BROCADE
A Broadcom Company

Safeguard your SAN with Brocade® Gen 7

Strengthening your network security to protect against threats and cyber attacks

Security is top of mind for data center administrators, especially since the sophistication and volume of cyber criminal activities have dramatically increased. Counterfeiting and tampering with hardware and software have become a lucrative illegal trade that leads to billions of dollars in losses across all industries. This kind of tampering within the data center can also cause serious damage and risk to your environment. Businesses that run on data and a distributed workforce are under immense pressure to protect their enterprise users against disruptions or outages while eliminating cybersecurity vulnerabilities.

You may feel your enterprise data is protected, but with hundreds of IT security vulnerabilities uncovered every year, it's important to keep up on the latest technology or risk leaving your infrastructure exposed. As threats continue to evolve, your security team will have new compliance requirements. These include switch account authentication, protocols allowed on the management interface, and limited duration SSL certificates for secure communications. It may be possible to manage each of these requirements manually, but Brocade® Gen 7 provides a better solution. Brocade Gen 7 products act autonomously to protect against security threats while quickly and efficiently maintaining optimal conditions, maximizing availability of your storage resources, and ensuring the highest levels of resiliency.

Cyber resiliency is at the core of Gen 7

Brocade Gen 7 Fibre Channel safeguards and modernizes your SAN against cybersecurity and business continuity challenges that threaten to disrupt data center operations.

Delivering innovative security features, hardening Fabric OS® (FOS) software, and validating hardware components makes Gen 7 the most cyber resilient storage network available. Deploying Gen 7 protects enterprises against cybersecurity threats as well as disruptions or outages from catastrophic events. Of course, Fibre Channel fabrics are secure by design based on controlled access between servers and storage as well as its isolation within a dedicated storage network. But Brocade Gen 7 technology further reduces the risk of vulnerabilities from malware and hijacking attacks by validating the integrity of the switch operating system, security settings, and hardware. Brocade Gen 7 also automates processes to enable optimum performance and resiliency. Its autonomous SAN capabilities transform billions of telemetry data points into automated actions to identify potential vulnerabilities and resolve issues proactively.

Security integrated by design

Security likely wasn't the primary reason you chose a Fibre Channel SAN. However, its point-to-point architecture prevents attackers from being able to see, let alone infiltrate connected storage devices. This, combined with integrated security features, delivers a strong line of defense to protect an organization's valuable digital assets. Brocade Gen 7 does just that. It is a cyber resilient network designed with security in mind and implements many security measures to protect an organization against vulnerabilities, making it the top network choice for mission-critical storage.

Secure boot

Brocade Gen 7 security starts with validating the integrity of the hardware and software platforms to ensure that the switch has not been altered, protecting against tampering of the hardware and its boot code. Every time a Brocade Gen 7 switch boots up it goes through a secure boot sequence that validates hardware components through a root of trust. In addition, it confirms that the software image is genuine, which authenticates that the switch, blades, and optics are also genuine. The control processor validates the integrity of the Fabric OS (FOS) boot image and upon detection of any anomalies, such as compromised hardware or software components, halts the boot process.

Secure hardware

Beyond validating the switch components, Small Form Pluggable (SFPs) transceiver optics are also validated on boot up to ensure that they are genuine. This safeguards against high failure rates often seen with counterfeit optics and ensures that the point-to-point data transfer authentication chain is maintained.

Secure software enterprise

Enterprise platforms (directors and enterprise switches) use Brocade Trusted FOS Certificates for FOS authenticity and current entitlement assurance. In FOS v9.0 and above, the root account is disabled by default. A new maintenance account has been implemented for use by OEM support providers and Brocade technical support when troubleshooting and diagnosing. The maintenance account has sufficient privileges to perform diagnostics commands, but in contrast to the root account, the maintenance account cannot access the native Linux OS that underpins FOS. In FOS 9.1 and above, FOS is hardened further by removing access to the root account altogether, prohibiting any direct access to the native Linux OS. This protects all updated FOS switches from hijacking and installation of malicious software.

