SHARE
EDUCATE • NETWORK • INFLUENCE

TECH 240

Quantum-Safe Data Path Security:

End-to-End Protection for IBM Z SANs with Next Gen Brocade and IBM z17

Jim Stewart
SE Manager – Enterprise, East and Canada
Broadcom

Quantum-Safe Data Path Security:

End-to-End Protection for IBM Z SANs with Next Gen Brocade and IBM z17

SHARE
EDUCATE • NETWORK • INFLUENCE

Description:

The rise of quantum computing necessitates a robust approach to secure the critical data path within Storage Area Networks (SANs). This session will outline Quantum-Safe Cryptography (QSC) principles, relevant standards, and a practical roadmap for future-proofing your storage network against emerging quantum threats.

We will detail how to achieve end-to-end quantum-safe data path security within the larger IBM z17 quantum-safe solution with Next-Gen Brocade Fibre Channel SAN solutions. The focus will be on hardening the SAN data path, exploring IBM b-type (Brocade) security features like secure boot, certificate management, federated authentication, and advanced FICON management for IBM Z. Learn specific commands and configurations administrators can deploy today to secure data in-flight and at-rest across the SAN fabric, ensuring comprehensive protection and compliance for tomorrow's quantum era.

WHY EVERYONE IS CONCERNED ABOUT CYBER SECURITY

The Impact of Data Breaches

$4.4M

*Global Average Total cost of a data breach**

241 days

*Average time to identify and contain a data breach**

**Cost of Data Breach 2025(IBM); The Financial Impact of Cyber Breaches on Businesses*

The Impact of Cyber Attacks on Small-Medium Businesses

46%

*of SMBs have experienced a cyber attack in their current business.**

1 in 5

*of these SMBs then filed bankruptcy or closed their business.**

*Mastercard survey of more than 5,000 small and medium-sized business owners across four continents

The Impact of AI generated Bad Bots

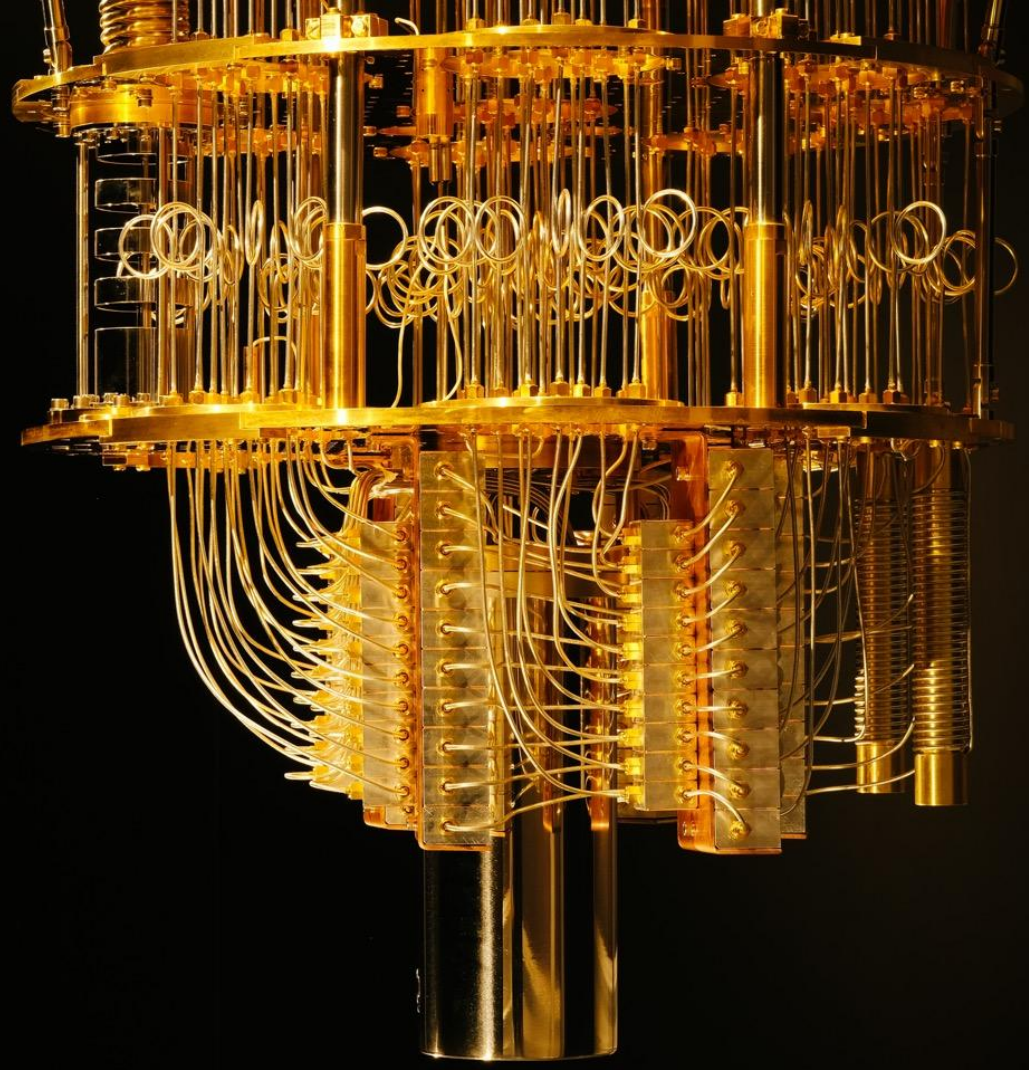
$10T

Estimated total cost 2025 cyber crime [1]

37%

of Internet Traffic in 2025 have been Bad Bots [2]

The Impact of Quantum Computers



Q-Day

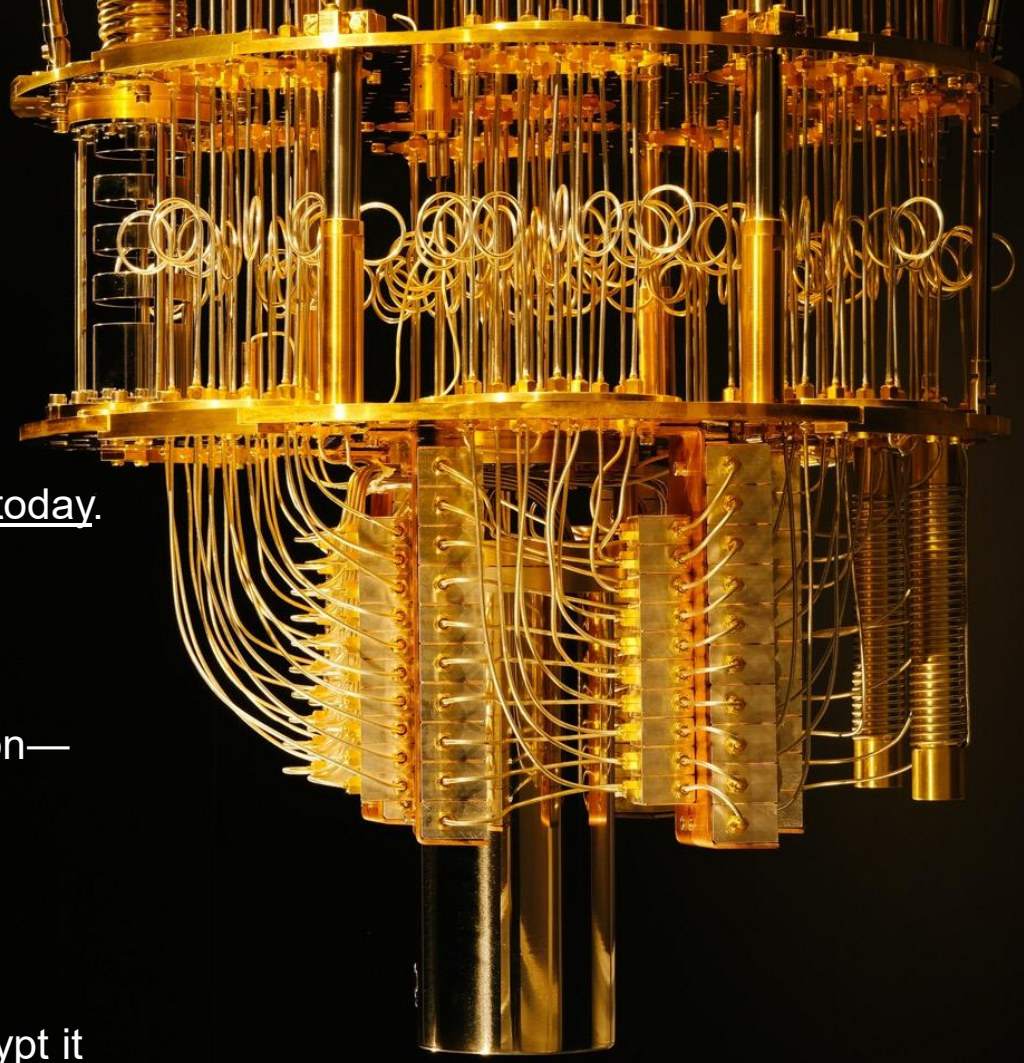
is coming.

*2030-2035**

The projected day when quantum systems can crack today's encryption

*https://cybersecurityventures.com/60-percent-ofsmall-companies-close-within-6-months-of-being-hacked/

Quantum Will Threaten Encryption



Quantum Computers

Expected to break widely used public-key encryption algorithms used today.

NSA: CNSA and Quantum Computing FAQ

Q-Day is Coming

The projected day when quantum systems can crack today's encryption—**potentially by 2033**, per NSA and NIST.

Q-day is Coming

"Harvest Now, Decrypt Later"

Threat actors may already be storing encrypted data, planning to decrypt it once quantum power is available.

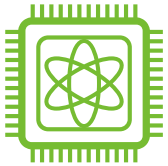
PQC (Post-Quantum Cryptography)

Algorithms that run on today's systems but are designed to resist both classical and quantum attacks.

