STRONGKEY™

MAKE BREACHES IRRELEVANT

OUR STORY.

While much of the cybersecurity industry tries to just keep attackers out through protecting the perimeter, StrongKey is focused on securing on what matters most to organizations: **your sensitive data.**

We provide an open source, comprehensive data security approach, deploying a combination of **encryption, tokenization, strong authentication (both PKI and FIDO), digital signatures, and key management.**

Securing your data this way means that when attackers breach your perimeter, the data they may access is still protected. This is how we **make breaches irrelevant.**

STRONGKEY HIGHLIGHTS.

GLOBAL ADOPTION WITH MARQUEE CUSTOMERS

StrongKey is protecting data in mission critical environments all around the world. Payment processors have trusted us with billions of dollars in transactions, banks with financial documents, and technology companies with their sensitive data.

DIFFERENTIATED PRODUCT, FULLY OPEN SOURCE

StrongKey has created an open source security appliance that has both replaced and won out over established key management companies. Our product — the Tellaro — is both easier to integrate and more affordable to operate than the competition. Our open source software means that our pricing is flat and affordable for customers.

INDUSTRY THOUGHT LEADERSHIP

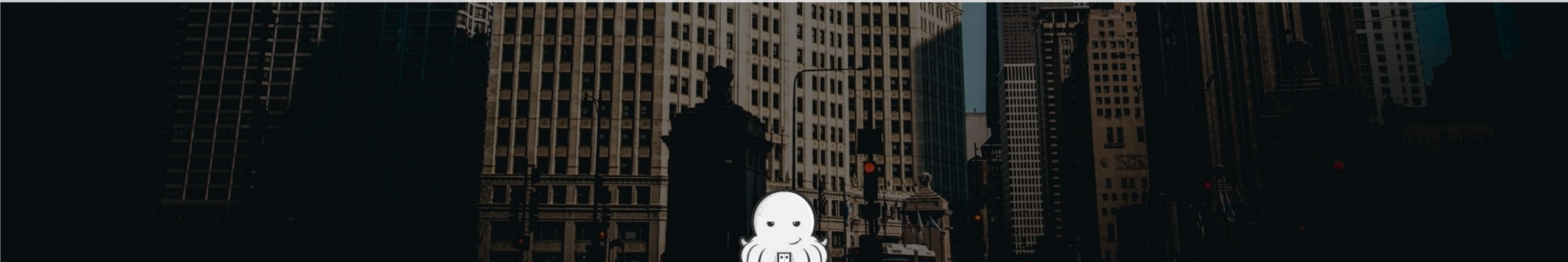
Our deep expertise in key management has led to inclusion on NIST projects, government appointments, and contributions to industry standards. We are prepared and actively developing to the next wave of trends: blockchain, IIoT, and post-quantum encryption.

BUSINESS USE CASES

StrongKey provides a variety of cryptographic services, delivered by our comprehensive security appliance — the Tellaro.

We either host our Tellaro in a cloud environment or deploy it on premises, based on customer operations and risk tolerance.

The following slides outline the various use cases for our cryptographic services.



INDUSTRY: PAYMENTS, BANKING, FINTECH

COMPLIANCE & REGULATIONS

PCI DSS

StrongKey tackles the most difficult controls of PCI DSS (key management). Customers pass their audits in 15 minutes or less. Our current customers include payment processors, banks, and merchants.

On recent deals, new customers have chosen StrongKey over industry giants (Thales and Amazon Web Services), as well as rising stars (Very Good Security). In all of these instances, StrongKey has been cited as both easier and more affordable than the competition.

P2PE

Our appliances underpin our customers who pursue P2PE certification in the payments sector. StrongKey provides end-to-end encryption using DUKPT, and applications never see the credit card number.

This eliminates the prime cause for data breaches and takes our customers' applications out of scope when complying to regulations.

PSD2

The European payments market has new regulations that mandate the use of "Strong Customer Authentication" (SCA) as part of PSD2.

StrongKey delivers SCA leveraging industry standards, including FIDO, which allows for frictionless authentication through biometrics on users devices. This creates an affordable, secure, and compliant way to meet PSD2 regulations.

ENCRYPTION & TOKENIZATION

TOKENIZATION FOR DATA SECURITY

We provide simple ways to encrypt and tokenize payments data, which helps with both data protection and many compliances .

Tokenizing data simply replaces it with a non-sensitive representative "token," meaning the data becomes meaningless to attackers.

