FHOOSH CYBERSECURITY PLATFORM

Elemental Data Encryption: The Case for Protection From Data Inception

White Paper | April 2017

FHOOSH®
FASTER DATA, MORE SECURE.™

ABSTRACT

There is more economic value online than ever before, and with the "Internet of Things" (IoT), we are generating far more valuable data now than in the past. There is an ecosystem for cybercriminals to acquire purpose-built tools to attack and break down the defenses protecting our data. Cybercriminals have the means, motive and opportunity to commit all forms of cybercrime. We must implement protection from data inception to protect our digital infrastructure and the FHOOSH™ Cybersecurity Platform protects data from the point of data capture, dramatically speeds data transfer and provides "always-on" compliance for highly sensitive data.

EXECUTIVE SUMMARY

Data is the lifeblood of our economy. With the data that we are now able to collect and analyze, we are learning more than ever about how we interact with the products we use and about the environment in which we live, work and play. Much of this data is highly sensitive and very valuable, and therefore must always be fully protected. But the data is under constant threat from cyber criminals and nation-states, so to fully protect the data, you need to protect it from the point when it is created, the inception point, so that it is never exposed.

The FHOOSH Cybersecurity Platform provides elemental data encryption and captures, transmits, stores and archives data in an always-protected state. Because of this, there are no transition points to attack where the data would otherwise be vulnerable while being transformed to an encrypted or decrypted state. Also, since the data is never in a plain-text state, moving that data through a network does not increase the scope for compliance or audit activities. The process stays compliant; the audit scope remains unchanged. This makes compliance easier and less expensive. FHOOSH calls this "always-on" compliance. Further, having encrypted backups that incorporate FHOOSH speeds the archiving process and delivers a more secure archive of the data.

The result is that you get greater protection, faster and better performance, "always-on" regulatory compliance and built-in threat detection for data at rest or in motion.

The FHOOSH Cybersecurity Platform also dramatically improves the speed at which data objects are transported from the endpoint where data is captured to either on-premises or cloud-based data centers, where it is archived, achieving up to 8x speed improvement over unencrypted data. This is built into the product, and with FHOOSH's implementation strategy, the bigger the files, the bigger the advantage. All the while, FHOOSH is monitoring the data under its protection, ready to detect inappropriate actions against the data and both alert on those activities, and take countermeasures to protect the data. This smart data protection methodology is delivered as a software solution and can be available on Windows, Mac, Linux, mobile and multiple single-board IoT devices. This gives your organization the ability to create complete end-to-end coverage with FHOOSH.

The result is that you get greater protection, faster and better performance, "always-on" regulatory compliance and built-in threat detection for data at rest or in motion.

INTRODUCTION: FUNDAMENTAL PROBLEMS PROTECTING DATA

Data has become an important raw material for all products, providing critical input for how the product performs and increasingly, how the product is used by customers. The number and diversity of uses for the data makes protecting the data a daunting task. Added to this, governments and other central bodies are implementing more comprehensive regulation.

During the first wave of Internet adoption, large companies and government agencies moved portions of their business processes to web-enabled platforms. Unbeknownst to many, a cybercrime underground was taking form and building a thriving economy, enabled by Tor and Bitcoin, that allowed those with the means (organized crime and nation-states) to interact commercially with those with the skills (hackers from all over the world).

As more value moved to web-enabled platforms, the incentives to attack and steal or corrupt that value increased. Security professionals, who could see the storm coming, were discounted as "Chicken Littles" and minimal compliance with regulations was often the only restriction placed on the business.

What led to the complacency? One assumption was that direct monetary theft was the only goal of cybercrime. Another assumption was that perimeter defense, the thick heavy shell protecting the soft pliant underbelly, would be effective as a long-term defense. Still another assumption was that if you didn't conduct financial business online, you didn't have anything of value to steal and you would not be a target.

These assumptions started being challenged around 2010. The groundwork, though, was laid by mid-2007 with the development of the Zeus banking Trojan. Over the course of the next five years, the connected world would see a series of cybercrime milestones. The Zeus Trojan demonstrated that cybercriminals could form an ecosystem, with skills and capability traded in an open market. Then we began to see large-scale breaches for personal information that was not necessarily related to financial information. Educational records, medical records and personnel records were added to credit card data as sought-after records with a market value on the dark web. In 2011 we saw a cyber-attack against RSA to steal one-time token key generation code, which would then be used to breach Lockheed Martin to steal plans for military weapons systems.

