SECURE CHANNELS

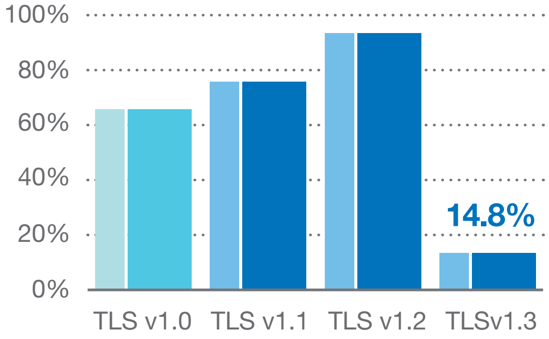
TECHNOLOGIES THAT ENABLE SECURITY, PRIVACY, AND AUTHENTICATION TO PROTECT **DATA-IN-TRANSIT** FROM TODAY'S CYBERCRIMINALS AND TOMORROW'S QUANTUM COMPUTERS

DON'T RELY SOLELY ON ENCRYPTED TUNNELS (SSL / TLS) TO PROTECT YOUR DATA

SSL/TLS encrypted tunneling protocols provide secure communication between connected devices. However, the pace at which these protocols have been updated and released have lagged behind the needs for additional data-in-transit security requirements. The flaws and weaknesses present in SSL/TLS continue to be exploited and attacked resulting in data being stolen. Additionally, the global migration to TLS 1.3 (only 14.8% of websites) continues to be slow.

The XOTIC™ cryptosystem provides post-quantum resilience, is TLS version agnostic, and when used to encrypt data prior to sending over SSL/TLS can mitigate Man-in-the-Middle attacks.

PROTOCOL SUPPORT (JUNE 2019)



RETAIN CONTROL OF THE ENCRYPTION PROCESS AND YOUR KEYS

When combined with Secure Channels' Secure Key Infrastructure (SKI), XOTIC encryption keys can be securely exchanged through a global cloud services network and stored or vaulted using any symmetric key management / HSM solution. Using SKI ensures that there is never a single key to be compromised or brute force attacked, but is a constantly changing key of variable length. Each key can leverage Quantum Random Number Generation (QRNG) entropy sources to protect the integrity of the key and the data that it's protecting.

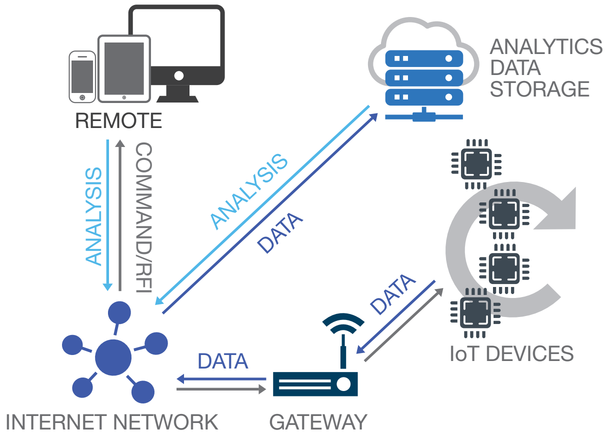
XOTIC®

SKI™
SECURE KEY INFRASTRUCTURE

STRONG, ULTRA-LIGHTWEIGHT ENCRYPTION ON ANY PLATFORM

The XOTIC cryptosystem is uniquely suited to protect data streams being transmitted from "constrained" low-power, low-compute devices. With an initialization time that's over 100 times faster than any symmetric encryption with the CSNA Suite of algorithms, XOTIC can encrypt and decrypt data in near real-time without the need for hardware acceleration. In high-throughput, low-latency environments such as relational databases, IoT/ connected devices, and 4K/8K streaming media use cases, XOTIC delivers superior security by not only exchanging the encryption keys at predefined intervals, but also by randomly modulating the bit length of the key between (512/1024/2048/4096-bit) at every block, packet or frame via Secure Channels' Wave Form Encryption™ (WFE).