FINANCIAL FILE PROTECTION & SHARING

We work with banks around the world to provide secure file protection (e.g., mortgage documents, banking documents) and set up secure file sharing between organizations.

DATA PROTECTION ACROSS INDUSTRIES

PROTECTING PII

We provide simple ways to encrypt and tokenize sensitive data, which helps with both data protection and many compliances (e.g., CMMC, GDPR, CCPA etc.).

Tokenizing data simply replaces it with a non-sensitive representative “token”, meaning the data becomes meaningless to attackers.

StrongKey can encrypt and tokenize billions of any type of object, eliminating the prime cause for data breaches.

FILE PROTECTION AT SCALE

StrongKey can build wide-ranging infrastructure to protect any type of file, including audio and video. This data protection infrastructure can be deployed in a hybrid way to make use of the cloud while securing key storage on prem.

SHARING SENSITIVE FILES

We built CryptoCabinet to provide the most secure transfer of files available using a combination of our key management, encryption, and FIDO strong authentication technologies.

FIDO: PASSWORD-FREE AUTHENTICATION

WHAT IS FIDO?

The FIDO Alliance is solving the world's password problem. Both a standard and an alliance of companies, FIDO is replacing passwords with something simpler and stronger: biometrics or physical keys. Learn more at loginwithfido.com

WHO SHOULD DEPLOY FIDO?

Any company or service that provides user authentication, whether it is username/password, multi-factor, or PKI, is a good candidate for adopting a FIDO server. FIDO authentication is both more secure and more user-friendly.

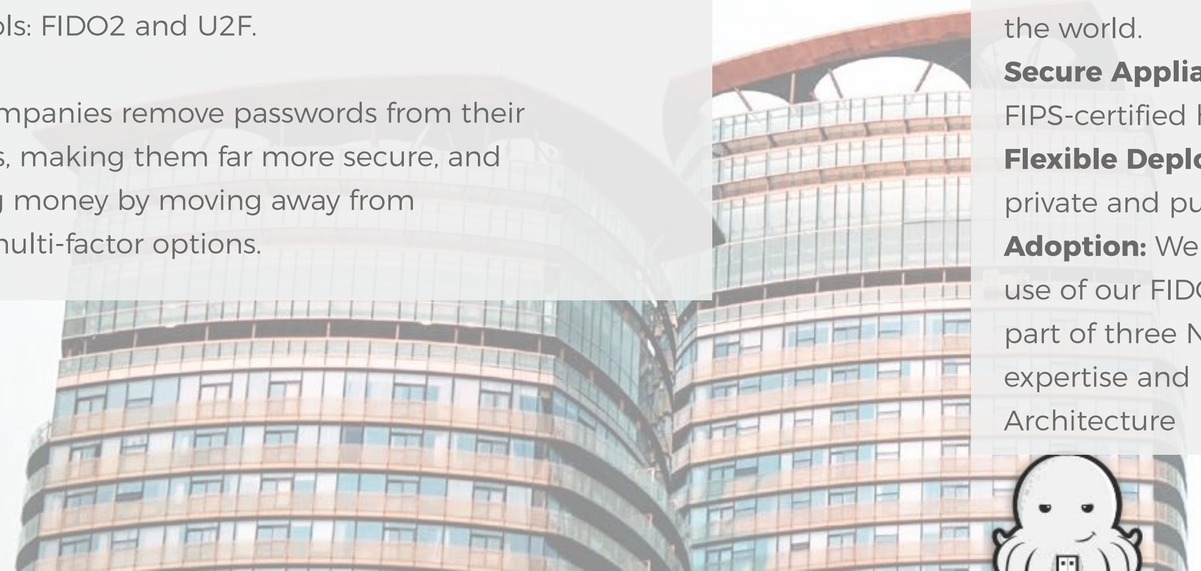
STRONGKEY AND FIDO

StrongKey has been a FIDO member since 2014, Our FIDO server is FIDO-Certified, making it the world's **first and only** open source FIDO server for two protocols: FIDO2 and U2F.

We help companies remove passwords from their applications, making them far more secure, and often saving money by moving away from expensive multi-factor options.