Emerging Security Requirements

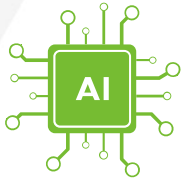
Threat exposure is escalating quickly, leaving businesses that don't upgrade at higher risk

Quantum Computing Risk



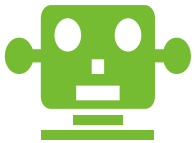
- Quantum computing is moving closer to practical use, bringing the potential to undermine today's encryption methods
- Quantum computers can successfully attack and break many existing algorithms in a fraction of time
- This compromises secure data, communications, and transactions across industries
- CNSA 2.0 is mandating Post-Quantum Cryptographic (PQC) algorithms for all products by 2030

AI Security Risks



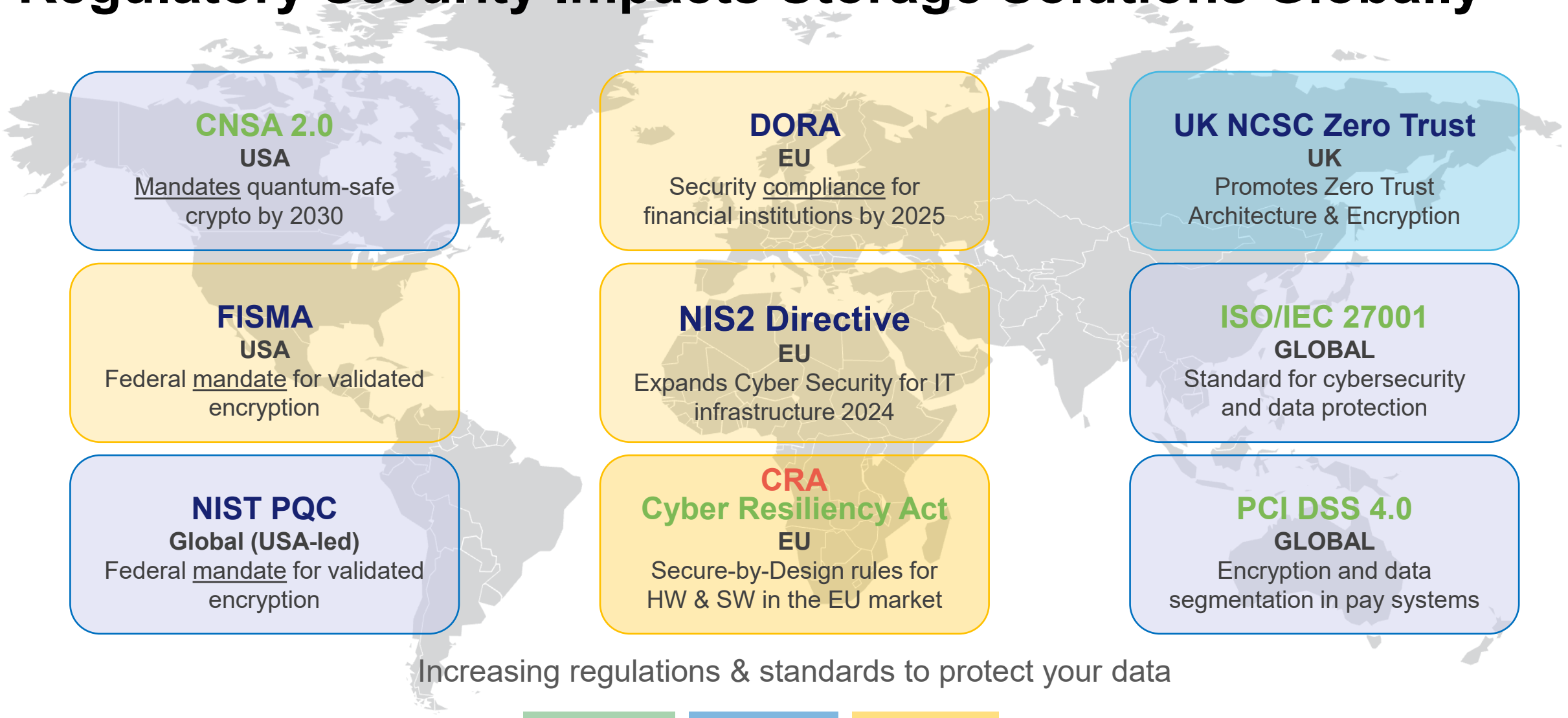
- While the power of AI open new worlds of possibilities for good they can also pose a risk
- Data curation exposures through potential data poisoning, the introduction of bias, and supply chain vulnerabilities
- Data sovereignty is a key consideration for IT
- Proprietary nature of the data is pushing decisions to keep data on premises

Rise of Bad Bots



- 37% of total internet traffic are bad, malicious bots (Imperva report)
- Attackers are using AI to build more adaptive bots that target APIs, abuse business logic, and drive fraud
- Organizations need stronger defenses to keep up with the growing scale and sophistication of automated threats
- NIS2 regulation due to the growing volume of CVEs every year, where bots are going after those flaws and weaknesses

Regulatory Security Impacts Storage Solutions Globally



CNSA 2.0
USA
Mandates quantum-safe crypto by 2030

DORA
EU
Security compliance for financial institutions by 2025

UK NCSC Zero Trust
UK
Promotes Zero Trust Architecture & Encryption

FISMA
USA
Federal mandate for validated encryption

NIS2 Directive
EU
Expands Cyber Security for IT infrastructure 2024

ISO/IEC 27001
GLOBAL
Standard for cybersecurity and data protection

NIST PQC
Global (USA-led)
Federal mandate for validated encryption

CRA
Cyber Resiliency Act
EU
Secure-by-Design rules for HW & SW in the EU market

PCI DSS 4.0
GLOBAL
Encryption and data segmentation in pay systems

Increasing regulations & standards to protect your data

Frameworks | Standards | Regulations

New regulations driving security enhancements

Increasing Encryption Requirements

2020

2021

2022

2025 - 2030

SolarWinds Security Event

- Equipment spoofed via rogue firmware impacting the US Federal Government's data security

US Gov. Executive Order

- Improve national cybersecurity
- Zero Trust Architecture
- CNSA 1.0 specification

UK Issues Guidance

- Intended for Enterprise Environment to implement Zero Trust Architecture

CNSA 2.0 Requirements

- Quantum Resistant Algorithms
- **Encryption Everywhere**

Cyber Resilience Act (CRA)

- Common EU requirements for hardware and software

CNSA/ENISA Timeline

- 2025: Shipments into US Govt. are **recommended** to include CNSA 1.0 or 2.0 components
- 2026: ENISA Expects to adopt QR algorithms
- 2030: Shipments into US Govt. are **required** to include CNSA 2.0 components

NIS2 Adoption (EU) - Network & Information Security Directive

- 2025: Adopt, publish measures Intended to improve the security of network and information systems across the EU

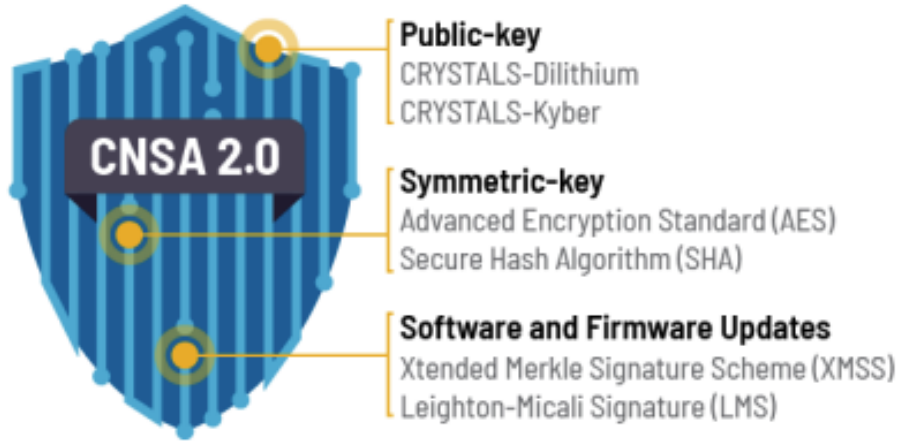
DORA (EU) - Digital Operations Resilience Act

- 2025: **Compliance** with legislative act to improve the IT security of **financial institutions** and their third-party service providers

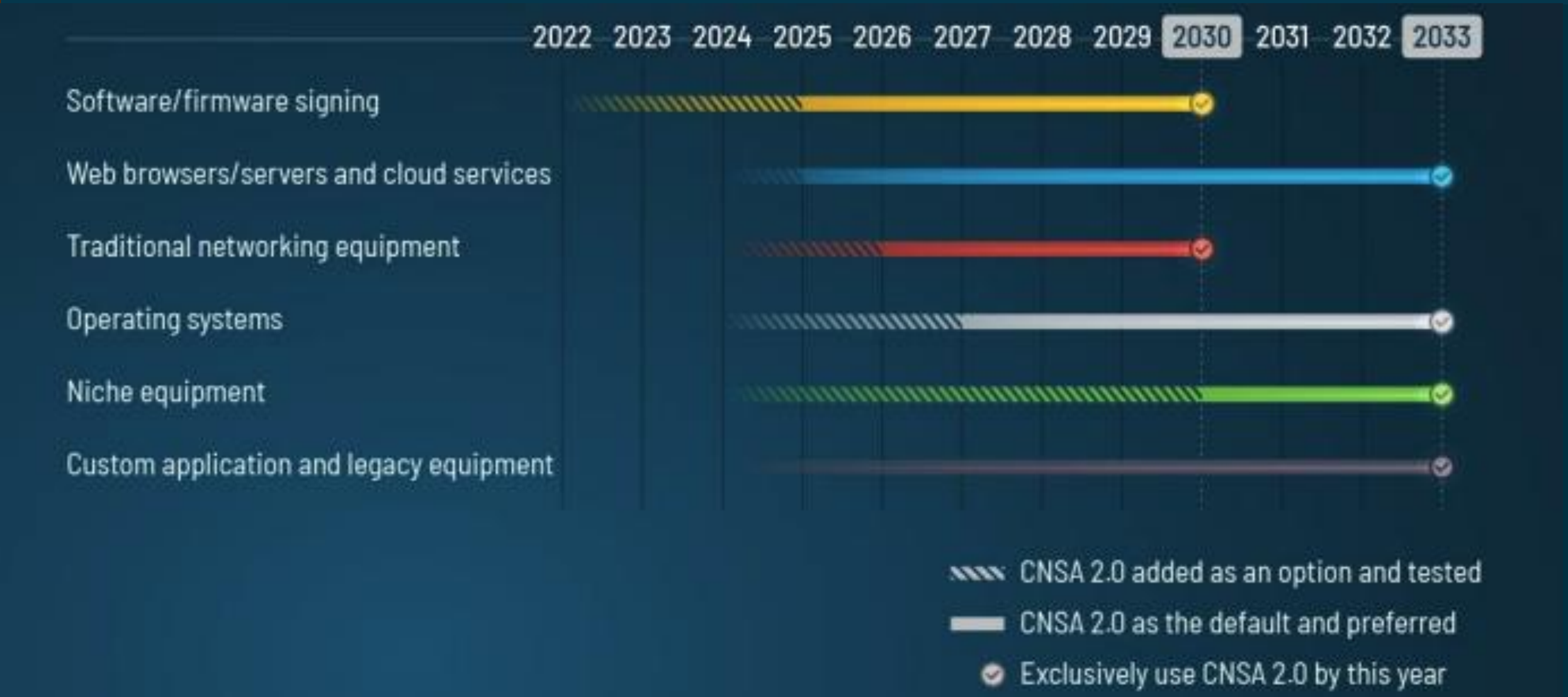
Is Your Storage Network Quantum Safe?

