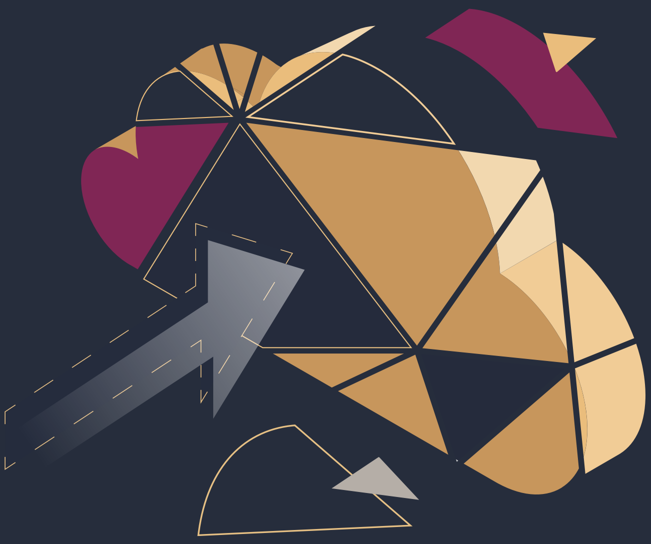
UNBOUND

( MATH OVER MATTER )

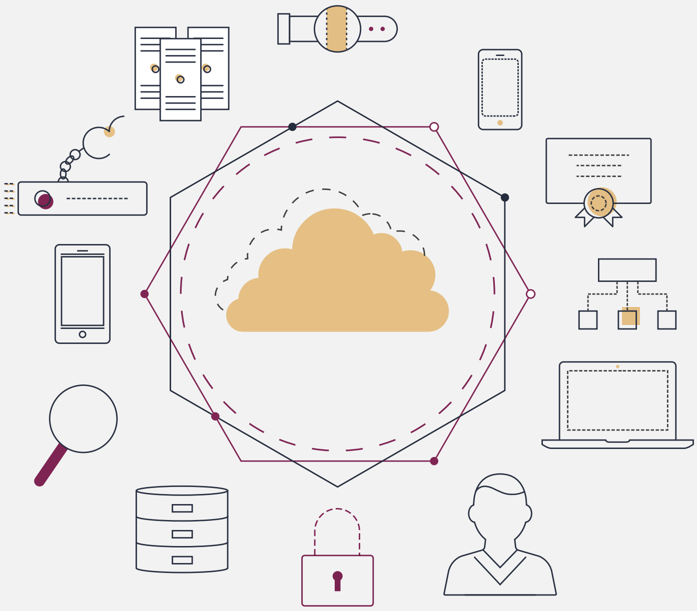
# CONTROL YOUR KEYS IN THE CLOUD

## Solution Brief



# Control in the cloud: Is it an oxymoron?

**As companies increase their reliance on cloud infrastructure and services, they inherently cede some control over their business to cloud service providers. But security and privacy of sensitive digital assets in the cloud is one area where companies must maintain full control.**



**By 2020, 92% of all data center workloads will be processed by cloud data centers, of which 68% will be in public cloud infrastructure.**

*Cisco Cloud Index, 2016-2021.*

Industry adoption of cloud is clearly on the rise. Cloud computing offers the benefits of flexibility, agility and operational efficiency that today's digital business environment demands. At the same time, use of the cloud means that companies need to relinquish some control over their assets to their cloud service providers (CSPs).

Trust is a key enabler for cloud adoption, because it enables organizations to accept this loss of control. You trust your cloud provider to ensure that internally used services are always accessible for day-to-day operations, and that your customer-facing services perform seamlessly, even when experiencing major spikes in consumption.