STRONGKEY'S FIDO SERVER

Full Featured: Enterprise-grade, FIDO-certified, and open source.
Expertly Built: Built by a company with 20 years of expertise in cryptographic key management and building PKIs all over the world.
Secure Appliance: When desired, FIDO can be deployed on FIPS-certified hardware.
Flexible Deployment: We can deploy FIDO in the cloud (both private and public) or into a customer's physical environment.
Adoption: We have customers in Europe and the U.S. making use of our FIDO server to improve their security. We've been a part of three NIST NCCoE projects making use of our FIDO expertise and FIDO server as a component of their Reference Architecture



FIDO USE CASES

REPLACE PASSWORDS & STRENGTHEN MFA

Any application that currently uses passwords can replace those passwords with FIDO, offer FIDO as a secure alternative, or use FIDO in place of current multi-factor options.

Organizations can integrate our FIDO server to remove passwords from their applications. This means better security and decreased costs (from fewer password resets and SMS charges).

PROTECT LEGACY WEBSITES

StrongKey has created a FIDO gateway to protect older websites that can't be modified directly to use FIDO.

Similar to a single sign-on mechanism, users can log into one FIDO-protected gateway and have access to multiple applications and websites — even those that can't be directly modified for FIDO.

MITIGATING E-COMMERCE FRAUD

StrongKey worked with NIST's National Cybersecurity Center of Excellence to leverage FIDO technology (using our product) to mitigate against e-commerce fraud.

FIDO can be used to decrease fraud during transactions.

PKI2FIDO

Many organizations currently rely on legacy PKI systems, particularly in banking and government. They may want to move to FIDO, so we have created an application that easily ports their credentials.

StrongKey is unique in our background in PKI and expertise in FIDO and can consult with organizations understanding how to navigate both environments.

PSD2

StrongKey FIDO can be used to fulfill the Strong Customer Authentication mandate of Europe's PSD2 regulations in a frictionless way.

TRANSACTION CONFIRMATION

Beyond PSD2, FIDO can be used to confirm any transaction to ensure it comes from an authorized user. We have demonstrated this use case in viewing and exchanging medical information as well as payments transactions.

Please note: While the NCCoE competitively selected StrongKey, the NCCoE and NIST do not explicitly endorse companies or products.

PUBLIC KEY INFRASTRUCTURE

OUR CAPABILITIES

PKI

A PKI from StrongKey has the following benefits:

- Simplifies certificate life cycle management
- Protects sensitive data collected by IOT devices
- Authenticate humans, servers, routers, WAPs, applications, IOT, etc.
- Issues and manages tens of millions of digital certificates
- SOAP/REST web services for custom integration
- Hosted, on-premises, and hybrid solutions available

OUR BACKGROUND

We have been in the PKI business for almost 20 years, with implementations across the globe. We have built a PKI for one of the largest pharmaceutical companies in the world, a central bank of a country, and one of the largest telecoms, among others.

OPEN SOURCE

Our open source architecture guarantees your costs stay low, and comes with no per-certificate fees or usage limits.

QUICK DEPLOYMENT

We have extensive experience in being able to set up PKIs in under 90 days.

INDUSTRY FITS & USE CASES

INDUSTRIAL IOT & DEVICE KEY MANAGEMENT

Our key management and flexible deployment can be embedded in industrial IOT devices and environments. This ensures the security of the data the devices receive, store, send, and process. Use cases extend through Smart Cities, manufacturing, and power.

MEDICAL DEVICES

We have secured connected medical devices to combat counterfeiting.

TRADITIONAL PKI DEPLOYMENTS

Any environment involving smart card personnel authentication systems.

KEY MANAGEMENT: OTHER USE CASES & READY-TO-DEPLOY BUSINESS SOLUTIONS

Key management is the root of all we do. We often have undertaken projects that involve customization that we later turn into product offerings. These are a listing of these use cases.

SITE CERTIFICATE MANAGEMENT

Centrally and automatically manages the lifecycle of free TLS server certificates, using the ACME protocol from LetsEncrypt.org.

CRYPTOCABINET FOR SECURE FILE SHARING

We built CryptoCabinet to provide the most secure transfer of files available using a combination of our key management, encryption, and FIDO strong authentication technologies.

RANSOMWARE SOLUTIONS

CryptoCabinet can also be used to protect files against the threat of ransomware.

DIGITAL SIGNATURES FOR DATA INTEGRITY

StrongKey can deploy digital signatures within workflows to ensure data integrity. The signing keys are strongly protected. This workflow can fit into existing customer architectures.

SELF ENCRYPTING DRIVE PROTECTION

Organizations who have too much information to encrypt at the application layer can make use of StrongKey to protect Self-Encrypting Drives (SEDs). We provide a fully automated process for provisioning, escrow, and recovery of millions of keys.

