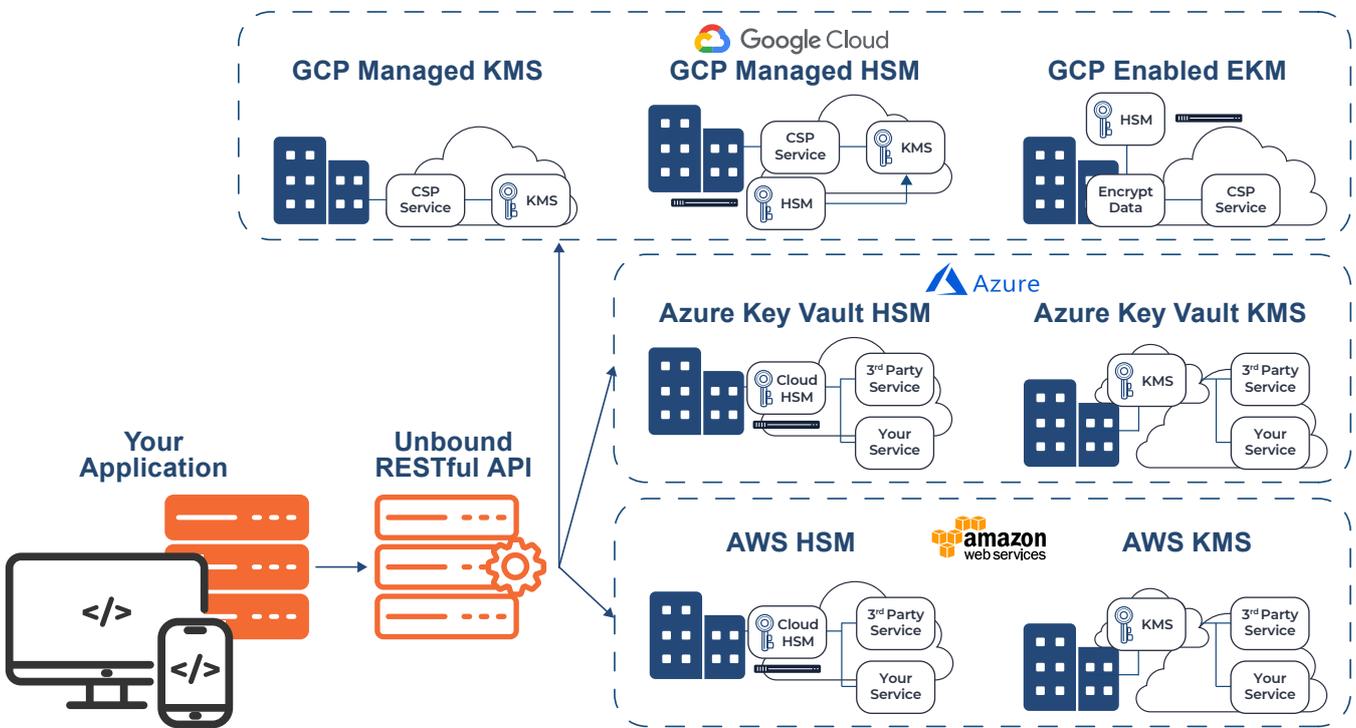
Unbound has developed CORE with the multiple and hybrid cloud key environment in mind, considering the special challenges for organizations using multiple CSPs.

These challenges typically include:

- Conforming to the cryptography allowed by the CSP's key management system (KMS)
- Relinquishing control and ownership of the cryptographic keys and key policies to the CSP
- Different levels of trust in different key locations/CSPs
- Different levels of trust with various HSM models used in conjunction with CSPs – across multiple geographic locations
- Gaining visibility to where all keys are being stored, and how they are being used



1 - Typical setup when integrating with multiple cloud providers



2- Setting up a multiple cloud key management scheme with Unbound

Information Security

With Unbound CORE, every team in your client's organization – no matter where they are located – can know exactly where keys are and how they are being used. Secure keys from a single pane of glass across any environment – including VM, database and storage encryption, enterprise PKI (public key infrastructure), code and document signing, and more.

