ParaDoxBox™
DATA SECURITY PLATFORM

ParaDoxBox neutralizes emerging threats and mitigates the risk of unauthorized disclosure of enterprise data - even in the event of a breach

Enterprise end-point encryption management for multi-platforms. The ParaDoxBox Data Security Platform incorporates rich enterprise administration features as well as Secure Channels' patented PKMS2 (Pattern Key–Multi-Segment–Multi-Standard) **E3 Protocol** (**Enhanced Encryption Engine** mode/toolkit). Built for the enterprise, environment customizable.

It's estimated that 96% of data stolen in enterprise breaches was unencrypted, and therefore exposed to malicious actors. In many cases, the failure to protect sensitive data was due to the difficulty involved in deploying encryption within an enterprise environment or be ill-prepared in protecting every endpoint. Secure Channels' ParaDoxBox Data Security Platform fills these gaps by providing administrators an intuitive, user-friendly, comprehensive management interface while providing a wide array of encryption options and enterprise management functionality - ensuring positive control over users, billing, and data access.

Key Product Benefits: Exponentially Increase Security

Pervasive Encryption

The ParaDoxBox Data Security Platform can be easily deployed to all of an enterprise's laptops and workstations (either by download, isolated sandbox environment, or group policy installation). Once installed and registered, it can be used to provide any desired combination of full disk, partition, volume, hidden volume, file and file-for-sharing encryption at the administrator's discretion. All users can encrypt all data, all the time. ParaDoxBox's administrative functionality guarantees that the enterprise retains complete, secure control of keys, ensuring data access.

Computational Future Proofing

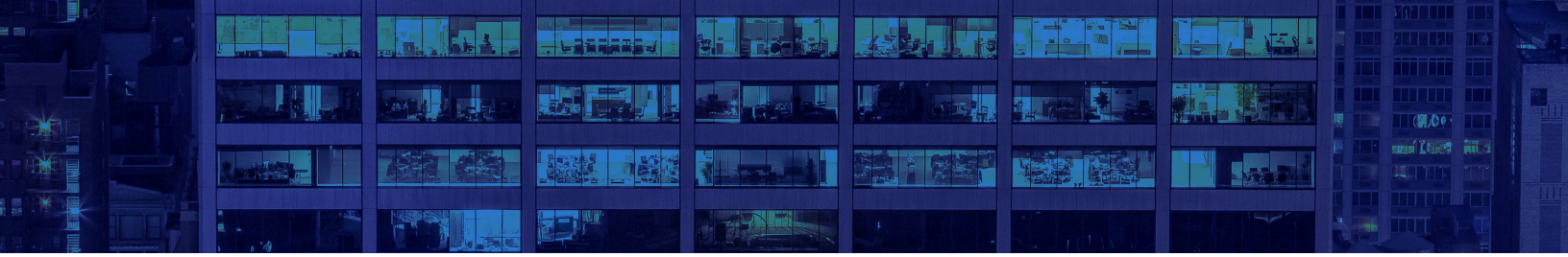
The ParaDoxBox Data Security Platform incorporates Secure Channels' PKMS2 E3 Protocol encryption that has been mathematically proven* to extend the effective key length of standard 256-bit ciphers by approximately 50% to 387 bits. As a result, the use of ParaDoxBox provides security guarantees against both conventional and quantum improvements in computing power. These versions also provide fallback security: Even if one of the ParaDoxBox encryption suite's ciphers is found to be insecure, data protected using the PKMS2 E3 Protocol remains protected. Additionally, the effort an attacker must exert to recover an entire message is significantly increased.

