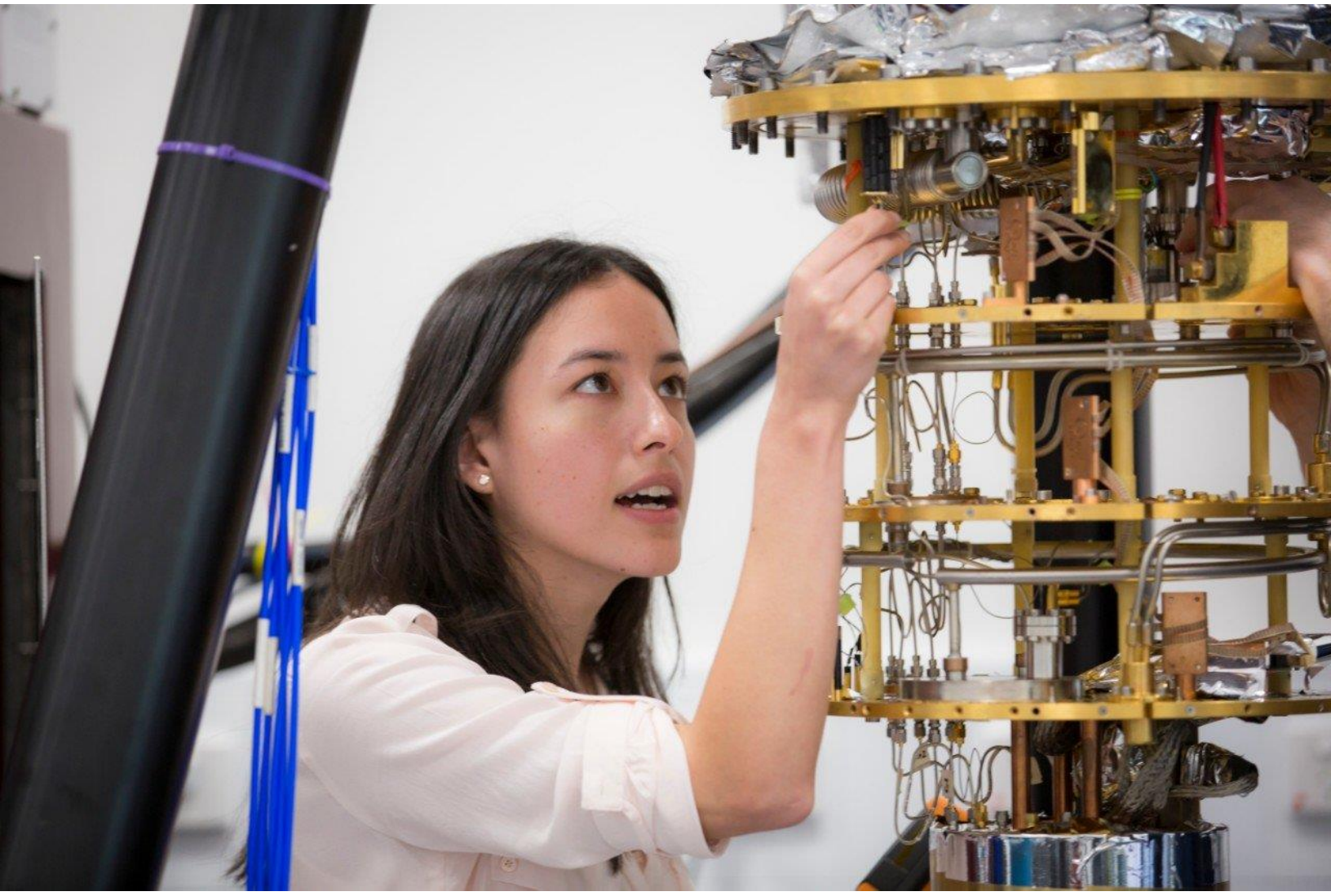
Secured2 Quantum-Secure™
Whitepaper 2023

Secured2, the world's first quantum-secure data protection



www.secured2.com

Executive Level Summary

- Secured2 utilizes a game-changing new form of data security called **QuantaMorphic™ Physical-Based Data Security,** the world's first commercially available and widely used quantum-secure™ security. We have been in the market for six years with our groundbreaking security servicing companies that range from banks, law firms, healthcare providers, and local government.

- S2 owns a complete, end-to-end solution to the terrifying cyber crises that threaten our nation and economy. It is instantly scalable and "plug and play." It has been crashed-tested by dozens of cyber experts at the highest levels of the commercial, academic, and Intelligence communities **without a single breach** of our security. **Our solution is backed by a cyber indemnification warranty from Lloyd's of London.**

- Secured2 protects data beyond encryption and is quantum-secure™ with our patented **shrink> shred> secure> restore** methodology. Data for storage is masked, compressed, randomized & anonymized with our quantum-secure™ security. Data is shredded into small segments, and each segment is given a layer of NIST standards-based encryption for added complexity, but it is not required to be quantum-secure™. All data sent over the wire is non-sequentially sent, so packet sniffers and bad actors cannot decipher the data transmitted over the Internet, wireless networks, or satellite systems. Secured2's quantum-secure™ security fits inside today's existing security investments. So, no hardware or retooling of the Internet like other quantum solutions.

- Secured2 is **delivered as an API** to easily be integrated into applications, run from the cloud, private cloud, or local storage. It can be deployed as a transport protocol using 'book-ends' and modified to fit into an ASIC chip that provides hardware-level data security. **Secured2 is NOT data sharding** a horizontal scaling technology. We are a security technology that shreds data and physically disperses the digital confetti our algorithm creates.

- The Secured2 is the most **cost-effective** security solution in the market today. It will significantly reduce the expense of becoming quantum-secure™ as we don't require expensive quantum computers or force customers to move off existing cyber security investments. We fit inside your existing infrastructure and are a software solution.

- It's no coincidence that we have developed strategic partnerships with Microsoft, AWS, Google, and Oracle.

Disclaimer

The information provided in this document was created in December 2022 and is accurate as of the time of this writing. Secured2's systems, platform, technology, and policies are ever-changing to protect our customers. Therefore, it is possible that some of the information could change as we continually improve our services to exceed our customer's growing needs.

