carahsoft

Securing the Future: Bacula Enterprise and Post-Quantum Cryptography

How Bacula Systems is building quantum-safe data protection for enterprise and critical infrastructure

---

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Bacula Systems, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

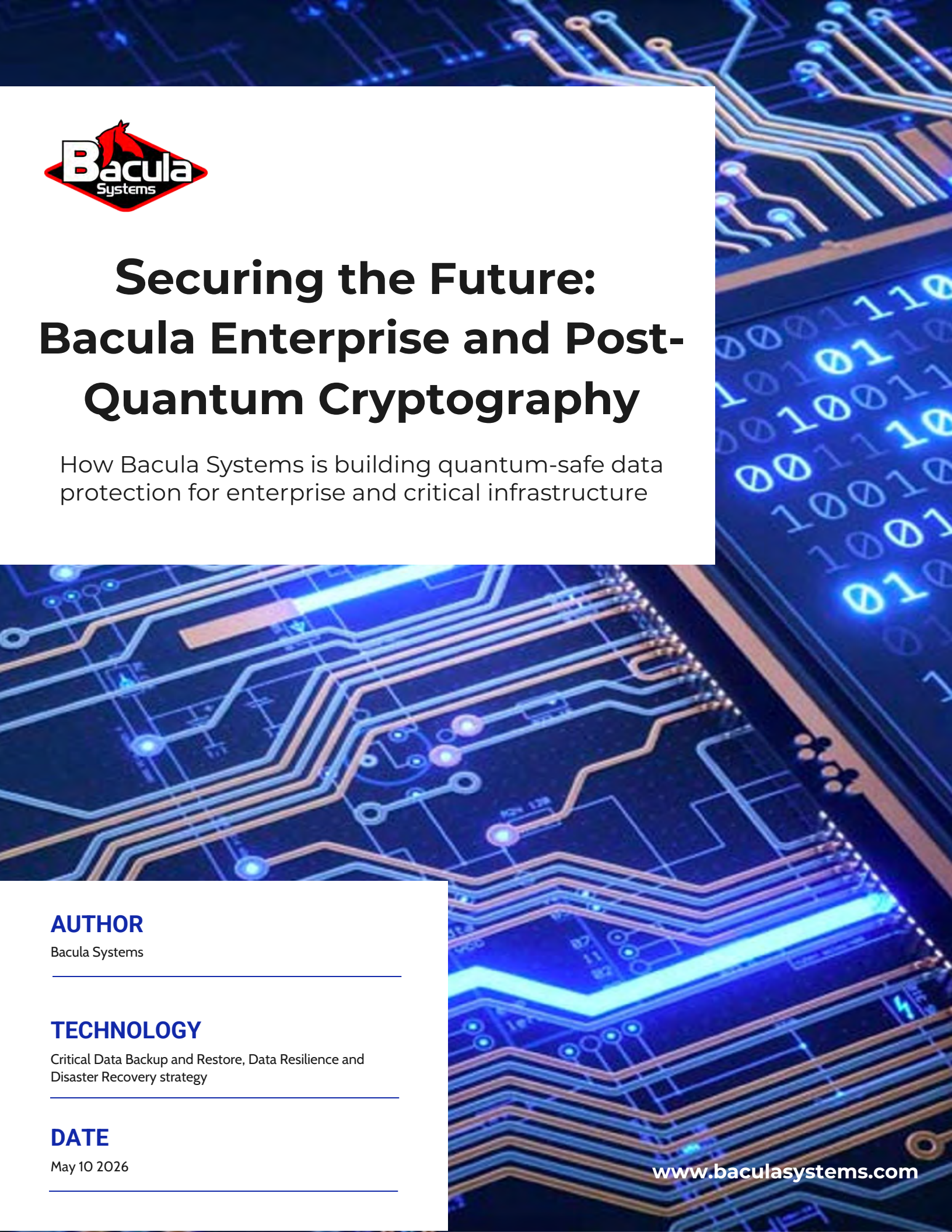
Explore More Resources:
carah.io/BaculaSystemsResources

Join Events & Webinars:
carah.io/BaculaSystemsEvents

Discover Technology Solutions:
carah.io/BaculaSystems

Learn About Procurement:
carah.io/BaculaSystemsContracts

Connect With Our Team:
BaculaSystems@carahsoft.com
571-590-4040



Securing the Future: Bacula Enterprise and Post-Quantum Cryptography

How Bacula Systems is building quantum-safe data protection for enterprise and critical infrastructure

AUTHOR

Bacula Systems

TECHNOLOGY

Critical Data Backup and Restore, Data Resilience and Disaster Recovery strategy

DATE

May 10 2026

www.baculasystems.com

Table of Contents

Executive Summary

Why Bacula's Architecture Delivers Exceptional Quantum-resilient Protection

The advent of quantum computing represents the most fundamental shift in cryptographic security since the invention of public-key encryption. Enterprises that store sensitive data today — including long-term backup archives — face a real and immediate risk: data encrypted with classical algorithms can be harvested now and decrypted later, once quantum computers become sufficiently powerful.

Bacula Systems has assessed this risk comprehensively and is executing a structured, standards-driven roadmap to ensure that Bacula Enterprise remains a quantum-safe data protection platform. Key elements of our posture include:

- Bacula's core backup data has always been protected by AES symmetric encryption — the same class of algorithm recommended by NIST for quantum-era security, requiring only a key-length adjustment (AES-256) for long-term resilience.
- Bacula leverages OpenSSL as its cryptographic engine. The latest OpenSSL release — version 4.0, published in 2026 — includes native implementations of three of the NIST PQC algorithms (ML-KEM, ML-DSA, and SLH-DSA).
- Bacula Enterprise source-code compatibility tracks each new OpenSSL release; end-to-end customer availability follows as supported operating systems ship those packages.
- Our roadmap integrates post-quantum key exchange and authentication into TLS communications across all daemon-to-daemon channels — securing the control plane alongside the data plane.
- Documentation, certificate generation, hash functions, and operational guidance are being reviewed and updated to align with NIST and NSA quantum transition requirements.

"Bacula customers benefit today from quantum-resilient data-at-rest encryption. In the near future, they will benefit from end-to-end quantum-safe communications across the entire backup infrastructure."

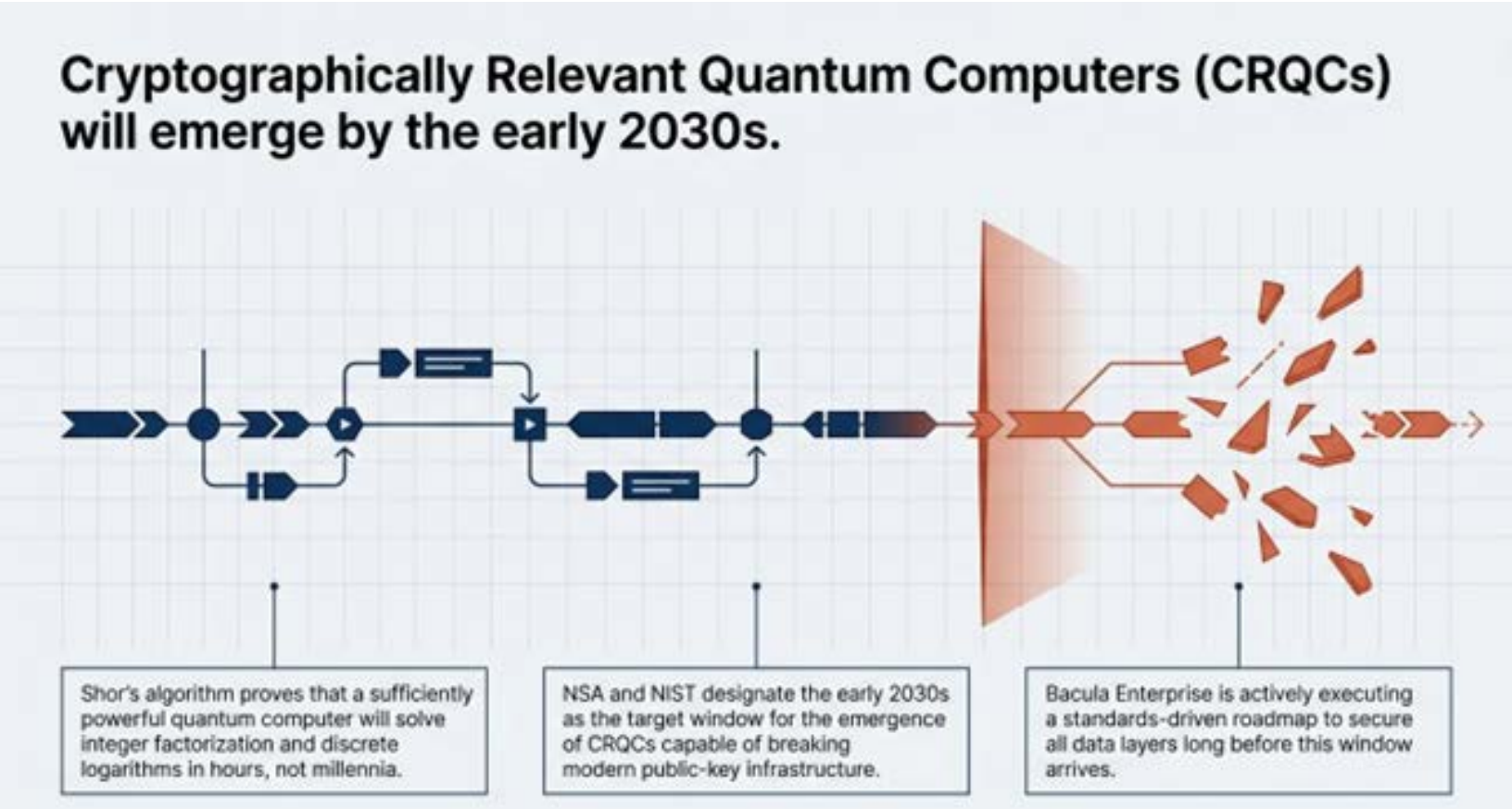
This whitepaper explains the threat, describes the global standards response, benchmarks our position against the competitive landscape, and details Bacula's technical strategy and delivery roadmap.