Commercial National Security Algorithm (CNSA) Suite 2.0 security regulation

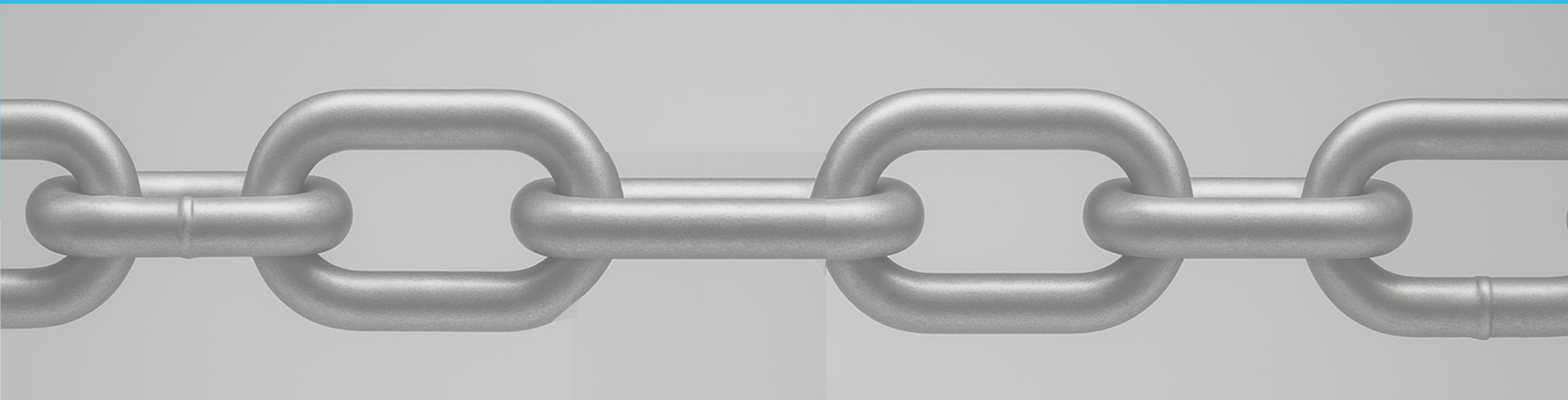
- The **NSA's CNSA 2.0** defines new cryptographic standards to defend against quantum attacks.
- **Future compliance** will require adoption of CNSA 2.0 across all systems.



CNSA 2.0 Timeline – Are You Ready?



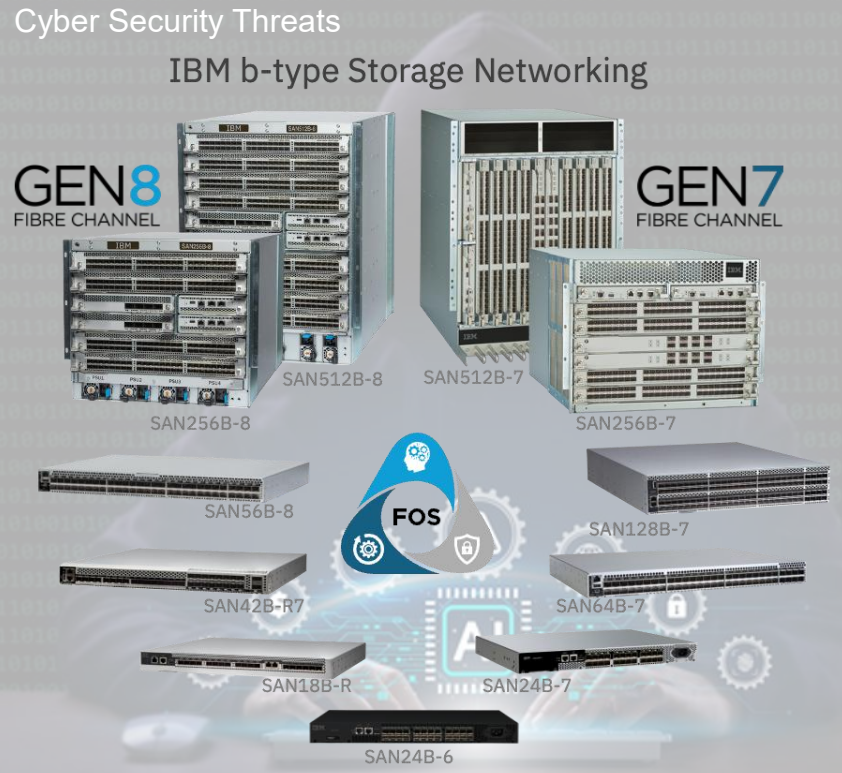
SECURITY REQUIRES END-TO-END SOLUTIONS



IBM's Strength:
Secure Operational Resiliency Solutions

SHARE
EDUCATE • NETWORK • INFLUENCE

OPERATIONAL RESILIENCE for the DATA



OPERATIONAL RESILIENCE for the DATA PATH

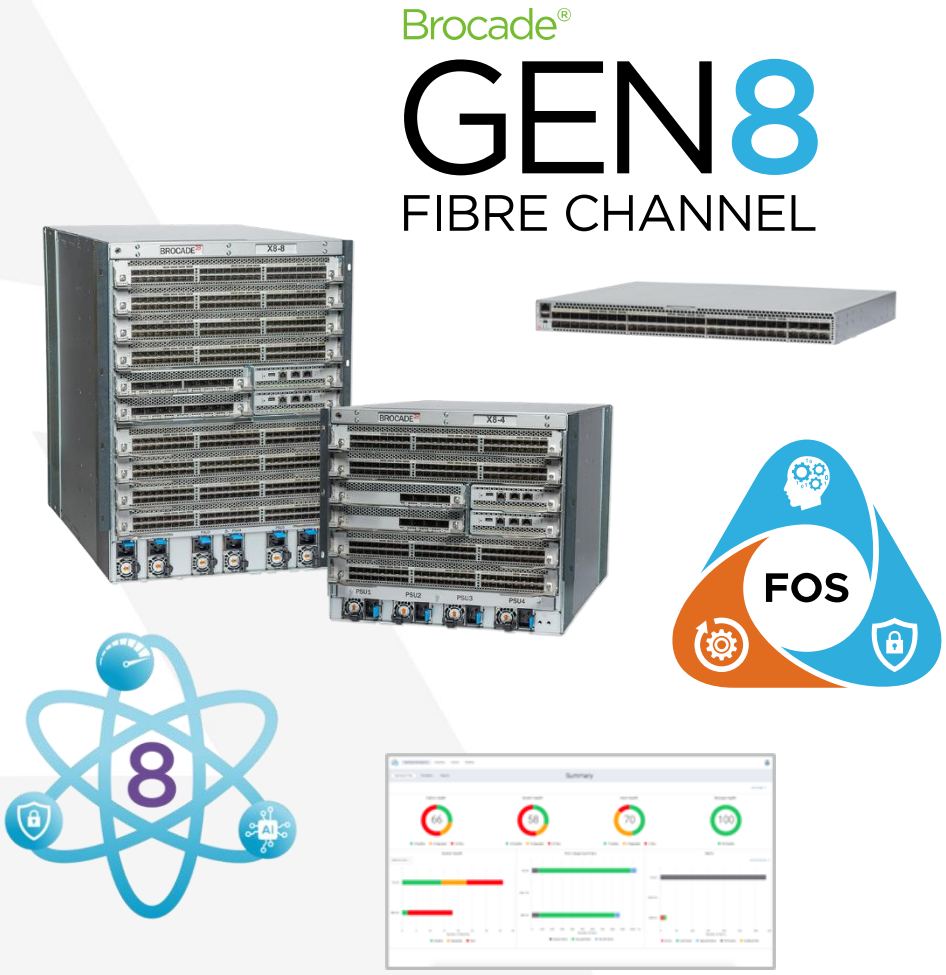
Industry's First Gen 8 128G Fibre Channel Platforms

SHARE
EDUCATE • NETWORK • INFLUENCE

The most secure, high-performance storage network for enterprise AI

What's New?

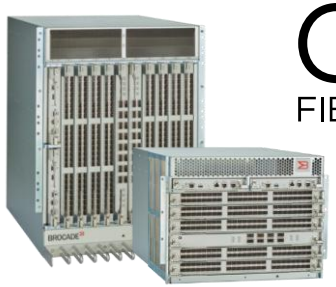
- ASIC – Condor 6
- Transceivers
  - 128G SWL SFP+ and Gen 8 ICL OSFP 128G
- Fabric OS – FOS 10.x
  - Quantum-safe SAN and AI-powered autonomy technology
- Platforms
  - Gen 8 X8 Directors and G820 Switch
- Brocade SANnav v3.x
  - Robust security architecture and new features to automate daily tasks, simplify operations and accelerate troubleshooting



Brocade FICON Portfolio

SHARE
EDUCATE • NETWORK • INFLUENCE

Brocade®
GEN7
FIBRE CHANNEL



Brocade X7 Directors

Brocade G720 Midrange Switch

Brocade 7850 Extension Switch

Gen 7 Port Blades: FC64–48, FC64-64
Extension Blade: SX6 Extension Blade

Brocade®
GEN8
FIBRE CHANNEL

Brocade X8 Directors

Gen 8 Port Blade: FC128-48

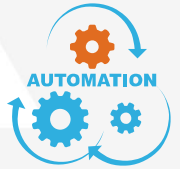
Brocade G820 Switch

Brocade SANnav Management Portal

Brocade SANnav Global View

Brocade Autonomous SAN

Fabric Operating System (FOS)



Rest API

Integrated Security

Brocade has Mainframe DNA

70%
of all transactions by value go through IBM mainframe [1]

40 years
of reliable connectivity to storage

9 of the top 10
of largest public banks rely on IBM Storage and Brocade SAN

1985	1990	1995	2000	2005	2010	2015	2020	2025
IBM 3090	ES/9000	System/390	z900	z990	z9	z10	EC12	z13	z14	z15	z16	z17
								LinuxONE Releases ★1	★2	★3	★4	★5

Bus/Tag and ESCON Extension
- 1986 CTC Extension/B&T
- 1991 High Speed Printer Extension
- 1993 Tape Storage Extension
- 1993 T3/ATM WAN Support
- 1995 Disk Mirroring Support

ESCON Introductions
- 1994 9032 ESCON Directors
- 1999 FICON Bridge

ESCON & FICON Extension
- 1998 IBM XRC Support
- 1999 Remote Virtual Tape
- 2001 FCIP Remote Mirroring
- 2003 FICON Emulation for Disk
- 2005 FICON Emulation for Tape

