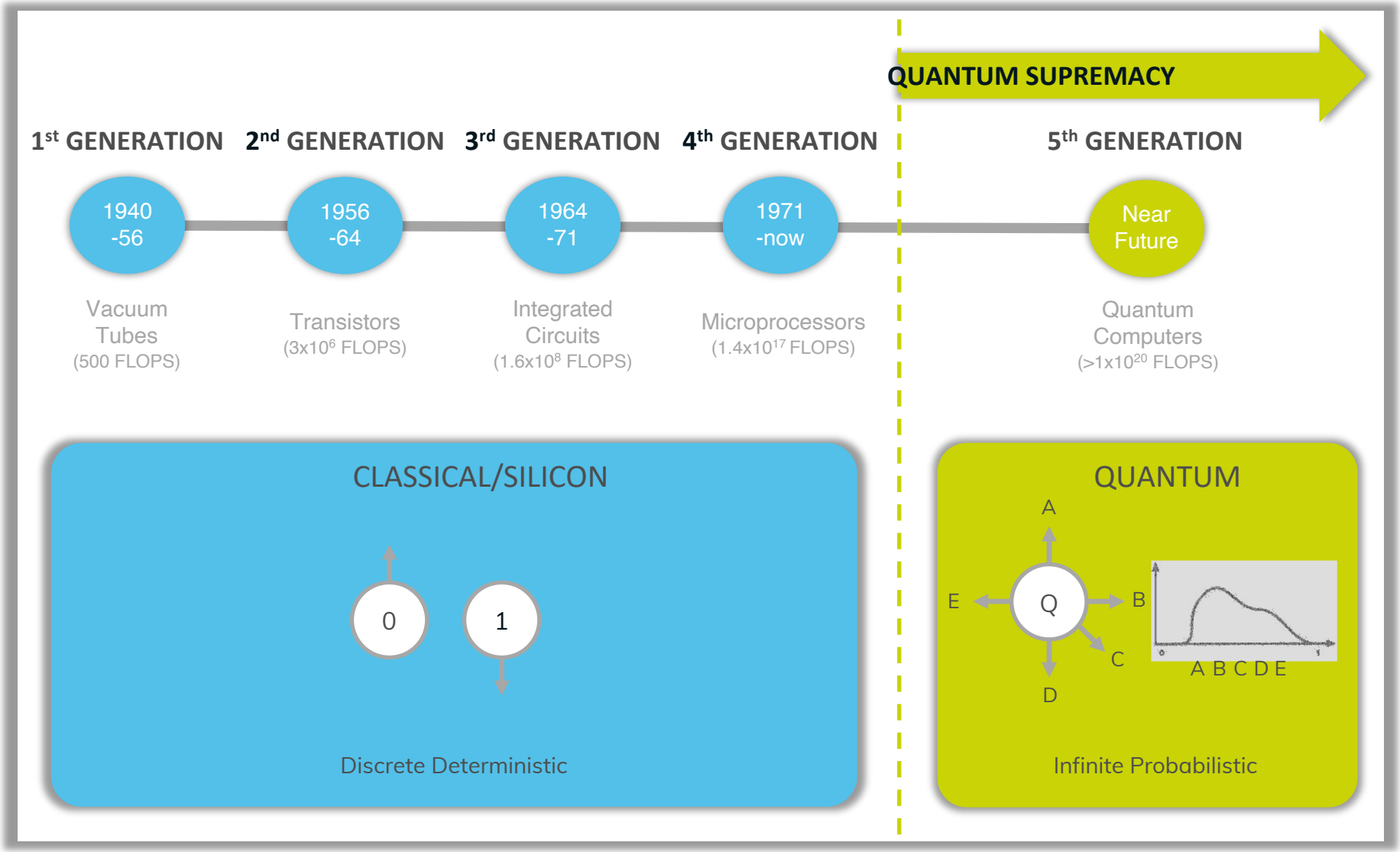
Post-Quantum

Quantum Ready Cybersecurity Solutions

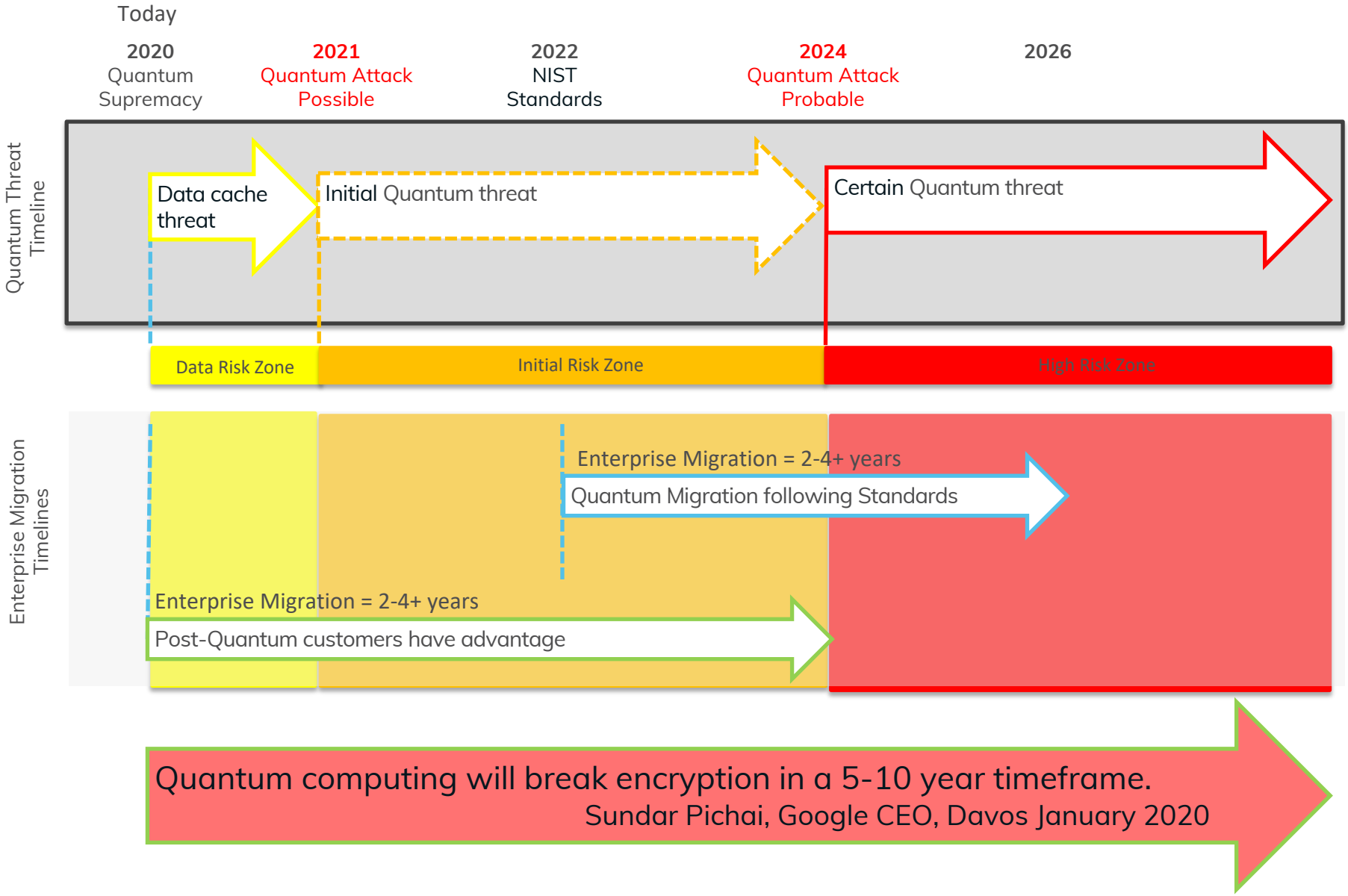
"Quantum computing will break encryption in a 5-10 year timeframe."
Sundar Pichai, Google CEO 22 Jan 2020

