FROST & SULLIVAN

2024 PRODUCT LEADER

IN THE GLOBAL POST-QUANTUM CRYPTOGRAPHY INDUSTRY

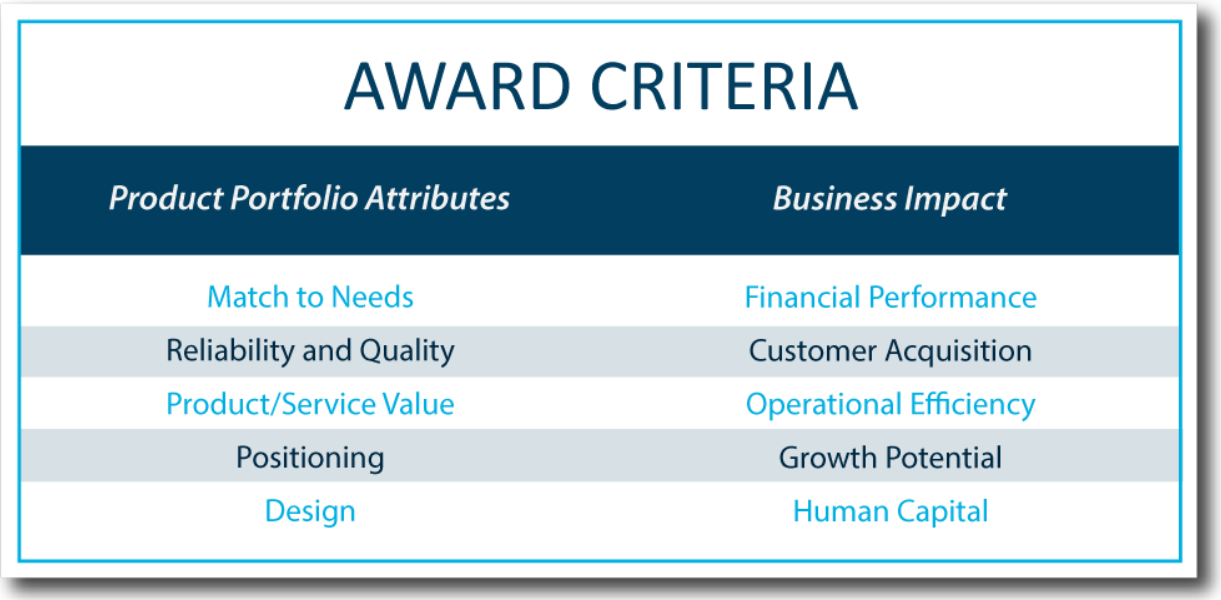
QuSecure

FROST & SULLIVAN

2024 BEST PRACTICES AWARD

Best Practices Criteria for World-Class Performance

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



Changing Needs for a New Era

Cryptographic migrations are not new, with algorithms previously deemed secure, like DES, MD5, and SHA-1, becoming deprecated with advances in computation and the development of new forms of attacks. For organizations, these transitions are typically painful processes involving high levels of investment, concerns about interoperability, operational disruptions, and lack of expertise resulting in errors. Compared to previous transitions, the migration to post-quantum cryptography (PQC) will be of much higher scope due to the increased complexities of digital infrastructure and operational environments.

The potential risks from a cryptographically relevant quantum computer to the security of data, digital services, and business operations have significant implications for the wider economy and geopolitics. Starting with the most sensitive industries and business cases, planning and migrating to quantum-safe architectures will be one of the top priorities in board rooms and government agencies in the coming years. Especially for organizations operating in highly regulated and scrutinized environments, protecting customer and organizational propriety data without disruption to the enterprise will be of utmost importance. Particularly for governments, financial institutions, and healthcare providers, potential harvest now and decrypt later scenarios render the quantum threat more than just a future problem.

The new era is also expected to set off a trend of faster-changing and ever-evolving algorithms, with some being broken and others being used for specific use cases. This potential churn is due to possible flaws in both new and existing algorithms, as well as their susceptibility to new forms of attacks as cryptoanalysis improves. In this context, crypto-agility will be a central piece for all organizations in providing operational

> *"QuSecure's cryptographic orchestration creates a new layer for cryptographic protocols and algorithms, enabling centralized management, monitoring, and immediate policy changes at scale. Owing to its easy deployment and configurations across devices and applications, QuProtect offers rapid upgrade of legacy infrastructure, interoperability, and policy-driven crypto-agility for current and future regulatory and compliance requirements."*
>
> ***- Özgün Pelit***
> ***Sr. Industry Analyst***

flexibility to changing needs and requirements. This will require defining standards and policy, as well as the ability to rapidly swap algorithms en masse and without disruption to the larger operations.

A New Approach: Cryptographic Orchestration

QuSecure's software solution brings an innovative approach to the ongoing cryptography modernization and PQC migration efforts being undertaken by governments and enterprises. The company's proprietary solution, QuProtect, offers the ability to upgrade digital infrastructure to quantum-resistant architectures without code change or disruptions to day-to-day operations. QuProtect utilizes initiator and receiver proxies as the fundamental cryptographic unit, creating an additional layer to protect sessions and data in a post-quantum way with its patented QSL protocol. By hot-swapping cryptography, the offering provides two independent layers of encryption, with the ability to deploy post-quantum algorithms, enact policy, and modify parameters like key lengths and rotation frequencies through its central management console QuProtect Orchestrator.