WHY STRONGKEY TELLARO?

COMPETITIVE DIFFERENTIATION OF OUR PRODUCT

EASE OF IMPLEMENTATION

We expose a simple API for our customers to integrate. There's no proprietary code, and no lock-in. Customers have integrated in as little as an hour.

AFFORDABLE

Because we are open source, our customers use the appliances as much as they want — unlimited applications, transactions, users, and records.

SECURE AND FLEXIBLE

We only offer the most secure deployments: single tenancy and exclusive customer ownership of keys — but we offer on-prem and hosted solutions.

SCALABLE OPTIONS

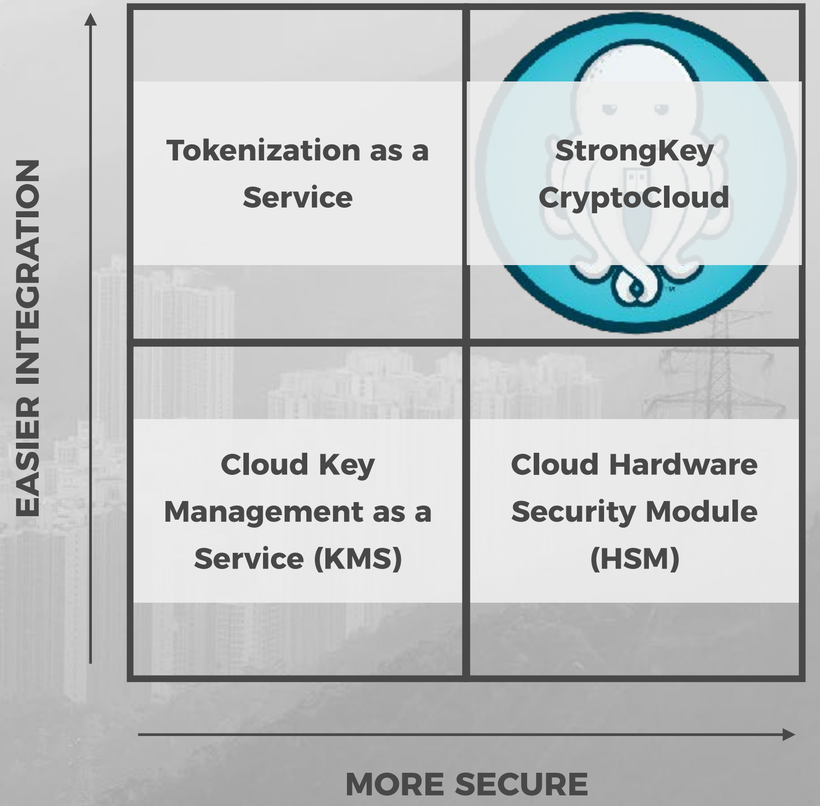
We offer multiple appliance sizes, the smallest appropriate for even a small startup — but the core cryptography is the same. It's easy to grow and scale with StrongKey.

STRONGKEY CRYPTOCLOUD

StrongKey CryptoCloud gives you the ease of cloud key management with the security of single-tenant hardware. Work with our simple APIs to integrate industry-leading cryptography secured by FIPS-certified hardware hosted on dedicated, single-tenant appliances in StrongKey's data centers. StrongKey's CryptoCloud is a complete and flexible cryptographic solution that enables the flexibility of cloud deployments while not compromising on security.

BENEFITS:

- Dedicated cryptographic hardware, with you controlling all keys
- Scales with your business
- Affordable and open source
- Secure, while still taking advantage of the cloud's benefits



STRONGKEY TELLARO.

The Tellaro

Our security appliance is called the “Tellaro.”
The appliance can be deployed on premises, or hosted by StrongKey or a partner as cloud cryptographic services.

Deployment Options:

- On premise. Appliances reside in customers’ data centers, which gives maximum control and security.
- Private Cloud: A single-tenant hosting in StrongKey affiliated data centers, giving minimal effort with high security.
- Multi-Tenant Cloud: Select cryptographic services are available in a multi-tenant fashion, providing cost savings with high levels of security.

