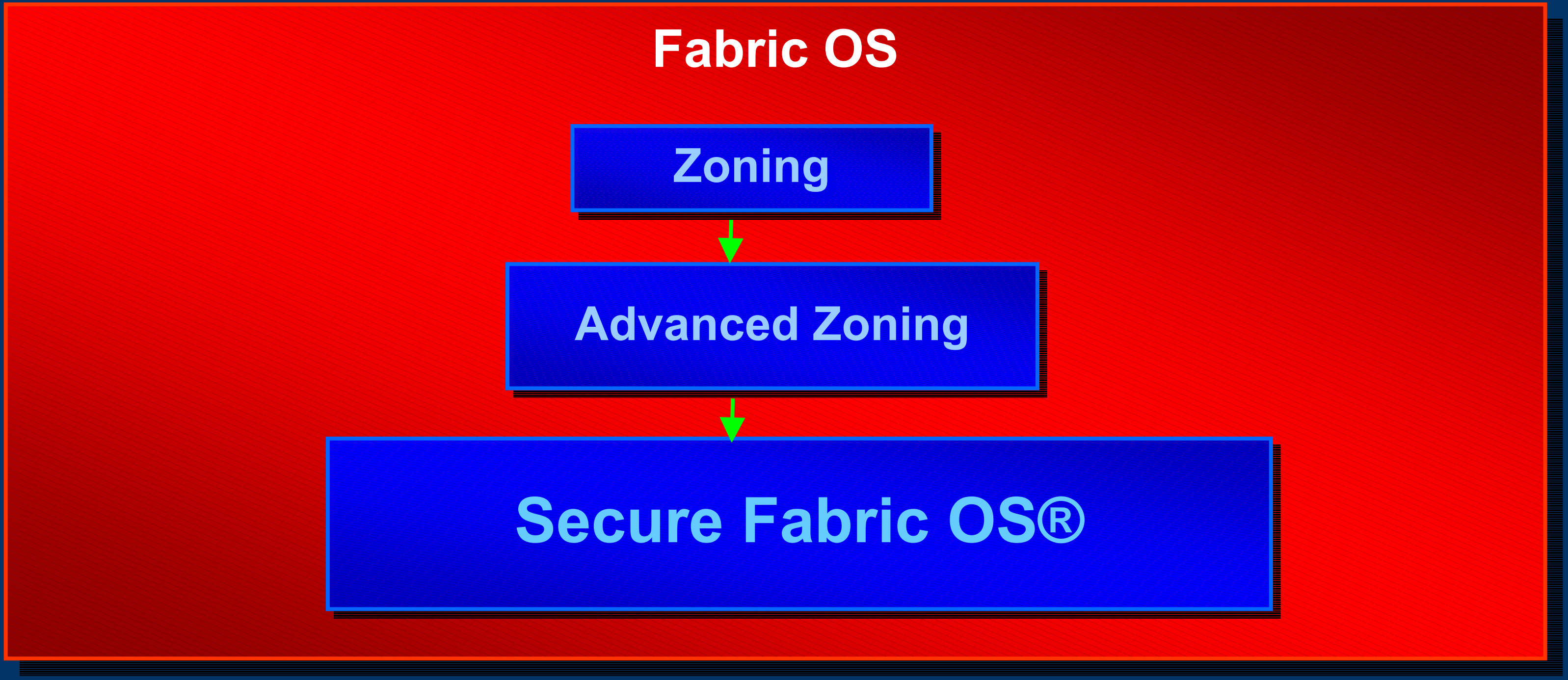
Brocade Enterprise-Class Security



Fabric OS

Zoning

Advanced Zoning

Secure Fabric OS®

Brocade Secure Fabric OS

- Brocade Secure Fabric OS is a licensed software product that provides a complete set of security capabilities within Brocade fabrics.
  - Centralized security management (trusted switches)
  - Fabric-wide security policies to control all access and to maintain ‘configuration integrity’
    - Port level access control
    - Switch level access control
    - Management access controls (Telnet, SNMP, HTTP, API, Serial port etc.)
  - Encryption of management data such as passwords and logins
  - Strong and non-repudable authentication between switches