Introduction

Private organizations and branches of the Government / Military regard data security as one of their most pressing challenges. At Secured2, we recognize that security is not only a top priority but an immediate need. We have been diligently developing the next-generation data security technology that will protect your data no matter where it lives or is sent.

From data traveling across the Internet, moving between data centers, sending across wireless or satellite networks, or data at rest in the cloud, the Secured2 solution was designed to protect your data from any unauthorized breach.

We wrote this document to help CEOs, CIOs, CISOs, and security operations teams who want to learn more about Secured2 gain a deeper understanding of our technology. We have assumed that the reader of this document has a basic understanding of cryptographic and quantum computing concepts.

The evolution of our encrypted systems & the quantum threat

Traditional encryption has been described as taking data as input (called plaintext) and transforming the plaintext into an output (called ciphertext) which is now protected. This is done through an algorithm, such as the Advanced Encryption Standard (AES). AES encryption requires a 'secret' or 'key' to unlock or decrypt the ciphertext back into its plaintext format. This security algorithm was first published in 2001 and has been the standard for global data security since.

AES encryption has a significant shortcoming. Its developer, Joan Daemen, and Vincent Rijmen, have provided no mathematical proofs that can demonstrate that AES encryption is secure. The only claim they have made is that it would take the most powerful classical computer more than 1000+ years to brute force attack the AES algorithm. This mistakenly assumed that computers would not advance in processing power, nor would factoring algorithms be developed to accelerate the factoring of large numbers. These two events have accelerated the ability to brute force factor the AES encryption keys and break the algorithm.

As we look at the cybersecurity space today, nation-states like China, Russia, and the United States, have spent billions of dollars developing computational infrastructure and algorithmic capabilities that can break AES encryption. It's well known that the most significant nation-states, including the United States, have ongoing offensive information-gathering programs.

Code breaking has rapidly evolved over the past few years as new computational capabilities have emerged, such as exascale computing and quantum computing. These large computing platforms are capable of unrivaled data processing. Today, an exascale computer can do 1000 petaflops of processing. That's 1000 quadrillion calculations per second. That may sound fast, but the fastest known quantum computer from China, called the Zuchongchi 2.1 now capable of 66 qubits. This astonishing processing power is 10 million times the speed of the world's fastest supercomputer.

We need to worry about these new developments in computational power, along with new software programs that can harness this computing power to break encryption. These programs find patterns in the AES random number generator (that is only a pseudo-random number) and decrypt the keys. This is not a brute force attack on one key, but it is an attack that will disarm AES encryption. When you combine the processing power of these computers with new software programs, encryption cannot protect data no matter where it is stored. Therefore, there is an immediate risk to all our encrypted systems and why the Internet, our data, and our encrypted systems are at risk.

Where will these threats emerge? China will be the first nation-state to use this technology against the United States. Today, China is leading the quantum revolution. They have twice as many patents as the United States. They are also investing over $10 billion in the country's National Laboratory for Quantum Information Sciences and developing the largest quantum computer in the world. These advancements give China significant capabilities and pose an immediate threat to our country and global allies.

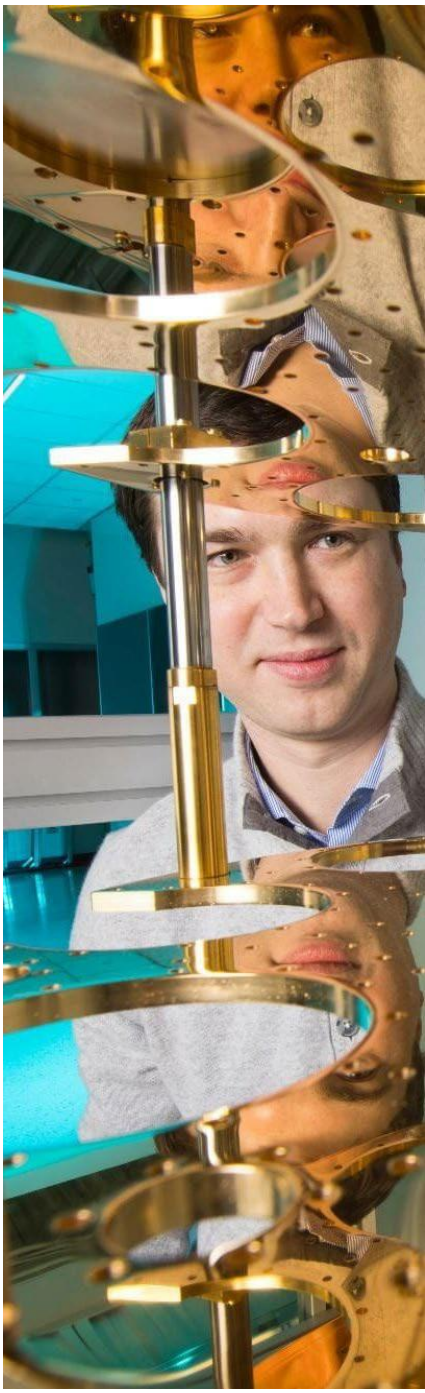
Why most quantum encryption efforts are failing

As quantum computers are moving from the lab into operation, there is a rush for companies to develop post-quantum encryption. You are hearing terms like quantum-resilient, quantum-proof, quantum-secure™ , quantum encryption, and quantum cryptography used frequently. There are now many terms to describe different approaches to protecting data and ensuring secure communications. So, how do you make sense of everything, and what technology protects data?

First, to understand the quantum security market space, you must understand basic concepts and how they are deployed. Today there are three main areas of quantum data security, each with a different approach to data protection:

- Post-Quantum Cryptography
- Quantum Key Distribution (QKD)
- Quantum Cryptography

When we started Secured2, we evaluated all these concepts and spent countless hours researching these different approaches from a technical perspective. We soon recognized that the technologies mentioned above are not the future and do not solve the data security problem in a post-quantum world.



Here, I summarize each approach being developed and why we chose not to pursue development:

Post-Quantum Cryptography

Post-Quantum Cryptography describes algorithms that prevent direct attack by a quantum computer. These use mathematically based formulas to protect the public-key infrastructure. Many of these algorithms have been developed through the NIST post-quantum program to develop new standards to protect our data systems.