The World Economic Forum, in their 2016 report, cites $2 trillion as the worldwide cost of cybercrime by 2019, up 400% since 2015.

There is now an increasing urgency for improving our cybersecurity. The World Economic Forum, in their 2016 report, cites $2 trillion as the worldwide cost of cybercrime by 2019, up 400% since 2015. It is imperative that we re-establish and maintain the trust in our online markets, or risk trillions of dollars in economic value, as extraordinary and intrusive new measures would be required to prove the validity of each transaction. This would slow our economic engine and severely impact the customer experience.

WITH THE IoT, IT'S NOT GOING TO GET ANY EASIER

The initial wave of Internet adoption was largely people interacting with systems. Whether the process these people were executing was to purchase something as a consumer or transfer money from one of their bank accounts to another (a B2C process) or was to interact behind the scenes with a supply chain system or billing system or human resource system (a B2B exchange), the interactions had a human element. While we created massive troves of data, which became known as "big data," we did so at human scale.

Big data pools, such as consumer purchase information, were created by collecting millions of consumer transactions, such as all the books purchased on the Amazon book site. Bigger data pools, such as all the searches conducted by all the users of Google's search engine, and even bigger data pools, such as all the logs of every login attempt across an entire organization over a given time, were still created one record at a time, based on a human taking an action (buying something, searching for something, logging into a system).

Now, however, with the Internet of things, the "IoT," we allow machines (things) to interact directly with each other. The IoT consists of vast numbers, now billions and soon to be trillions, of sensors (that collect data) and actuators (which allow some devices to move or act in some way). Taking advantage of ever-improving miniaturization, materials development and cost efficiencies, we can now put very low-cost, high-resolution sensors, actuators and even processors (computers) on ever-smaller devices and take advantage of universal high-bandwidth, low-cost wireless communications to generate, collect, process and transmit enormous amounts of data. The result, of course, is even bigger data. Mountains and mountains of data. Data lakes are replacing data pools.

The IoT consists of vast numbers, now billions and soon to be trillions, of sensors (that collect data) and actuators (which allow some devices to move or act in some way).

Early in the first Internet wave, the Internet of people, we were primarily concerned with protecting the immediate transaction. The data generated at the endpoint, for example, to make the purchase. We didn't have huge troves of online data to steal, and the (comparatively) few records we did have were offloaded to back-office systems that weren't yet connected to the Internet. Very shortly, as data accumulated and more systems became interconnected, this changed. It is now critical to protect not only the transactions but the pools of data we have started creating and putting online.

In the current Internet wave, the Internet of things, the data captured at the endpoint might be sensor data, telemetry for instance, or richer data, such as video. Sometimes that is innocuous data that we don't need to protect. But sometimes, the data stream is precious or sensitive. Maybe a video baby monitor, a video security camera, a police body camera, drone images or surveillance video at a power plant.

Gary Hayslip, former Deputy Director and Chief Information Security Officer for the City of San Diego, provides some helpful context:

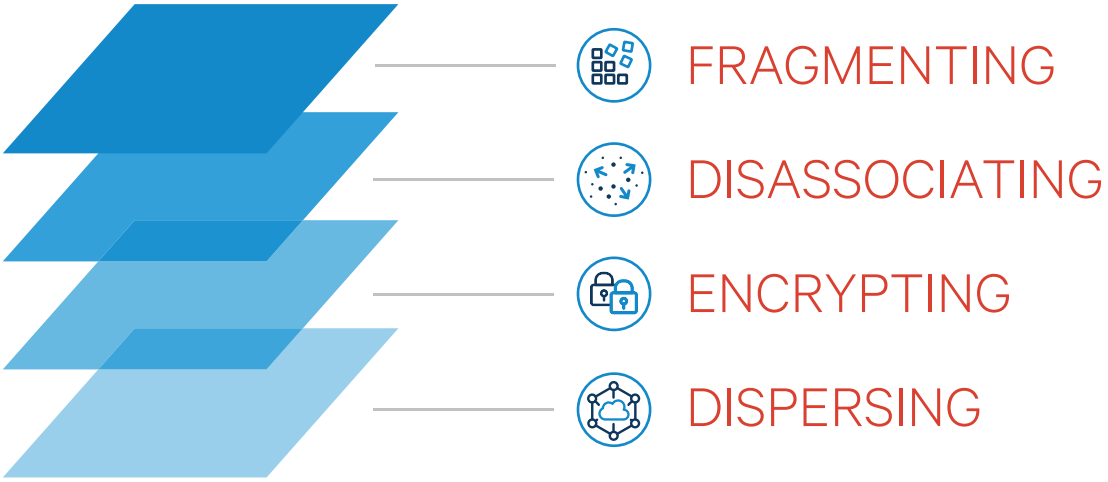
> "People think of city networks as one sprawling network in a box, but the reality is I have 24 disparate networks with technologies from servers and PCs to handheld devices, police cars, fire and rescue, street cameras and environmental controls. **The data for these networks is constantly changing** and with new smart city industrialized Internet of Things platforms the data is ever richer with context. However, cities are environments that operate **24/7** which means there are many legacy technologies intertwined with these new smart city technologies resulting in risk exposure from this mix of old and new enterprise systems. This mix results in unknown risk exposures to the data created, processed and stored in these systems **which is why I recommended FHOOSH** to provide us the ability to remediate and manage some of this risk. By being able to **protect data from the capture point** and **protect all of my legacy data** using the same platform, I can be effective with my limited resources and protect my city's vital assets at the same time."

