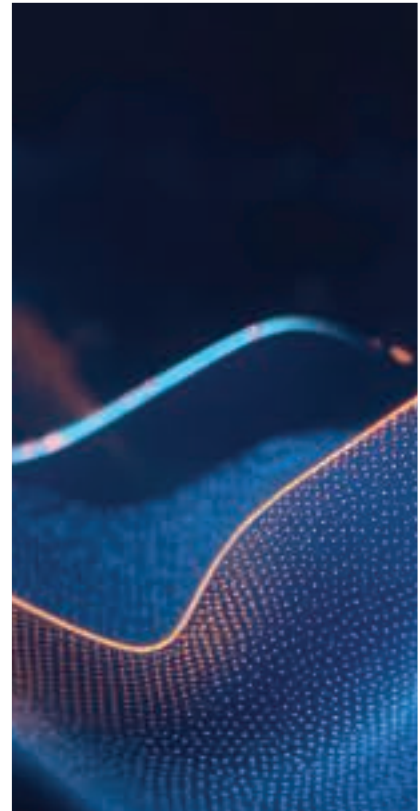
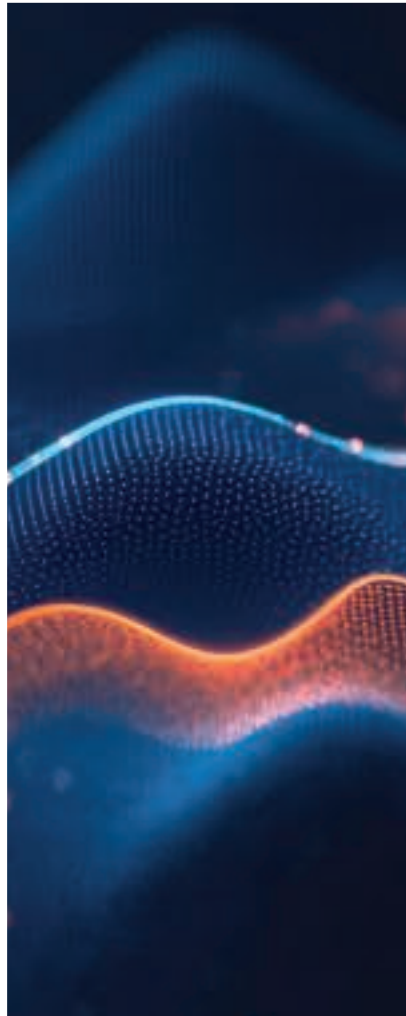


FROST & SULLIVAN
BEST PRACTICES



2026

GLOBAL POST-QUANTUM
CRYPTOGRAPHY

**ENABLING TECHNOLOGY
LEADERSHIP**



Table of Contents

Best Practices Criteria for World-Class Performance 3

The Transformation of the Post-Quantum Cryptography Industry 3

 A Data-Centric Approach to Adapt Continuously4

 Targeting High-Value PQC Use Cases.....5

 Extending Data Protection Across the Existing Stack.....6

Conclusion 6

What You Need to Know about the Enabling Technology Leadership Recognition..... 7

Best Practices Recognition Analysis..... 7

 Technology Leverage7

 Customer Impact7

Best Practices Recognition Analytics Methodology..... 8

Inspire the World to Support True Leaders 8

About Frost & Sullivan 9

The Growth Pipeline Generator™ 9

The Innovation Generator™ 9

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Certes excels in many of the criteria in the Post-Quantum Cryptography space.

RECOGNITION CRITERIA	
Technology Leverage	Customer Impact
Commitment to Innovation	Price/Performance Value
Commitment to Creativity	Customer Purchase Experience
Stage Gate Efficiency	Customer Ownership Experience
Commercialization Success	Customer Service Experience
Application Diversity	Brand Equity

The Transformation of the Post-Quantum Cryptography Industry

The migration to post-quantum cryptography (PQC) is a major undertaking, requiring organizations to identify where vulnerable cryptography is embedded across applications, infrastructure and data, determine what can be upgraded, and then execute migration at scale. There is increasing focus on visibility through initiatives such as cryptographic bills of materials (CBOMs), which are critical for understanding an organization’s cryptographic estate and prioritizing migration. However, this will be a prolonged, resource-intensive process requiring significant investment, cryptographic dependency analysis, and phased deployment across heterogeneous environments, particularly where legacy or mission-critical systems cannot easily be taken offline or upgraded. The challenge is further compounded by the fact that PQC is not a one-time transformation: cryptographic standards will continue to evolve, with today’s NIST-approved algorithms representing only the first generation of a potential, longer-term cycle of change.