Secure Fabric OS® : Solution Example

Problem

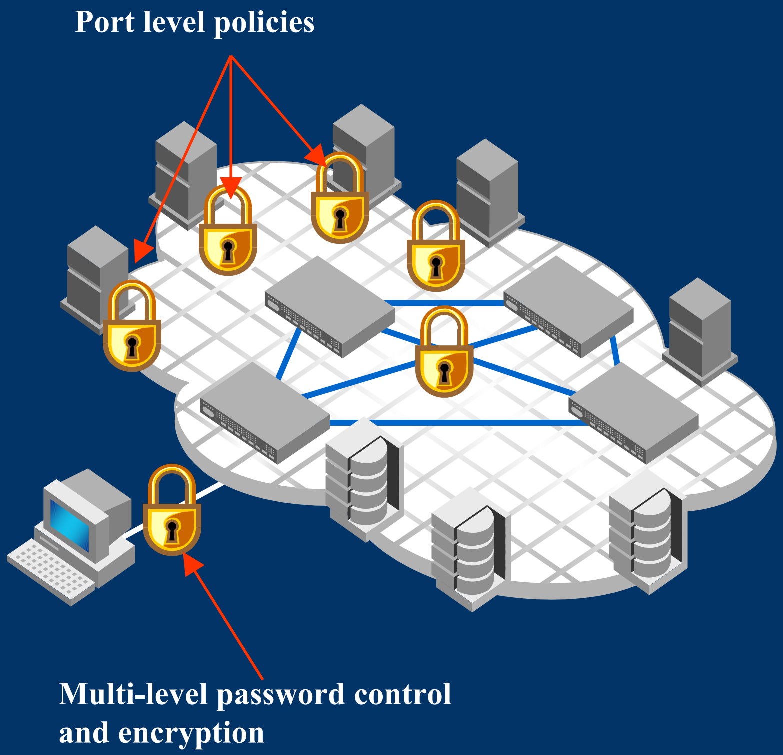
- Government contractor with sensitive data
- Needed more control on their servers and user level access to the SAN resources

Solution

- Brocade Secure Fabric OS®
- Port level access policies used to tightly control server access to the fabric
- Multi-level password control and strong password encryption