The idea behind the QuProtect platform echoes the successful approach of moving disparate networking devices to SD-WAN for simplifying and automating operations, improving performance and user experience, increasing agility, reducing costs, and eliminating errors. In a similar way, QuSecure's cryptographic orchestration creates a new layer for cryptographic protocols and algorithms, enabling centralized management, monitoring, and immediate policy changes at scale. Owing to its easy deployment and configurations across devices and applications, QuProtect offers rapid upgrades of legacy infrastructure, interoperability, and policy-driven crypto-agility for current and future regulatory and compliance requirements.

QuSecure's platform consists of three independent products for different use cases: QuProtect Web App Security for websites and web applications; QuProtect Network Security for network traffic between servers; and QuProtect Core for router-to-router communications. Through deployment of proxies in the initiator or the receiver ends, the solutions work transparently and require no code change to end-user or server-side applications. Securing the link between proxies, the static and ephemeral key encapsulation mechanisms (KEMs) provide authentication and generate new key pairs for individual sessions. QuProtect supports all NIST Round 4 finalists and offers the ability to seamlessly swap between algorithms directly through the single pane of glass management console QuProtect Orchestrator. Through its added orchestration layer, QuProtect in effect enables classic and post-quantum encryption to work in tandem.

Addressing Today's and Tomorrow's Challenges

QuSecure currently has its solutions deployed with large players in the telecommunications, financial services, transportation, healthcare, and energy industries, as well as with government entities. These

> *"Depending on organizations' unique security needs and requirements, strategic priorities, or operational environments, QuProtect offers value in individual application areas. Owing to its flexibility, the solution can be rapidly deployed for singular use cases like securing high-risk connections, sensitive data-at-rest, file transfers, or cloud routing, in addition to covering entire networks. With the security vendor ecosystem upgrading to PQC in their offerings, QuProtect provides protection for organizations' crown jewels today."*
>
> ***- Özgün Pelit***
> ***Sr. Industry Analyst***

industries typically underpin many other sectors, with services that are offered downstream and a complex matrix of dependencies. Some of the specific applications of QuProtect in use today include securing satellite communications, 5G messaging apps, military operations center communications, and online wallets. QuSecure has ongoing partnerships with AWS, Accenture, Arrow Electronics, Dell, and Red Hat, in addition to its wide reseller network. The company is also part of the General Services Administration (GSA) Schedule, allowing pre-approved procurement for US federal agencies.

Depending on organizations' unique security needs and requirements, strategic priorities, or operational environments, QuProtect offers value in individual application areas. Owing to its flexibility, the solution can be rapidly deployed for singular use cases like securing high-risk connections, sensitive data-at-rest, file transfers, or cloud routing, in addition to covering entire networks. With the security vendor ecosystem upgrading to PQC in their offerings, QuProtect provides protection for organizations' crown jewels today. As enterprises go through lengthy and complex discovery and inventory processes in their migration journey to PQC, the solution also allows the testing of new algorithms with the existing encryption in place.

PQC constitutes a paradigm shift for the cryptographic systems of the past decades, as well as to how cryptography is used and managed. However, with limited large-scale deployment and implementation to date, organizations need to prepare for potential vulnerabilities and operational complexities that the new algorithms will bring. Enabling full control in an agile and modular way, QuProtect allows organizations to refine their cryptography against such risks and for specific use cases. By offering ease of deployment, adaptability to new requirements and flexibility of use in individual applications, QuSecure's offering addresses current challenges and future needs.

Conclusion

With ever-evolving use cases, security requirements, and operational complexities, cryptography and crypto-agility will play a much bigger role for organizations in the future. In the context of PQC and beyond, QuSecure brings a disruptive approach to how cryptography is deployed and managed. Coupling full control with simplicity, the company's offering uniquely positions itself in the ecosystem of cryptographic modernization.

For its strong overall performance, QuSecure is recognized with Frost & Sullivan's 2024 Global Product Leadership Award in the Post-Quantum Cryptography industry.

What You Need to Know about the Product Leadership Recognition

Frost & Sullivan's Product Leadership Award recognizes the company that offers a product or solution with attributes that deliver the best quality, reliability, and performance in the industry.

Best Practices Award Analysis

For the Product Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Product Portfolio Attributes

Match to Needs: Customer needs directly influence and inspire the product portfolio's design and positioning

Reliability and Quality: Products consistently meet or exceed customer expectations for performance and length of service

Product/Service Value: Products or services offer the best value for the price compared to similar market offerings

Positioning: Products serve a unique, unmet need that competitors cannot easily replicate

Design: Products feature innovative designs, enhancing both visual appeal and ease of use

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

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 Engine™

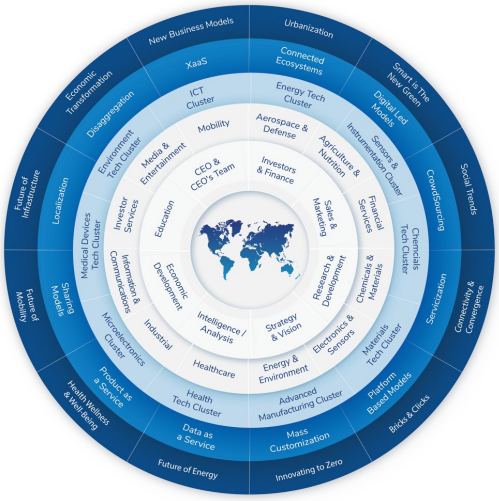
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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:

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