WD Advances Next-Generation Trusted Infrastructure with Industry's First Post-Quantum Cryptography Hard Drives to Help Secure the Future of AI Data

May 18, 2026

Ultrastar® HDDs currently in customer qualification introduce PQC-ready secure boot and firmware protection, establishing a new standard for device trust in the Quantum Era

SAN JOSE, Calif.--(BUSINESS WIRE)--May 18, 2026-- Western Digital Corporation (Nasdaq: WDC), the storage foundation of the AI-driven data economy, today announced a significant step in next-generation infrastructure security with the integration of post-quantum cryptography (PQC) into its newest high-capacity Ultrastar® UltraSMR hard disk drives. As AI infrastructure evolves from compute-centric deployments to data systems that persistently retain information across every inference, training run, and interaction, the durability and security of that data becomes foundational, not optional. These drives are currently in qualification with multiple hyperscale customers, reflecting strong early interest in quantum-resilient storage architectures.

AI data systems generate and retain massive, long-lived data sets. Securing that data over decades, not just years, must be a core requirement of modern infrastructure. WD's launch of the first hard drives to implement NIST-approved quantum-resistant algorithms marks a definitive industry transition — from theoretical planning to deployed hardware-level defense. By hardening the root of trust, WD provides a critical safeguard against threats like harvest now, decrypt later (HNDL) and similar attacks. This helps protect the massive data lakes fueling today's AI innovations against the cryptographic protection-breaking power of tomorrow's quantum computers. WD is among the first to bring post-quantum cryptography into production storage infrastructure, helping lead the industry's quantum transition with deployed, standards-aligned, infrastructure-level protection, setting a new baseline for trust in AI-era data systems.

Why Post-Quantum Storage Security Matters Now

As AI infrastructure and workloads generate and retain data in perpetuity, the value of that accumulated data grows, and so does the urgency to protect it against threats that are advancing faster than most organizations anticipate.

- **Long data lifecycles and extended IT service windows widen vulnerabilities**. Enterprise storage infrastructure typically remains in service for five years or longer, a timeframe that may overlap with the emergence of cryptographically relevant quantum computers.
- **As decryption capabilities advance, so do the strategies of sophisticated adversaries.** HNDL is a present-day threat. Adversaries may collect encrypted or signed data today with the intent to decrypt or forge security signatures once quantum capabilities mature. Organizations must begin to prepare for long-term cryptographic resilience today.
- **Firmware-level attacks present a critical risk.** Device-level trust is becoming increasingly important as security architectures evolve. A quantum-enabled adversary could potentially forge digital signatures on firmware updates, allowing malicious code to appear authentic and compromising drive security.

WD's PQC Implementation

WD's PQC implementation on the new Ultrastar DC HC6100 UltraSMR is designed to help protect device trust chains from manufacturing through field service. This implementation represents more than a feature enhancement; it reflects a broader shift toward embedding quantum-resilient security directly into the foundation of data infrastructure. The focus is on securing device-level trust, including firmware integrity and key management, rather than data-at-rest encryption.

Key elements include:

- Algorithm selection: ML-DSA-87 (NIST FIPS 204) for high-assurance code signing, with dual-signing using RSA-3072 combining proven and emerging cryptographic standards to ensure strong, resilient security
- Infrastructure readiness: PQC-capable public key infrastructure (PKI) and hardware security module (HSM) workflows deployed to support key issuance, rotation, and lifecycle management
- Operational continuity: Dual-signing and rollback safeguards designed to support deployment across diverse fleets without disrupting current operations

"As AI data compounds and becomes more valuable and long-lived, securing it for the future is no longer optional. Quantum computing represents one of the most significant technology transitions of our time, and it is advancing faster than many organizations anticipate. The security architectures that have protected enterprise storage for more than a decade will need to evolve," said Dr. Xiaodong (Carl) Che, Chief Technology Officer and Senior Vice President at WD. "Integrating post-quantum cryptography into our Ultrastar enterprise-class drives is part of our commitment to helping customers stay ahead of threats that are already present in the form of HNDL attacks. By aligning with NIST standards and CNSA 2.0 today, we are helping enterprises

build a clear, low-friction path to quantum-safe storage infrastructure."

As quantum security requirements advance, data protection at the infrastructure layer is becoming a baseline requirement for AI-driven enterprises. WD is helping define the next baseline for trust in AI infrastructure, where security is embedded at the foundation of the system, not added as an afterthought. WD expects to expand PQC capabilities across additional enterprise hard drive product lines over time.

Additional resources:

Blog: Post-Quantum Cryptography for Enterprise HDDs
White Paper: Why Now and How WD Will Help Enterprise Migration

About WD

WD, also known as Western Digital, builds the storage infrastructure that powers certainty in the AI-driven data economy. At the forefront of innovation, WD partners with the world's leading hyperscalers, cloud service providers, and enterprises to deliver reliable storage solutions that are proven and trusted at scale. Driven by a culture of innovation and execution, WD helps customers store, protect, and use the world's data with confidence. Follow WD on LinkedIn and learn more at **www.wd.com**.

Forward-Looking Statements

This press release contains forward-looking statements within the meaning of federal securities laws, including statements regarding expectations for: the company's product development plans, including the integration of post-quantum cryptography into the company's products. These forward-looking statements are based on management's current expectations and are subject to risks and uncertainties that could cause actual results to differ materially from those expressed or implied in the forward-looking statements. Key risks and uncertainties that could cause actual results to differ materially from those expressed or implied in the forward-looking statements include: adverse global or regional conditions, including new or additional tariffs or trade restrictions; the company's dependence on a limited number of qualified suppliers; volatility in demand for the company's products; the impact of business and market conditions, including inflation, increases in interest rates and an economic recession; the outcome and impact of the company's completed separation of its HDD and Flash businesses; the impact of competitive products and pricing; the company's development and introduction of products based on new technologies and expansion into new data storage markets; risks associated with cost saving initiatives, restructurings, acquisitions, divestitures, mergers, joint ventures and the company's strategic relationships; difficulties or delays in manufacturing or other supply chain disruptions; hiring and retention of key employees; the company's level of debt and other financial obligations; changes to the company's relationships with key customers; compromise, damage or interruption from cybersecurity incidents or other data system security risks; actions by competitors; any decisions to reduce or discontinue paying cash dividends or repurchasing shares of the company's common stock; the company's ability to achieve its greenhouse gas emissions reduction and other sustainability goals; the impact of international conflicts; risks associated with compliance with changing legal and regulatory requirements and the outcome of legal proceedings; and other risks and uncertainties listed in the company's filings with the Securities and Exchange Commission (the "SEC"), including the company's Annual Report on Form 10-K filed with the SEC on August 14, 2025 to which your attention is directed. You should not place undue reliance on these forward-looking statements, which speak only as of the date hereof, and the company undertakes no obligation to update or revise these forward-looking statements to reflect new information or events, except as required by law.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260518685490/en/

Media Contact:
WD.Mediainquiries@wdc.com

Source: Western Digital Corporation