***Risk factors*:** To date, NIST released its four finalist algorithms, and of the four in the first two weeks, the two main algorithms, Crystals-Kyber and SIKE, were both breached. SIKE was breached using a single CPU classical desktop computer which was very damning for the algorithm. The viability of these new algorithms is suspect, and to date, the leaders of DoD/DISA acknowledge they have no faith in these new algorithms and shouldn't. They are all based on mathematical complexity, which we have learned can be broken. The days of 'complex math' protecting data are over.

Quantum Key Distribution (QKD)

QKD is a communication method that implements a cryptographic protocol utilizing quantum mechanics. It allows two parties to share a random secret key known only to them. This secret key can encrypt and decrypt messages. A primary function of QKD is detecting any third party trying to gain knowledge of the key.

One component of this new method of security is using quantum superpositions and quantum entanglement to transmit information in a quantum state. If anyone intercepts the communication, this interruption will disrupt the quantum state, and the communication is aborted, protecting the communication.

Risk factors: QKD falls short as a viable solution. It's expensive, hard to implement, requires specialized hardware, and is still an unproven solution. As Bruce Schneier, a leading cyber security expert, said, "QKD is as useless as it is expensive."

Quantum Cryptography

Quantum Cryptography (aka Quantum Encryption or Quantum Security) is known as the practice of leveraging quantum mechanics to enhance security and to detect a bad actor, who is eavesdropping on secure communication. Quantum cryptography utilizes the laws of physics that say's "it's impossible to identify the location of a particle without changing the state of the particle." The technology works by sending photons, which are "quantum particles" of light that are sent across an optical link.

Risk factors: The challenges with Quantum Cryptography are it's expensive to implement, needs specialized equipment, has limited signal distance, and isn't tested enough to know its complete risk profile. Several companies, including Google, IBM, and Toshiba, have announced initiatives in this area. To date, there is still no commercially available solution, and it will take years to turn quantum cryptography into something that can be consumed by the mass markets.

As we examined the above technologies, we concluded that none of these could meet our objective of providing post-quantum data security.

Secured2's game-changing approach to quantum-secure™ security

As we developed our quantum-secure™ physical-based security, we had several critical requirements for our solution, including the following.

- Protect data at rest and in transit without the need for math-based encryption
- Must be quantum-secure™, API-delivered, and embeddable
- Must fit inside of today's existing Internet, encryption, and PKI standards
- Don't rebuild the entire Internet and go through years of validation
- Don't require special hardware or costly equipment
- Make it easy to deploy and integrate
- Works with all significant storage vendors, collocation, and cloud providers

The solution that Secured2 developed to address all these factors and the need for immediate quantum-secure™ security is what we call QuantaMorphic™ Data Security (QMDS). QMDS is a new way to think about protecting data by running data through a multi-step algorithm that protects data beyond encryption and is quantum-secure™ .

The Secured2 solution can be implemented quickly via cloud services, an API, or direction integrations. The flexible nature of our security algorithm makes implementation easy, but we can embed it into cloud services or place our security at the disk level in a cloud stack. The flexibility around deployment makes it unique in the industry. Think of Secured2 as a data processing technology.

One future aspect we are looking to develop is to modify our security algorithm to fit into an ASIC chip, embedding our technology into the operating system. This will protect data from a CPU and move it directly into multiple partitions in a hard drive. No one is offering this product today, and our relationship with Intel can quickly integrate our solution into chips.

Secured2's quantum-secure™ protection of data at rest

Secured2 protects all customer data stored at rest using our industry-leading quantum-secure™ security. We can do this with no action or intervention by Peraton or your customers.

Secured2's multi-step algorithm

Secured2 uses several layers to protect data. A layered approach creates complexity and redundancy that will thwart any bad actor trying to gain access to protected data.

To understand how Secured2 protects data, it is essential to know how Secured2 protects customers' data using our **shrink > shred > secure > restore** methodology.

The first step of our algorithm **'shrinks'** data by compressing the data utilizing our proprietary compression method. This method can reduce the data size by up to 80% for ASCII data and a lesser amount for already compressed data, like video files. Our compression solution works on all formats of known data and is the base layer of our algorithm. As part of 'shrinking' data, we also 'convert' data into a random format unreadable to a bad actor and act as an additional protection layer.

The second step in our algorithm is the **'shred'** layer of protection. In this step, we take the compressed file and break it into randomized segments that turn a file into digital confetti.

The third step adds a layer of **'secure'** protection by adding a layer of encryption. We provide the option of AES encryption to meet NIST standards and can also implement the new NIST post-quantum encryption standards. We do not need to add an encryption layer for protection. We only do it to meet NIST standards and fit inside existing PKI investments.

The last step is to restore data. To do this, a user verifies identity from any authentication methods, and our solution reverses the process to restore the shredded data segments.

In a typical implementation, Secured2 QuantaMorphic™ security is delivered as an API but is flexible and can even be integrated into ASIC chip technology.

QuantaMorphic™ Data Security

As the market races to find new ways to augment or even replace current encryption systems due to the quantum threat, Secured2 has developed, patented, and presented the industry's first, vetted, tested, and viable post-quantum data security solution. Our industry-leading QuantaMorphic™ solution utilizes our patented technologies and concepts that include:

- **Data conversion** – converting data into a random format that masks the data.
- **Binary data segmentation** –breaking data into small segments, each individually encrypted using classical AES encryption or new NIST post-quantum encryption algorithms.
- **Decentralized / Multi-Mesh Storage** –distributing data fragments into multiple clouds, hybrid, or local storage locations.
- **Non-Sequential Packet Delivery** –sending data packets randomly, with no sequential order, and eliminating the threats of packet sniffing or other means of data gathering.

These unique solutions, when combined, provide the unique and quantum-secure™ features of QuantaMorphic™ data security. Unlike traditional encryption that relies on 'math' to protect data, QuantaMorphic™ security protects data through randomization, binary data separation, and non-sequential delivery of data across the Internet. We only allow the data to be reassembled if the recipient or user can use physical verification or identification system like facial recognition, MFA, Biometrics, etc.

