SecurityFirst™
Data-Centric Cyber Solutions

WHITE PAPER

Securing Data with Cryptographic Splitting

The next evolution of encryption

Introduction

Every business and government entity, in the wake of daily devastating cyber-attacks, must deal with the risk and liability of protecting regulated and secret data. Even the US Government has recognized the glaring weaknesses in its IT infrastructure – extending to its military, government contractors, and ultimately to commercial operations. In the balance lies penalty cost, competitiveness, risk to personal privacy, and ultimately individual cost as personal information is lost, corrupted, or used for nefarious purposes.

Acknowledging this risk, Governments around the world have initiated legislation to force improved compliance to data protection schemes – from numerous US based requirements, to the most recent European General Data Protection Regulation (GDPR) requirement to protect the Personal Identifiable Information (PII) of its citizens – regardless of location in the world – with significantly higher penalties.

Unfortunately, too many organizations have taken a blind eye to the problem and lack common basic protections – a shocking reality. Further, as breaches have expanding in sophistication, we've come to recognize that even basic protections with existing perimeter protections (firewalls, etc.) are but temporary roadblocks for any skilled hackers. Basic encryption (where randomly used), likewise, does little to deter these hackers who can penetrate networks and usurp the IDs of authorized users to gain access to easily accessible data – with or without encryption.

Beyond Perimeter Protection

Now – introduce the Cloud – our next generation of IT infrastructure – expanding to IoT – the Internet of Things – providing incredible access to nearly any data – including access to mine, yours, and anyones personal data. Incredibly cost efficient, easy to use, easy to adjust to the immediate needs of business, government, and individuals – the Cloud has become the beneficiary of progress, but also the bane of security experts who see the inherently huge risk of potential corrupted access and ease of infiltration into the Cloud infrastructure.

Today – there are new, dramatic, low cost approaches to mitigate and eliminate these risks. Security technology has long focused on the access (network centric protection) – trying to keep people out of the network that protects access to data. But with the Cloud and IoT transition – we've created the (currently) ultimate network access infrastructure and forgotten about the core … it is the data itself that needs to be protected – not from any access, but from unauthorized access and the ability to control that access. It is the data itself that needs to be protected with the strongest, highest performant protection solutions. Now, aligning these two concepts, stronger protection AND access controls, provides the core DATA-CENTRIC protection needed in the future of Cloud and IoT environments. Securing the network is good, but can never provide complete security in this ever-growing network of connectivity. Managing data privacy, access controls, and with the strongest encryption becomes the mandate every enterprise, commercial or government, must embrace and adopt with growing urgency.

Unparalleled Security

So what can be done? The answer lies with the enormous increase in computing speed and processing capability that can make solutions possible today that have never been practical before. Now, software solutions can be deployed that

provide virtually unbreakable encryption with strong access controls, meet the needs of easy installation and management, provide low cost and seamless operation, and does it all without performance impact or excessive processor utilization. Cloud operation can be managed via on or off-premise management and includes transparent, effective management of keys. Integrated policy, provisioning and management is accomplished with a simple to use management console.

SecurityFirst™ is the technology leader in Data Centric protection and access controls using Cryptographic Splitting to bring this new and more powerful approach to data protection. It has been tested by knowledgeable experts and found ready to meet the goals for widespread adoption in either on-premises enterprise systems and/or the migration to all-important Cloud environments. Key Federal credentials have already been earned (FIPS 140-2, EAL4+, Secret, and Top Secret) associated with one or more product solutions – both directly and through OEM partners.

Cryptographic Splitting provides unparalleled security to the data, independent of whether the network is breached, by first encrypting using traditional means and then cryptographically splitting the just encrypted data at the bit level by placing the bits randomly into one or more predetermined "secure data shares". If any computer location is breached, any "secure data share" obtained is totally meaningless and unreadable and the data is absolutely secured. This unique architecture underlies and enables other important aspects including efficient, low cost, secure key management, automatic fault tolerance and restoral, seamless control of policy and provisioning, access logging for audit readiness and compliance, and built-in separation of duties which protect data against a Snowden-type insider threat.

About SecurityFirst

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack such as malware or ransomware. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

About DataKeep

DataKeep™ secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs.

Security teams can define and log access policies by job role and manage privileged and superuser access to block insider and external threats. DataKeep securely protects data at the source no matter where data resides, encrypting data at the volume or file level for attached storage or before sending to object storage. Native backup and restore commands can be leveraged to enable prompt recovery of archived data in the event of a ransomware attack.

DataKeep's ability to support M of N distributed shares allows companies to encrypt, split and distribute data across multiple object store locations or vendors for business continuity and operational efficiency. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency. Secure your most valuable assets – your data, your brand and your reputation – with Datakeep.

SecurityFirst™
Data-Centric Cyber Solutions

For a product demonstration or more information call 1.888.884.7152 securityfirstcorp.com