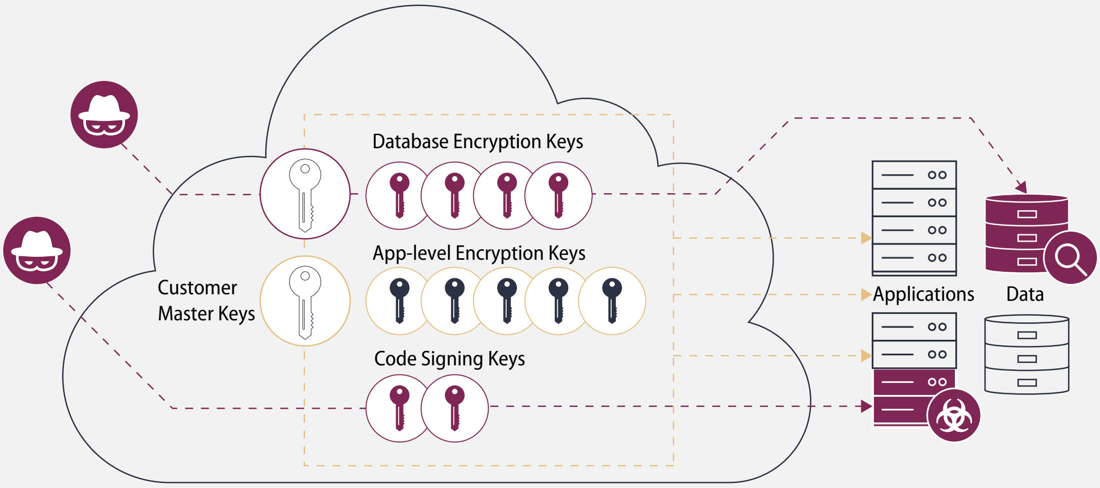
When it comes to security and privacy, however, loss of control, even to the most trusted cloud providers, is a risk that should not be accepted. Protecting your valued  assets and confidential data is a fundamental business need, with breaches potentially leading to devastating and irreparable consequences.

Recent publicized security breaches, such as the Capital One breach, which ranks as one of the biggest in history. The hacker behind this breach accessed sensitive information including social security and credit card numbers that were stored in the servers of a third-party cloud computing company contracted for use by Capital One. This breach and others, have shown us that businesses are ultimately held liable for the protection of their sensitive data and applications, wherever they reside.

This reality raises a true business challenge: **How can businesses stay in control of safeguarding their digital assets in an increasingly dispersed IT environment?**

# Controlling your keys in the cloud is critical

**Of all the data elements used in the cloud, cryptographic keys are by far the most sensitive and crucial to protect. Cryptography is the foundation for protecting business data and applications, and its integrity relies on keeping secret keys from unauthorized access, misuse or loss. Key control in the cloud is therefore a crucial requirement for many enterprises making the cloud transition.**



> *Cryptographic keys play a vital role in securing applications and data in the cloud. Having those keys compromised may put your business at serious risk. For example, a compromised code signing key could be used to illegitimately sign arbitrary applications, even malware, in your organization's name, potentially resulting in revenue loss and heavy reputation damage. In another example, a stolen customer master encryption key could be used to expose all the database encryption keys protected by that key. This can lead to a massive breach of sensitive data such as employees' or customers' personally identifiable information (PII), resulting in revenue and reputation loss, negative publicity, violation of privacy regulations and legal repercussions.*

Cryptography is the underlying technology behind data encryption, application integrity validation, digital signing, authentication, and other security functions that are core enablers of the digital economy. As businesses place more valuable data and rely on more services running in the cloud, the importance of cryptography in the cloud environment grows.

The strength of a cryptography implementation depends on the strength of protection of the cryptographic keys. Compromise or loss of these keys could render damaging results, such as massive data theft, or tampering with proprietary application code for malicious purposes.

Control of keys in the cloud should therefore be treated as a business imperative, particularly by companies that are using them to secure sensitive or high-value resources.

Traditional HSMs, which use purpose-built hardware to protect keys, are inherently incompatible with the fast-paced, ever-changing, software-defined world of the cloud. Though highly secure, HSMs are much slower and harder to adapt to changes such as adding support for new crypto algorithms or scaling to support sudden usage spikes. In the cloud, there is a true need for a key protection solution that offers high flexibility and usability, without compromising on security.

# What do you need in order to control your keys?

**Having control over your cryptographic keys in the cloud means having the ability to see and regulate all aspects of the keys' usage, throughout their lifecycle.**

## 1 PROTECTION OF KEY MATERIAL

Preventing unauthorized use or stealing of key material. This requires not only secure storage and access controls, but also assurance that the cloud provider cannot disclose your keys even if subpoenaed.