FICON Introductions
- 2002 **2G FICON**
- 2002 FICON / FCP Intermix
- 2001 FICON Inband Mgmt
- 2001 64 Port Director
- 2002 140 Port Director
- 2005 256 Port Director
- 2006 **4G FICON**
- 2008 DCX Backbone
- 2008 768 Port Platform
- 2008 Integrated WAN
- 2008 **8G FICON**
- 2008 Accel for FICON Tape
- 2009 New FCIP Platforms

Gen 5 FICON
- 2011 DCX 8510
- 2012 **16G FICON**
- 2014 16G Extension
- Added Features:
  - ✓ Port Commissioning
  - ✓ Health Checker z/OS
  - ✓ FICON Dynamic Router
  - ✓ Forward Error Correction
  - ✓ Multi-Hop configs
  - ✓ 64G ICLs

Gen 6 FICON
- 2016 X6 Directors
- 2016 **32G FICON**
- 2016 32G Extension
- Added Features:
  - ✓ FICON Express32/S
  - ✓ FCIP & IP Extension
  - ✓ ISL Encryption
  - ✓ 128G ICL Support
  - ✓ Virtual SANs
  - ✓ FC Endpoint Security Support

Gen 7 FICON
- 2020 X7 Directors
- 2021 **64G FICON**
- 2023 64G Extension
- Added Features:
  - ✓ Safeguarded SAN
  - ✓ Traffic Optimizer
  - ✓ FICON Logical Switch
  - ✓ SANnav for FICON

NEW
Gen 8 FICON
2025 **128G**

INRANGE Technologies Corporation · CNT · McDATA · BROCADE A Broadcom Company · BROADCOM

Gen 8 Standard Feature Requirements

Seamless integration into pre-existing Brocade Fibre Channel (FC) networks

- Backward compatibility with Gen 6 & Gen 7 FC networks
- Forward compatibility with future FC generations

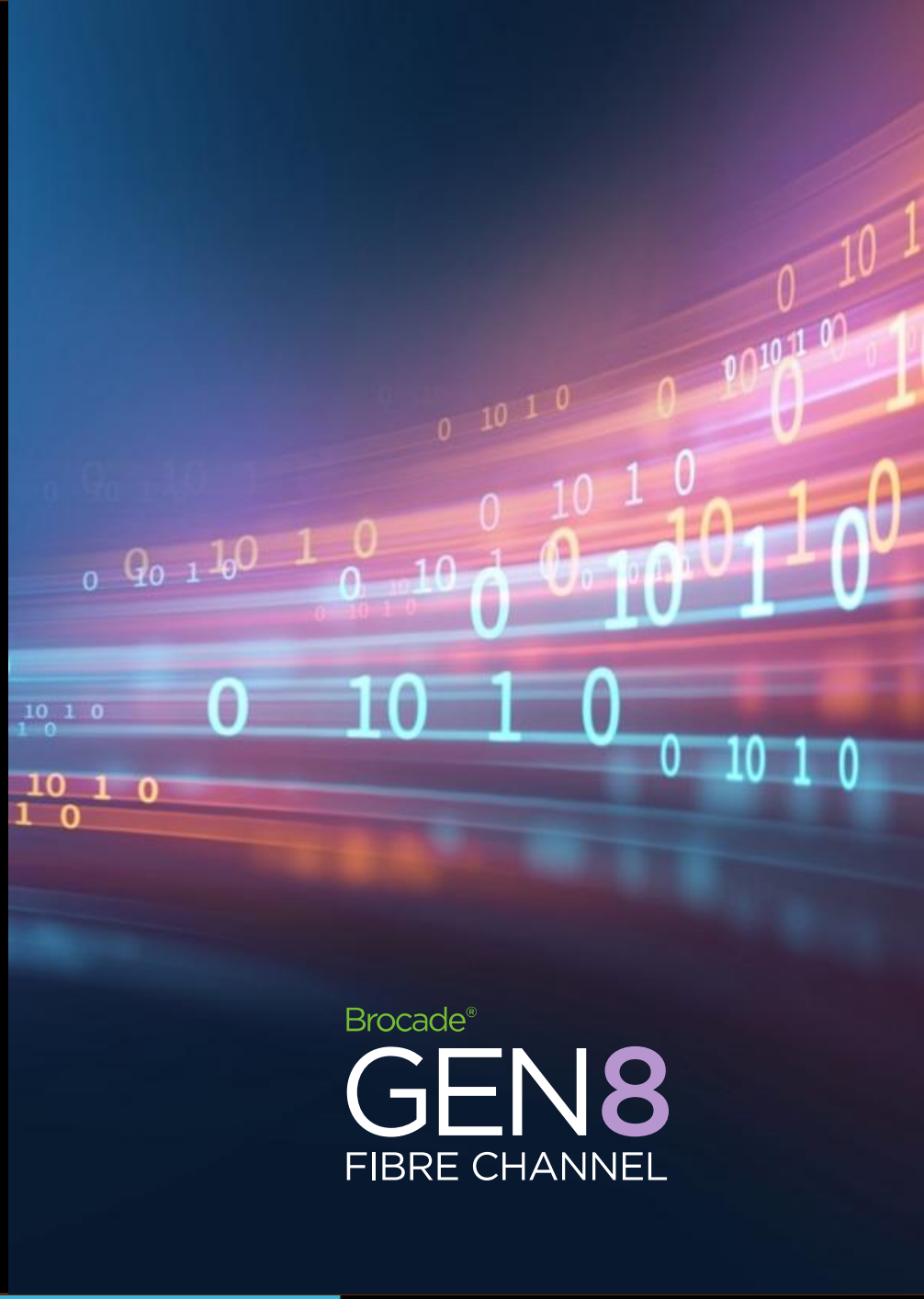
Utilization of pre-existing physical layer infrastructure

- LC and SFP-DD connectors
- SFP+ and SFP-DD transceivers
- OM3/OM4/OM5 cable infrastructure

Support for same physical distances as prior generations

- 100m multi-mode fiber (MMF) over OM4/OM5 cables
- 2km / 10km single-mode fiber (SMF) over OS2 cables

Enhance and Evolve Data Path Security

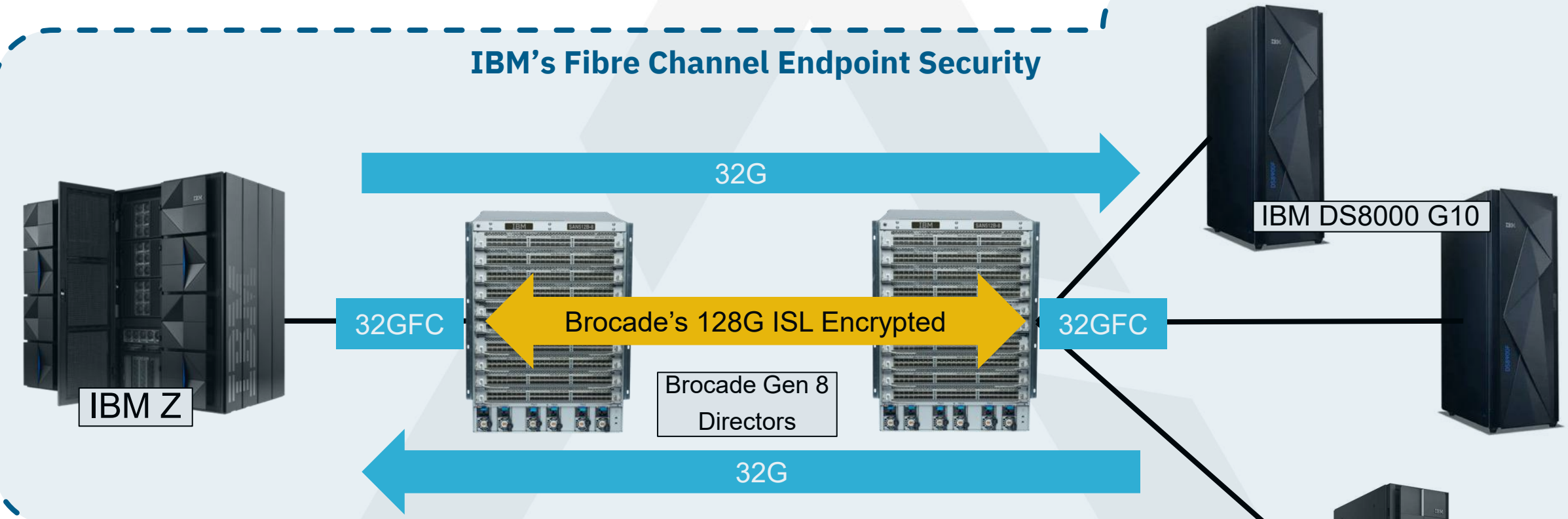


FIBRE CHANNEL ENDPOINT SECURITY

Quantum Safe
Data Path

FICON Express32s with Enhanced Security

IBM's Fibre Channel Endpoint Security



- **Eliminates Insider Threats -** Ensures only trusted, authenticated devices
- **Zero Performance Impact -** Encrypts 100% of data in flight at hardware speeds
- **Simplified Compliance -** Reduces audit complexity by extending secure "perimeter"
- **Simplified SAN Configuration** – Compatible with IBM b-type ISL Encryption