Thinking back to the endpoint transaction of the online purchase, the credit card transaction is a few hundred bytes, while the endpoint data captured for a high-definition video camera is almost 50 megabits per second. Certainly, streaming technology reduces the bandwidth required to transmit useful video (for humans to watch) to well below 50 Mbps, but the point is that the IoT, given the ability to capture orders of magnitude more data per sensor, combined with orders of magnitude more sensors than humans, means that we have many orders of magnitude more sensitive data to protect, transmit and store. Security with speed becomes paramount.

A BETTER MOUSETRAP – FHOOSH'S UNFAIR ADVANTAGE

Going back in time again for a moment, Google reimagined the search problem and solution and built a content search and delivery platform that was so much better than the other solutions that they rose, in a very short time, to become by far the dominant search engine. This happened because they did not slightly improve basic search engine technology, they rethought the premise and designed a new solution from the ground up. They recognized that the goal was not to index all submitted content. The goal was to index all content. All content everywhere. They challenged premises and assumed that every unsolvable problem was just another opportunity to have fun solving a new problem. They recognized that to achieve their goal of making all information available to everyone in the world they had to think differently, from the ground up.

FHOOSH has reimagined the problem of securing data. The initial goal for FHOOSH was to secure personal data to create a completely secure personal profile, consisting of the most sensitive information a person has, such as their financial data, medical data and identity data. The desire was to make this profile (imagine an eWallet on steroids) available to the user from any device at any time that the user was connected. To truly meet that requirement, the data had to be secure no matter where it was stored: on the device, at a company data center or in the public cloud. This meant the FHOOSH engineers had to take a wholly new approach to securing the data. They designed a data protection methodology that would protect the data no matter where it was stored.



How did they do this? They looked at data protection with fresh eyes. FHOOSH was developed from architecture through implementation with security in mind. As they were breaking down the problem, they realized that encryption, by itself, was powerful but inadequate and very hard to get right. (For a more detailed analysis of that problem, please see the FHOOSH white paper: "Dispersed Data Encryption: The Key to Better Information Security"). They designed a much more robust data protection methodology that combined data fragmentation, disassociation of the data and metadata, encrypting the data and then dispersing the encrypted data. These four techniques, used in combination, render the data significantly more secure. The result is a product that bakes in data protection at an elemental level.

By fragmenting the data, they have essentially created a giant jigsaw puzzle out of the data object, but minus the perfectly interlocking edges that aid the player in reassembling the puzzle. Staying with the puzzle analogy, by disassociating the data from labels, columns and tags, they've wiped away the pictographic hint that players rely on to group pieces that belong in sections of the puzzle together. After they have completely scrambled the pieces, they encrypt each individual puzzle piece of the data with a separate cryptographic key. The flexibility of this solution allows the customer to use the AES 256-bit gold standard encryption strength, or to choose a different encryption algorithm to support legacy systems if needed. The encryption library is abstracted such that any cryptographic standard may be used, allowing you to provide equal support for legacy applications and keep benefiting as the cryptographic world continues to mature. After the pieces of the puzzle are encrypted, the encrypted pieces are dispersed. To continue our analogy, the puzzle pieces are randomly chucked into puzzle boxes unrelated to the original puzzle and stored in separate closets throughout your house, or at your neighbor's house or in lockers at the bus terminal. Anywhere there is space for the box. If someone happens upon a box, they get one piece of something, which doesn't at all resemble a piece of a puzzle. They get data dust, not information diamonds.