INTERNET OF THINGS ECOSYSTEM



SECURE CHANNELS

TECHNOLOGIES THAT ENABLE SECURITY, PRIVACY, AND AUTHENTICATION TO PROTECT **DATA-AT-REST** FROM TODAY'S CYBERCRIMINALS AND TOMORROW'S QUANTUM COMPUTERS

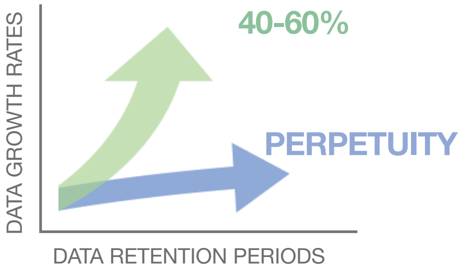
WORRY-FREE DATA PROTECTION OF BACKUP/ DR/ CLOUD DATA

The quantity and retention periods of enterprise data stores are growing dramatically. Enterprise data is growing at a rate of 40 - 60% per year. Retention rates are increasing due to the threat of ransomware attacks and renewed emphasis on having additional backups and better BC/DR practices. Big Data analytics is also a primary driver in keeping large quantities of data in perpetuity.

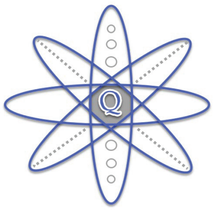
Billion dollar investments are being made by governments and large organizations to build powerful quantum computers (estimated to be completed in the coming 8-10 years) that will execute programs exponentially faster and could also be used to attack encryption algorithms. Experts recommend moving to quantum-resilient forms of encryption today. Cryptography options available within the government's CSNA Suite may not provide adequate protection.

Cloud-provider or server-side "check box" encryption options often do not encrypt the data itself but rather just the storage hardware the data resides on, are complicated to navigate, and are often misconfigured leaving data unprotected. Leveraging the XOTIC cryptosystem to encrypt data at the source, prior to sending data to be stored off-site or in the cloud, can protect it from unwanted cloud provider access (using your keys) or prying governments' eyes.

MASSIVE DATA EXPLOSION



QUANTUM COMPUTING 8-10 YEARS AWAY



☑ **CHECK BOX ENCRYPTION**

SECURE?

2019 REPORT VERIFIES THAT (EXTENSIVELY) USING ENCRYPTION SAVES MONEY

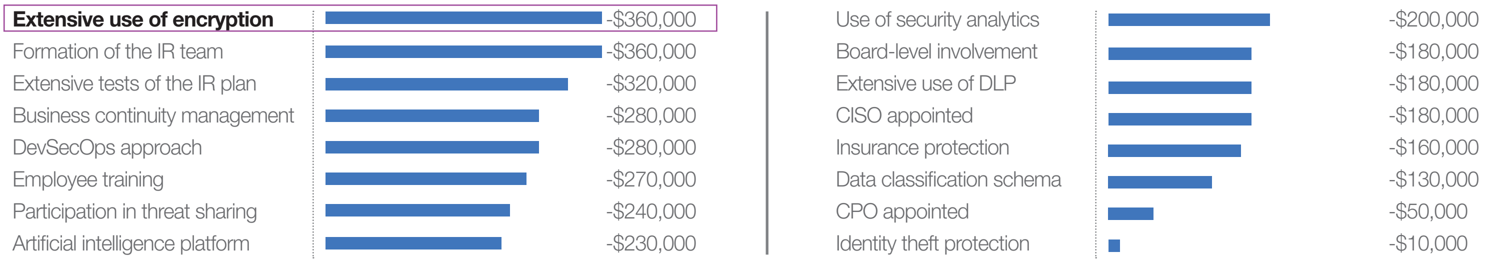
As the global average cost of a data breach continues to increase to USD $3.92M, and even higher for U.S. companies at USD $8.19M, the "extensive use of encryption" continues to be one of the major factors in helping to reduce overall costs.

To enterprise organizations, this means that using encryption can represent a very positive return on investment if implemented throughout the organization.

XOTIC cryptosystem encryption can be used extensively in a wide variety of use cases without the use of additional modes of operation (required by block ciphers). XOTIC allows organizations to choose their desired encryption strength. XOTIC default bit strength is 512-bit, but much longer 4,096-bit keys could be selected to provide "archive strength".

How factors increase or decrease the total cost of a data breach

Difference from average total cost of US $3.92 million



Extensive use of encryption	-$360,000
Formation of the IR team	-$360,000
Extensive tests of the IR plan	-$320,000
Business continuity management	-$280,000
DevSecOps approach	-$280,000
Employee training	-$270,000
Participation in threat sharing	-$240,000
Artificial intelligence platform	-$230,000
Use of security analytics	-$200,000
Board-level involvement	-$180,000
Extensive use of DLP	-$180,000
CISO appointed	-$180,000
Insurance protection	-$160,000
Data classification schema	-$130,000
CPO appointed	-$50,000
Identity theft protection	-$10,000

*According to 2019 Cost of of a Data Breach Reportconducted by the Ponemon Institute, sponsored by IBM