

SEPTEMBER 2026

Securing Data Assets in the Era of Frontier Agentic AI Threats

Scott Sinclair, Practice Director; and Monya Keane, Senior Research Analyst

Abstract: The emergence and threat of cutting-edge frontier agentic AI reveal that legacy systems cannot keep up with modern security threats and ongoing AI scans for vulnerabilities. Organizations, therefore, need to modernize infrastructure, including the SAN, to best protect the IT application and data environment. Fortunately, Brocade, a Broadcom company, has enhanced its cyberthreat resiliency capabilities, and its Brocade Gen 8 SAN hardware and software are integrated with multiple increased cyber resilience benefits.

Introduction: Responding to the threat of frontier agentic AI

The rise of AI-weaponized threats is reshaping data center security and putting unprecedented pressure on IT organizations to keep up with and protect their data centers from rapidly evolving security risks.

Large-scale frontier agentic AI models are able to reason, write code, interpret data, and automate complex workflows. But in the wrong hands, frontier agentic AI acts as a security threat multiplier. Attackers no longer use limited threads of iterative manual or automated probing; by leveraging frontier agentic AI, they can execute thousands of automated, parallel attacks to pinpoint and exploit vulnerabilities in hours rather than months. Instead of a single hacker, there are now entire automated armies relentlessly trying to break in. In fact, according to the [Zero-Day Clock](#), an independent project that tracks cybersecurity intelligence feeds and gathers data on vulnerability disclosures and exploits, the median time-to-exploit (TTE) [reached 1.6 days in 2026](#) and is projected to shrink to hours or minutes in the future.

Organizations are only as strong as their weakest link. Bad actors will target older, outdated hardware and software to find vulnerabilities and gain access. The pace at which attackers identify and exploit vulnerabilities requires IT teams to ensure that their infrastructure is equipped with the latest patches and security enhancements.

They also need the latest infrastructure because AI-empowered attackers make legacy infrastructure a threat to the organization's cyber resilience strategy. The latest product generations are the first to be updated and protected against frontier agentic AI models. Older generations will always lag behind, and, in some cases, it will not be possible to protect them from certain vulnerabilities: Depending on the age of the code, fixes may not be available at all, or there can be long delays for fixes to older open source packages.

In data storage environments, the effort includes modernizing the storage networking ecosystem, where infrastructure upgrades can often lag. The latest [Brocade Gen 8](#) technology offers multiple cyber resilience benefits in contrast to legacy Gen 6 and earlier hardware.

Cyberthreats create urgency to replace legacy infrastructure

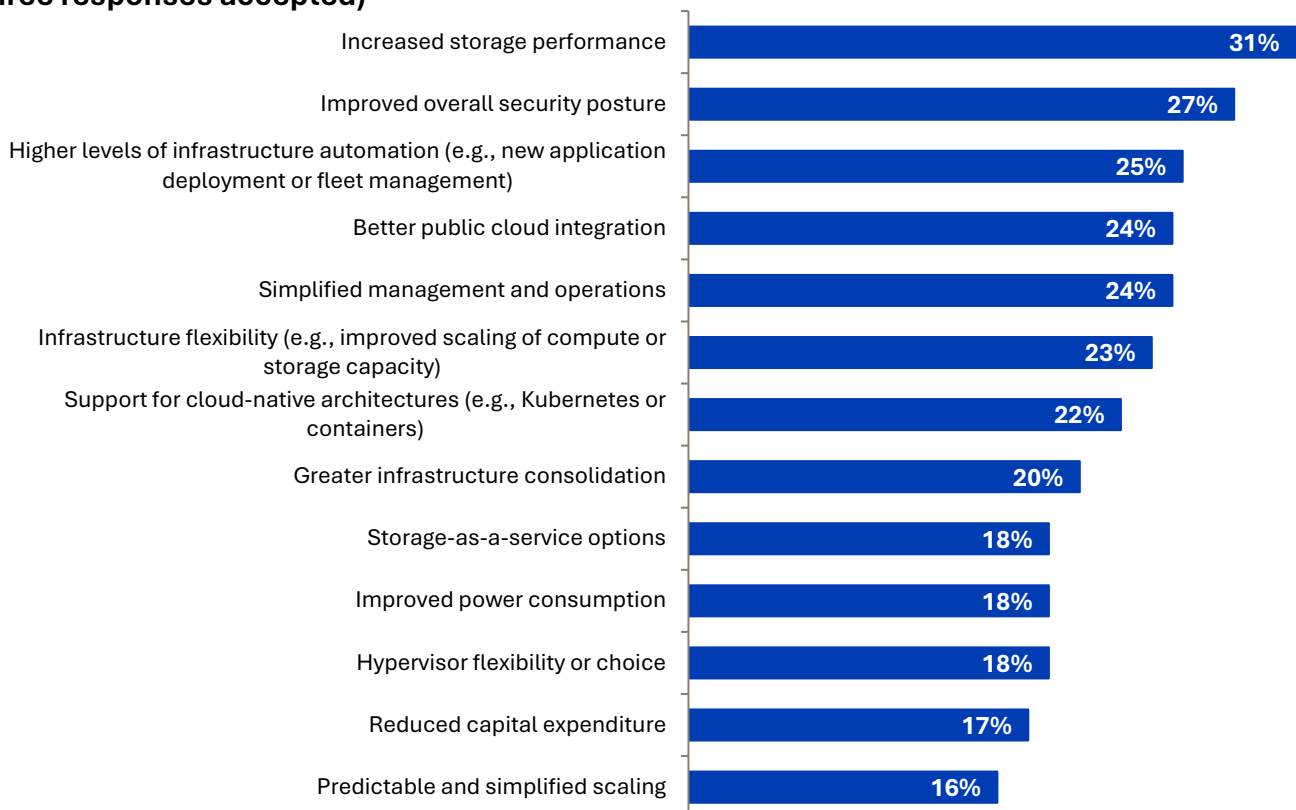
Omdia research shows that concerns about cyberthreats stemming from frontier agentic AI fuel increased infrastructure investment. Ensuring that the IT infrastructure environment always possesses the latest cyber resilience capabilities is a fundamental strategic factor when making infrastructure investments. According to Omdia research, improving cybersecurity and resilience against cyberattacks was the most commonly identified justification for making new IT infrastructure investments, cited by 32% of respondents.¹

