AGILE ENCRYPTION

YOUR ENTERPRISE IS AGILE
YOUR ENCRYPTION SHOULD BE

The Reality

9.198 Billion Data Record Breaches Since 2013
1.9 Billion Data Record Breaches in the first half 2017
<5% were **"Secure Breaches"** where encryption was used
122 records lost every **SECOND**

Two Steps

- Eliminate as much collection and storage of sensitive data as possible
- Encrypt the remaining sensitive data at rest and in transit

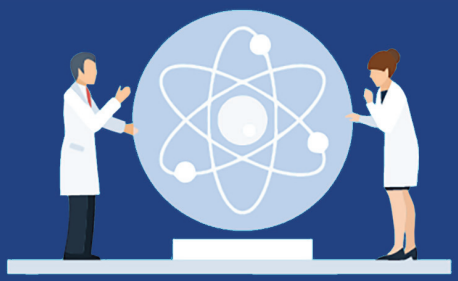
Best Practices

- Become aware of the type of encryption being used, which applications are using it and how it is used
- Decentralize encryption and decryption
- Centralize key management with distributed execution
- Support multiple encryption standards and algorithms
- Central user profiles for authentication and access to keys
- Do not require decryption/re-encryption for key rotation
- Keep comprehensive log files and audit trails
- Use a standardized solution to support fields, files and databases
- Support third party integration
- Rotate keys and algorithms

Quantum Quandary

- By 2022, quantum computing will be in a position to crack some RSA keys in near-real time (Gartner, 2017)
- All three of the most commonly used cryptographic schemes and algorithms can be broken by future quantum computing

Types of Cryptography



Quantum Breakable

- RSA encryption
- Diffie-Hellman key exchange
- Elliptic curve cryptography

Quantum-resilient

- Lattice-based cryptography
- Code-based cryptography
- Multivariate cryptography

Build crypto-agility into the enterprise

Cryto-agility: implementing cryptography to ensure that replacing the algorithms is relatively straightforward without changing the function of the application (Gartner, 2017)

SECURE CHANNELS

PARADOXBOX

PARADOXBOX™

Crypto-agility today

Layered, multi-variate

Cryptanalysis Future Proofing

ParaDoxBox's Superencipherment Engine improves the security of your critical data and extends the useful life of current encryption algorithms through a patented use of layering and segmentation encryption techniques

Computational Future Proofing

The Superencipherment engine improves security and provides a hedge against improvements in computing power by providing a keyspace of approximately 50% greater than that offed by conventional symmetrical block ciphers

Bypass and social engineering resistant

Enhanced Enterprise Encryption

- Your data is your data
- Whenever
- Wherever
- Protect it

SECURE CHANNELS

PARADOXBOX