The Quantum Threat to Data Protection

Why Classical Encryption Is at Risk

For decades, the security of digital communications and stored data has rested on mathematical problems that classical computers cannot solve at scale — integer factorization for RSA, discrete logarithms for Diffie-Hellman, and elliptic curve problems for ECC. These form the backbone of encryption, authentication, and secure key exchange across the entire IT landscape.

Shor's algorithm, a quantum computing breakthrough, demonstrated that a sufficiently powerful quantum computer could solve these problems in hours rather than millennia. While today's quantum machines are not yet large enough to threaten production systems, the trajectory is clear. Government agencies including the NSA are targeting the early 2030s as the window in which cryptographically relevant quantum computers (CRQCs) could emerge.



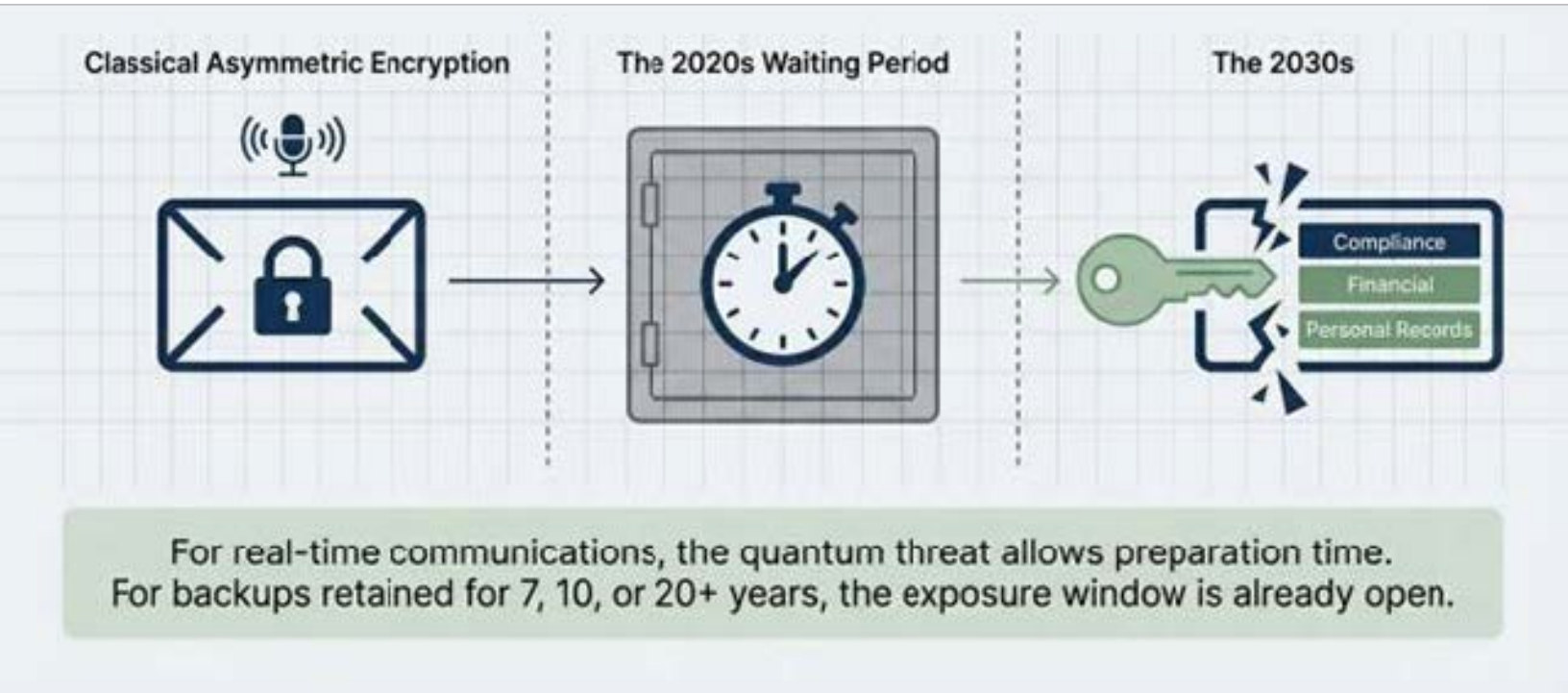
The Backup-Specific Risk: Harvest Now, Decrypt Later

For most IT systems, a future quantum threat allows some time to prepare. For backup and archival systems, the risk is already present.

Long-term backup archives — compliance data, financial records, sensitive personal information — are often retained for 7, 10, or even 20 years. Adversaries are actively harvesting encrypted data today, storing it with the intention of decrypting it once quantum hardware matures. This is not speculation; it is an observed and documented threat vector referenced in NSA and NIST guidance.

The most exposed systems are those protecting data with long retention periods — exactly the profile of enterprise backup archives managed by platforms like Bacula Enterprise.

Long-term backup archives face an immediate threat from "Harvest Now, Decrypt Later" campaigns.



What Is Post-Quantum Cryptography (PQC)?

Post-Quantum Cryptography does not mean quantum hardware — it means new mathematical algorithms, running on classical hardware today, designed to resist attacks from both classical and quantum computers. PQC algorithms are based on mathematical problems that remain hard even for quantum computers, such as lattice problems, hash functions, and error-correcting code structures.

PQC is not an incremental improvement to existing algorithms. It represents a generational transition — comparable to the shift from symmetric-only to public-key infrastructure in the 1990s — requiring deliberate, planned adoption.

The NIST PQC Standards: What Enterprises Need to Know

In 2016, the U.S. National Institute of Standards and Technology (NIST) launched a global initiative to define quantum-resistant cryptographic standards. After nearly a decade of rigorous international review — drawing 82 submissions from 25 countries — the first standards were finalized in 2024.