## 2 KEY LIFECYCLE MANAGEMENT

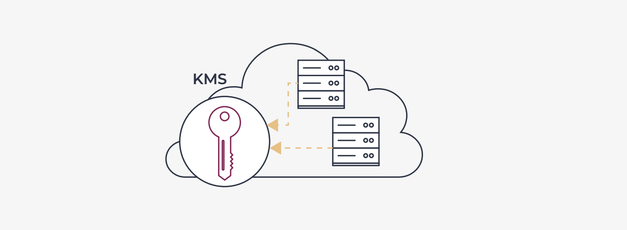
Ability to see and manage all keys, from generation through usage, rotation and revocation. The ability to revoke keys instantly upon need, for example when suspect key usage behavior is detected, is essential.

## 3 LOGGING AND AUDITING

Full real-time tracking of all key operations, for uses such as ongoing management, auditing, reporting, and anomaly detection.

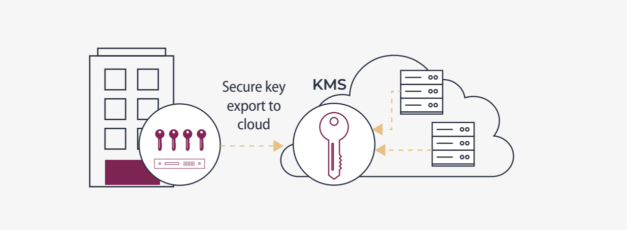
# Current cloud key management options: Tradeoff between control and usability

**CSPs are investing efforts in expanding their IaaS offerings to provide enhanced key control. While current solutions are making progress toward answering customer demands, they still represent a hard compromise between control and usability.**
**Further, current solutions are often vendor-specific and incompatible with other vendors' HSMs, key management and cloud services, adding complexity and cost for customers adopting hybrid cloud environments.**



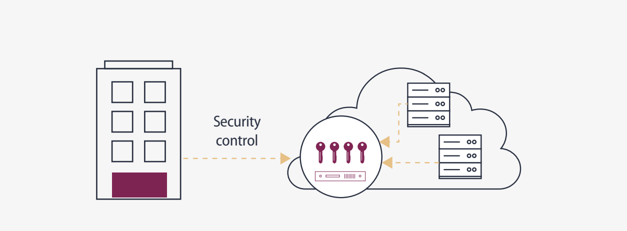
## CSP'S NATIVE KEY MANAGEMENT SERVICE

Cloud IaaS providers offer key management services as part of their security offerings. These services are designed to provide a cloud-native experience, and are typically pre-integrated with a range of other native services of the respective cloud vendor for ease of use. At the same time, the CSP manages the customers' keys while customers have limited or no control over their keys. In addition, customers are bound to the features and usage limitations of the service, and cannot use the keys for general purpose crypto needs.



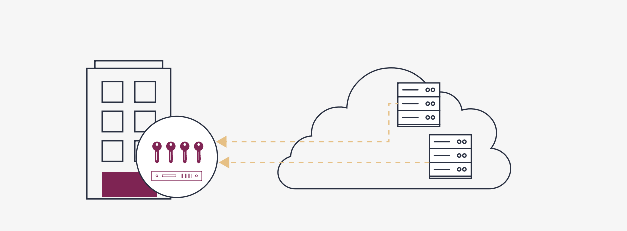
## BRING YOUR OWN KEY (BYOK)

The BYOK feature enables businesses to create their own keys in an on-premises HSM, and then securely export them for use by the cloud IaaS provider's native key management service. This option gives customers more control over their keys. However, once keys are exported and stored in the cloud, they are out of the business' control. This approach is also more complex for customers to maintain than the standard native cloud key management service because they need to manage the HSMs, the full key lifecycle and the export process.



## CLOUD HSM

Some CSPs offer customers the use of dedicated HSMs installed in the cloud. This gives customers yet more control over their keys than native CSP and BYOK options, though less than on-premises HSMs as the HSMs are managed by the CSP. General purpose cryptography is supported, but integration with the provider's native cloud services is limited. Further, the service does not provide key lifecycle management capabilities. Performance, functionality and elasticity are inhibited by the flexibility limitations of hardware.



## HOLD YOUR OWN KEY (HYOK)

The HYOK option is designed to give customers maximum control. In this approach, customers store and fully manage their own keys in an on-premises HSM, and applications in the cloud connect to the on-premises data center to perform cryptographic operations whenever needed. Performance of HYOK is significantly lower than the other options due to the need to transmit much more data across locations. Maintenance and flexibility are also negatively affected due to the need for customers to obtain and manage their own hardware.