FOS provides customizable cryptographic templates that are easily loaded onto a switch to meet specific security requirements. In FOS 9.1.1 and above, platforms are FIPS140-3 (level 1) "FIPS Inside" certified and customers who want to use stronger cryptographic ciphers can choose to do so. Support for SSL certificates for secure communications is available by default in FOS, and certificates are continuously monitored for validity. Users are alerted 60 days before a certificate expires to provide adequate time to generate/install a new certificate.

Easier switch certificate management

Brocade software automates the distribution of SSL certificates across the fabric by supporting the use of wildcard certificates, or certificates with multiple Subject Alternative Names (both FQDN and IP addresses). This means that the same certificate can be used for all switches or a group of switches depending on requirements. Prior to certificates expiring, alerts are provided to inform the admin to replace the certificates. Certificates can easily be installed in bulk using Brocade SANnav™ Management Portal or REST.

Secure licensing

Brocade hardware and software licensing is protected with strong encryption to ensure that the licenses installed are legitimate with no tampering.

Monitoring and alerting of security changes

Brocade SANnav software provides monitoring and alerting on security configuration changes and events. It also allows organizations to create customizable monitoring and alerting thresholds to meet their specific security requirements.

Daily security assessment

Brocade Support Link (BSL) services include a daily security assessment of the SAN's security configuration, fabric health, fabric consistency, performance and utilization, allowed protocols, account management, access control lists, and long-distance links across the entire fabric. You'll see comparisons and guidance towards best practice security configurations for your Brocade SANs so that you can identify any inconsistencies and take steps for resolution.

Autonomous SAN technology enables a cyber resilient network

Cyber resiliency goes beyond safeguarding your SAN against cyber attacks. Brocade Gen 7 also protects your SAN from IT disruptions and disasters with autonomous SAN technology that learns, optimizes, and heals on its own. These capabilities automate processes to ensure optimal performance, enable non-stop operations and maximize management automation.

To simplify management, Brocade Gen 7 products harness powerful analytics and advanced, built-in automation. Leveraging these capabilities enables organizations to transform billions of data points into automated actions that ensure the reliability and performance of critical applications, virtual infrastructure, and NVMe storage. By understanding and analyzing network telemetry data in real time, the SAN can automatically make intelligent decisions on traffic prioritization and congestion mitigation to ensure nonstop operations. With automated congestion detection and resolution, Brocade Gen 7 instantly mitigates impacts to applications and resolves issues much faster, freeing up valuable admin time.

Self-learning

Brocade products proactively monitor I/O performance and behavior data points through integrated network sensors to gain deep insight into the environment. Brocade technology can detect abnormal traffic behavior and degraded performance to automatically take corrective action, eliminating the potential impact of these issue.

Self-optimizing

Brocade technology utilizes actionable intelligence to maximize and ensure optimal network performance for applications and storage. Brocade Traffic Optimizer guarantees critical application performance by automatically prioritizing traffic. This advanced capability classifies and separates traffic with similar characteristics such as protocol, speed, and latency. In addition, Traffic Optimizer can avoid application performance impacts by automatically isolating traffic adversely impacting other flows.

Self-healing

Brocade Gen 7 raises the bar for network availability through automatic avoidance and recovery features, delivering a self-healing SAN. When potential disruptions are detected, the network will automatically identify when a device or traffic is not acting correctly and sets a course for recovering or avoiding issues without intervention. The monitoring and correlating of traffic behavior enables the identification of congestion at the start and goes beyond determining an underlying cause, to addressing the entire fabric congestion issue. With this information, Brocade Autonomous SAN capabilities can detect congestion issues on a fabric, and then notify the affected devices (servers and storage) to take action. This real time notification allows the fabric to automatically mitigate potential issues before they impact the business. With a set of corrective actions for congestion events, Brocade products provide admins with trusted default congestion actions or customized fabric responses.