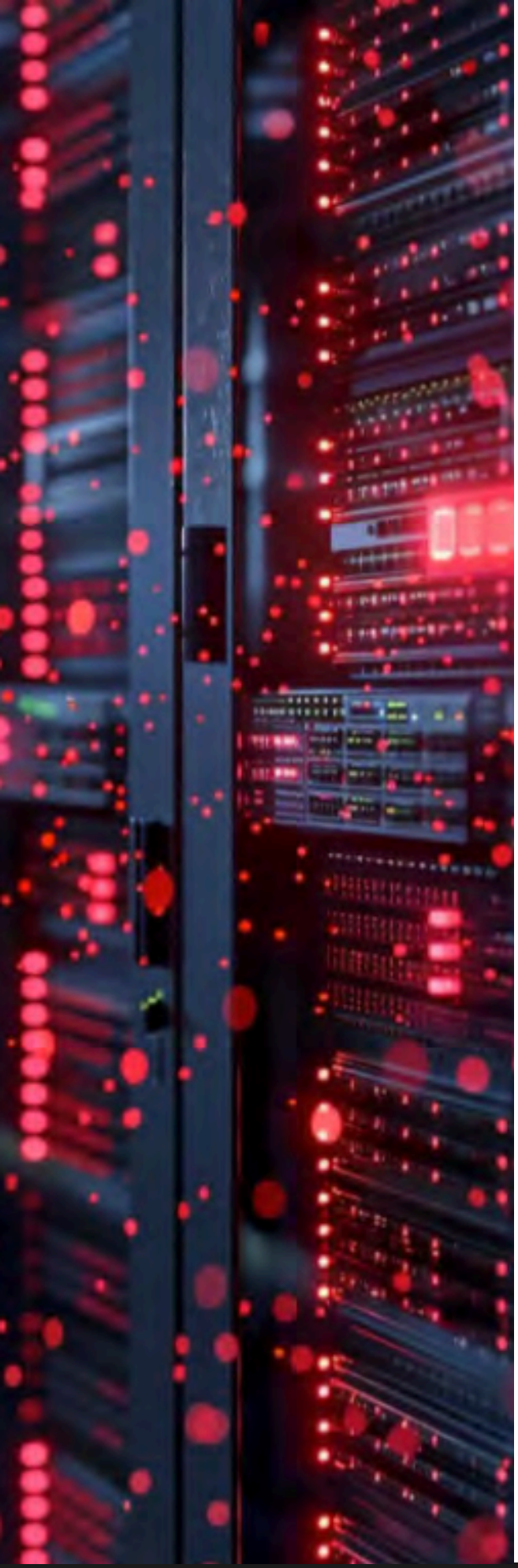
Bacula is adopting the finalized 2024 NIST Post-Quantum Cryptography standards.

Standard	Mathematical Foundation	Enterprise Purpose	Bacula Status
ML-KEM (FIPS 203)	Lattice (CRYSTALS-Kyber)	Key Encapsulation / Exchange	Primary PQC mechanism
ML-DSA (FIPS 204)	Lattice (CRYSTALS-Dilithium)	Primary Digital Signatures	Primary PQC mechanism
SLH-DSA (FIPS 205)	Hash-based (SPHINCS+)	Stateless Signatures	Secondary option
FN-DSA (FIPS 206)	Lattice (FALCON)	Compact Signatures	Tracking for adoption post-draft

Context Note: After nearly a decade of international review of 82 submissions, NIST finalized these distinct mathematical foundations to ensure resilient, multi-layered security.

FIPS Standard	Common Name	Purpose	Status
ML-KEM (FIPS 203)	CRYSTALS-Kyber	Key Encapsulation / Key Exchange	Finalized 2024
ML-DSA (FIPS 204)	CRYSTALS-Dilithium	Digital Signatures (primary)	Finalized 2024
SLH-DSA (FIPS 205)	SPHINCS+	Hash-based Signatures (stateless)	Finalized 2024
FN-DSA (FIPS 206)	FALCON	Digital Signatures (compact)	Draft standard pending
HQC	Hamming Quasi-Cyclic	Key Encapsulation (diversity hedge)	Selected 2025; standard pending

NIST's message to industry has been unambiguous: **do not wait.** Begin integrating these algorithms into products and protocols now. For Bacula Systems, this means planning for ML-KEM and ML-DSA as primary post-quantum mechanisms — with SLH-DSA as an important secondary option, and FN-DSA tracked for adoption once its standard is finalized — and treating algorithm agility as a first-class design principle.



Regarding the implementation of quantum-resistant cryptographic standards, NIST's message to industry has been unambiguous: do not wait. Begin integrating these algorithms into products and protocols now.

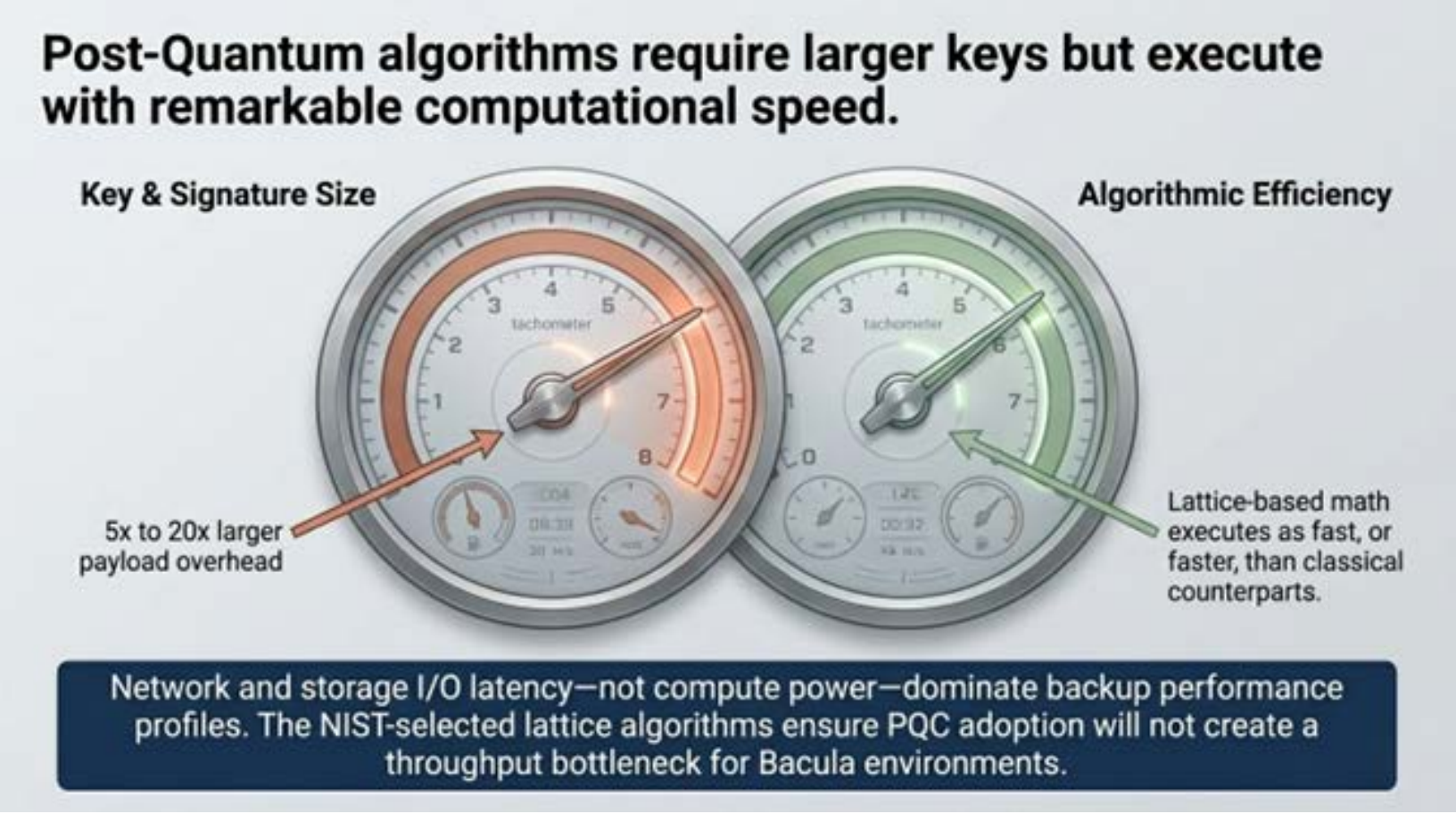
For Bacula Systems, this means planning for ML-KEM and ML-DSA as primary post-quantum mechanisms — with SLH-DSA as an important secondary option, and FN-DSA tracked for adoption once its standard is finalized — and treating algorithm agility as a first-class design principle.

Algorithm Agility: The Strategic Imperative

A key lesson from the NIST process is that no single algorithm family should be treated as unconditionally secure.

The PQC portfolio deliberately spans multiple mathematical foundations — lattice problems, hash functions, code-based systems — so that if one family is ever threatened, others remain robust.

Bacula's cryptographic architecture is being designed with this principle in mind: the ability to swap, combine, or extend algorithms without re-architecting the platform.



Performance and Operational Implications

Key and Signature Size Overhead

PQC algorithms do carry a size overhead relative to classical equivalents — keys, ciphertexts, and signatures are typically 5× to 20× larger depending on the algorithm. However, modern compute, storage, and network infrastructure has grown to the point where this overhead is acceptable in the vast majority of enterprise deployment scenarios.