Broadcom Storage Networks provide Quantum Safe Data Paths – Local and Remote

SHARE
EDUCATE • NETWORK • INFLUENCE

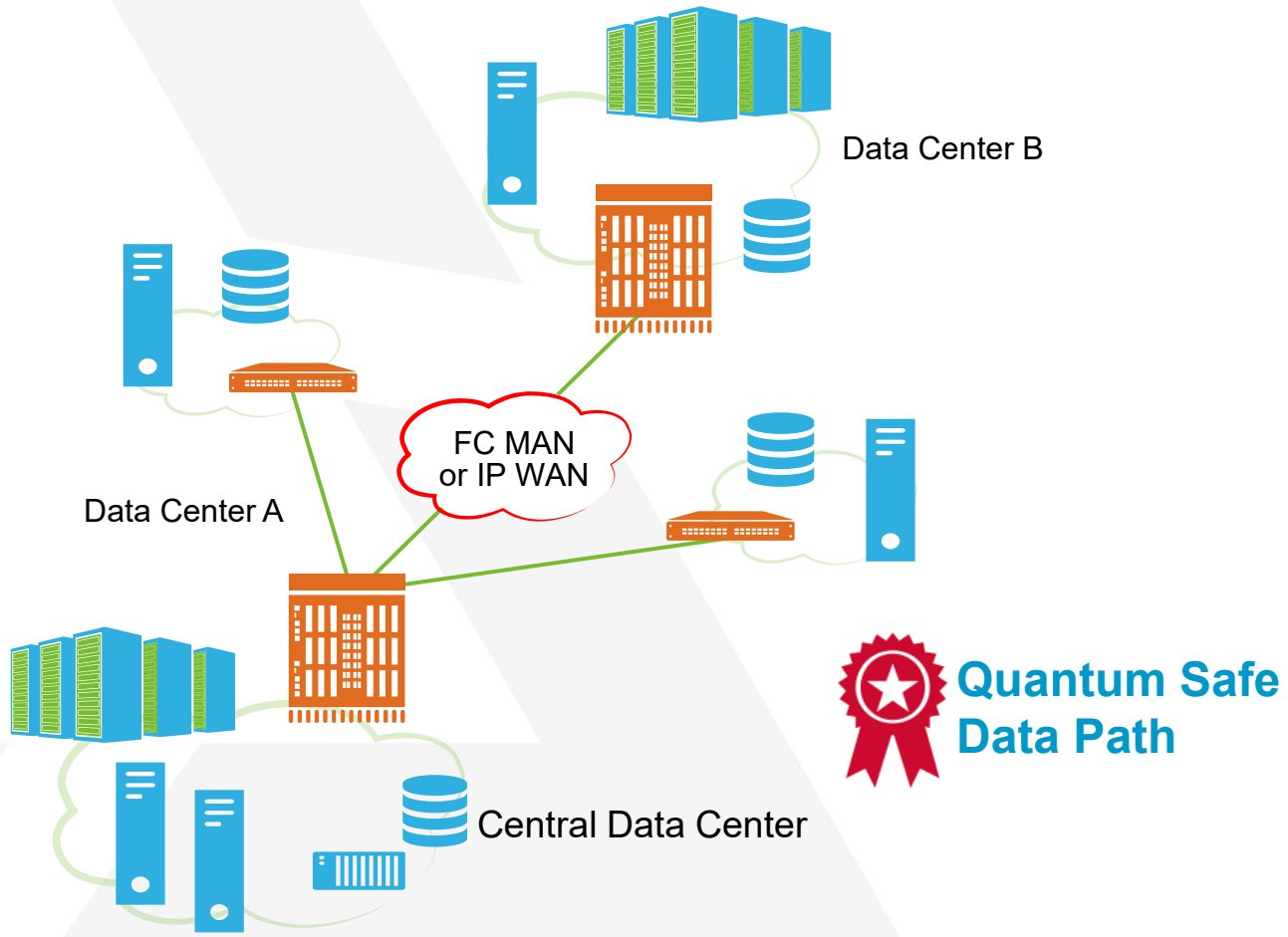
Encryption matters to be resistant to attacks from quantum computers

Broadcom fabrics mitigate threats by securing data flows with quantum safe, **AES 256 encryption**

Broadcom encrypts communication within and across data centers, not data at-rest

1. **Server-to-Storage Encryption**
   - SecureHBA End-to-end encryption
2. **Storage-to-Metro Encryption**
   - Switch-to-switch encryption
3. **Storage-to-WAN Encryption**
   - FCIP IPSec over long-distance WAN links

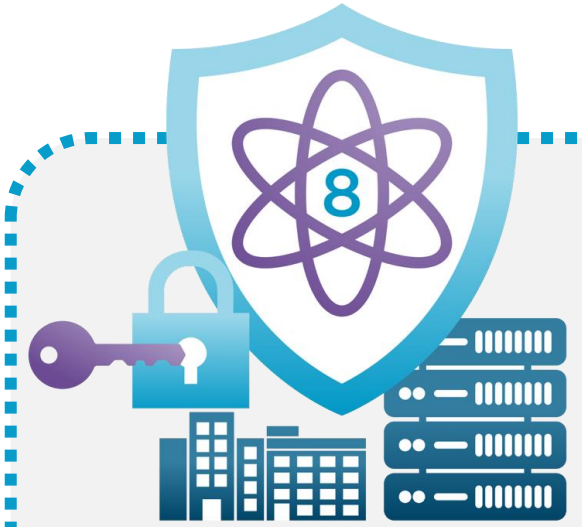
Switches, Software, HBA implementing **Zero Trust architecture** and **multi-factor authentication** (MFA)



QUANTUM SAFE SAN

Quantum Safe
Data Path

Defending the Data Center in the Quantum and AI Era



GEN8
FIBRE CHANNEL
SECURITY OVERVIEW

Fortify Fabrics

- Deploy advanced cryptographic algorithms to block sophisticated attacks.

Prevent Hijacking

- Stop malicious software installation with enhanced anti-tampering tech.

Lock Down Access

- Minimize the attack surface using embedded mandatory access controls.

Detect Instantly

- Monitor and alert on security configuration changes in real time.

Validate Integrity

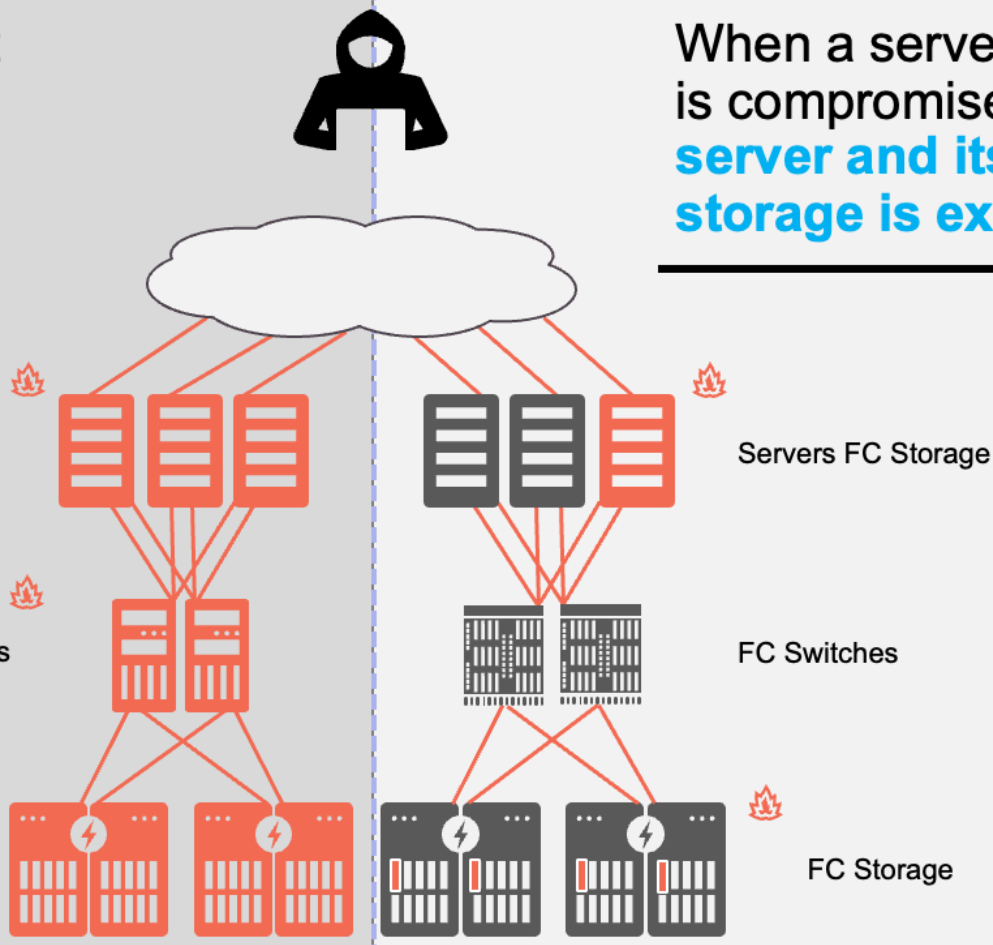
- Ensure the security of IBM b-type hardware and software automatically.

Fibre Channel Storage Networks are Inherently More Secure

SHARE
EDUCATE • NETWORK • INFLUENCE

When a server with Ethernet Storage is compromised **everything is exposed**

When a server with FC Storage is compromised **only that server and its allocated storage is exposed**



Ethernet
Any-to-Any Network

Fibre Channel
Point-to-Point Network

Cybersecurity ATTACK SURFACE = Area or Systems VULNERABLE to HACKING

Is Your Storage Network Quantum Safe?

Time to Move to New Post Quantum Cryptography (PQC)

SHARE
EDUCATE • NETWORK • INFLUENCE

Brocade Gen 8 is quantum-safe, protecting sensitive data and critical infrastructure from future quantum computers

- Brocade fabrics secures data flows in-flight within and across data centers with quantum-resistant, AES 256-bit encryption

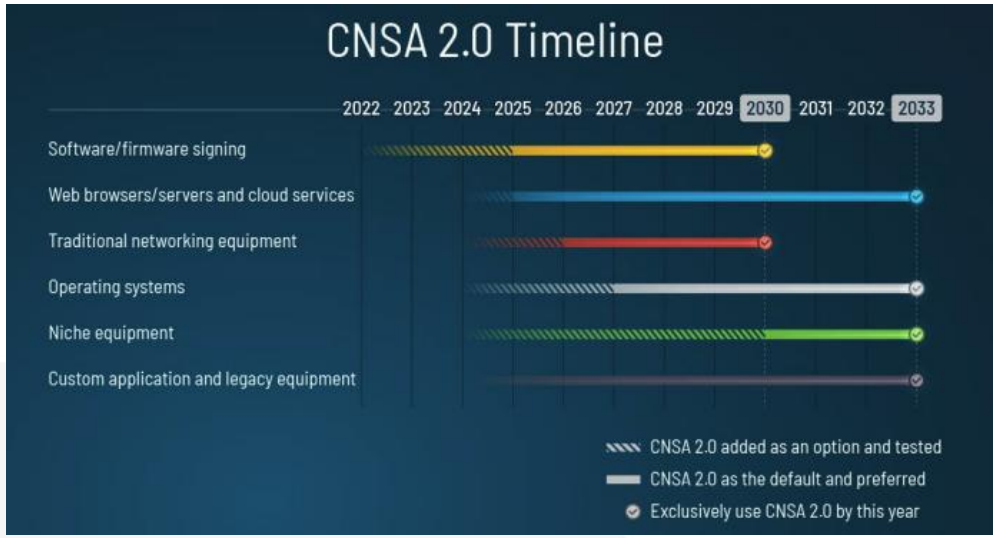
- Brocade Gen 8 supports Post Quantum Cryptography in FOS v10.x
  - SSH and SSH KEX
  - TLS Sign/Verify and Key Encapsulation
  - Stronger ciphers for symmetric encryption and hashes
  - IKEv2 with PQC for Extension