Information Security with Unbound at a Glance

- Many Keys. One Platform – Manage all your information, no matter where or how it is stored, from one central and secure platform.
- Seamless Integration – Upgrade to CORE without disrupting any existing workflows
- Deploy Anywhere – Secure keys across any cloud, multiple clouds, on-prem, in physical machines, in VMs, or in containers. Secure any information, anywhere, any time
- Reduce Risk – Don't lose track of your critical information. No matter who is performing an operation, or from where, your team will know what is being done and how.

Identity Security

Unbound CORE Identity is a solution for authenticating users and machines. Users and enterprise employees can be authenticated using their mobile phones or laptops by replacing smartcards, one-time password tokens, SMS-based OTP and the like with an MPC-protected software solution.

The Unbound CORE Identity SDK makes it easy to seamlessly integrate strong authentication into mobile apps and endpoints so that it is invisible for users, improving both security and usability.

The solution achieves high security by preventing key theft since keys never exist in whole on any device at any point of their life cycle, by providing non-repudiation, and by not being vulnerable to social engineering. All operations are audited, and users are managed in the Unbound CORE key management console. Unbound CORE Identity also protects server-side keys and certificates used in existing authentication solutions, like federated authentication with SAML tokens.

How CORE Identity works

- MPC algorithms between the endpoint and the CORE server authenticate transactions, secure data, and govern operations – greatly reducing the possibility of brute force attacks, side channel attacks, social engineering threats, and other common pitfalls of hardware and software token authentication methods.
- All operations are cryptographically verified, leaving a tamper-proof audit trail in real-time.
- By eliminating the single point of compromise, CORE provides an extremely high level of security for most sensitive keys such as authentication, signing and encryption – ensuring resistance from cloning, Sim Swaps or tampering even on compromised devices

CORE Identity can be used for:

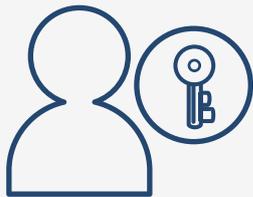
- SDK for mobile authentication
- Enterprise endpoint security

For strategic partners whose primary focus is mobile security and authentication, Unbound's CORE for Identity product is an amazing solution for companies with a large customer base to which they offer a mobile application. We can secure the authentication of this mobile app, achieving secure passwordless authentication with relatively minimal effort.

Identity Security with Unbound at a Glance

- Supports standard cryptography: RSA, ECC, AES
- Secures advanced cryptography: PQC, blockchain
- Secures password and data objects
- SDK easily integrated with any mobile app
- Ability to support third-party APIs, REST API, and any scripting language
- Tamper-proof audit logs can be exported to other systems
- Seamlessly integrates into existing workflows

CORE for Identity Security Use Cases



Secured Authentication



Replace HW token



Sign a Transaction



Phone as a Key Chain



Go Password-less

Use Cases

CORE for Information Security

- An international software development firm streamlining their code signing operations by deploying Unbound CORE over their national and international servers, reducing operational strain on multiple teams.
- A multi-faceted enterprise organization in the financial services industry securing their TLS certificates, their databases, and their applications with CORE during the process of virtualization.

CORE for Identity Security

- A global bank replacing passwords as the identity authentication system for over 10,000 mobile end users – without disturbing any workflows or preexisting code.
- A national bank replacing millions of hardware and software tokens with easy – yet secure – software-based authentication for their entire network, while still meeting strict regulatory requirements, and while also reducing the total cost of ownership (TCO).
- A high-profile messaging and communications network replacing smartcards as their means of authorizing transactions in over 200 countries with a software-based, built-in authentication system and reducing severe operational strain on the organization.

How We Work with MSSPs

Commercial Model

MSSPs can offer the Unbound CORE platform separately, or integrate the CORE platform within the MSSP. Our pricing model can be offered to customers on a monthly basis or on an annual basis. Lucrative volume discounts will apply based on revenue targets. Unbound is happy to provide more details once an NDA is signed.