# Comparison of current cloud key management options

| | CSP'S NATIVE KEY MANAGEMENT SERVICE | BRING YOUR OWN KEY (BYOK) | CLOUD HSM | HOLD YOUR OWN KEY (HYOK) |
|---|---|---|---|---|
| CONTROL | ○ | ◑ | ◕ | ● |
| PERFORMANCE | ● | ● | ◑ | ◔ |
| MAINTENANCE | ● | ◑ | ◕ | ◔ |
| FUNCTIONALITY | ◑ | ◑ | ◕ | ◕ |
| HYBRID CLOUD SUPPORT | ○ | ◔ | ○ | ◑ |

# New paradigm for cloud computing: Control Your Own Key (CYOK)

**Based on its innovative vHSM technology, Unbound delivers the first pure-software key protection with mathematically guaranteed security at a level comparable with physical HSMs, breaking the control vs. usability tradeoff for cryptographic keys in the cloud.**

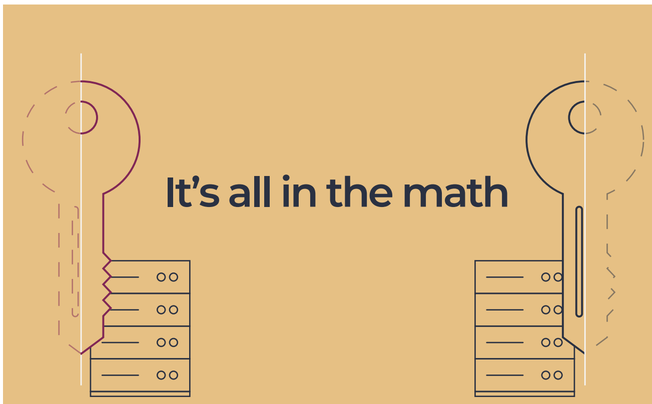
Unbound Key Control is a key protection and management solution that frees businesses to fully leverage the benefits of the public cloud while maintaining strict control of their cryptographic keys.

As a standards-based software solution, Unbound Key Control allows enterprises to centrally manage all their cryptographic keys for all use cases, across clouds and on-premises infrastructure.

Unbound Key Control eliminates the need for traditional physical protection of keys by ensuring that **keys are never exposed in the clear at any point in their lifecycle – not even when generated, in use, or at rest**. By eliminating the single point of compromise, you can stretch the secure boundary far beyond a traditional physical casing.

**Key features:**

- ✓ Runs on any infrastructure: on-premises data center, private cloud, public cloud
- ✓ Full key lifecycle management for all keys across any cloud or on-premises infrastructure
- ✓ Supports all industry-standard HSM and key-management APIs as well as all standard crypto algorithms
- ✓ Full deployment, provisioning, and management automation
- ✓ Easy-to-use interfaces and REST APIs for straightforward integration with cloud-native applications
- ✓ Complete tamper-proof audit logs covering every cryptographic operation



## It’s all in the math

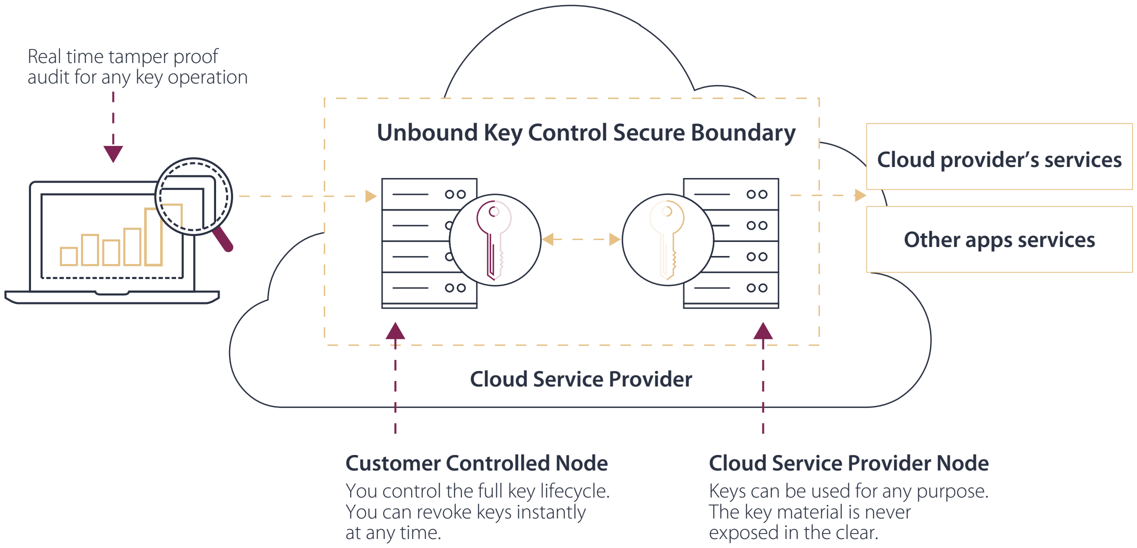
***Unbound vHSM technology** is based on secure multiparty computation (MPC), a field within cryptography that enables the two or more parties to jointly compute a function without revealing their respective inputs. Both privacy of the inputs and correctness of the output are mathematically guaranteed.*