Computational Performance

Many PQC algorithms are highly efficient in practice. Lattice-based schemes such as ML-KEM and ML-DSA are specifically noted for their speed — often comparable to, or faster than, classical counterparts in key operations. Network and storage I/O latency dominate the performance profile of backup systems, meaning that PQC adoption will not create a meaningful throughput impact for Bacula deployments.

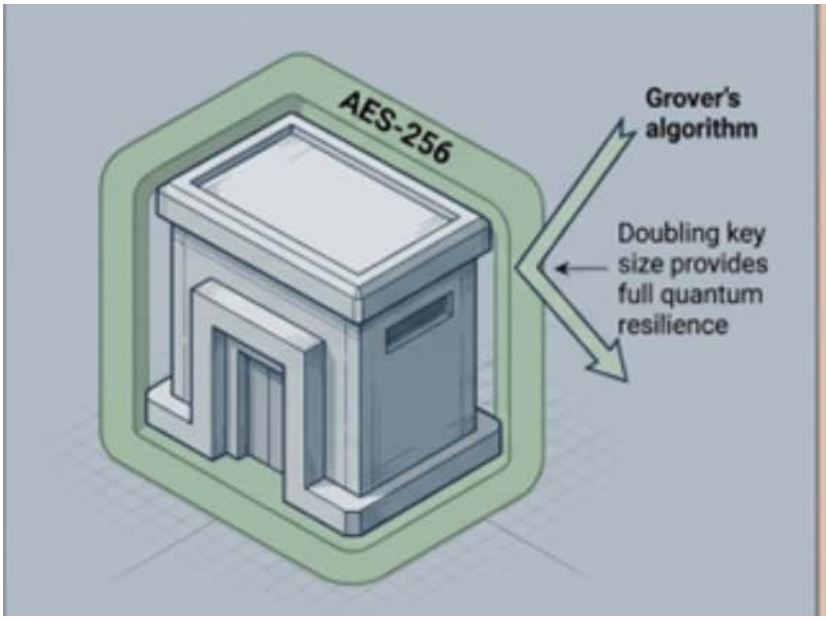
Compute is not a blocker for PQC adoption. The NIST-selected algorithms were chosen precisely for their combination of security strength and performance efficiency.

Symmetric Encryption: Already Quantum-Resilient

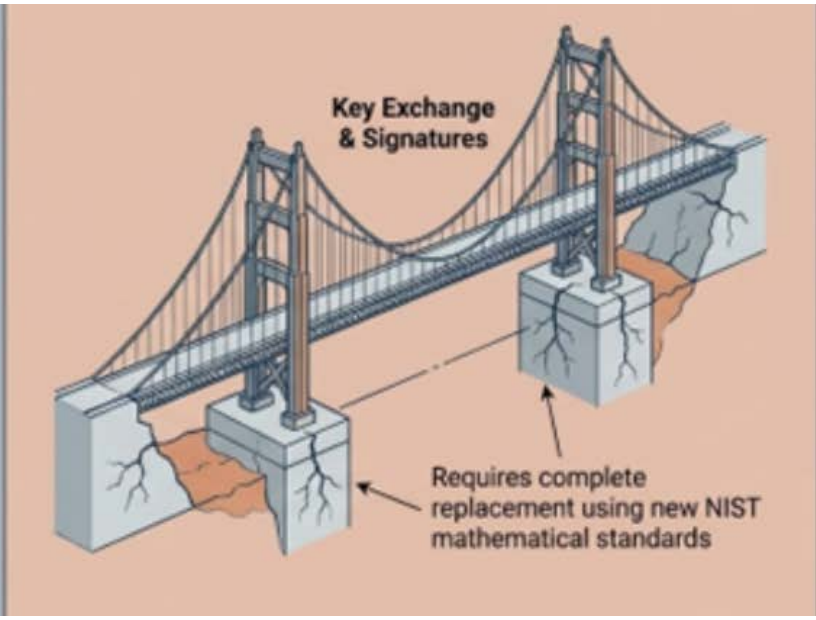
An important and often underappreciated point: symmetric encryption algorithms such as AES are significantly more resistant to quantum attack than public-key systems. Grover's algorithm provides only a quadratic speedup for brute-force attacks — effectively halving the security level of a symmetric cipher — which is addressed by simply doubling the key size. AES-256, which Bacula uses for backup data encryption, already meets this bar.

The same logic applies to hash functions. SHA-256 remains secure at an intermediate level; SHA-384 provides stronger future-proofing. The practical guidance from NIST is clear: focus the majority of migration energy on replacing public-key mechanisms (key exchange, digital signatures) rather than overhauling symmetric encryption.

Symmetric data-at-rest requires only a thicker wall, while communications require a new structural foundation.



Already Quantum-Resilient. Bacula protects core backup data with AES-256, requiring zero algorithmic overhauls.

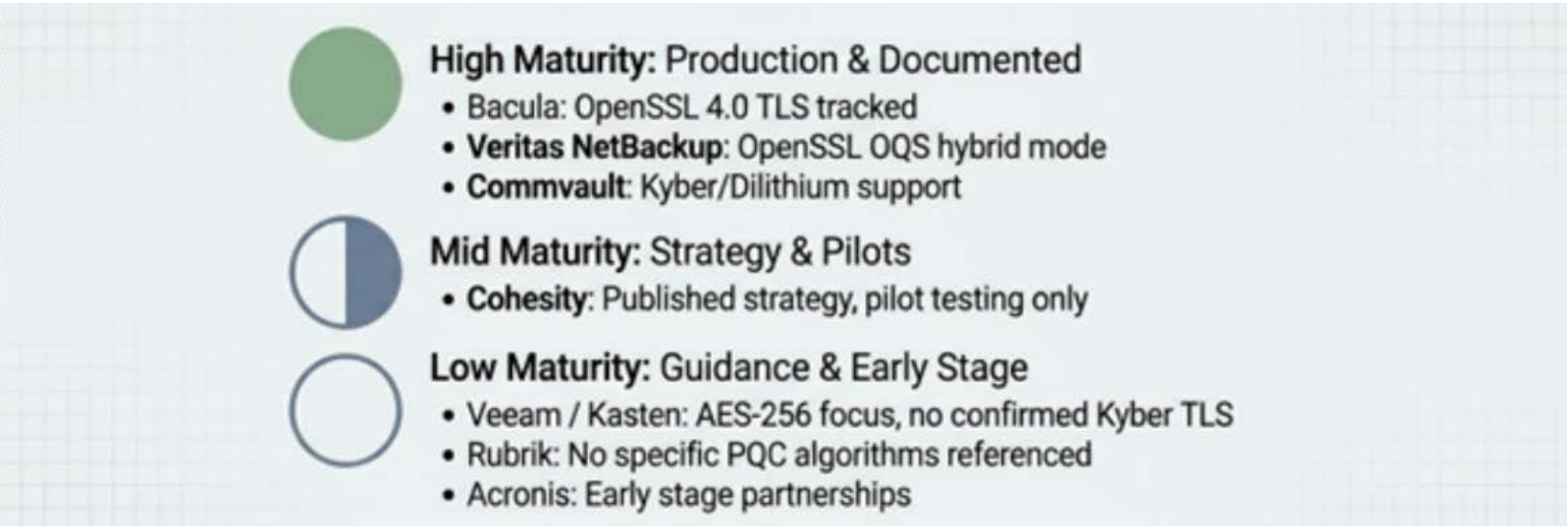


The PQC Gap: Deamon-to-daemon channels and TLS authentication demand an entirely new class of algorithms

Competitive Landscape

Bacula Systems monitors the PQC posture of major backup vendors closely. The following represents our assessment of the current state of the market as of early 2026.

The enterprise backup market shows a stark divide between verified implementations and marketing guidance.



Strategic insight: Marketing-only PQC statements are insufficient. Credible capability requires specific commitment to OpenSSL 3.5/4.0 or OQS-based implementations. Bacula closes this gap with a documented, active engineering path.

The market pattern is clear: vendors who have committed to specific OpenSSL 3.5/4.0 or OQS-based implementations have the most credible claims. Marketing-only PQC statements without documented product capabilities should be evaluated accordingly. Bacula's approach — grounded in OpenSSL compatibility already complete and active engineering investment — effectively closes this gap with a credible, documented implementation path.