Secured2 can fit inside your existing security investments

To implement an emerging data security technology, you must meet, then exceed, the pre-existing standards that have taken years to create, proliferate, and mature. The emerging quantum cryptographic solutions do not fit these existing standards and will require years of evaluation before becoming an industry standard. Secured2 is unique because we not only meet these standards, but we also fit inside these standards.

The Secured2 quantum-secure™ solution is a 'data processing' technology that transforms, randomizes, physically separates, and disperses data into physically separated locations. By function, our security is secure but what's different about our quantum-secure™ security is that our solution fits directly inside the existing security investments already in place. For instance, we can use transport layer security (TLS), we can leverage AES encryption for each packet of data in our shredding process, and we can even leverage FDE encryption at rest. We also can incorporate any future standards into our solution quickly. By building our solution this way, we can take advantage of existing standards but enhance them to make the solutions 'quantum-secure™ .'

The Secured2 solution can be implemented quickly via cloud services, an API, or direction integrations. The flexible nature of our security algorithm makes implementation easy, but we can embed it into cloud services or place our security at the disk level in a cloud stack. The flexibility around deployment makes it unique in the industry.

One future aspect we are looking to develop is to modify our security algorithm to fit into an ASIC chip, embedding our technology into the operating system. This will protect data from a CPU and move it directly into multiple partitions in a hard drive. No one is offering this product today, and with our development partner Foxconn we believe we can quickly build this solution.

Secured2's quantum-secure™ protection of data at rest

Secured2 protects all customer data stored at rest using our industry-leading quantum-secure™ security. We can do this with no action or intervention by Peraton or your customers.

Secured2's multi-step algorithm

Secured2 uses several layers to protect data. A layered approach creates complexity and redundancy that will thwart any bad-actor trying to gain access to protected data. We are quantum resistant because even if you break the encryption layer, data is still protected.

To understand how Secured2 specifically protects data, it is crucial to know how Secured2 protects customers' data using our **shrink > shred > secure > restore** methodology.

The first step of our algorithm **'shrinks'** data by compressing the data utilizing our proprietary compression method. This method can reduce the data size by up to 80% for ASCII data and a lesser amount for already compressed data, like video files. Our compression solution works on all formats of known data and is the base layer of our algorithm. As part of 'shrinking' data, we also 'convert' data into a random format unreadable to a bad-actor and acts as an additional layer of protection.

The second step in our algorithm is the **'shred'** layer of protection. In this step, we take the compressed file and break it into small segments that are user-defined in size. Typically, a standard implementation will have 5K segments of binary shredded, then put in a randomized sequence, so there is no specific order of the segments. Each segment gets mapped, and that map is also shredded & seeded for extra protection. As a final step, we add a layer of AES encryption to each individual segment to ensure we meet today's existing data security standards and add additional layers of complexity to the design of our multi-step algorithm.

In the third step, **'secure,'** we take the highly scrambled and randomized 5k data segments and transmit them randomly across the wire using TLS. In this step, data is converted, randomized, compressed, encrypted, and sent randomly over the wire. If a hacker intercepts a transmission, they get unusable data. We send the data randomly into a decentralized mesh of at least three physically separated storage containers that are user-defined. Secured2 is storage agnostic on the backend of our solution and fits into any storage solution in the market today. All we need is a destination to deliver protected data segments.

In the last step, **'restore,'** customers can quickly and easily reconstitute the highly secure data by providing identity using a customer's authentication. With a standard installation, we utilize industry-leading authentication solutions such as Google Auth, Microsoft Auth, and AWS Cognito. We can also support any authentication system a customer chooses for an additional integration fee.

Secured2 Key Management

Secured2's proprietary key generation solution

For every Secured2 customer, all data stored at rest or sent over the wire runs through our security algorithm. As part of this process, we use encryption and other proprietary methods to protect data. Since we use encryption, we do hold two sets of encryption keys. One of the weak points in any security solution is holding keys. In most cloud implementations, the cloud providers hold the keys and can access any data stored in their cloud environments. Some cloud providers, like AWS, allow you to use your own key management solutions, but this function is generally limited to large IT organizations with the capability to manage keys. Usually, companies use a third-party vendor to manage keys or the cloud providers themselves.

Secured2 has developed a unique way to generate private keys, which differs from every cloud data provider today. First, it's based on a randomized seed and password associated with a dual private key. Second, each segment within a file gets a new seed and password. We do this because it adds extra layers of data protection. So, if you unencrypt one file segment, you cannot put together the whole file. This concept ensures we put controls and methods in place that make it impossible for a bad actor to compromise any data segment they intercept or steal.

Our unique key structure makes it impossible for bad actors to break our security. To breach our security with a typical email, a bad actor would have to find the physically separated storage containers where the segments live (3 or more to thousands). The bad actor would then have to decrypt each small 5k segment and know the exact order to restore the data segments. Then the bad actor would need to decompress and unmask the trans-mutated data with our masking technology. The hacker would need to verify identity to reverse the process and would have to break the industries' best identity management systems.