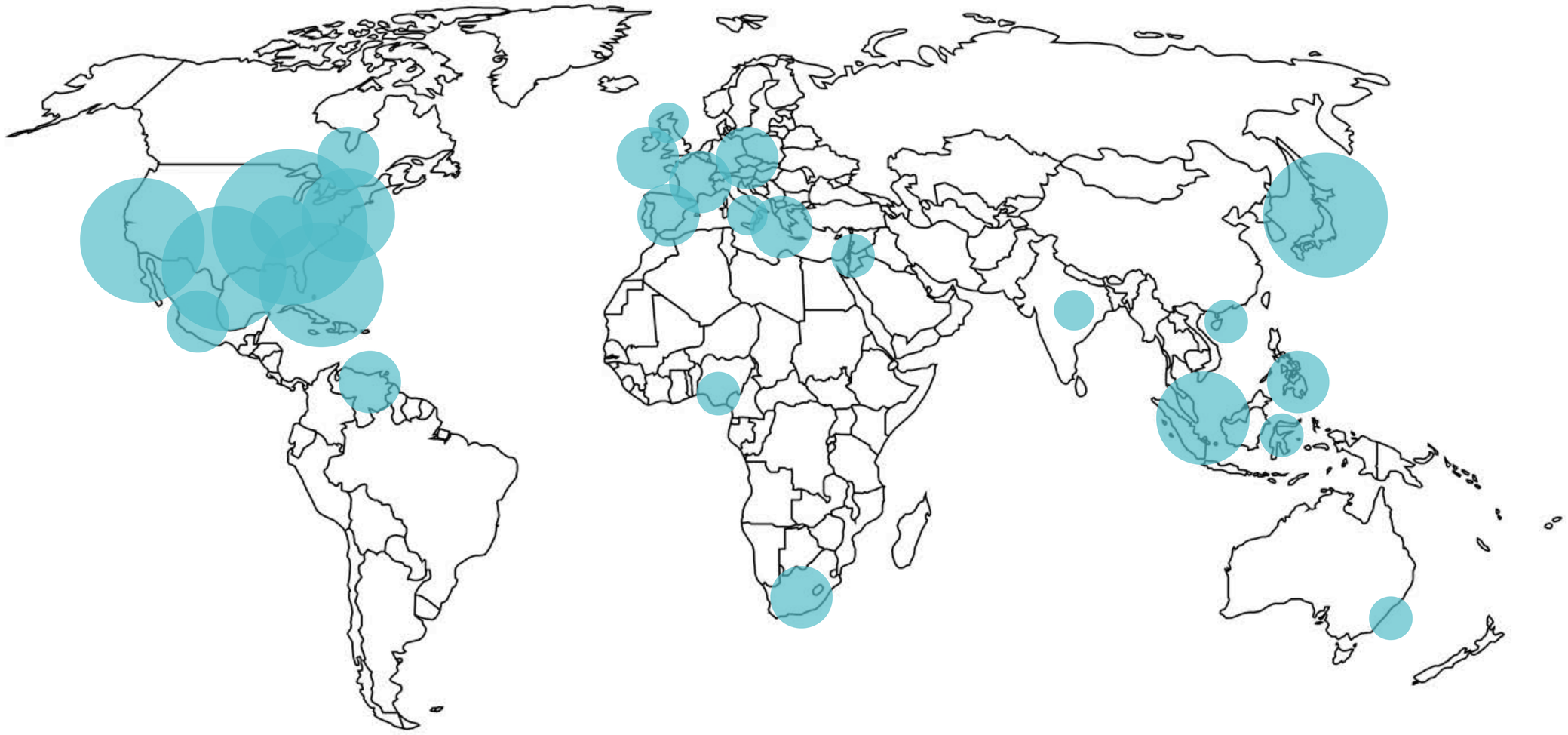
Every Appliance comes with:

- Single-tenant, FIPS 140-2 Certified Hardware Cryptoprocessor (HSM or TPM) to Level 2 or 3, depending on customer choice
- High Availability with Active-Active Clustering
- Option for Client Key Custodians / Client-controlled Keys
- Easy-to-integrate REST and SOAP web service APIs, taking the complexity out of cryptography
- Access to StrongKey’s U.S. support team to help with integration, troubleshooting, and security patching

FIPS-Certified Hardware Key Management Appliances

STRONGKEY CUSTOMER BASE

StrongKey has a global customer base and partner network.
Our top industry served is payments and fintech, while we also have presence in banking, technology, health care, telecommunications, and government.
Our customer sizes range from startups to large enterprises.



THANKS!

HTTPS://STRONGKEY.COM
GETSECURE@STRONGKEY.COM