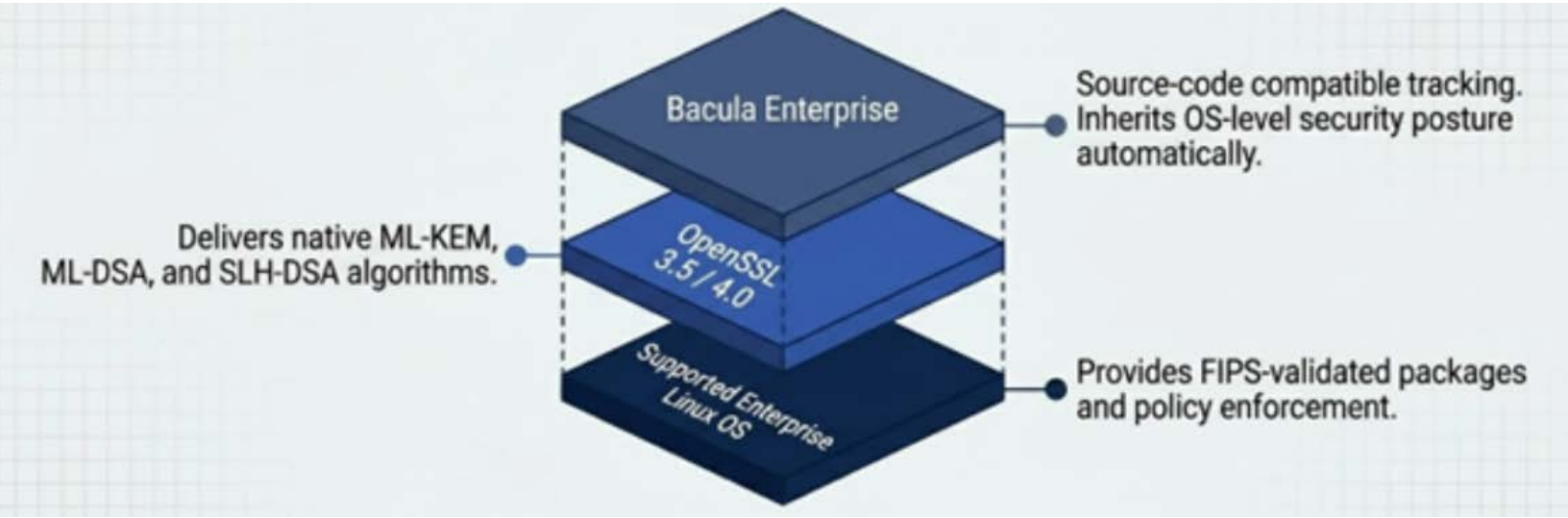
Vendor PQC Status

Vendor	PQC Status	Notes
Veritas NetBackup	Production (TLS)	PQC hybrid TLS mode available via OpenSSL OQS provider. Concrete product-level capability documented.
Commvault	Production (announced)	Full support for Kyber, Dilithium, SPHINCS+, and FALCON across key exchange and signatures. Strong marketing and technical documentation.
Cohesity	Strategy + Pilots	Published PQC strategy (monitor → extend → adopt). Active pilot testing. Primarily preparatory, not a single 'enable PQC' feature yet.
Veeam / Kasten	Guidance only	Emphasizes AES-256 and quantum-aware operational messaging. No confirmed Kyber/Dilithium TLS product support as of early 2026.
Rubrik	No public detail	Cyber-resilience messaging does not reference specific PQC algorithms or implementation details.
Acronis	Early stage	Historical interest in PQC partnerships; no clear current product-level PQC page found.
Dell / IBM	Roadmaps	Enterprise-level strategy documentation exists; implementation typically deferred to downstream components (OpenSSL, OS TLS stacks, HSMs).

Bacula Enterprise: Current Posture and Strategic Direction

Strong Foundations - Today

Bacula Enterprise is built on cryptographic foundations that are already well-positioned for the quantum transition. Several elements of our current architecture align directly with NIST's quantum-era guidance. **Bacula's Architecture eliminates cryptographic vendor lock-in by utilizing a globally audited engine.**



Takeaway: Because Bacula consumes the OpenSSL provided by your supporte OS, customers operting on FIS-configured platforms inherit that exact compliance posture wthout a proprietary vendor upgrade cycle.

Capability	Bacula's Quantum Posture
Data-at-rest encryption	AES symmetric encryption — highly resilient to quantum attack when using AES-256 key lengths.
Cryptographic engine	OpenSSL — version 4.0 (released 2026) provides native ML-KEM, ML-DSA, and SLH-DSA support. Bacula source code tracks each OpenSSL release; deployment availability follows as supported operating systems ship the corresponding packages.
TLS communications	All daemon-to-daemon communications protected by TLS. PQC-enabled TLS configuration is the immediate next engineering milestone.
Hash functions	Currently MD5 and SHA-1 referenced in documentation. SHA-256 and SHA-384 adoption underway in documentation and defaults.
Certificate generation	Being reviewed to ensure all auto-generated certificates use quantum-resilient algorithms and key lengths.

The PQC Gap: Key Exchange and Authentication

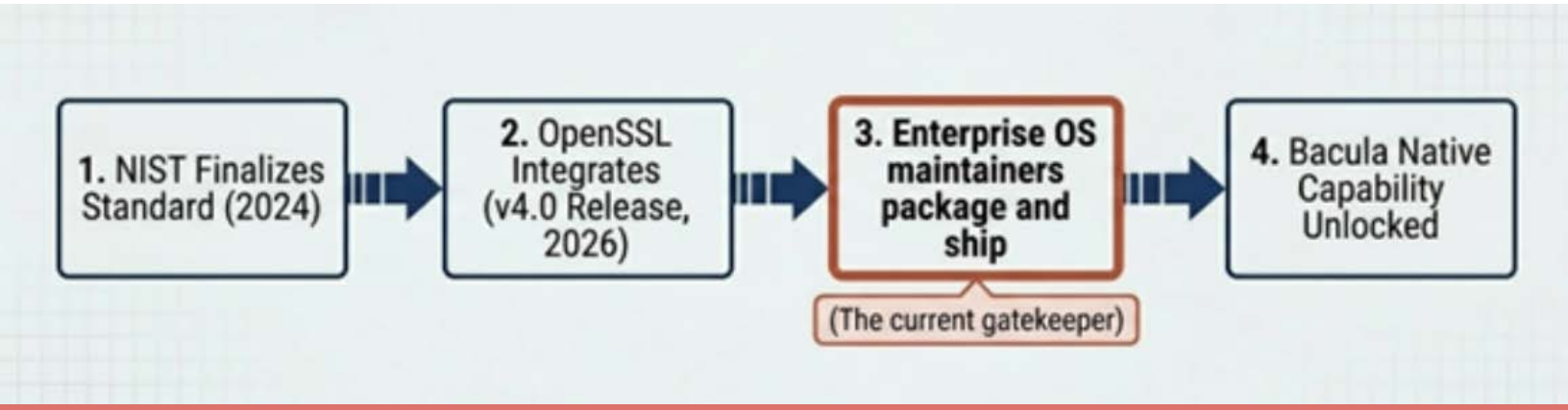
While data-at-rest encryption is well-protected today, the areas most exposed to quantum risk are key exchange, authentication, and digital signatures — the mechanisms that govern how backup clients authenticate to directors, how TLS sessions are established between daemons, and how software updates and certificates are validated.

These are precisely the areas addressed by the new NIST standards (ML-KEM for key exchange, ML-DSA for signatures, with FN-DSA expected once its standard is finalized), and they represent the primary focus of Bacula's PQC engineering roadmap.

OpenSSL 4.0: The Enabling Foundation

The most significant development for Bacula's PQC trajectory is the OpenSSL project's introduction of native, production-grade PQC support — first delivered in OpenSSL 3.5 and continued in OpenSSL 4.0, released in 2026. Both releases provide native implementations of three of the four NIST PQC algorithms: ML-KEM (key exchange), ML-DSA, and SLH-DSA (digital signatures). FN-DSA is not yet covered, as its standard remains in draft. Bacula Enterprise is being aligned with these OpenSSL releases at the source-code level, making this the fastest and most standards-aligned route to PQC-enabled TLS for any platform that relies on OpenSSL.

End-to-End PQC availability relies on a standard-driven operating system pipeline.



Warning: Source-code compatibility is necessary but not sufficient. Production deployments are governed by the OS. Keeping enterprise Linux distributions current is a fundamental security imperative to access PQC-enabled TLS through standard channels.