In addition, Brocade Gen 7 stops unhealthy links from affecting application performance. It will identify “sick but not dead” links, which impact fabric performance and frame delivery as the result of physical layer issues. FPIN notifies devices and HBAs when a path is unhealthy, making multipath handling of a “sick” link possible and more effective. Brocade Monitoring and Alerting Policy Suite (MAPS) monitors all links across the fabric. When a link integrity issue or physical layer issue is identified, causing sub-optimal or stalling application performance, the multipath stack is made aware and directed to decommission the “sick” or impaired path, moving all traffic to use only healthy paths. This capability greatly improves the effectiveness and the responsiveness to physical layer issues resulting in better application performance and avoidance of potential application outages.

Realize high levels of security, reliability, and performance

Protecting your data from cybersecurity vulnerabilities is a critical part of your overall business strategy. Your SAN needs to be able to act autonomously to quickly and efficiently maintain the highest levels of security and resiliency while maximizing performance. By upgrading your storage network, you can remove the risks of legacy technology exposing you to unwanted vulnerabilities and disruptions.

Brocade, a Broadcom company, is working constantly to address the evolving threats you're facing to ensure business continuity and safeguard your data. Brocade Gen 7 integrates security and autonomous SAN management technologies to enable a cyber resilient network that's built to take the guesswork out of protecting and managing your data. With automated administrative routines and processes, you'll see dramatic savings in time typically spent troubleshooting issues, optimizing application performance, and maintaining high levels of security.

These are the critical capabilities that make Brocade Gen 7 the foundation you need to protect against cyber attacks, IT disruptions, and disasters.

Learn how Brocade Gen 7 capabilities ensure optimal performance and strengthen the level of security in your network

Download

Visit **www.broadcom.com/modernize-your-san**

or contact your local sales representative **broadcom.com/how-to-buy**

BROCADE
A Broadcom Company

Enable a Cyber-Resilient, Autonomous SAN with Brocade® Gen 7

Take the guesswork out of protecting and managing your data

Data is moving faster in the data center than ever before, which makes it challenging to manage and protect your infrastructure. Managing data growth, combined with the need for rock-solid reliability, and the requirement to maintain high levels of security can be cumbersome. With the next generation of servers and storage, the complexity and scale of traffic will continue to grow, but throwing faster infrastructure at the problem will not be good enough. Your SAN needs to be smarter. It needs to automate management tasks to simplify and enable non-stop operations while ensuring optimal performance and strengthening the level of security in your network.

Brocade Gen 7 changes everything

Brocade® Gen 7 Fibre Channel delivers far more than just speed and latency improvements. It brings new levels of powerful analytics, advanced automation, and integrated security capabilities to enable a cyber-resilient SAN.

These capabilities safeguard your SAN against cyber attacks, IT disruptions, and disasters, while learning, optimizing, and healing on its own. Brocade Gen 7 proactively monitors application and network performance and takes immediate action to dramatically improve application availability and the reliability of the network.

This document outlines seven ways you can benefit from upgrading to Brocade Gen 7 capabilities that automate processes to ensure optimal performance and enable non-stop operations. At the same time, these capabilities strengthen the level of security in your network to protect against security threats around the clock.

First, we will review how the Brocade Self-Learning capabilities identify all devices on the network and set a baseline for application performance to identify potential issues that require remediation. Next, we'll cover how Self-Optimizing and Self-Healing actions mitigate issues caused by device speed mismatch and can mitigate common causes of network congestion. Then we'll show how Brocade Gen 7 technology reduces the risk of vulnerabilities and attacks by monitoring data and hardware across the SAN to identify malware and hijacking attempts as well as other performance issues. You'll also see how Gen 7 protects rather than replaces your existing investments—allowing you to run legacy infrastructure in tandem without sacrificing performance.

BROCADE
A Broadcom Company