Post-Quantum Cryptographic Algorithms

Public-key
ML-DSA (CRYSTALS-Dilithium)
ML-KEM (CRYSTALS-Kyber)

Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates
Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)



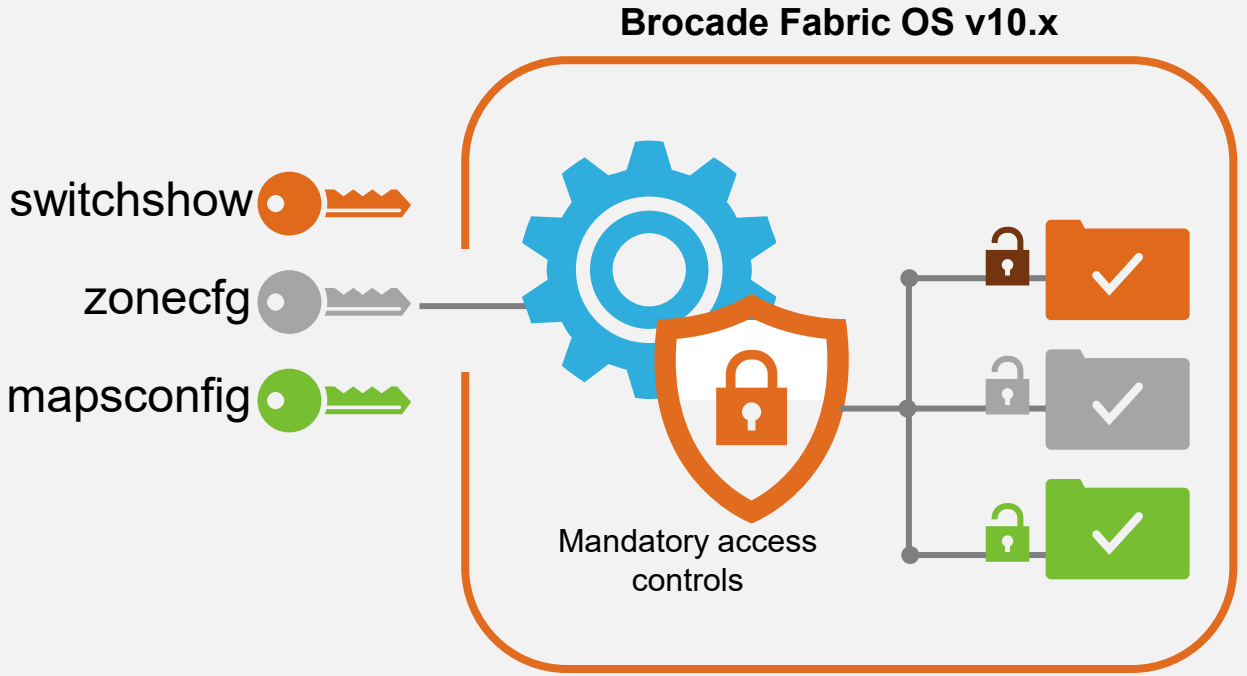
Brocade Gen 8 Technology Further Hardens the SAN

SHARE
EDUCATE • NETWORK • INFLUENCE

Minimize attack surface with embedded mandatory access controls

- Enforce strict access using principle of least privilege architecture
- Grants access to only the minimum resources and permissions necessary
- Reduces attack surface and stops malware spread
- Minimizes damage from errors or misuse
- Improves security, resilience, and compliance efficiency

Principle of Least Privilege Architecture



Federated Authentication

Secure and automated identity management with token-based authentication

Multi-factor Authentication (MFA)

- Passwords are risky (weak, re-use, sharing)
- MFA adds layers of security
- Requires multi-verification factors:
  - something you know (ex: PIN)
  - something you have (ex: mobile device)
  - something you are (ex: fingerprint)

Federated Authentication (FA)

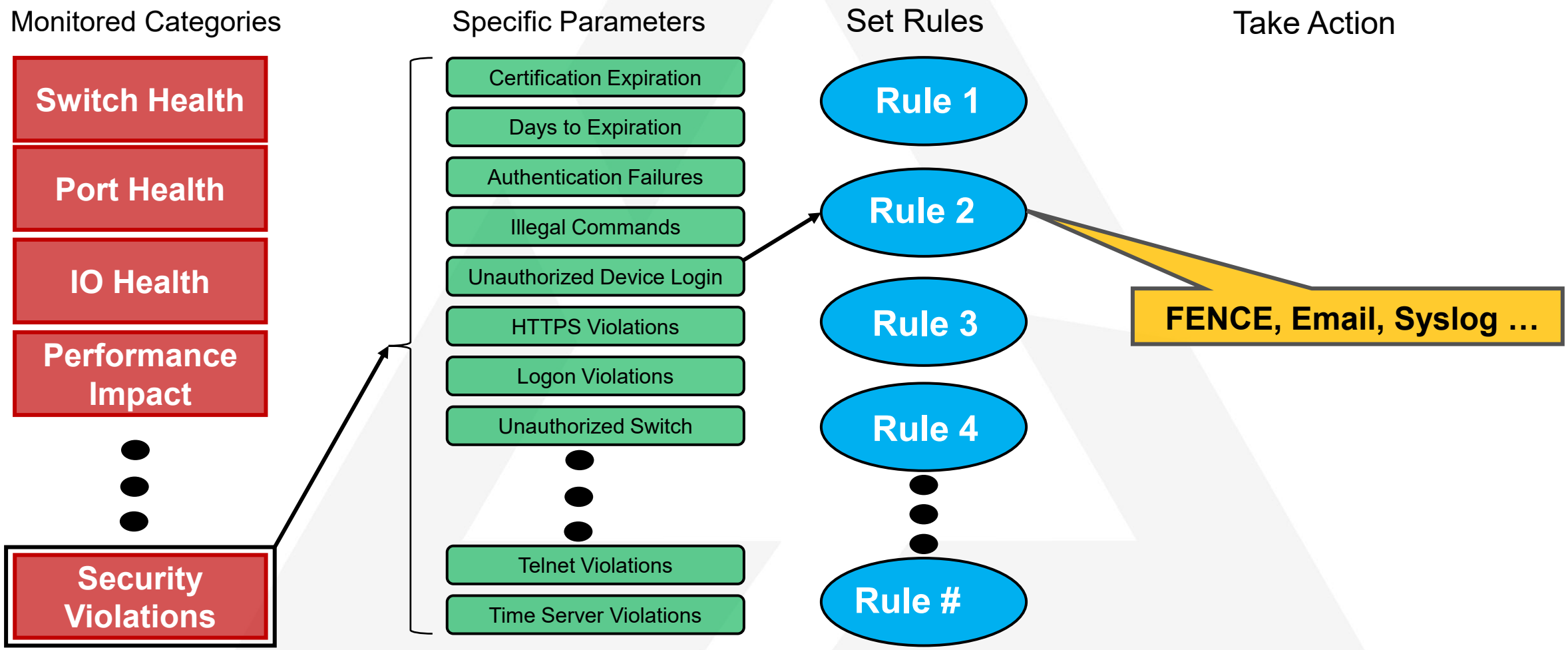
- Validate through MFA with Identity Provider (IdP) trusted by Brocade FOS
- The trusted IdP authenticates user
- Secure access token sent by IdP
- Allows user access with associated privileges

Brocade Fabric Vision Feature includes MAPS

Monitoring Alerting Policy Suite

SHARE
EDUCATE • NETWORK • INFLUENCE

Enhanced Monitoring, Logging, Alerting for Security and much more



SANnav Manages and Monitors SAN Security Across Fabrics

SHARE
EDUCATE • NETWORK • INFLUENCE

Enforces and maintains the highest levels of security

Harden Security

- Build and quickly deploy customizable security thresholds
- Monitor and alert for security configuration changes and events
- Enforce secure access and prevent unauthorized changes

SANnav v3.0 Strengthens Access Controls

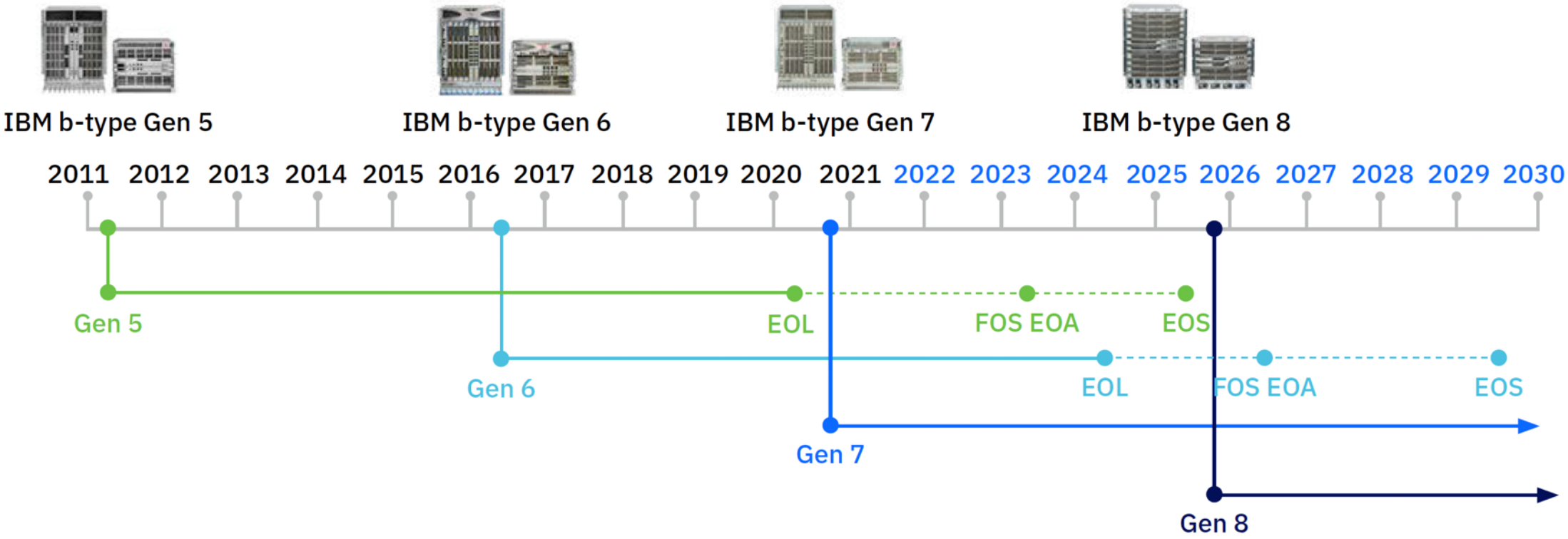
New features enforce secure access and prevent unauthorized changes