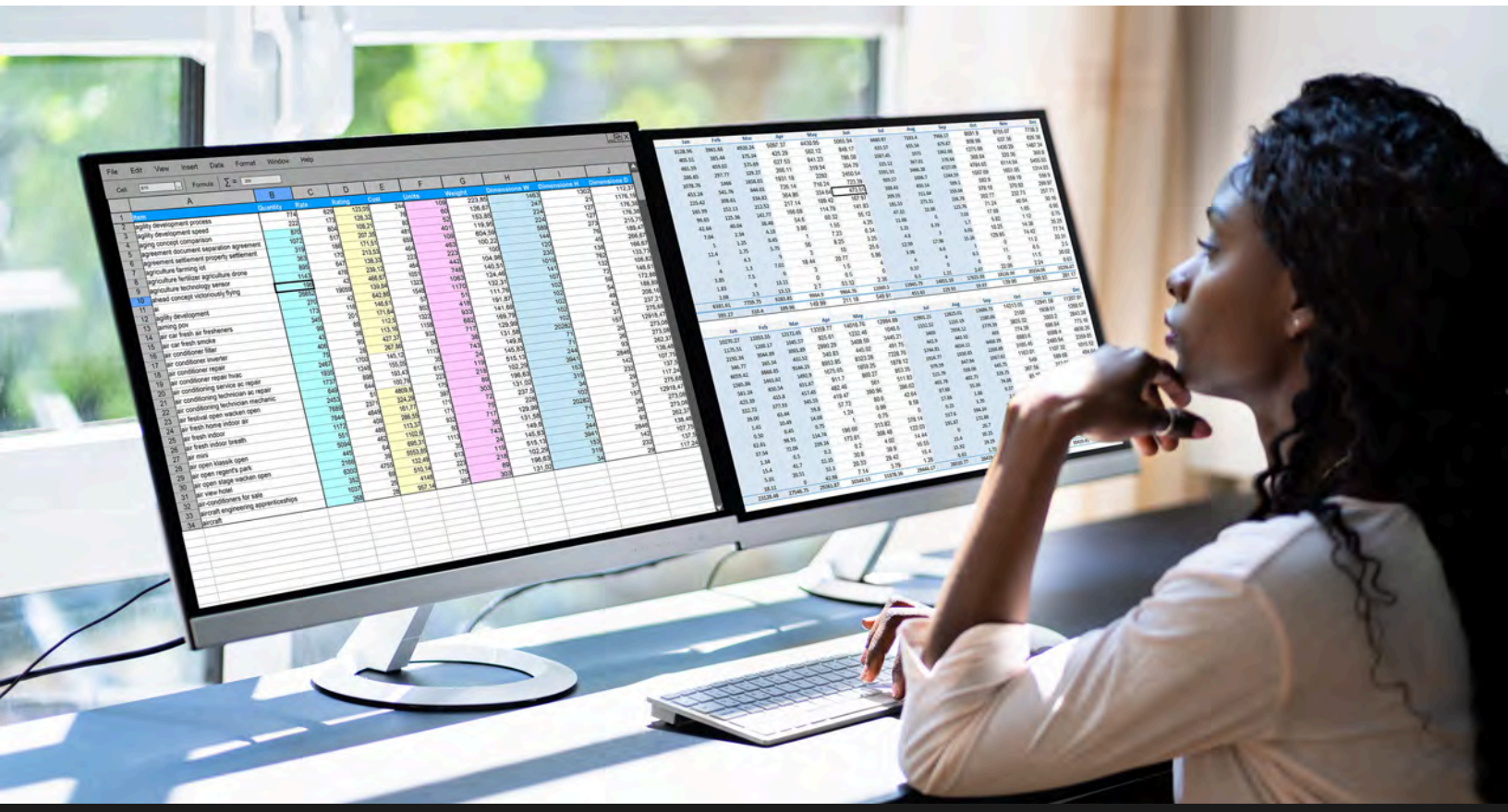
When new OpenSSL packages ship, Bacula will be immediately compatible with PQC-resistant communications

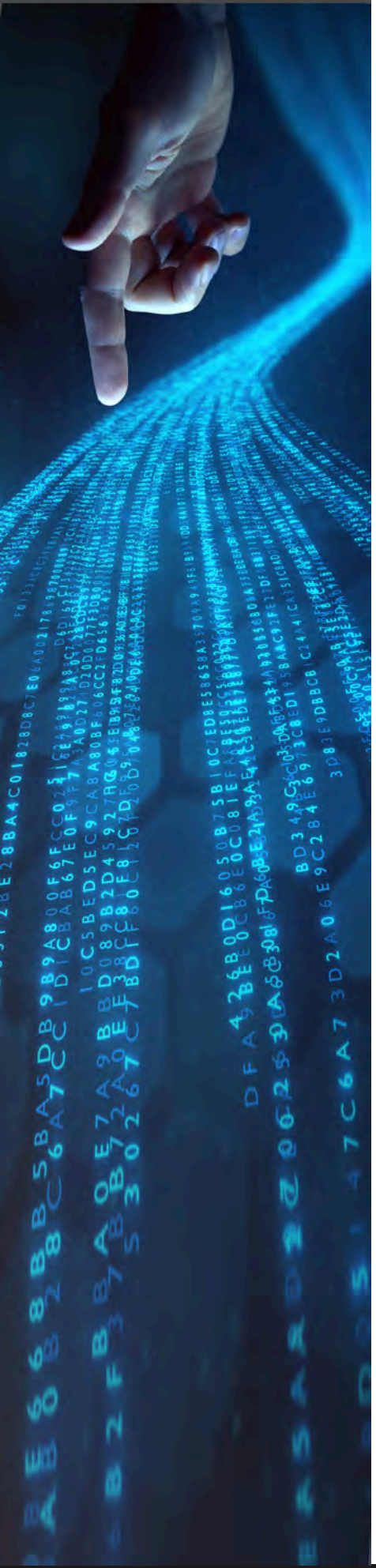
It is important to recognize that source-code compatibility is a necessary but not sufficient condition for end-customer availability. Production OpenSSL deployments are governed by the operating system: it is the OS maintainers who package, build, and ship OpenSSL — and supported enterprise Linux distributions do not refresh major library versions quickly.

As of this writing, most enterprise OS releases are still some distance from shipping OpenSSL 3.5 or 4.0 in their stable channels. As soon as those distributions ship the new OpenSSL packages, Bacula Enterprise will be directly compatible with PQC-resistant communications.

This makes one operational point worth emphasizing: keeping operating systems current is itself a security imperative, and is a prerequisite for accessing PQC-enabled TLS through standard distribution channels.

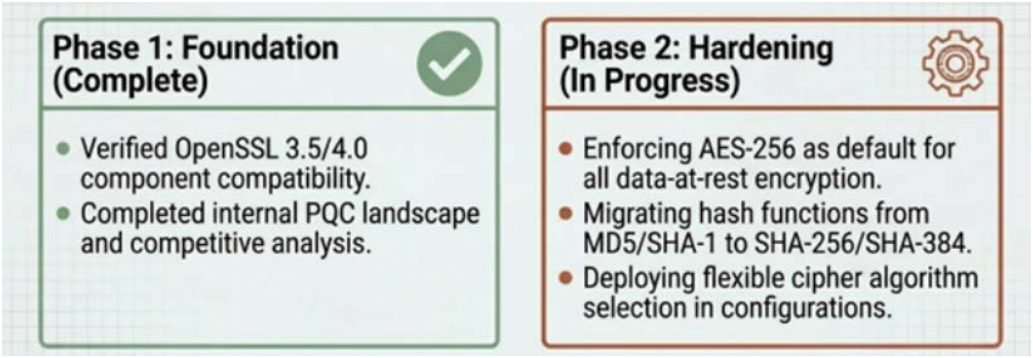
By building our PQC implementation on the OpenSSL 3.5/4.0 line rather than proprietary or pre-standard libraries, Bacula ensures customers receive algorithms that have been subject to years of international cryptographic scrutiny, not vendor-specific implementations that may diverge from final standards.





Bacula PQC Delivery Roadmap

Bacula Systems is executing a phased PQC integration program aligned with OpenSSL and OS ecosystem maturity. The roadmap is structured to deliver immediate security improvements for existing customers while building toward comprehensive quantum-safe protection.