NOT ALL ENCRYPTION IS CREATED EQUAL

Another aspect of the FHOOSH Cybersecurity Platform critical to the data protection model is that each fragment of disassociated data is encrypted using a different key. In a sense, this is a best-of-both-worlds implementation. The FHOOSH key management system addresses issues that leave many field-level encryption schemes overwhelmed with too many keys to manage and retrieve securely, and file, disk or database-level encryption that can potentially unlock very large blocks of data with a single key, thus creating a much easier vector of attack. This is an important difference with multiple implications.

1	2	3	4	5	6
Transport layer encryption	***Full-disk/whole-disk encryption***	***File-level/database-level encryption***	***Column-level encryption***	***Field-level encryption***	***Application-level encryption***
Protects data in motion	Encrypts all contents of disk	Encrypts individual files or databases	Encrypts only the sensitive data	More granular data protection	Full granularity by user/session
No protection for data at rest	One key unlocks everything	Must encrypt even non-sensitive data	Complex code, more keys to manage	More complex code/key management	Awkward reporting and analytics

To understand why, let's look a little closer at some of the common implementations of encryption.

1. ***Transport layer encryption***, as implied by the name, encrypts the transmission of data between two devices. TLS (transport layer security) and SSL (secure socket layer) are two of the most common forms of transport layer encryption used on the internet. SSL was the standard for many years, but was deprecated by NIST in 2014 and has also been replaced with TLS, starting in June of 2016, by the PCI-DSS V3.1 standard. In their previous white paper, FHOOSH talked about flawed encryption implementations. This is an example. The encrypted data, which was scrambled using AES-256, is unreadable. But to establish a secure connection, the two endpoints, say a PC browser and a web server, need to negotiate for and exchange keys to be able to make the secured connection. The method for establishing secured keys for SSL was attacked, and over time was eventually defeated. While FHOOSH builds in additional security to handle the key exchange correctly, some browser-based implementations do not. Also, while many users assume that data encrypted at the transport layer is forever secure, even TLS only encrypts data that is in transit. There is no provision for data to be encrypted while at rest, in other words, while stored on the device or in the database on the server.

2. Another category of encryption is commonly known as ***full-disk encryption or whole-disk encryption***. The objective here is to encrypt the disk itself. Implementations vary: in some cases, every bit of data is encrypted, in others, small amounts are left in plain text to enable bootstrapping or initial boot-up of the operating system or data block. And again, the cipher text itself is unreadable. In many cases, optimization can be built in at the operating system (OS) level or even directly on the chip, producing very small impacts on performance to encrypt and decrypt. The weaknesses again are with implementation. In full-disk encryption, a single key, or in some cases, a single key per partition, is all it takes to unlock the entire disk. With physical possession of the disk the implementation of the full-disk encryption can be defeated, as was the case with the San Bernardino shooting suspects from the December 2015 incident. The FBI had physical possession of the work phone of one of the suspects and contracted with a firm that had developed a technique to bypass the ten-try limitation on the passkey, and therefore subject the phone to an extensive brute-force attack. This eventually led to accessing the contents of the disk. This incident shows that with time and physical possession of the device, OS-level encryption schemes can often be either defeated or bypassed.

3. A third category of encryption is commonly referred to as ***file-level encryption or database-level encryption***. This is more granular than full-disk encryption in that individual files or entire databases are encrypted separately using a single key per file object. While potentially more secure than a single password to unlock a whole disk, because you can usually not take advantage of the same kinds of optimizations performance starts to slow down. The larger the files, the more work that must be done to encrypt and decrypt them. In the case of database-level encryption, every read/write call to the database must go through the same encrypt/decrypt routines to use the data. Performance can now become a major concern if there are millions of transactions per day all hitting the same database. And again, a single key can unlock the entire trove of data.

4 To both improve performance and provide more granular protection, another category of encryption called ***column-level encryption*** is often deployed. In this scheme, individual columns of data deemed sensitive are encrypted, sometimes with different keys. Columns that aren't considered sensitive are left in plain text. This has the advantage of decreasing the workload of encrypting and decrypting every read/write call, but at the cost of more keys to manage, and more complexity.