July 2020

EVOLUTION OF COMPUTING



QUANTUM READINESS RISK ZONE



TYPES OF CRYPTOGRAPHY

	Pre-Q Security?	Post-Q Security?
Symmetric Key Cryptography	YES	x 2 -> YES
Quantum Encryption	N/A	N/A
Public Key Cryptography – Pre-Quantum • RSA • Elliptic curve THIS IS THE PROBLEM	YES	NO
Public Key Cryptography – Post-Quantum • Code based • Lattice • Multivariate • Supersingular isogeny	N/A	NIST is in the process of selecting candidates to become future standards

WHO AND WHAT ARE AFFECTED?

- All internet infrastructure / applications needing public key cryptography
- Systems with expected use / data storage > 5 years
- National security – much longer
- Identity & access management, e.g. payments, privacy, confidentiality
- IOT devices, e.g. driverless cars, drones, utility controls
- Blockchain & cryptocurrencies

HOW DOES ONE CRACK PUBLIC KEY CRYPTOGRAPHY?

- It is very simple, it is called Integer Factorisation
- If p and q are two Prime Numbers and n = p x q
- What are p x q to get 15? 3 x 5 !
- How about 39? 3 x 13 !
- How about 400 digits? 500 digits? 617 digits?
- Shor's Algorithm + Quantum Computer
  = Frankenstein Monster → Master of the Universe

INTERESTED PARTIES TO GO POST-QUANTUM

- Government - both good and bad
- Standards setting bodies, e.g. NIST, ETSI, IETF
- Scientific & academic institutions
- Commercial enterprises
  - Users - banks, custodians, insurers, healthcare providers
  - Suppliers - Intel, IBM, Google, Honeywell, Post-Quantum & others

HOW READY ARE WE?

- NIST Post-Quantum Cryptography Competition
- Round 1 - 82 submissions with 69 qualified
- Round 2 - 26 candidates left
  - Encryption / Key Encapsulation Mechanism schemes - 17
  - Signature schemes - 9
- Everyone is watching and waiting for the final round candidates
- All agree there will be more than one candidate selected

Commercialisation Considerations

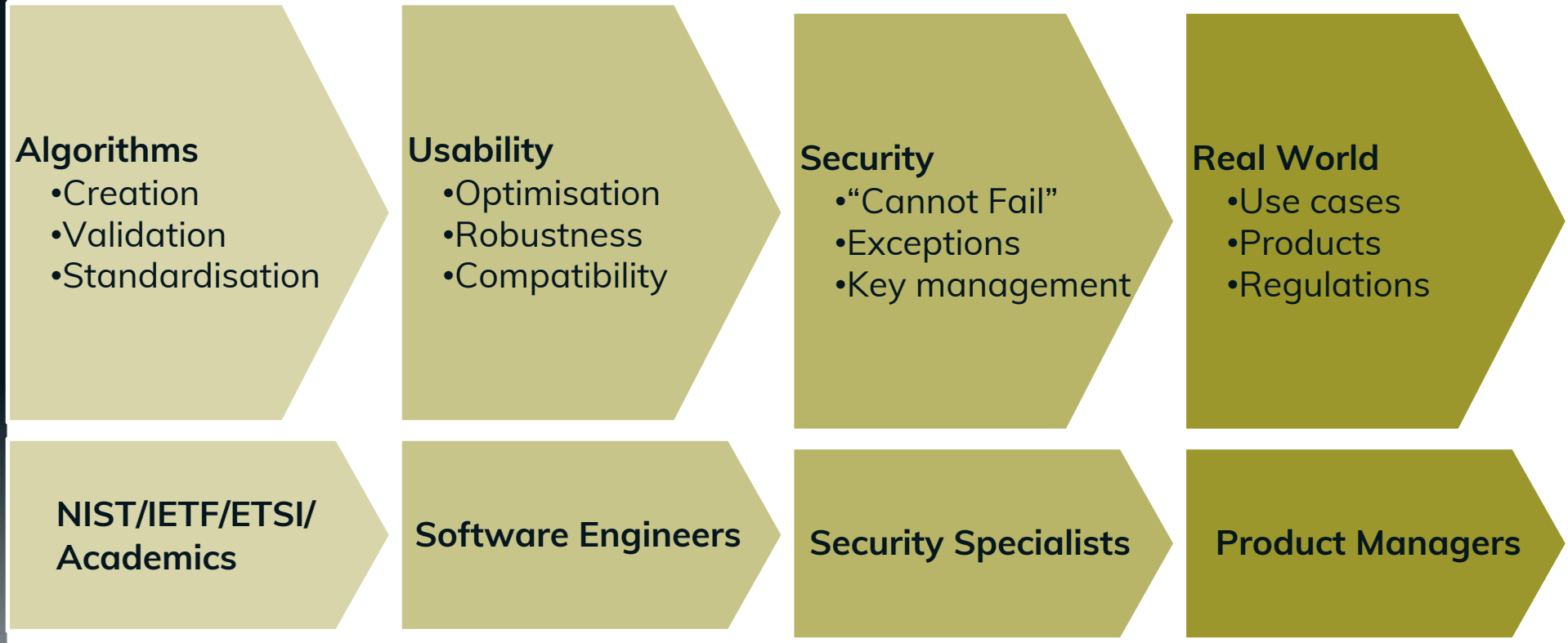
- Hardware development relatively advanced in quantum encryption
- Software development in PQC sporadic and inconsistent
- Everyone is waiting for the NIST protocols to be chosen
- However, critical sectors need to future proof systems now
- PQC essential if upgrading systems in the next few years
- Crypto-agile hybrid approach is the favourite route
- Interoperability is key