- Hardens SANnav security by using podman container architecture, preventing malice attacks and accidental mistakes
  - Removes root access - it is no longer required to install/run/manage SANnav
  - Podman for managing containers on Linux, Docker containers removed
- Leverages Principle of Least Privilege architecture
  - Reduces the attack surface by running SANnav on SE Linux server
- Employs quantum-resistant LMS cryptographic hash-based functions
  - Verifies FOS firmware is genuine on download
- Provides security REST APIs to allow customers' centralized audit and compliance systems to retrieve all SANnav user information

REFRESH FOR LATEST SECURITY FEATURES

Quantum Safe
Data Path

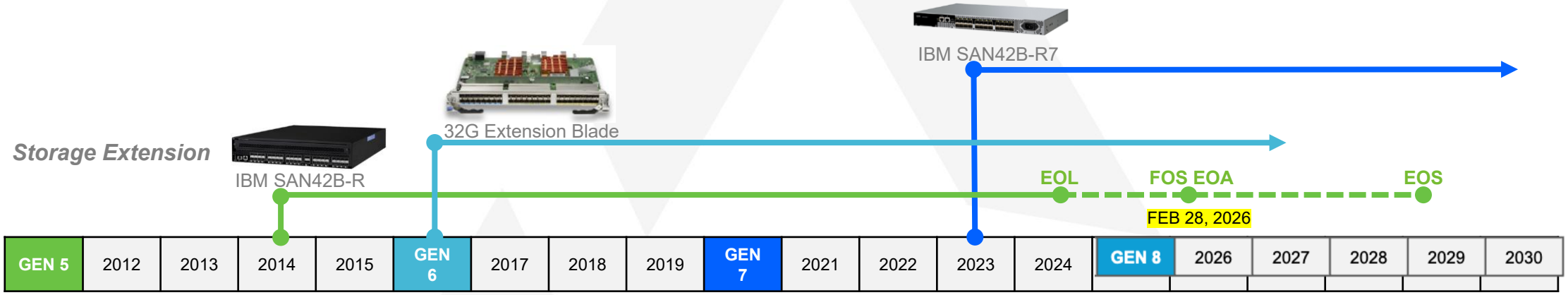
Important FICON Support Notes



1. **All Gen 5 Technology is EOS (End Of Support)**: *Immediate refresh for all Gen 5 SAN installations.*
2. **Gen 6 SAN is not supported with z17**
   - Lead with Gen 8 Directors, fall back to Gen 7 if needed
   - Combine with z17 and/or DS8000 G10 refresh

Position Gen 8 SAN for greatest Z investment protection

Important Extension Support Notes



- **Gen 5 Extension (SAN42B-R) is Fabric OS EOA (End of Availability) on Feb 28, 2026**
  - No additional scheduled FOS updates
  - Limited security patches
- **Gen 6 Extension (SX6 blade) is available in Gen 6 and Gen 7 Directors**
  - z17 is supported
  - No zNext support
- **Gen 7 Extension (SAN42B-R7) provide best investment protection for non-chassis extension**

Refresh legacy SAN42B-R with SAN42B-R7 Routers

Mainframe Support with IBM Z Platforms

	SAN Router	SAN Switches		SAN Director Blades				
Brocade Product	7850 Extension (Gen 7)	G820 (Gen 8)	G720 (Gen 7)	**FC128-48** (Gen 8)	FC32-48 (Gen 6)	SX6 Extension (Gen 6)	FC32-X7-48 (Gen 6 Enhanced)	FC64-48 (Gen 7)
	 24x32G FC ports 16x10/1GbE 2x40GbE	 64x128G FC ports	 64x64G FC ports	 48x128G FC ports	 48x32G FC ports	 16x32G FC ports 16x10/1GbE 2x40GbE	 48x32G FC ports	 48x64 GFC ports
z17	✓	✓	✓	✓	X	✓	✓	✓
zNext	✓	✓	✓	✓	X	X	X	✓
zNext+1	X [3]	✓	X[3]	✓	X	X	X	X[3]

Qualification Policy

- Active Brocade products for Mainframe that have not reached End of Life (EOL, aka "WFM - Withdrawn from Market" or "LCS - Last Customer Ship") will be qualified and supported with a new IBM Z platform when it is announced.
- Inactive Brocade products that have an announced EOL date will not be qualified or supported with future IBM Z platforms.

Brocade FICON Support for future Z platforms (the Statement of Direction, SOD, based on current projected timelines, is subject to change)

1. **z17 support:** the z17 will be qualified and supported for the full product lifecycle of Brocade G720, G820, 7850, X7 and X8 director blades:
   - FC64-48 port blade, FC64-64 port blade (for replication only), FC32-X7-48 port blade, SX6 extension blade, and FC128-48 port blade.
2. **zNext planned support:** The Z generation following the z17 will be qualified and supported for the Brocade Gen 7 and Gen 8 products including the G720, G820, 7850, and these X7 and X8 blades:
   - FC64-48 port blade, FC64-64 port blade (for replication only), and FC128-48 port blade.
3. **zNext+1 planned support:** The Z generation following zNext will be qualified and supported with the Brocade products that have not reached EOL at that time. Based on historical Z release schedules, Brocade Gen 7 products will likely have reached EOL by zNext+1 launch. Gen 8 products should be active and supported.
4. **Gen 7 EOL:** There are no current plans to EOL the Brocade Gen 7 products (launched in Sept 2020).
5. **Gen 7 EOS:** When Gen 7 products reach EOL, Brocade offers up to five years of support for the hardware and 2 years support for FOS software updates after EOL.

FICON Qualification Notices can be found here: https://www.broadcom.com/info/brocade/mainframe-san

Secure SAN Decommissioning

Best practice when taking equipment out of service

- Switch decommissioning command is provided for customers to erase all data on the switch (CF and seeprom) prior to decommissioning.
- This is a destructive operation which render the switch unusable.

```
sw0:admin> switchdecommission
This operation will erase the firmware on the switch, and it should be returned to the service
provider.
**********************************************************************
Please contact your service provider for a special authorization code.
License ID : (10:00:c4:f5:7c:16:9c:94)
**********************************************************************
Enter decommission authorization code(DAC):
Authorization successful. Switch decommission started.....
/**********************************************************/
Switch decommission has started. Please do not power off the switch.
Switch Decommission is completed.
Please return the switch to the service provider.
/**********************************************************/
```

BROCADE'S EVOLVING SECURITY CAPABILITIES

Quantum Safe
Data Path

Brocade's Evolving SAN Security Strategy

SHARE
EDUCATE • NETWORK • INFLUENCE

FOS v9.0

- Certificate management and LDAP Enhancements
- Force default pw change (SB-327), `maintenance` account, `root` disabled per default
- Secure Boot (Gen 7 platforms), Secure Optics, FC-SP2

FOS v9.1

- Certificate management and LDAP Enhancements, hardening of Linux commands
- Removed access to `root`, enhanced `maintenance` account - v9.1.1 switch decommission
- Certifications: FIPS inside, CC, BSI (& CNSA 1.0 support)

FOS v9.2

- CyberArk support
- Certificate management and LDAP Enhancements, hardening of Linux commands
- Secure by Design, OpenSSL 3.0.7
- MFA with RSA SecurID enhanced with REST support

Brocade's Evolving SAN Security Strategy

SHARE
EDUCATE • NETWORK • INFLUENCE

FOS v9.2.1

- Federated Authentication
- Deprecation of TACACS+

FOS v9.2.2

- PW character increase (510), Default Secure Complex PW profile
- Secure SMTP (cert authentication only)
- No inline passwords –full CLI history
- Deprecation of non secure protocols ++

Brocade's Evolving SAN Security Strategy

SHARE
EDUCATE • NETWORK • INFLUENCE

FOS v10.0.0

- CNSA2.0 –Quantum safe
- OpenSSH v9.9, OpenSSL 3.5.0
- PoLP - Mandated Access Control (SELinux) and removal of ROOT
- Unified IP Filter Policy
- TLS v1.3 for MS Entra and SMTPS
- Anti Tampering detection
- Configupload w/ Checksum
- Web Tools can be disabled

Brocade SAN Integrates with QRadar SIEM

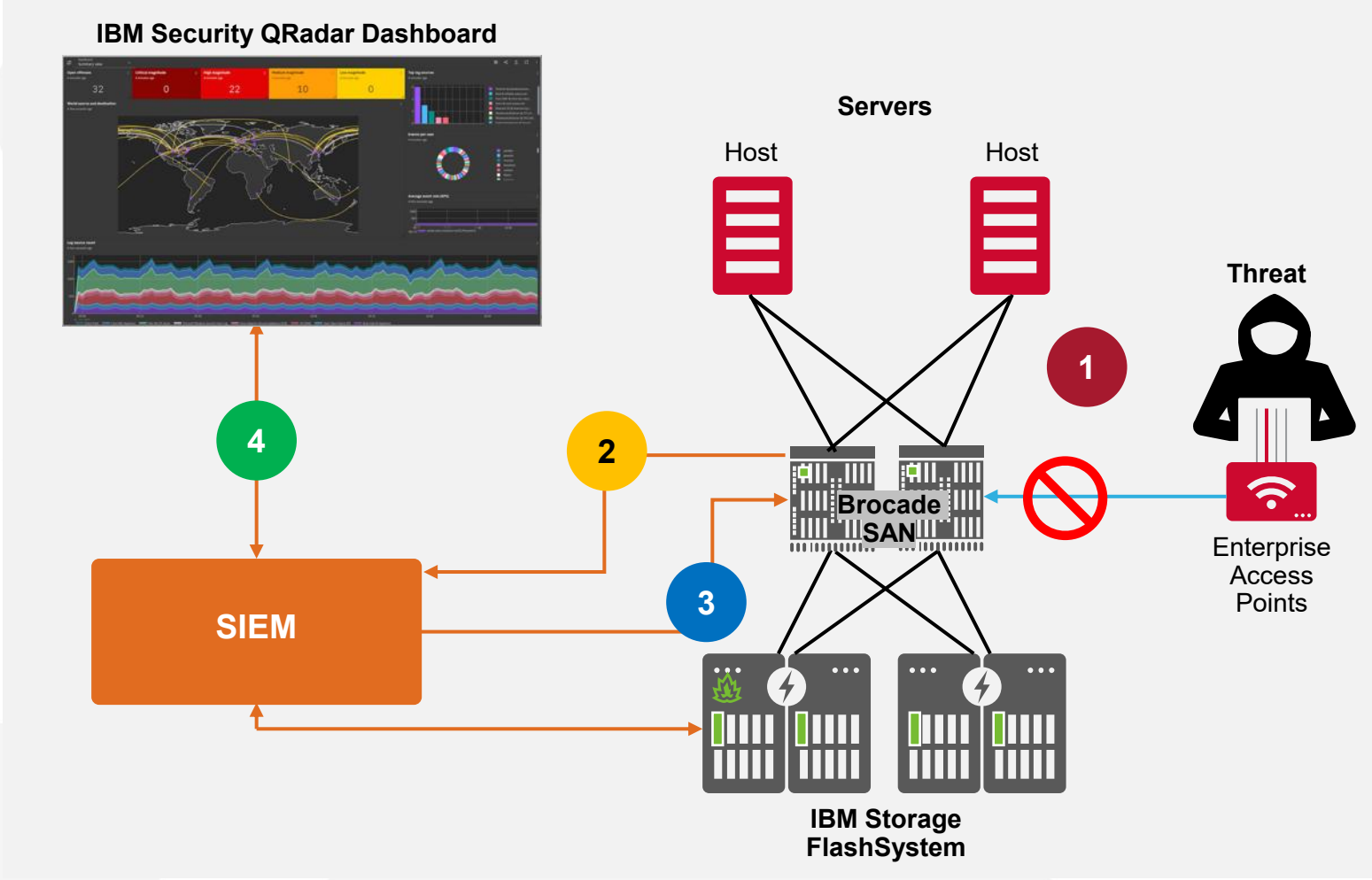
Early detection and automated incident response