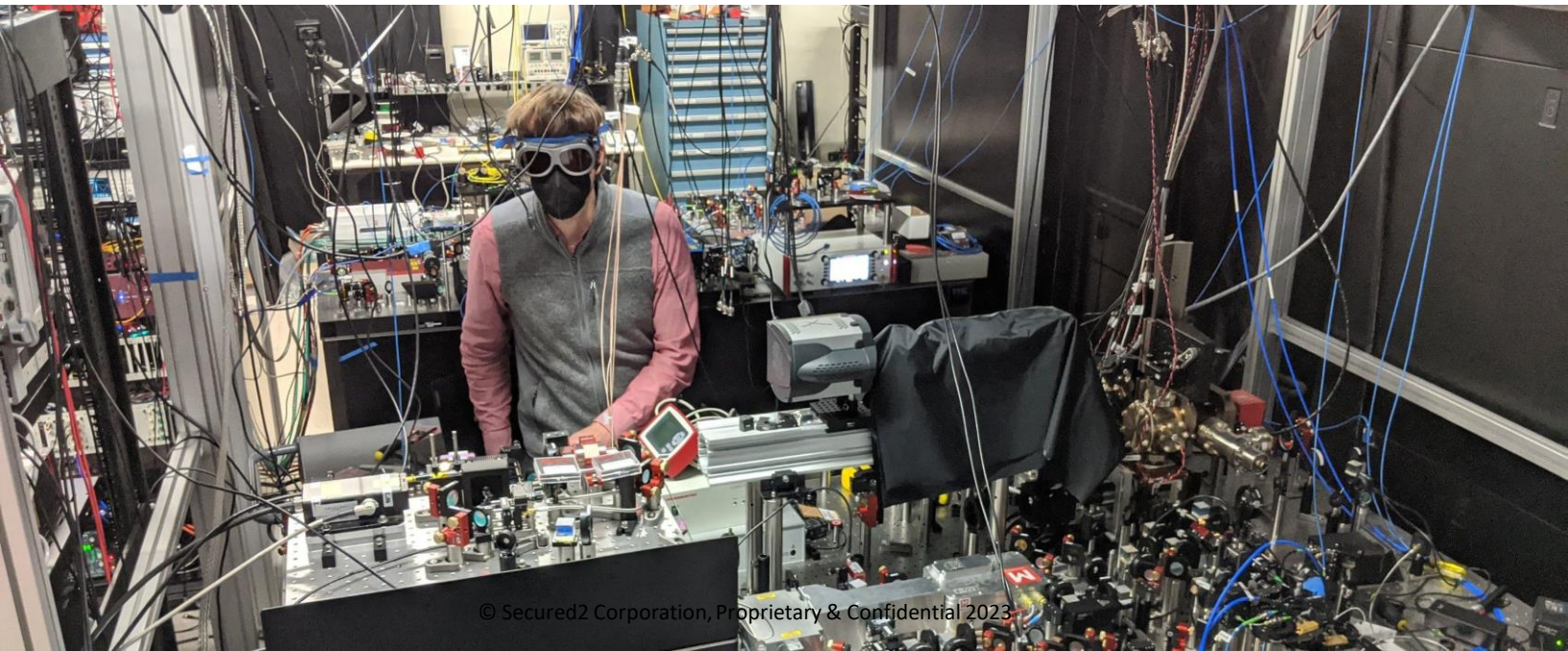
See Addendum A

How does our multi-step algorithm work?

To better understand the flow of data through our algorithm, exhibit B is a graphic that illustrates from the point of data origin to secure data in transit to self-defined storage (cloud, multi-cloud, local, or hybrid).

Starting on the left, data is created on a device (PC, laptop, tablet, mobile device), and the data is secured via an application integrated with our security. The data is then ingested into our security through an event-based API integrated into the application. After the data is ingested, it's run through our multi-step algorithm that protects the data beyond encryption, making it quantum-secure™ . Then the data is randomly transmitted over the wire and randomly distributed into customer-defined storage.

See Exhibit B



Isn't Secured2 like Data Sharding?

Many IT professionals have confused Secured2 with a technology called 'data sharding.' Sharding has been available for years and was introduced in the 90s to facilitate the horizontal scaling of a database. It breaks data into two or more chunks called logical shards. These shards get distributed across separated database nodes called physical shards. So, all the shards, when combined, equal the entire dataset. Sharding was developed because it solved the problem of spreading the load of large databases allowing for faster processing. Extensive database queries can get slow, and sharding offers a way to 'speed up' the queries. This technique is also contrasted against another scaling technique called vertical scaling, which involves upgrading the hardware to achieve faster queries. This means adding faster CPU and Memory to achieve database speed improvements. Secured2 does not utilize sharding nor is sharding a security technology. It's a storage technology.

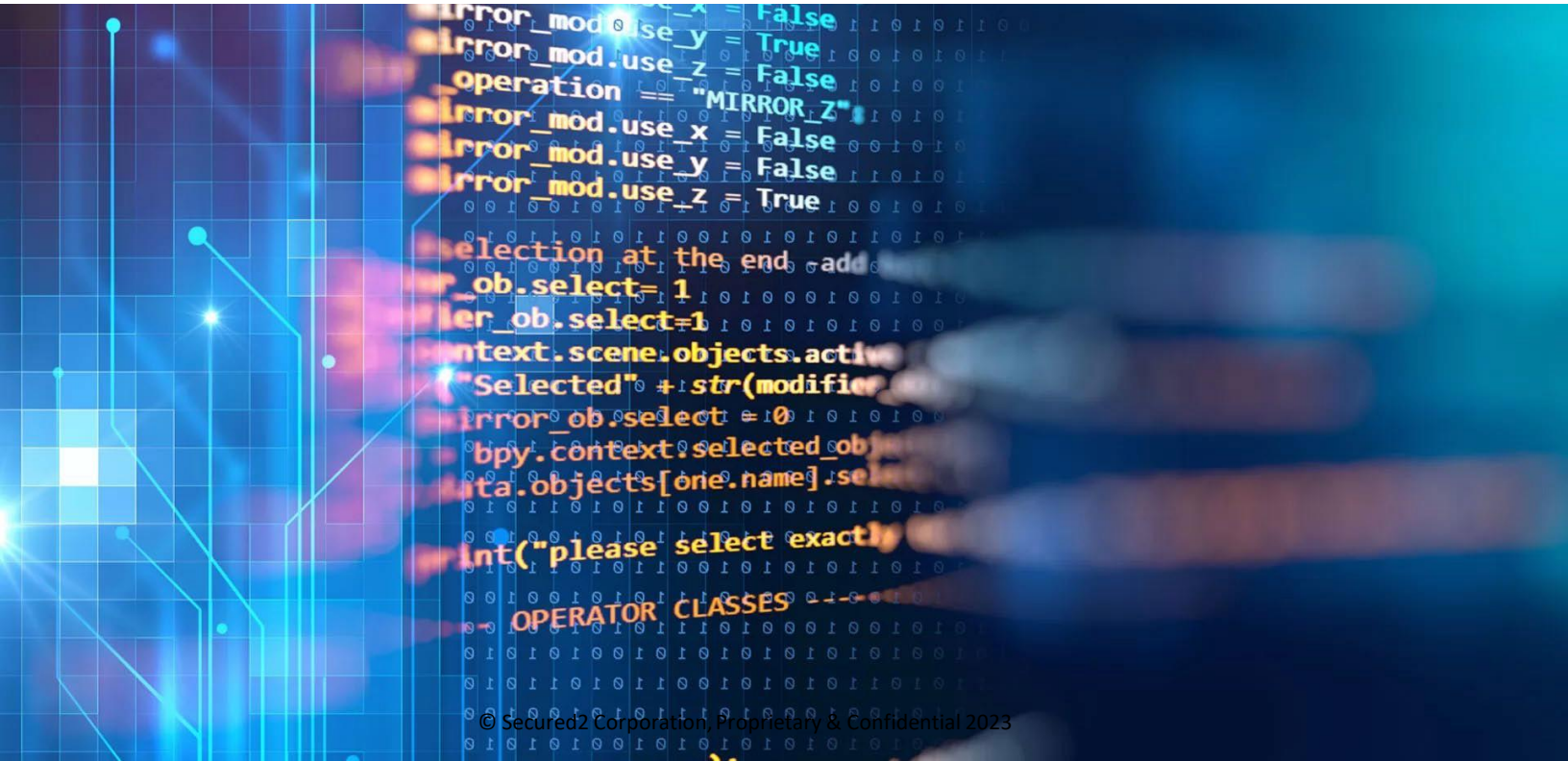
While sharding data can make scaling ' big data' more manageable, it can become a major security liability. If you break a database into chunks (shards), the chunks are threaded together so a hacker can string the database back together if they can access just one node of the sharded database. Since all shards are logically connected to one another in multiple nodes, more nodes equal more threats because the threat canvass increases. The other challenge is that since sharding is a 'table' related function, any corruption of a table can make it very difficult to return the database to its unsharded state. So sharding is a database acceleration technology, not a data security technology.