Bypass and Social Engineering Attack Protection

The ParaDoxBox Data Security Platform all but eliminates the threat of bypass and social engineering attacks using Secure Channel's SUBROSA® technology, which provides a multifactor authentication gateway to ParaDoxBox, supporting knowledge, possession, biometric, machine inherence and external location based manage knowledge factor authentication credentials that can be tailored or combined based on enterprise requirements to provide the desired level of authentication assurance. SUBROSA's credentials technology, are long (thousands or tens of thousands of bits), non-human readable, binary strings that are unknown to but easily entered by the user. Users can't reveal what they don't know and they can't share what they can't read or write down.

**A mathematical analysis of PKMS2 was conducted by Dr. Jonathan Katz, Vice President of Cryptography Engineering, Secure Channels Inc., Professor, Computer Sciences, University of Maryland. Cryptoanalysis conducted by Dr. Yevgeniy Dodis, Professor, Computer Science, Courant Institute of Mathematical Sciences, NYU; Dr. Matthew Green, Assistant Professor, Computer Science, The Johns Hopkins University; Dr. Stefano Tessaro, Assistant Professor, Computer Science, University of California, Santa Barbara*

SECURE CHANNELS



ParaDoxBox uses On-The-Fly-Encryption (OTFE) to encrypt and protect data on endpoints. OTFE ensures that data is never persistently stored in an unencrypted state. OTFE incorporates the PKMS2 Protocol, best of breed symmetric ciphers, enhanced authentication technology, and enterprise controls for key management, account management and billing. ParaDoxBox offers enhanced security that flexibly supports enterprise requirements.

- Intuitive, easy-to-use interface
- Protects device, files, and entire volumes
- Administrators securely designate encryption scope (disk, partition, volume, file, share, Cloud location, etc.), storage locations and the algorithms and modes of operation that encrypt data
- Incorporates PKMS2 and SUBROSA® multifactor authentication

"Encryption protects our data. It protects our data when it's sitting on our computers and in data centers, and it protects it when it's being transmitted around the Internet. It protects our conversations, whether video, voice, or text. It protects our privacy. It protects our anonymity. And sometimes, it protects our lives…Encryption works best if it's ubiquitous and automatic… "

- Bruce Schneier

Feature	ParaDoxBox 1.2.5.0
Security Bit Strength	~387 (When used in PKMS2 mode)
Superencipherment	Yes
Cloud-Based Containers	Yes
Multi-Algorithm Selection	Yes
Hidden Containers	Yes
Pre-Boot Authentication	Yes
Single Sign On	Yes
Custom Authentication	Yes
Multiple Keys	Yes
Passphrase Strengthening	Yes
Trusted Platform Module	Yes
File Systems	Any OS supported filesystem

Operating Systems	Windows/Unix
Encryption Algorithms	AES, Simon, Twofish, Serpent, MARS, Speck, Aria, Camellia
Modes of Operation	CBC, GCM, PKMS2
Key Hashing Algorithms	SHA-256, SHA-384, SHA-512, SHA3-256 (future), SHA3-384 (future), SHA3-512 (future), PBKDF2
Authentication Factors	Knowledge, Possession, Biometric, Machine Inherence, Location

*File encryption refers to the encryption of a file such that the file can be shared with a user who does not use the container application. Upon attempting to open the encrypted file, the recipient will enter the shared key.

Feature	ParaDoxBox 1.2.5.0
Multifactor Authentication	
- Knowledge Factor	Yes
- Possession Factor	Yes
- Inherence Factor (Biometric)	Yes
- Machine Inherence	Yes
- Location Factor	Yes
Full Disk Encryption	Yes
Partition Encryption	Yes
Volume Encryption	Yes
Hidden Volume Encryption	Yes
File Encryption	Yes
File-for-Sharing-Encryption*	Yes
Swap Space Encryption	Yes
Hibernation File Encryption	Yes
Supported Algorithms	Yes
- AES	Yes
- Simon	Yes
- MARS	Yes
- Twofish	Yes
- Serpent	Yes
- Speck	Yes
- Aria	Yes
- Camellia	Yes
PKMS2 Mode of Operation	Yes
Customizable Per Customer Requirements	Yes