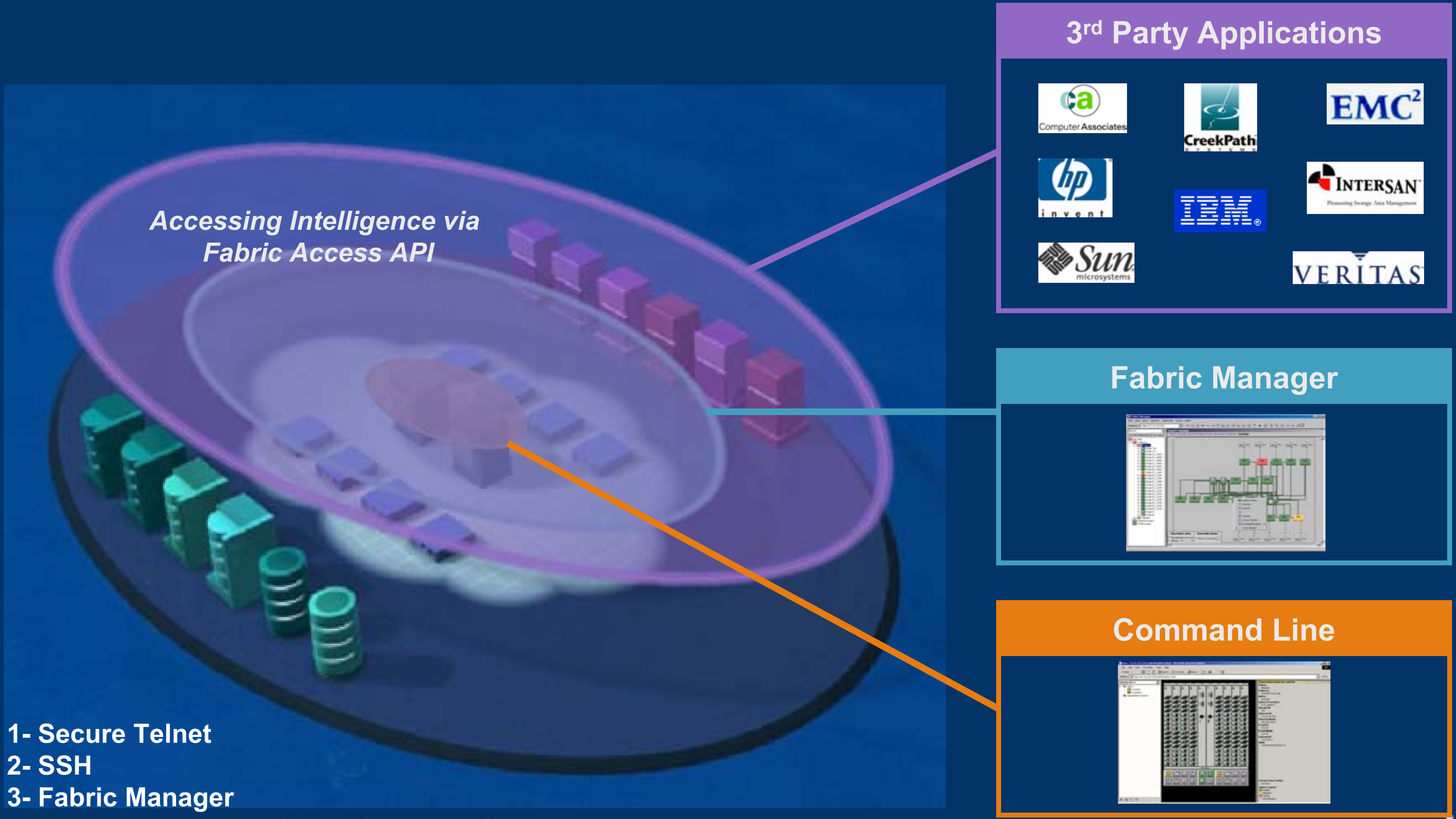
Result

- A more Secure SAN infrastructure
- Tighter access control to the fabric
- Stricter adherence to internal security policies
- Higher compliance with government requirements for protecting sensitive information