See Exhibit C for details on sharding.

How does Secured2 differ from Sharding?

As described, sharding is a database technology that creates data where chunks are placed in different nodes to 'speed up' the access of data queries in a database. You can rebuild the entire dataset if you break into a single node or container. Again, sharding is not a security function but a way to increase a database's query speeds by spreading the load on multiple servers.

In contrast, Secured2 is a multi-step security algorithm applied to a single file. Secured2 is a file-level decentralization technology that protects data by turning it into digital confetti. Then each confetti segment is randomly distributed into multiple physically separated storage locations of a customer's choosing. With Secured2, you cannot rebuild a database with one data confetti segment. With Secured2, if a bad actor breaks into a container, they cannot reconstruct the dataset because they get no valuable data. They get a bunch of scrambled and unusable ciphertext. They would need to break into all the physically separated containers where the data was randomly segmented, they would need to break the encryption of each segment, they would need to reassemble the data in the precise order it was shredded, they would need to unmask the data, decompress, and as well verify identity to reverse the process. It's impossible.



Summary

Closing Summary

There is a reason Secured2 has attracted partnerships with leading cloud providers like Microsoft, AWS, and Google. There is a reason MITRE called us, met with us, and wanted to invest in us. They see our technology as the future of data security and that Secured2 could make them a leader in this space, not a follower. We also chose to work with Peraton, one of the largest and most capable cyber integrators for the government and military, deploying our solution across the military & government. Ensuring you have a partner; you can trust deploying our solution in your most sensitive of data hauls.

Our technology is not a short-term fix but a technological leap forward that will protect data for generations. We have carved out a portfolio of seminal patents for quantum-secure™ data protection. Microsoft, IBM, Apple, RedHat, Marvell, Nokia, Sanyo, Sony, CISCO, Sandisk, Texas Instruments, and Samsung have referenced our patents in their filings. And we can demonstrate that the Secured2 QuantaMorphic™ solution is the only quantum-secure™ security in the market with proof that it's secure and can scale affordably into the existing Internet infrastructure.

In a post-quantum world, a straightforward answer to the quantum threat is **Secured2.**