The increased focus on infrastructure modernization to improve cyber resilience extends to the data storage ecosystem as well. Most surveyed organizations (78%) agreed that growing cyberthreats have caused them to evaluate storage-level security,² such as technologies to improve the security posture of the data storage ecosystem (including storage systems and the network).

The need to improve the security posture of the storage environment is also among the top two reasons why storage decision makers either keep or replace their current storage infrastructure (see **Figure 1**).³

Figure 1. Top factors leading to storage infrastructure replacements

What will be the most significant factors in your organization’s decision to retain or change its current storage infrastructure in the next refresh or purchase? (Percent of respondents, n=193, three responses accepted)



Source: Omdia

¹ Source: Omdia Research Report, [2026 Technology Spending Insights: The Race for Success as AI Spans the Globe](#), March 2026.

² Source: Omdia Research Report, [The Storage Modernization Imperative](#), April 2026.

³ Ibid.

Why frontier agentic AI requires IT teams to accelerate modernization

Innovations often find their way into attackers' hands before they can be fully utilized by IT teams. Artificial intelligence is no different. Agentic AI models, especially complex, advanced frontier models, can quickly analyze code bases, identify potential exploits, and enable attackers to accelerate the use of those exploits and scale the number of targets to be attacked.

Historically, cyberthreats relied on human attackers manually finding distinct flaws. The process could take months and deep expert skills and knowledge to uncover exploits. IT teams leveraged the extended time window to test and deploy security patches and updates. Frontier agentic AI models change the game by:

- Giving attackers powerful tools that quickly analyze massive amounts of data to identify what may have previously been considered low-severity flaws and then connect them into a single, critical attack path.
- Accelerating code exploitation that used to take months of manual examination can now be accomplished in hours.
- Simplifying the development of customized attack software to weaponize identified exploits.
- Enabling even lower-skilled threat actors to deploy advanced cyberattacks, thereby increasing the frequency and prevalence of attacks overall.

One outcome of the rise of these new threats is that IT teams must change their perception of legacy infrastructure. Older, static, “set and forget” infrastructure is now far more likely to leave an organization exposed and vulnerable. That older infrastructure may in fact be the “weakest member of the herd”—the very point that hackers can exploit to gain entry into an environment.

Unfortunately, vendors do not have the bandwidth to rapidly ensure that their entire catalogs of legacy hardware stay up to date with security patches. They will always prioritize newer hardware and software when it comes to analyzing potential security flaws and addressing those flaws with patches or updates. With old hardware, fixes may not even be available, and there can be lengthy delays for fixes to older open source software packages.