5 ***Field-level encryption*** is a category that provides yet additional granularity. Each field within the column, often referred to as a row for relational databases, is encrypted with a separate key. As you can imagine, this would be quite an advantage for an application that maintains a database that contains data for thousands or millions of customers. Each field, each customer data point, is protected by a separate key. Stealing an individual key yields little comparative value over unlocking a whole file, database or disk with a single key. But, this comes with a price. The key management issue that began to take form with column-level encryption has exploded. Every time a protected field needs to be written or retrieved, a separate key lookup needs to be done first. This can create such a performance drag that techniques to cache and reuse keys are often used, many of which create new vulnerabilities that make stealing keys easier. Also, with all those keys to manage, including deprecated keys for archived encrypted copies that are necessary to successfully restore backups, losing (mismanaging) keys becomes a very real problem. And if the key is lost, the data is unreadable. Further, if that key was paired with an encrypted backup, disaster recovery then becomes virtually impossible.

6 A final category of encryption that we will cover is referred to as ***application-level encryption***. Application-level encryption is carried out within the application, before the data is written to the database. In this case, more flexibility is given to the developer in that individual users can, based on access rights and job roles, be given the right to decide while using the application whether to encrypt individual fields of data. While the flexibility provides the building blocks for tailored security, implementations are spotty because individual users have different interpretations of security needs and are provided different levels of training, and utility can suffer. Searches, reports and monitoring are all challenged to one degree or another when different applications and different users are contributing pre-encrypted data to a common database.

With this as background, it is easy to see why the FHOOSH Cybersecurity Platform is such a breakthrough. The combination of fragmentation, disassociation, encryption and dispersal provides a superior implementation of encryption. The strength of the cipher is the same, but the weaknesses are eliminated. There is plenty of granularity to render the system extremely difficult, and therefore unattractive, to attack by brute force. And, instead of slowing system performance, the FHOOSH implementation is significantly faster.

LAYERS OF PROTECTION

There are two additional built-in security features that strengthen the FHOOSH Cybersecurity Platform. At the beginning of this paper, we said that the data needs to be secure wherever it is stored, including in the public cloud. Encryption has emerged as an important strategy for protecting data in the public cloud. To make public cloud options more palatable to companies, most vendors have added encryption as a feature that the customer can turn on at will. But when encryption is provided by the vendor, the customer must trust that it is implemented correctly, and the customer must cede important elements of control. Besides the implementation scheme, in most cases the vendor holds master keys and is, therefore, subject to attack or subpoena. The most common method of securing keys in a key management system is to implement encryption as described above. The exact vendor-by-vendor details don't matter as, depending on the method chosen, the same deficiencies cascade to the key management system that would be present in the encrypted user data. Not so with FHOOSH. The FHOOSH User and Key Management system uses the same superior data protection methodology to protect the user information and keys. This is all critical information, and should be afforded the same level of protection as the primary data object. With FHOOSH, there are no second-class data citizens. The user and key data is first fragmented, then disassociated, encrypted and dispersed. That makes attacking the user and key data just as difficult as attacking the primary data. In the unlikely event that a single fragment is ever located, data dust is all that has been retrieved. There is no way to determine what the data fragment represents.

The FHOOSH User and Key Management system uses the same superior data protection methodology to protect the user information and keys. This is all critical information, and should be afforded the same level of protection as the primary data object. With FHOOSH, there are no second-class data citizens.

The FHOOSH development team never stops modeling the threats that might expose the data. These threat models led to the initial decision to use a stronger, four-part combination of security techniques to build superior encryption, and to the decision to apply the same combination of security techniques to protect the user and key store. Another feature that is a result of the threat modeling is a series of built-in alerts and counter actions that execute automatically when attacks against the data are detected. If attacks are detected against streaming data protected by FHOOSH, the segment being attacked is automatically retransmitted after the key is rotated. If erroneous compound keys are used to try to unlock FHOOSH data files or a data fragment that is managed has been accessed outside of FHOOSH, the keys are automatically rotated. These are just some of the conditions FHOOSH can detect. In every case, appropriate defensive measures are taken and the administrators are alerted to the activity.