Exhibit A – Secured2's proprietary key generation system

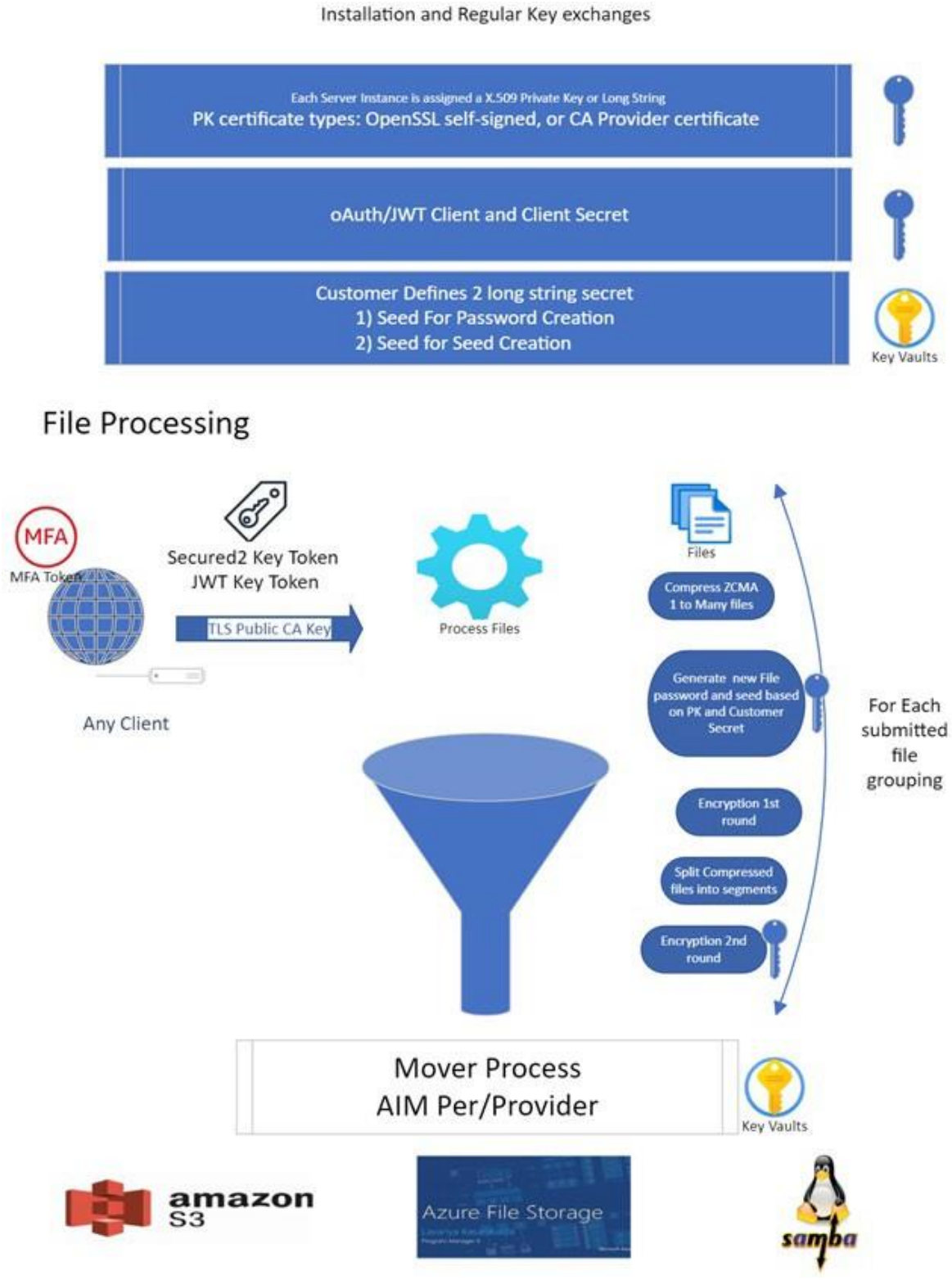


Exhibit B – How Secured2 protects your data (high level view)

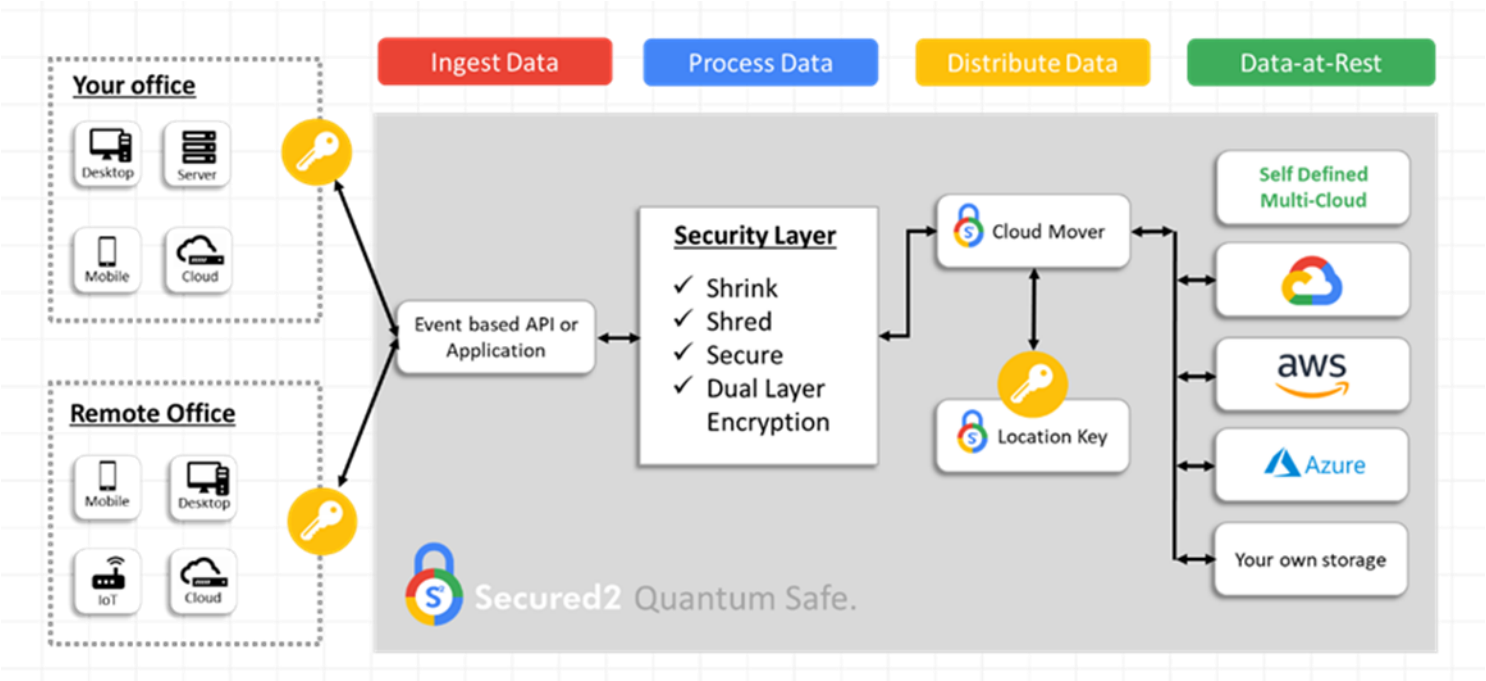
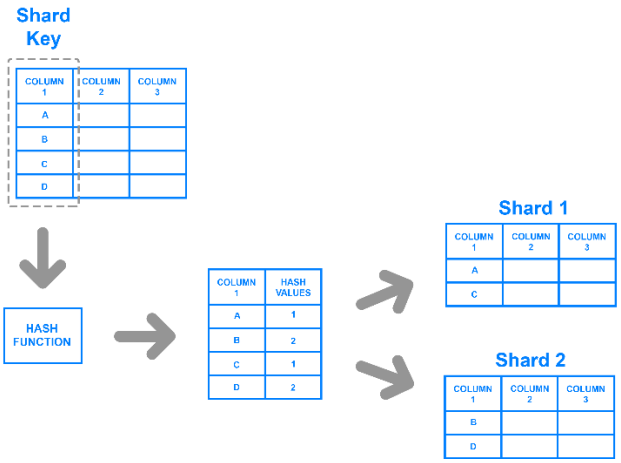
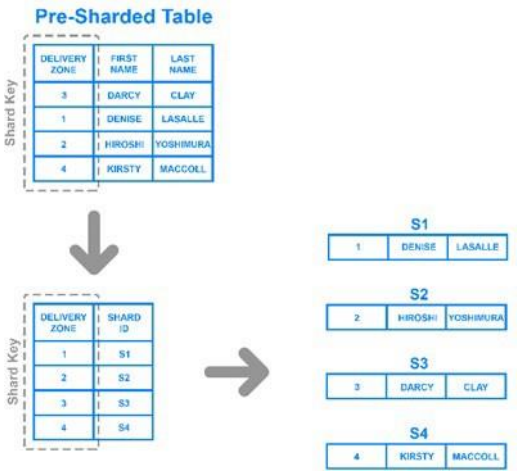