Brocade Gen 8 Fibre Channel's proactive approach to securing digital assets with frontier agentic AI models

If legacy systems cannot keep up with modern security threats, then the only way to maintain active threat protection and guarantee compliance is to run the latest hardware and software. It is especially vital to update the storage networking infrastructure, given its critical spot in the data path and its role in ensuring data availability. Specifically, IT decision makers should prioritize modernizing older (i.e., Gen 6 or prior) SAN switches to the latest Brocade Gen 8 technology.

The storage network's essential role in ensuring application and data availability often leads to it being an infrastructure category that IT teams are reluctant to change. But its central location in the data path necessitates that those teams make sure they are leveraging the latest active threat protection and compliance capabilities.

Fortunately, Broadcom has prioritized enhancing its cyberthreat resiliency capabilities across its Brocade product line over the last seven years, and its Brocade Gen 8 SAN network hardware and software are integrated with multiple increased cyber resilience benefits. Brocade engineering takes a proactive approach to addressing the threat of frontier agentic AI-based attacks by:

- Leveraging frontier agentic AI models and automated penetration tests during development cycles to actively isolate and patch vulnerabilities before they hit production.
- Continuing to leverage frontier agentic AI models to proactively scan released code and patch the software to minimize vulnerabilities post-release.
- Dedicating an active threat-response engineering function to further accelerate remediation and fixes.
- Enforcing mandated access control within its software to minimize the attack surface.

In these ways, Brocade is minimizing the exposure to frontier agentic AI in the hands of cyber criminals by identifying and fixing potential exploits before the code leaves its internal testing processes. This proactive use of frontier agentic AI complements Brocade's existing cyber resilience capabilities, which include the following:

- **Physical isolation with Fibre Channel.** Brocade SAN technology leverages the Fibre Channel protocol which, unlike Ethernet, relies on a non-routable, point-to-point architecture to naturally segment storage traffic from the LAN or other internal network traffic. This removes multiple attack paths common to traditional Internet Protocol data center networks. The physical separation of the technology also helps eliminate the human error-related risk of misconnecting/misconfiguring networks.
- **A principle-of-least-privilege architecture.** Brocade implements strict principle-of-least-privilege architecture through mandatory access controls within its Fabric OS (FOS) software, which eliminates privileged root-level access. The result is a hardened attack surface with contained privileges, minimizing the exposure of any entry point, and preventing common hijacking and malware exploits leveraged by cyberattackers.
- **Integrated, certificate-based hardware and software validation.** Brocade leverages an integrated silicon root of trust model to ensure hardware and firmware authenticity and protect against tampering attempts. Brocade Trusted FOS Certificates are monitored continuously by Brocade firmware to verify the software's authenticity.
- **Continuous security posture management.** Brocade SANnav Management Portal provides real-time fabric configuration visibility along with autonomous security assessments to alert administrators if policy drifts occur. While Brocade's physical isolation-related cyber resilience minimizes cybersecurity risks associated with network misconfiguration, continuous posture management adds assurance that the environment will remain configured exactly as expected.
- **Quantum-safe encryption.** Brocade leverages quantum-resistant algorithms to resist quantum attacks, protecting sensitive data and critical infrastructure from future quantum computers. This enables organizations to comply with the directives by CNSA 2.0, EO14412, and equivalents for other regions. Similar to frontier agentic AI models, quantum computing looms on the horizon as a potential weapon for bad actors to use in the future to attack encryption algorithms.

Conclusion

The convergence of frontier agentic AI capabilities with malicious intent fundamentally alters the risk calculus for IT infrastructure investments. Traditional approaches to extending legacy infrastructure lifecycles through incremental patching are untenable when adversaries can compress months of vulnerability research into hours of automated exploitation.

With median time-to-exploit (TTE) dropping in 2026, organizations face an asymmetric battle. They must achieve near-perfect protection, but attackers only need to find a single exploitable weakness. What distinguishes Broadcom's approach with Brocade Gen 8 is the recognition that defensive strategies must mirror offensive capabilities. By turning the tables on the bad actors who threaten enterprise security—deploying frontier agentic AI proactively for penetration testing and vulnerability scanning—Brocade has shifted the security paradigm from reactive patching to predictive hardening.

The frontier agentic AI era demands a recalibration of what constitutes a “good enough” security posture. Organizations continuing to operate on legacy infrastructure timelines certainly will be outmatched by adversaries. The question is how quickly organizations can modernize before the window of defensive advantage closes entirely.

In an environment where attackers have weaponized exploitation, defenders must weaponize resilience. For the storage networking layer, that effort should begin with Brocade Gen 8 technology and the proactive security architecture it provides.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

Get in touch: www.omdia.com askananalyst@omdia.com