Organizations therefore need an approach that can continuously adapt as algorithms and requirements evolve but cannot afford to wait until the migration is complete to address the risk. The threat of “harvest now, decrypt later” means sensitive data can be stolen today and decrypted once sufficiently capable quantum computers become available. This is particularly significant for data with long regulatory, legal or commercial lifespans, where information compromised today may remain valuable and expose the business in the future. As a result, protecting vulnerable data and critical applications now needs to run in parallel with the longer-term migration effort. While CBOMs and broader cryptographic visibility

provide the foundation for a safe and prioritized migration, organizations should simultaneously deploy measures to protect high-value data today, enabling them to reduce immediate exposure while progressively moving the wider estate towards quantum-resistant cryptography.

A Data-Centric Approach to Adapt Continuously

“Rather than waiting for individual application and infrastructure vendors to release quantum-safe update, and subsequently undertaking potentially disruptive upgrades and redeployments, businesses can centrally manage cryptographic changes through the Cryptographic Abstraction Layer and apply them across data flowing between applications and infrastructure. This enables a more gradual introduction of quantum-safe protection with limited disruption while progressively upgrading embedded cryptography as part of a broader PQC migration program.”

**- Ozgun Pelit,
Sr. Industry Analyst**

Certes is an established provider of data-centric quantum-safe security, drawing on more than 20 years of experience, 1,000+ customers, and a global footprint across the US, EMEA and APAC. Its approach is centered on protecting the data itself rather than requiring businesses to immediately replace or re-engineer the cryptography embedded within every application and infrastructure component. The platform provides quantum-safe protection for applications across any infrastructure, using customer-owned keys to support data sovereignty and, critically, crypto-agility to adapt as cryptographic standards evolve. This data-centric approach is designed to address the

immediate risk of “harvest now, decrypt later” while enterprises undertake the longer-term migration of their embedded cryptography.

A core element of Certes’ offering is its Cryptographic Abstraction Layer (CAL), which sits between applications and infrastructure and abstracts cryptographic protection away from the underlying technology stack. Rather than waiting for individual application and infrastructure vendors to release quantum-safe update, and subsequently undertaking potentially disruptive upgrades and redeployments, businesses can centrally manage cryptographic changes through the CAL and apply them across data flowing between applications and infrastructure. This enables a more gradual introduction of quantum-safe protection with limited disruption while progressively upgrading embedded cryptography as part of a broader PQC migration program. Certes therefore advocates a parallel approach of protecting critical data immediately through a centralized, crypto-agile layer, while using visibility and governance to migrate the underlying applications and infrastructure over time.

Certes’s solution is built around the principle of continuous adaptation, with the data itself serving as the common security layer across applications and infrastructure. Because protection travels with the data, organizations do not need to determine whether every underlying application or infrastructure component is quantum-safe. The solution comprises the Certes Enforcement Point (CEP), which performs encryption and decryption within the data path, and the Certes Policy Manager (CPM), which centrally manages policies and cryptographic controls. A key differentiator is Certes’s policy-specific key architecture, whereby individual policies have dedicated keys that can be rotated on a regular basis and managed concurrently at scale. Each policy-controlled application or data flow can use independently managed key material, with separate rotation schedules and customer-controlled key components.

“Certes is designed to augment rather than replace existing security and network investments. Its patented Layer 4 payload protection enables the platform to remain transparent to applications, infrastructure and existing network controls, allowing tools such as monitoring, SD-WAN and other network components to continue operating as before. Customers can therefore add data-centric protection without having to re-architect their environments or sacrifice existing technology investments.”

**- Ozgun Pelit,
Sr. Industry Analyst**

Combined with its quantum-based random number generation capabilities, this provides granular control over data protection while supporting rapid changes to cryptographic policies. The result is a model where the cryptographic layer can evolve independently of the applications and infrastructure, securing data in motion as organizations undergo large-scale migrations.