Summary: Phase 1 and 2 focus on maximizing the quantum-resilience of Bacula's existing symmetric and hashing architectures, creating a fortified baseline.

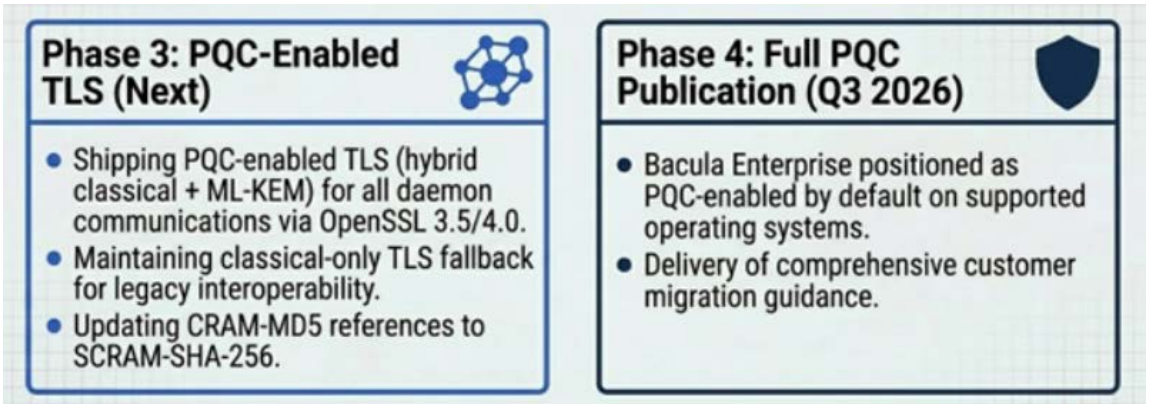
Phase 1: Foundation (Complete)

- OpenSSL 3.5/4.0 compatibility verified across Bacula Enterprise components
- Internal PQC landscape analysis and competitive assessment completed
- PQC knowledge base article published internally

Phase 2: Hardening (In Progress)

- Flexible cipher algorithm selection in Bacula configuration
- Documentation updates: PQC secure options; removal of deprecated/weak algorithm references
- AES-256 enforced as default for data-at-rest encryption; guidance updated throughout
- PQC Conceptual Guidance added to public documentation (data at rest + communications)
- Review of hash function usage — migration from MD5/SHA-1 to SHA-256/SHA-384

Bacula Delivery Roadmap: PQC-Enabled TLS and Full Migration



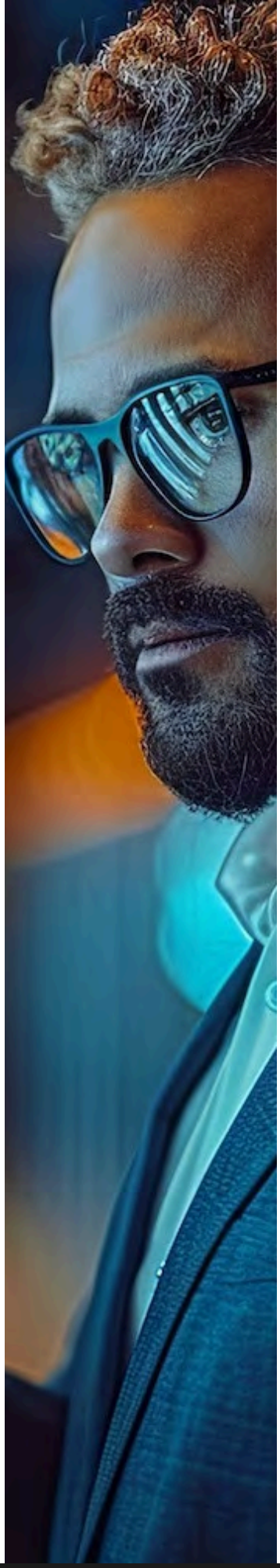
Summary: Phase 3 and 4 deliver the new mathematical foundations for key exchange and authentication , securing the communications control plane.

Phase 3: PQC-Enabled TLS (Next)

- Ship PQC-enabled TLS via OpenSSL 3.5/4.0 (hybrid classical + ML-KEM) for all daemon communications
- Fallback to classical-only TLS maintained for interoperability with legacy environments
- PQC-enabled TLS available as default configuration in new package releases
- OS/OpenSSL/Bacula version compatibility matrix published for supported configurations
- Review and update of certificate generation tooling (BWeb, REST-API, TLS helpers)
- CRAM-MD5 references updated to SCRAM-SHA-256 across documentation and defaults

Phase 4: Full PQC Publication and Migration Guidance (Q3 2026)

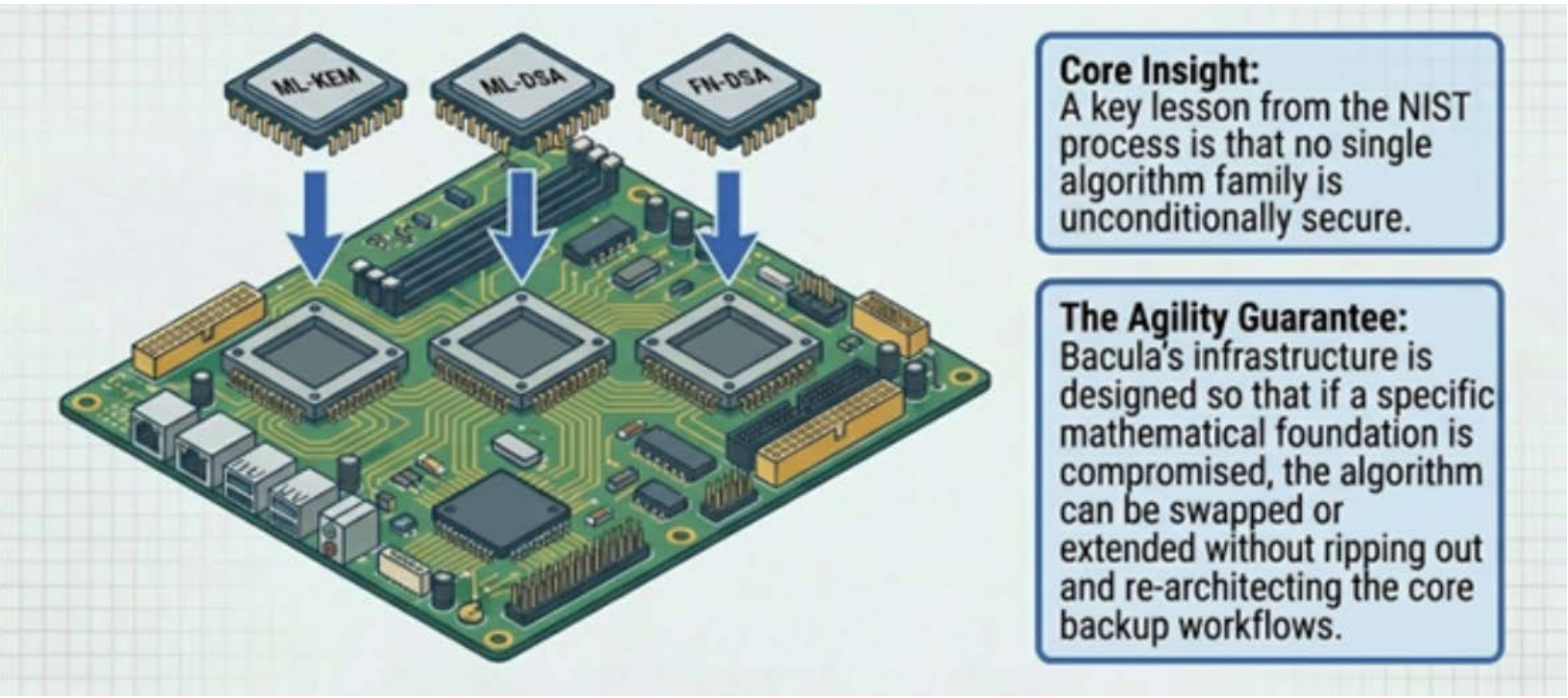
- Customer migration guidance covering the move to PQC-enabled configurations
- Bacula Enterprise positioned as PQC-enabled by default on supported operating systems, as those systems ship updated OpenSSL packages
- Updated security documentation and customer-facing materials reflecting PQC posture



Why Bacula Enterprise for Quantum-Safe Data Protection

The PQC transition is not merely a technical checkbox. It requires a vendor with the architectural flexibility, engineering discipline, and long-term commitment to maintain cryptographic agility across decades. Bacula Systems brings several distinct advantages to this challenge.