UBIQUITOUS AVAILABILITY AND FLEXIBLE DEPLOYMENT OPTIONS

Critical to the strategy of protecting data from the inception point is the availability of FHOOSH on the common IoT device platforms, from smartphones to single-board computers. Lightweight, highly flexible FHOOSH software will be available on multiple platforms, including Mac OS X, Linux, Windows, IOS and Android, as well as Raspberry Pi and other single-board computers. This, along with support for standard interfaces including Amazon S3 API, support for Python, out-of-box API functionality and REST-based services will allow you to design a data protection scheme that can treat data captured on every device equally, protecting all data from inception. Data capture that is integrated with FHOOSH is captured securely, and then can be securely transferred or streamed, depending on the implementation. Secure streaming protects the confidentiality, integrity and availability of the data by automatically detecting any irregularities in the streamed secure fragments and taking appropriate countermeasures, such as rotating the keys and retransmitting the affected fragments. The result is a secure, high-fidelity stream. The transferred data is automatically stored under FHOOSH protection with full key management. Data capture integrated with the FHOOSH Cybersecurity Platform is therefore never at risk. The organization can create complete end-to-end coverage with FHOOSH.

Data captured at inception with FHOOSH is therefore never at risk. The organization can create complete end-to-end coverage with FHOOSH.

FASTER PERFORMANCE

Another significant advantage of the FHOOSH Cybersecurity Platform is the certified exponential performance improvement obtained when protecting large files and data objects. Because of the way the FHOOSH Cybersecurity Platform fragments data and encrypts those fragments independently, it can simultaneously operate on more than one fragment at a time, and achieve up to 8x faster speeds over storing data unencrypted. This builds in two advantages that automatically increase over time. First, recall that Moore's law states that the number of transistors in a dense integrated circuit will double every two years. Remarkably, this has held true for roughly four decades. While the rate of growth in transistor density is now starting to slow, other developments, including the number of cores, the number of threads and the density of storage, have continued to increase. As the number of cores and threads continues to increase, the ability of the FHOOSH engine to operate on fragments simultaneously also increases. This allows the FHOOSH Cybersecurity Platform to provide a significant speed advantage because the density of storage, the fidelity of sensors and the availability of bandwidth will likely continue its upward projection. Let's explore how. First, the rate of improvement of data capture will likely outpace the rate of bandwidth expansion for the foreseeable future. That means there will be a significant advantage to fragmenting and encrypting the data before transmission. Second, the increase in data capture fidelity and the density of data storage capacity will enable new uses for data which in turn will drive a greater need to capture and process more large files. The FHOOSH Cybersecurity Platform builds in investment protection by automatically improving performance as compute power improves through high core density and available threads. In other words, FHOOSH is future-proofing the investment by taking advantage of the increasing number of threads.

A second performance advantage is that the FHOOSH Cybersecurity Platform transmits and stores larger files faster. Because FHOOSH is operating on smaller, independent data fragments, network bandwidth is utilized more effectively and IO channels on storage devices are optimized, creating an accelerating factor that, like the advantage created by multi-threading, provides greater gains for larger files. As data file sizes continue to increase for all the reasons outlined in this paper, the advantage provided by the FHOOSH Cybersecurity Platform increases in magnitude and therefore increases in value. Simply put, the FHOOSH Cybersecurity Platform improves data security and improves performance. The result: with FHOOSH, protecting data is now easier, faster and more secure than leaving it unencrypted.

The result: with FHOOSH, protecting data is now easier, faster and more secure than leaving it unencrypted.

BETTER BACKUPS

Because the FHOOSH Cybersecurity Platform is available as APIs, with Python, Java and C support, REST-based calls, standard interfaces for Amazon S3 APIs and full scriptability, FHOOSH can be used to design a backup capability for your critical files and databases that will take full advantage of the performance boost you get from FHOOSH. That means you can finish the backups more quickly, which in turn means you can back up more data, more often, and disperse your backups to implement a robust disaster recovery capability. You can design a backup approach to automatically locate FHOOSH-encrypted backups in separate data centers, separate AWS zones, or any other scheme that fits your requirements. Further, you can build in automatic test routines that validate the integrity of your data and alert you if there are any problems. Backups are one of the most important strategies to protect your business from downtime due to disaster or cyber-attack. But backups are rarely fully implemented because they take so long and can't complete in the prescribed window or aren't fully tested to make sure the data is recoverable in the event of an emergency. With FHOOSH, you can finally have a secure, highly available backup strategy.