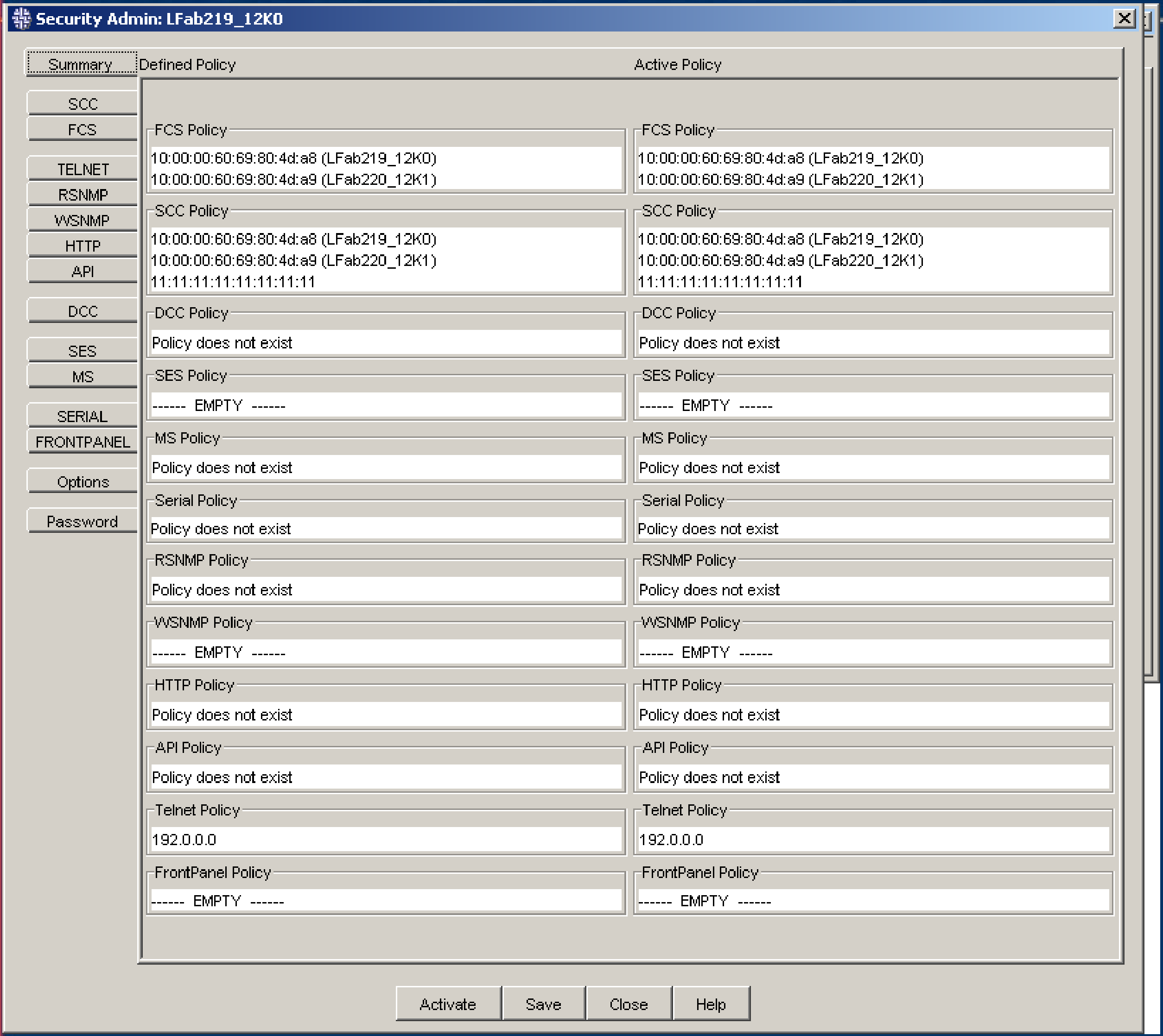
Manage Security

Integrated Fabric Management Applications



1- Secure Telnet
2- SSH
3- Fabric Manager
4- Fabric Access API (Pearl Scriptable)

Fabric Manager - Security Policy Administration



	Defined Policy	Active Policy
FCS Policy	10:00:00:60:69:80:4d:a8 (LFab219_12K0) 10:00:00:60:69:80:4d:a9 (LFab220_12K1)	10:00:00:60:69:80:4d:a8 (LFab219_12K0) 10:00:00:60:69:80:4d:a9 (LFab220_12K1)
SCC Policy	10:00:00:60:69:80:4d:a8 (LFab219_12K0) 10:00:00:60:69:80:4d:a9 (LFab220_12K1) 11:11:11:11:11:11:11:11	10:00:00:60:69:80:4d:a8 (LFab219_12K0) 10:00:00:60:69:80:4d:a9 (LFab220_12K1) 11:11:11:11:11:11:11:11
DCC Policy	Policy does not exist	Policy does not exist
SES Policy	------ EMPTY ------	------ EMPTY ------
MS Policy	Policy does not exist	Policy does not exist
Serial Policy	Policy does not exist	Policy does not exist
RSNMP Policy	Policy does not exist	Policy does not exist
WSNMP Policy	------ EMPTY ------	------ EMPTY ------
HTTP Policy	Policy does not exist	Policy does not exist
API Policy	Policy does not exist	Policy does not exist
Telnet Policy	192.0.0.0	192.0.0.0
FrontPanel Policy	------ EMPTY ------	------ EMPTY ------

- Secure Fabric OS management
- Security Policy control
- Security audit & reporting
- Multi personality (manage secure & non-secure Fabrics from a single console)

Security/Cryptographic Mechanisms in Secure Fabric OS

Authentication:

- Fibre Channel Authentication Protocol (FCAP) – PKI-based security
  - Switch Link Authentication Protocol (SLAP) – subset of FCAP
  - Protocol used to authenticate switches (E_Ports) within a fabric

Privacy:

- RSA Public Key Encryption (1024-bit keys) as well as Secure Shell (SSH)
  - For encrypting passwords between the manager and the switch
  - MD-5 for hashing passwords within the switch
- Advance Encryption Standard (AES) – 128-bit keys
  - For encrypting the switch's private key used in digital signatures and password encryption/decryption processes

Integrity:

- Digital signatures on security parameters distributed from the FCS (trusted switch)