Algorithm Agility by Design: Bacula is adopting a fluid architecture, not just a new algorithm



Linux-Native Architecture

Bacula was engineered from the ground up for Linux and enterprise open-source environments — the same ecosystem where OpenSSL is the dominant cryptographic library and where PQC adoption will be driven first. Our integration with the OpenSSL 3.5/4.0 line is a natural extension of our core architecture, not a retrofit.

No Vendor Lock-in on Cryptographic Dependencies

Unlike platforms that embed proprietary cryptographic implementations, Bacula relies on the globally audited OpenSSL library. A practical clarification matters here: whether a given OpenSSL build is FIPS-validated depends on who builds and packages it. In production, that is typically the operating system maintainer, and achieving FIPS compliance often requires specific actions at the OS level (enabling the FIPS provider, configuring the system policy, and using a build that has been certified for the target platform). Bacula consumes the OpenSSL provided by the supported OS, so customers operating on a FIPS-configured platform inherit that posture directly. When NIST finalizes additional algorithms or when operating system vendors ship updated PQC support, Bacula customers benefit through standard OpenSSL updates — no proprietary upgrade cycle required.

Proven Enterprise-Grade Security Architecture
Bacula's security architecture is trusted by some of the world's most security-conscious organizations, including NASA,, Deutsche Bahn, leading financial institutions, and the largest defense organization in the West.. Our approach to PQC follows the same principle that has guided our security engineering: adopt proven standards, maintain operational simplicity, and never sacrifice correctness for expediency.

Algorithm Agility by Design
Bacula's roadmap is being built with algorithm agility as a first principle — the ability to configure, update, or extend cryptographic mechanisms without re-architecting backup workflows. This is the operational requirement that NIST and the NSA emphasize most strongly: organizations should not be locked into a single algorithm family as the PQC landscape continues to evolve.

Recommended Actions for Bacula Customers

Regardless of where your organization sits on the quantum readiness curve, there are concrete steps you can take today with Bacula Enterprise to strengthen your cryptographic posture.

Immediate actions for strengthen your cryptographic posture today:

Action prompt: Engage your Bacula account team to schedule a comprehensive cryptographic review of your deployment prior to the default rollout of PQC-enabled TLS.

Immediate Actions

- Ensure all backup jobs use AES-256 for data-at-rest encryption. Audit existing job configurations and update any that reference shorter key lengths.
- Review TLS configuration for all Bacula daemon communications. Ensure TLS 1.2 or 1.3 is enforced and any outdated cipher suites are disabled.
- Upgrade to the latest Bacula Enterprise release and keep your operating system current. PQC-enabled TLS becomes available end-to-end as supported OS distributions ship OpenSSL 3.5 or 4.0, so staying current on both Bacula and your OS is the practical prerequisite for accessing PQC features as they roll out.
- Replace any MD5 or SHA-1 references in verification and hashing configurations with SHA-256 or SHA-384.

Near-Term Planning

- Engage your Bacula account team to schedule a cryptographic review of your deployment — identifying any configurations that may require updates before PQC-enabled TLS becomes default.
- Identify your longest-retention backup archives and assess their sensitivity. These are the data sets most exposed to harvest-now/decrypt-later attacks and should be prioritized for re-encryption or migration to AES-256.
- Review your enterprise TLS infrastructure (load balancers, proxies, firewalls) for compatibility with hybrid PQC key exchange. Bacula's PQC-enabled TLS will use hybrid mode for backward compatibility.

Strategic Alignment

- Align your organization's quantum readiness roadmap with NSA and NIST guidance. The NSA Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) targets 2030–2033 for complete migration of national security systems.
- For regulated industries (financial services, healthcare, defense, energy/OT), begin mapping PQC migration requirements to your compliance framework. IEC 62443, NIST CSF, and emerging EU quantum regulations will increasingly reference PQC standards.
- Engage Bacula Systems for a tailored Quantum Security Roadmap — a structured assessment of your backup environment's cryptographic exposure and a prioritized migration plan.

Contact your Bacula Systems account executive or write to sales@baculasystems.com to arrange a quantum readiness consultation.

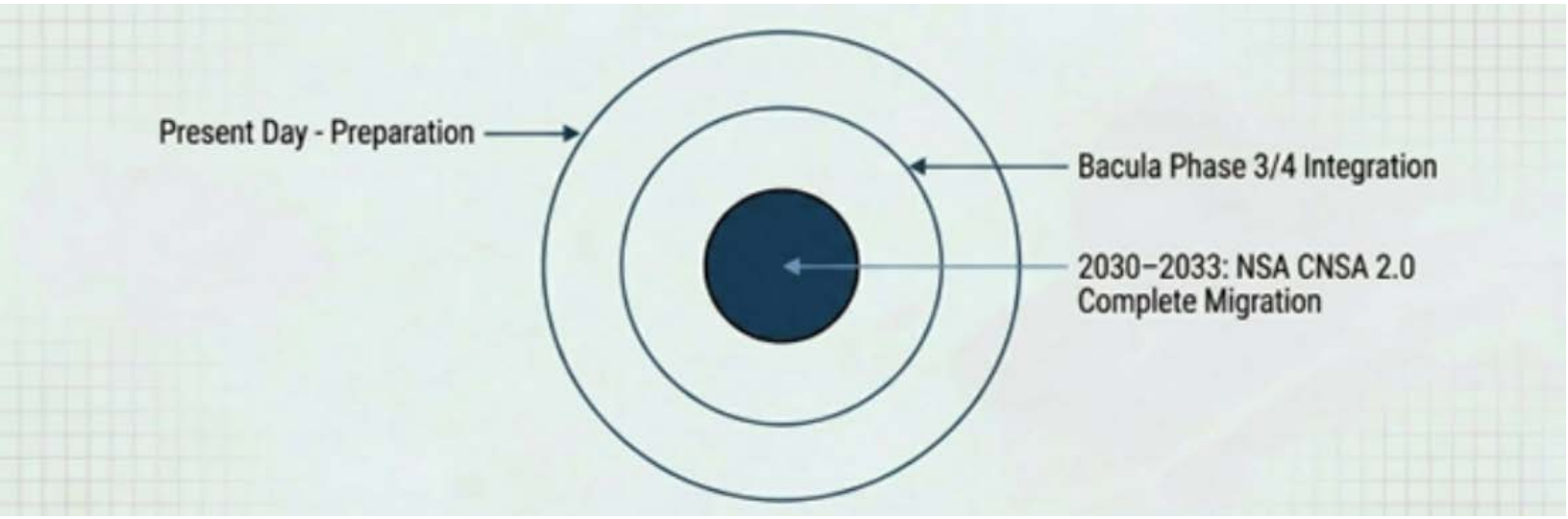
Conclusion

The quantum computing transition is not a distant hypothetical — it is an active, accelerating program being tracked by every major government and standards body in the world. For organizations that depend on long-term backup archives, the risk of 'harvest now, decrypt later' attacks makes cryptographic preparedness an urgent priority, not a future consideration.

Bacula Systems approaches this transition from a position of strength. Our use of AES symmetric encryption for data at rest already meets NIST's quantum-era guidance with appropriate key lengths. Our OpenSSL foundation is fully compatible with the new NIST PQC standards. And our engineering roadmap is actively delivering the tools customers need to operate confidently as the cryptographic landscape evolves.

We believe that the organizations best positioned for the quantum era will be those that start now — reviewing their configurations, engaging with vendors who have clear PQC roadmaps, and building the internal knowledge needed to manage this transition thoughtfully. Bacula Systems is committed to being a trusted partner through that journey.

Align your quantum readiness roadmap with global compliance timelines.



Final Insight: The transition is an accelerating program. For regulated industries (finance, health, defense, OT), frameworks like IEC 62443, NIST CSF and EU regulations are already moving toward mandatory PQC standards.

Start now to protect your data today, and for the decades ahead. Contact Bacula Systems for a tailored Quantum Security Roadmap consultation at **sales@baculasystems.com**

About Bacula Systems

Bacula Systems is an enterprise software company specializing in backup and data protection for complex, high-volume, and security-sensitive environments. Trusted by NASA, MIT, Deutsche Bahn, and hundreds of enterprises globally, Bacula Enterprise offers unmatched scalability, Linux-native architecture, and Swiss-hosted security — with no per-terabyte pricing and no lock-in.