1. **Threat**
   Continuous failed login attempts on the switch

2. **Identify/Detect**
   MAPS detects and sends syslog server log events to SIEM

3. **Protect/Recover**
   SIEM performs predicated response
   Example: Insert IP filter to block the offending IP address(es)
   Using API calls to the switch IP filter is configured

4. **Response**
   Offence registered in SIEM and handled for further investigation



ADDITIONAL RESOURCES

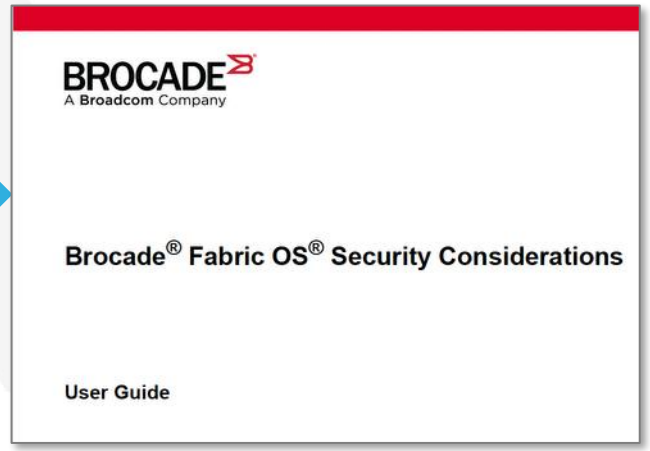
Quantum Safe
Data Path

Learn More About Security with Brocade SAN

Papers, training and user guides

Security Best Practice Guide

https://docs.broadcom.com/doc/FOS-Security-UG



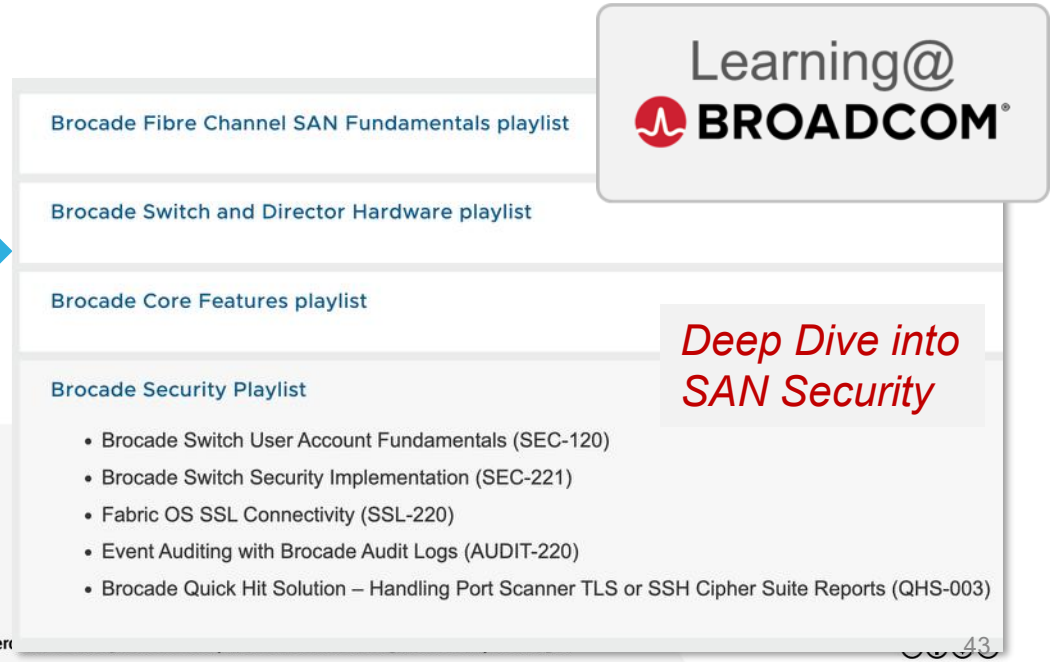
Secure your SAN in 30 pages

Brocade Fabric OS Admin Guide

https://techdocs.broadcom.com/us/en/fibre-channel-networking/fabric-os/fabric-os-administration/9-2-x.html

Brocade Security Training

https://brocade.csod.com/ui/lms-learner-playlist/PlaylistDetails?playlistId=0adbed3f-36af-471c-9cc3-af25e31ce46f



Deep Dive into SAN Security

SAN Qualification Notice

Brocade FOS and SANnav Support

- Latest Hardware and FOS Support
- New Feature Support
  - Fibre Channel Endpoint Security
  - FICON Logical Switch
  - Remote FICON CUP access from a CUP disabled switch
- Qualified for all IBM Z platforms
  - FCP and FICON

https://www.ibm.com/servers/resourcelink/

Qualification letters available here

https://www.broadcom.com/mainframe-san

Brocade Expert Series Videos
FICON Best Practices

FICON Expert Series – FICON Logical Switch (05 min 21 sec)

FICON Expert Series – Port Decommissioning (08 min 38 sec)

FICON Expert Series – SANnav for FICON (06 min 14 sec)

FICON Expert Series – Optimum FICON Design (13 min 20 sec)

FICON Expert Series – Optimizing FICON Performance with Brocade Gen 7 SAN (05 min 33 sec)

https://www.broadcom.com/solutions/data-center/storage-fabrics-technology/mainframe-san#ficon-expert-series

Industry Association Websites

- Fibre Channel Standard
  - https://standards.incits.org/apps/group_public/workgroup.php?wg_abbrev=t11
- Fibre Channel Industry Association
  - https://fibrechannel.org/
- Storage Networking Industry Association
  - www.snia.org
- Ethernet Alliance
  - www.ethernetalliance.org

Brocade SAN Links

- FOS manuals, release notes
  https://www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system
- SANnav manuals, release notes
  https://www.broadcom.com/products/fibre-channel-networking/software/sannav-management-portal
- Hardware manuals
  https://www.broadcom.com/products/fibre-channel-networking
- SFP data sheets and support matrix
  https://www.broadcom.com/products/fibre-channel-networking/transceiver-modules
- FOS, SANnav, BNA support matrix and Target Path info
  https://docs.broadcom.com/doc/Brocade-SW-Support-RM
- Software download (FOS, TruFOS certificate, SANnav)
  https://support.broadcom.com/user/brocade
- Licensing portal registration required
  https://portal.broadcom.com/group/licensing-portal
- Education registration required
  https://www.broadcom.com/support/education/brocade

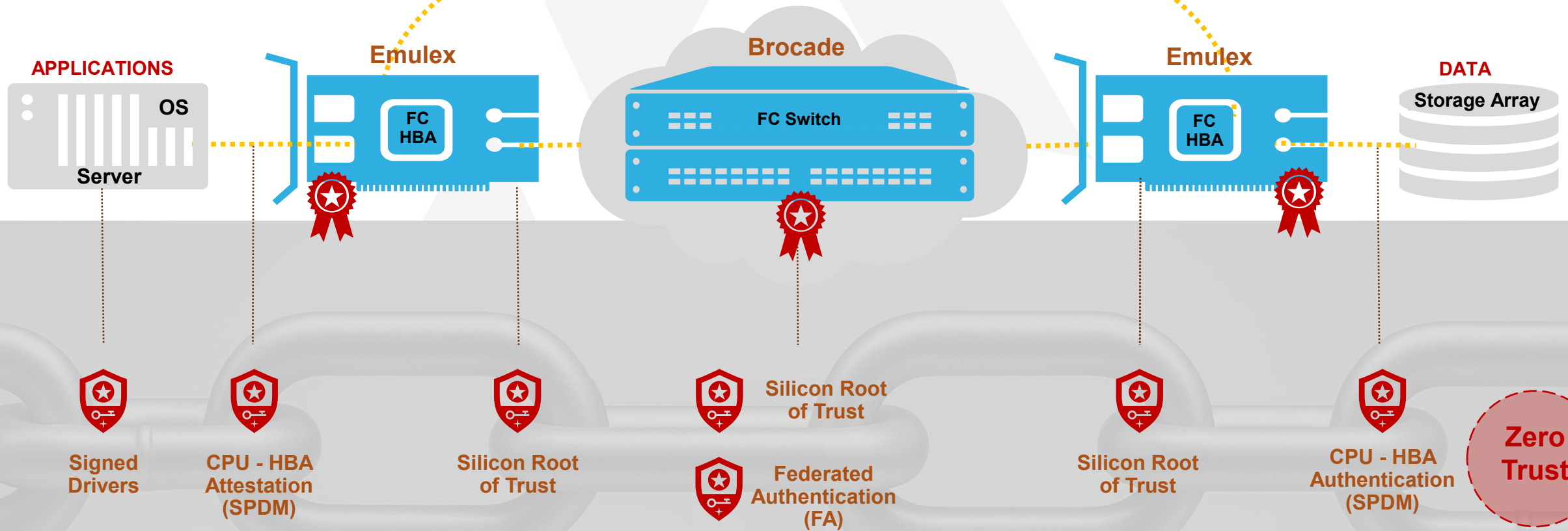
Brocade SAN and Emulex HBAs Deliver End-to-End Security

SHARE
EDUCATE • NETWORK • INFLUENCE

Quantum Safe

Data Path Security

End-to-End In-flight Encryption



Yo

Subr

attend:

RE

ORK • INFLUENCE

SHARE
EDUCATE • NETWORK • INFLUENCE

LinkedIn

TQRCG

jim.stewart@broadcom.com