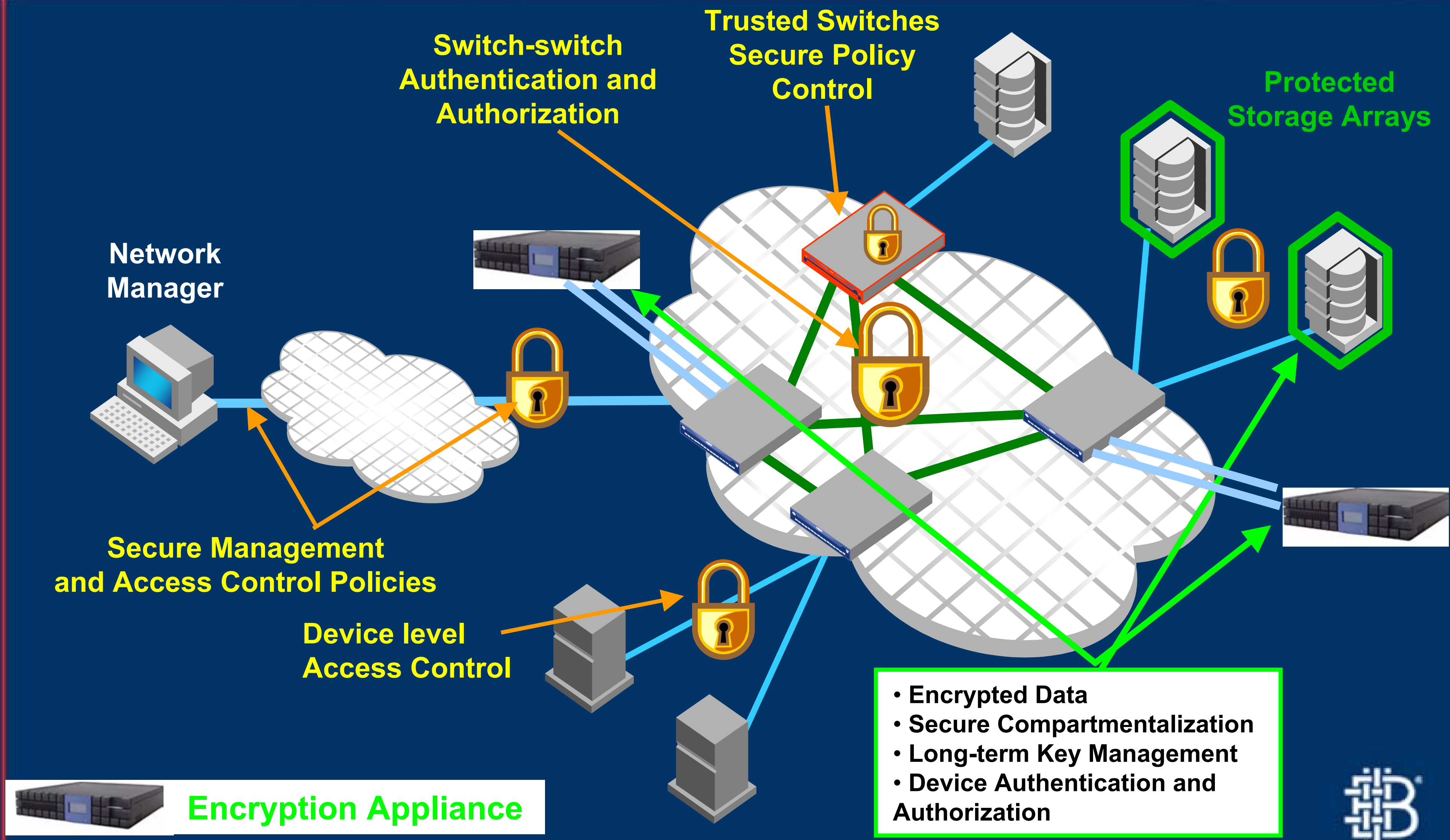
Non-Repudiation:

- RSA digital signatures
  - For authentication of switches
  - SHA-1 hash algorithm for the signature process
  - ITU X.509 v3 certificates

Access control:

- Comprehensive policies to control management and device access to the fabric

Fabric based security and Encryption appliances



Switch-switch Authentication and Authorization
Trusted Switches Secure Policy Control
Protected Storage Arrays
Network Manager
Secure Management and Access Control Policies
Device level Access Control
Encryption Appliance

- Encrypted Data
- Secure Compartmentalization
- Long-term Key Management
- Device Authentication and Authorization