If this was a car design

Air + Petrol = Combustion WOW!!! The rest? Not my problem!	But we need to: Design an engine Will it explode?	We also need to: Design the car Can it link up with the gearbox and chassis and tyres?	Finally, how about: Health & safety, regulations & Pricing?
Academics	Engineers	Security Specialists	Product Managers

REAL WORLD STEPS TO PRODUCTISATION

So, how do you create a PQC product?



Our Company's Productisation Timeline:

WHO ARE POST-QUANTUM?

Pioneers in quantum-safe enterprise security

- UK company with background in top secret grade data security
- Over 10 years R&D on Post-Quantum Cryptography
  - Only software focused company entering NIST final round
- PQ's unique enterprise software solutions allow companies to become quantum-ready now
- Identity-as-a-service (IDaaS) products already in use by major companies including Hitachi & Avaya

BARCLAYS NATO OTAN National Cyber Security Centre a part of GCHQ NIST HITACHI AVAYA amazon

WE HAVE TO START FROM SOMEWHERE → IDENTITY

WE START WITH
IDENTITY AS A SERVICE

- The collaboration with Avaya is our first quantum-ready solution
- We have also implemented this with Amazon Connect, AWS' virtual contact center solution for voice & chatbot
- Quantum risks factored into in the design and architecture
- We have to think about cryto agility -> A Hybridised Solution

INTRODUCING NOMIDIO

NomiDio

The world's most advanced Consumer Identity and Authentication as a Service

- **IDaaS** Biometric Bring Your Own ID tool
- **IDV** Remote Identity Verification
- **CIAM** Consumer Identity and Access Management (for both employees and customers)

IDAAS

DATA BREACH

All personal data is individually encrypted – encryption key is controlled by each end user

DATA PROTECTION COMPLIANCE

Nomidio is compliant with all data protection regulations and facilitates client compliance

BARRIERS TO IMPLEMENTATION

Nomidio is a complete Software-as-a-Service solution. No integration or implementation is required

PRIVACY

Self-sovereign – end users decide exactly who receives their personal data

MASTER KEY RISKS

Quorum technology is used to ensure that no one individual has privileged access

QUANTUM THREAT

NomiDio

Nomidio uses quantum-safe encryption. Nomidio is the only quantum-ready digital identity service