*In this practical implementation of MPC, a cryptographic key is broken randomly into two parts, and crypto functions - for example decrypting content encrypted with an RSA-2048 key - are performed jointly by two machines, each holding a portion of the key. Each side never reveals its key portion to the other. Further, the split to the two random key portions is continually refreshed. Therefore the only way to compromise the key is to compromise both machines simultaneously.*
*For more information, please read our MPC Primer.*

# How to control your own keys with Unbound: deployment examples

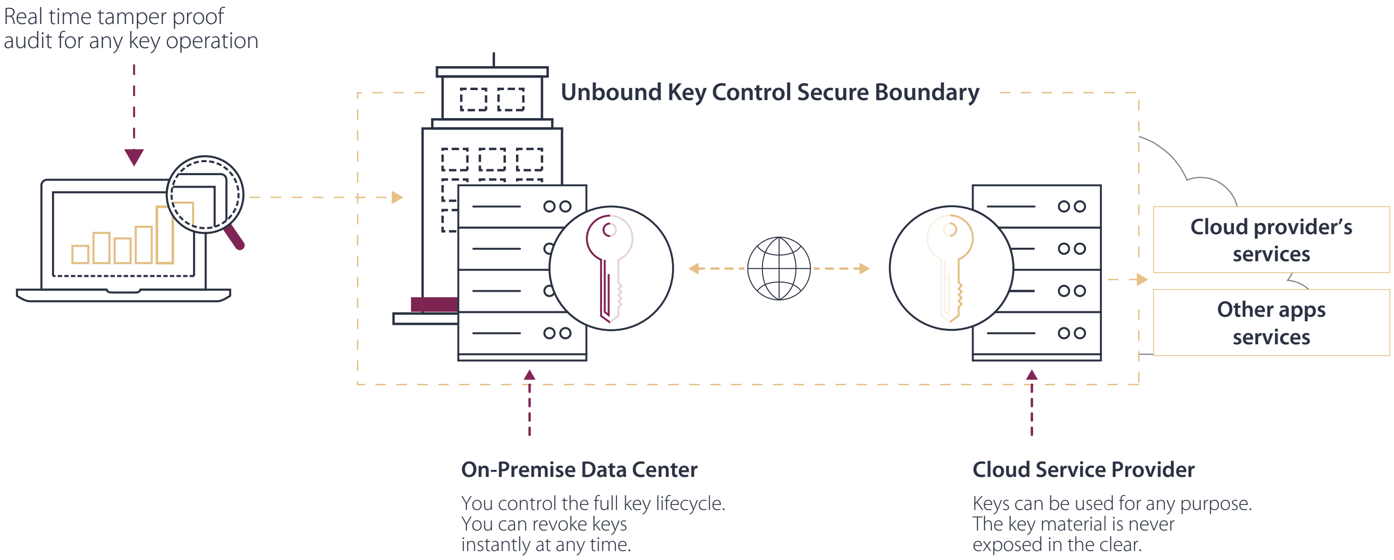
## EXAMPLE 1: CYOK

This implementation of Unbound Key Control (UKC) comprises two separate UKC nodes, both hosted on the same cloud platform. The customer node is controlled by the customer, while the CSP node is managed by the provider. The customer has full control of their own keys via the customer node, while apps can use the cryptographic keys in UKC via integration with the two products.