Target Verticals

Unbound has applications in almost every vertical, however the current specific targets are banks/financial institutions, and big tech companies. We also see a large potential opportunity in the healthcare space, once their adoption of cryptographic security becomes widespread.

Any company using encryption is a potential customer, and our most common use cases are the following:

- Database Encryption Key Management
- VMware vSphere: VM-Encryption Key Management
- Private Data Tokenization
- Application-Level Encryption
- Endpoint Encryption

Services, Support, and Benefits

MSSPs can benefit from hosting, managing, and deploying our services for downstream enterprise customers depending on the use case.

Full lists of integrations and developments can be found at our guides:

<https://www.unboundsecurity.com/documentation>

Advanced Security Solutions

As an MSP/MSSP, you and your clients can benefit from implementing the latest cryptographic key security technology available on the market today – without the heavy lifting of hiring an in-house security expert, and without the hassle of hardware.

- **Full-stack solutions:** Unbound offers solutions, not siloed by product. We apply cutting-edge cryptographic key management anywhere in your client's information technology infrastructure.
- **Simplicity and efficiency of deployment:** Unbound solutions do not need dedicated hardware to operate or custom coding to run and integrate with legacy and pre-existing systems. Both you and your clients benefit from a faster go-to-market time.
- **Flexible and aggressive pricing margins:** Unbound solutions are offered on a monthly, or yearly licensing agreement with a distinct volume discount. MSPs/MSSPs benefit from higher profit margins; clients benefit from lower prices for enterprise-grade systems.
- **Abundant technical support and resources:** Every Unbound solution includes robust, full-featured APIs and SDKs; a full documentation suite for each product line and most use cases; online product and technical training from our cryptographic key security experts; an extensive FAQ guide; access to our Partner Technical Knowledge Base; and 24/7/365 technical support.

Sales Enablement

To our Unbound-partnered MSP/MSSPs, we offer:

- **Materials to help increase your new business revenue** – including product brochures, sales kits, and the latest competitive information and research.
- **White labelling/co-branding** – Rebrand our solutions fully with your branding. We work seamlessly in the background.
- **Volume-based product discounting** – offer your clients competitive pricing which improves as your client base grows.
- **Free 30-day evaluations** – no hardware to be shipped. Utilize our software as a service, or as a hybrid cloud deployment
- **Tiered deal registration** – gain protection for your customer opportunities through our partner deal registration.
- **Renewal protection** – your customers stay with you for the life cycle of their license and renewal.
- **Marketing and awareness-building** – joint participation in social networking, press releases, and content/collateral (e.g., white papers, newsletters, and webinars).
- **Networking** – partner events and conferences.
- **Partner certification** – for sales and technical teams.
- **Access to resources** – including branding/style guides, sales campaign kits, and more.

Summary

Unbound is committed to advancing and elevating the partner community, while keeping an eye on evolving our solution in the constant changing security ecosystem. Our CORE platform provides cutting-edge cryptographic security for information security, identity security, and digital asset/blockchain security which holds to the highest standards of testing, is infinitely customizable, and does not disrupt existing workflows and integrations.

By partnering with us, your organization will receive guidance for selling Unbound's security solutions, and receive a simple, easy to sell integration which interfaces with existing platforms through APIs and SDK integrations. Unbound is committed to a high level of support during implementation, minimal IT disruption throughout the deployment process and special training and sales enablement to the partner's teams.



Unbound Security is the global leader in cryptography and empowers enterprise customers worldwide to confidently secure, manage and authenticate all critical business transactions, information, identity, and digital assets – anywhere, anytime. Unbound Security CORE is the enterprise platform of choice for secure key management, trusted by many of the world's largest banks and Fortune 500 companies. Unbound Security is a recent recipient of the Deloitte Fast 500 award and is headquartered in New York, with research and development facilities in Tel Aviv. Learn more at www.unboundsecurity.com and follow us on [LinkedIn](#) and [Twitter](#).