Exhibit C – Examples of Data Sharding

Key based sharding



Directory based sharding



Range based sharding

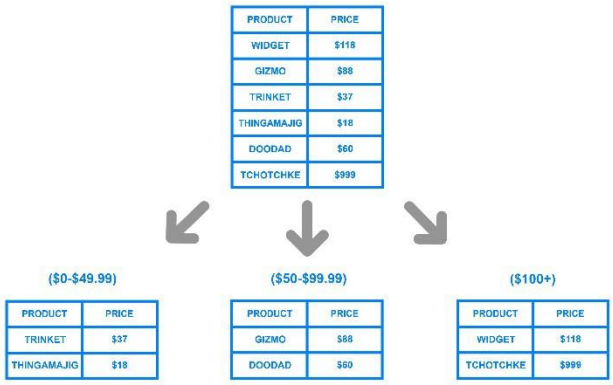


Exhibit D – Secured2 Patent Position

Patents	Title	Country	Inventors	Status
CRAM-001cn01	DIGITAL CONTENT MANAGEMENT AND DELIVERY	PCT	Daren Klum, Pagan, Fairchild, Hench	Issued
CRAM-001ep01	DIGITAL CONTENT MANAGEMENT AND DELIVERY	PCT	Daren Klum, Pagan, Fairchild, Hench	Issued
CRAM-001in01	DIGITAL CONTENT MANAGEMENT AND DELIVERY	PCT	Daren Klum, Pagan, Fairchild, Hench	Issued
CRAM-001us01	DIGITAL CONTENT MANAGEMENT AND DELIVERY	US	Daren Klum, Pagan, Fairchild, Hench	Issued
CRAM-004us01	TAMPER RESISTANCE EXTENSION VIA TAMPER SENSING MATERIAL HOUSING INTEGRATION	US	Daren Klum, Pagan, Fairchild, Hench, Hagen	Issued
CRAM-004us02	TAMPER RESISTANCE EXTENSION VIA TAMPER SENSING MATERIAL HOUSING INTEGRATION	US	Daren Klum, Pagan, Fairchild, Hench, Hagen	Issued
CRAM-005us01	HEAT DISSIPATION FOR A CHIP PROTECTED BY AN ANTI-TAMPER BACKGROUND	US	Daren Klum, Pagan, Fairchild, Hench, Hagen	Issued
CRAM-006us01	SECURE PRE-LOADED DRIVE MANAGEMENT AT KIOSK	US	Daren Klum, Pagan, Fairchild, Hench	Issued
20557.0001USU1	SYSTEMS AND METHODS OF DATA SEGMENTATION AND MULTI-POINT STORAGE	US	Daren Klum, Mark Hansen	Issued
20557.0001USP1	DATA BACKUP AND RETRIEVAL SYSTEM INCLUDING A DATA DIVISION COMPONENT AND DIVERSE STORAGE	US	Daren Klum, Mark Hansen	Issued
20557.0001WOU1	SYSTEMS AND METHODS OF TRANSMITTING DATA	PCT	Daren Klum, Mark Hansen	Issued
20557.0001USC1	SYSTEMS AND METHODS OF TRANSMITTING DATA	US Continuation	Daren Klum, Mark Hansen	Issued.
20057.0001USC2	SYSTEMS AND METHODS OF TRANSMITTING DATA	US Continuation	Daren Klum, Mark Hansen	Pending. Office action issued. Response due
20557.0001EPWO	SYSTEMS AND METHODS OF TRANSMITTING DATA	Europe - validated in Germany, France, UK	Daren Klum, Mark Hansen	Issued
20557.0002USP1	DATA CONVERSION METHOD	US	Daren Klum, Mark Hansen	Issued
20557.0002USP3	DATA CONVERSION DEVICE	US	Daren Klum, Mark Hansen	Issued
20557.0002USP2	DATA CONVERSION SYSTEM	US	Daren Klum, Mark Hansen	
20557.0002USU2	DATA CONVERSION SYSTEM	US	Daren Klum, Mark Hansen	Issued
20557.0002USU1	DATA CONVERSION METHOD	US	Daren Klum, Mark Hansen	Issued
20557.0002USU3	DATA CONVERSION DEVICE	US	Daren Klum, Mark Hansen	Issued
20557.0002WOU1	DATA CONVERSION DEVICE	PCT	Daren Klum, Mark Hansen	Issued
20557.0002EPWO	DATA CONVERSION DEVICE	EP	Daren Klum, Mark Hansen	Issued
20557.0004USP1	SECURED DATA STORAGE ON A HARD DRIVE	US	Daren Klum	Issued
20557.0004EPWO	SECURED DATA STORAGE ON A HARD DRIVE	EP	Daren Klum	Issued
20557.0004USU1	SECURED DATA STORAGE ON A HARD DRIVE	US	Daren Klum	Issued
20557.0004WOU1	SECURED DATA STORAGE ON A HARD DRIVE	PCT	Daren Klum	Issued
20557.0006USP1	SECURE DATA TRANSMISSION VIA EMAIL	US	Daren Klum, Mark Hansen	Issued
20557.0006USU1	SECURE DATA TRANSMISSION VIA EMAIL	US	Daren Klum, Mark Hansen	Issued
20557.0006WOU1	SECURE DATA TRANSMISSION VIA EMAIL	PCT	Daren Klum, Mark Hansen	Issued
20557.0010US01	MULTI-DIMENSIONAL RUN-LENGTH ENCODING	US	Daren Klum, Thomas Neafus, Andrew Kluge, William Kluge	Issued.
20557.0010WOU1	MULTI-DIMENSIONAL RUN-LENGTH ENCODING	PCT	Daren Klum, Thomas Neafus, Andrew Kluge, William Kluge	Issued