Targeting High-Value PQC Use Cases

Certes’s use cases center on protecting environments where conventional PQC migration is particularly difficult, including legacy applications, hybrid cloud and edge environments. This is especially relevant in financial services, where critical legacy systems can be

difficult to upgrade without disrupting core operations or introducing unacceptable levels of operational risk. Certes also supports resilience through its virtual air gap capability, allowing organizations to dynamically isolate critical applications, data flows and backups from the wider environment, while still maintaining controlled access where needed and preserving recovery capabilities even during an active attack or compromise scenario.

Beyond PQC migration, Certes’s solution can be used to control sensitive data flows and segment networks in a more granular and cryptographically enforced way than traditional approaches. Its encryption can prevent sensitive data from being exposed to internal or external LLMs when it should not be accessible, helping organizations maintain tighter governance over AI adoption and data usage. Cryptographic segmentation can also help separate IT and OT environments, reduce the risks associated with flat or overly connected networks, and limit lateral movement in the event of a breach. These use cases are increasingly relevant beyond financial services, with large multinational organizations across logistics, manufacturing and retail, as well as government organizations, all facing growing security, regulatory and operational pressures that require more adaptive and data-centric security models.

Certes provides a consistent, data-centric protection layer across hybrid and multi-cloud environments, addressing the inherent difficulty of deploying uniform data protection across highly fragmented infrastructures. Each environment, whether on-premises systems, private clouds, or public providers such as AWS and Azure, comes with its own native security controls, configuration nuances, and shared-responsibility models, making it challenging to enforce consistent policies and maintain equivalent levels of protection as data moves between them. Rather than relying on these disparate, environment-specific capabilities, organizations can apply their own policies and unique keys to data wherever it resides or moves, maintaining consistent protection across heterogeneous infrastructure. The solution can be deployed through physical appliances, virtual machines across platforms such as VMware ESXi, KVM, Red Hat and Nutanix AHV, as well as Windows and Linux client agents, allowing the same data protection approach to extend from the data center through cloud environments and to endpoints.

Extending Data Protection Across the Existing Stack

Certes is designed to augment rather than replace existing security and network investments. Its patented Layer 4 payload protection enables the platform to remain transparent to applications, infrastructure and existing network controls, allowing tools such as monitoring, SD-WAN and other network components to continue operating as before. The solution encrypts the Layer 4 payload while preserving the original network headers, allowing routing, QoS, monitoring, and flow visibility tools to continue operating normally. This provides data protection without requiring applications to be rewritten or the network to be re-architected.

Version 7 extends the reach of Certes's enforcement points to address the remaining gaps between the enforcement layer and applications or end users. It brings enforcement closer to workloads and users through expanded agent and cloud deployment options, reducing unprotected segments between applications, endpoints, and network-based enforcement points. The update is designed to simplify deployment across cloud environments and reduce periods where data may otherwise be temporarily unprotected during its network journey. By bringing enforcement closer to workloads, Certes aims to provide more comprehensive coverage while making its data protection architecture easier to deploy across modern cloud infrastructure.

Conclusion

The transition to post-quantum cryptography represents a complex, long-term transformation, with organizations needing to address fragmented technology estates, legacy systems, evolving standards and significant operational dependencies. With "harvest now, decrypt later" already creating risks for long-lived sensitive data, organizations must balance the considerable effort of large-scale migration with the need to reduce exposure and protect critical information throughout the transition. Vendors that can provide immediate protection while simplifying the complexity of migration therefore offer significant value, helping customers reduce risk today while progressing towards long-term PQC readiness.

For its strong overall performance, Certes is presented with Frost & Sullivan's 2026 Global Enabling Technology Leadership Recognition in the Post-Quantum Cryptography industry.

What You Need to Know about the Enabling Technology Leadership Recognition

Frost & Sullivan's Enabling Technology Leadership Recognition identifies the company that applies its technology in new ways to improve existing products and services and elevate the customer experience.

Best Practices Recognition Analysis

For the Enabling Technology Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

STEP		VALUE IMPACT	
		WHAT	WHY
1	Opportunity Universe	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	Transformational Model	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	Ecosystem	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	Growth Generator	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	Growth Opportunities	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	Frost Radar	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	Best Practices	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	Companies to Action	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at <http://www.frost.com>.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fueled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)