AUTOMATIC COMPLIANCE

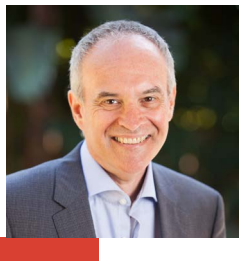
With the importance of data security at top of mind for regulators, insurers and any company that acts as a steward of sensitive information, almost every organization has one or more standards-based data security regimes they must comply with as a matter of regulation or contractual obligation. Key provisions in these standards describe the importance of encryption for data in transit and at rest. A common example is the PCI-DSS 3.2 standard for credit card data. Any system that handles full payment card data, either within a transaction, storing such data, or transmitting that data is included and the standard mandates encryption for key management in section 3, for secure transmission of payment card data in section 4, for application development standards in section 6, for identity management in section 8 and for monitoring and testing in section 10. In each case, using FHOOSH provides key steps toward complying with these standards.

Further, 47 of the 50 U.S. states, as well as the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands, have breach notification laws (only Alabama, New Mexico and South Dakota do not), and all states that have such laws (except Tennessee) include a safe harbor for encrypted data. Therefore, the FHOOSH "always-on" approach to compliance provides a critical capability to meet compliance requirements.

The FHOOSH "always-on" approach to compliance provides a critical capability to meet compliance requirements.

CONCLUSION

We are generating orders of magnitude more sensitive data today than in the past. With the explosion in the growth of object sizes due to increasingly sophisticated sensors, a new approach to data protection is needed. The FHOOSH Cybersecurity Platform delivers on three critical needs simultaneously. First, data is protected from its inception. Because FHOOSH handles the data from the point of capture, it is never exposed. Second, because FHOOSH always handles the data in its protected state, FHOOSH provides "always-on" compliance for highly sensitive data. This provides an important safe harbor for international data privacy regulations. And finally, because of FHOOSH's approach to data protection, you get enormous speed improvements, typically up to 8x faster than storing unencrypted data. Because of how FHOOSH achieves these faster speeds, the investment in FHOOSH is not only future proofed, but the speed improvement actually increases over time as files get bigger. With FHOOSH, you can confidently protect your data from inception, resulting in greater protection, faster and better performance, "always-on" regulatory compliance and built-in threat detection for data at rest or in motion.



BILL BONNEY

Bill Bonney is the Vice President of Product Management at TechVision Research. His professional areas of expertise include more than 25 years of experience in Information Technology, Information Security and Privacy, Cybersecurity, Identity and Access Management, Organization Strategy and Risk Management. His expertise ranges from risk analysis and security and technology program design to mastery of control frameworks and business process engineering. Bill is a co-author on the book, "CISO Desk Reference Guide: A Practical Guide for CISOs."

Bill has held senior management positions in Information Technology and Information Security, most recently as a Director of Information Security and Compliance at Intuit, Inc., a Fortune 500 provider of personal and small business financial products. Prior to Intuit, he was a Principal with Ensemble Consulting, where he provided interim CIO services to Silicon Valley clients, including Callidus Software and InVision Technologies. Prior to Ensemble, he was the Director of Global Information Technology for Unify Software.

Bill is a security evangelist and is a member of the Board of Advisors for the CyberTECH security company incubator and the Board of Advisors for FHOOSH.

ABOUT FHOOSH

FHOOSH, Inc. develops high-speed cybersecurity software solutions that protect data from inception, in transit and at rest at speeds certified up to 8x faster than storing even unencrypted data. FHOOSH delivers on the promise of “faster data, more secure” using patent-pending protections that fragment, disassociate, separately encrypt and then disperse data upon capture at the edge/endpoint through to the cloud for storage or archiving. The platform enables stronger data protection with faster performance, built-in threat detection, ransomware safeguarding and “always-on” regulatory compliance, which boosts system speeds and also reduces cyber attack surface.

With FHOOSH security built in from architecture to implementation, an unauthorized interception or breach nets only data “dust” instead of information diamonds. FHOOSH software easily integrates with both legacy and new technologies, and is the right option to secure data in any cloud, IoT or enterprise environment.

For more information, contact:
FHOOSH, Inc.
7660 Fay Avenue, Suite H136
La Jolla, CA 92037

(888) 4 - FHOOSH
info@fhoosh.com
fhoosh.com

Share this White Paper