Real time tamper proof
audit for any key operation
Unbound Key Control Secure Boundary
Cloud provider's services
Other apps services
Cloud Service Provider
Customer Controlled Node
You control the full key lifecycle.
You can revoke keys instantly
at any time.
Cloud Service Provider Node
Keys can be used for any purpose.
The key material is never
exposed in the clear.

## EXAMPLE 2: HYBRID CYOK

In this setup, the UKC customer node is on-premises, while the CSP node is the IaaS cloud platform. The customer has ultimate control of the keys, and it is guaranteed that the keys cannot be compromised by any adversary in the cloud, even by a rogue admin or a CSP served with a subpoena. Apps can use the cryptographic keys in UKC via integration with the two products.


Real time tamper proof
audit for any key operation
Unbound Key Control Secure Boundary
Cloud provider's services
Other apps services
On-Premise Data Center
You control the full key lifecycle.
You can revoke keys
instantly at any time.
Cloud Service Provider
Keys can be used for any purpose.
The key material is never
exposed in the clear.

# What makes CYOK unique?

**Only Unbound lets you fully control your own keys in the cloud while maintaining excellent usability.**

## SECURITY

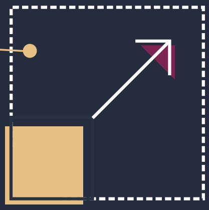
Keys are never in the clear throughout their lifecycle. Keys exist as two random shares stored separately and never united. Full logs and real-time auditing of all crypto operations.

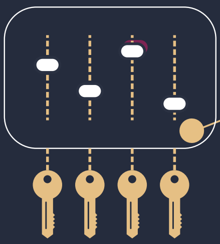
## FLEXIBILITY

Easily extend your key management to any multi- cloud or hybrid environment. Upgrade to support new cryptographic keys and algorithms at the speed of software.

## ELASTICITY

Scale up or scale down key management resources as you need quickly, with an infinitely elastic pure-software solution.





## EFFICIENCY AND EASE-OF-USE

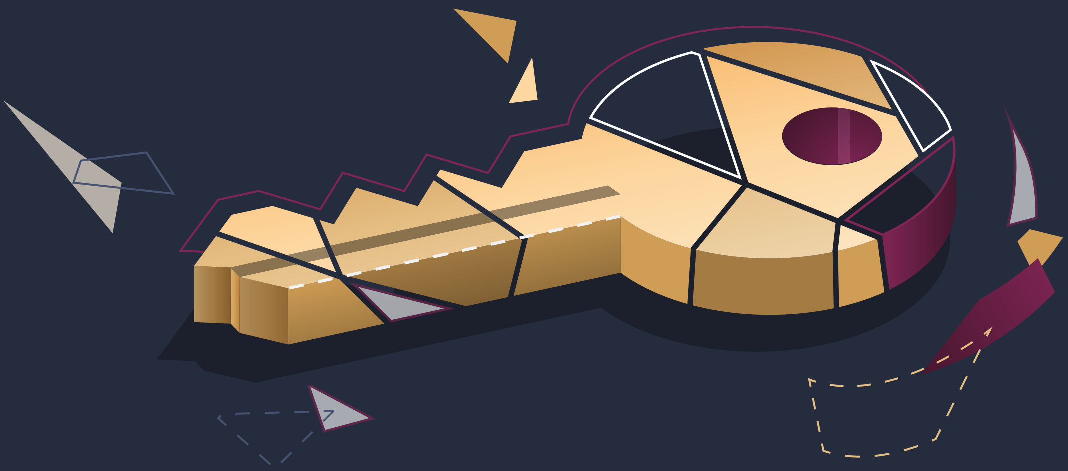
Deploy a single solution across all on-premises, private cloud and public cloud workloads.
Manage all your keys, everywhere, through a single pane of glass.

UNBOUND

# Control your keys

As you migrate more of your core business assets and operations to the cloud, don't compromise when it comes to the foundation of your security – protecting your cryptographic keys.

Gain full control of your keys with a solution that provides you both security at a level comparable with HSM, and all the flexibility and agility of a software-defined solution designed for the cloud.



## Learn how to Control Your Own Keys in Google Cloud Platform

Schedule a Demo

Unbound Tech
www.unboundtech.com | contact@unboundtech.com

Follow Us