Enterprise Migration Timelines

2020 Quantum Supremacy

2021 Quantum Attack Possible

2022 NIST Standards

2024 Quantum Attack Probable

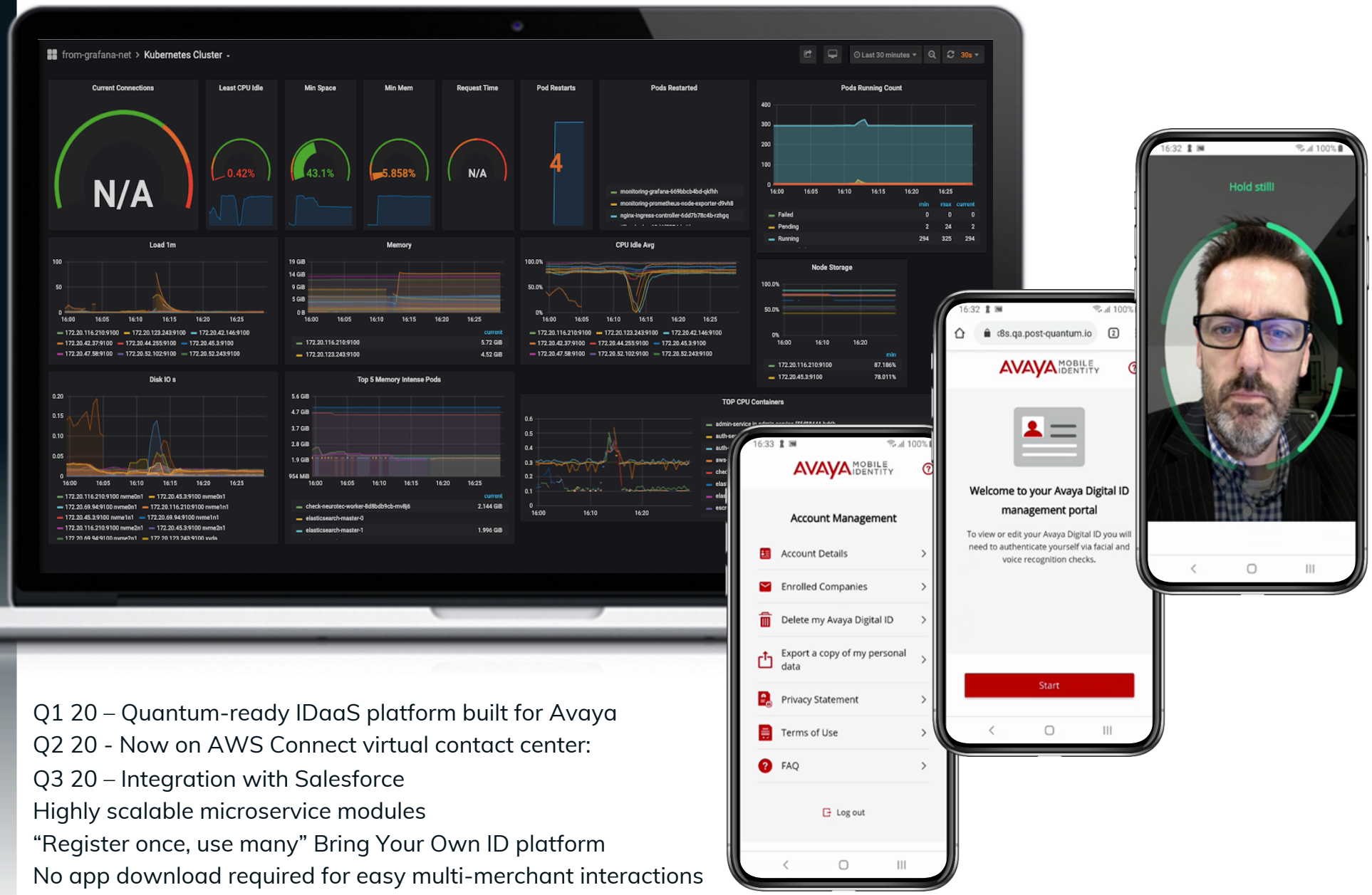
2026

Post-Quantum customers have quantum-ready solutions now with crypto agility

Other customers start thinking after NIST decision

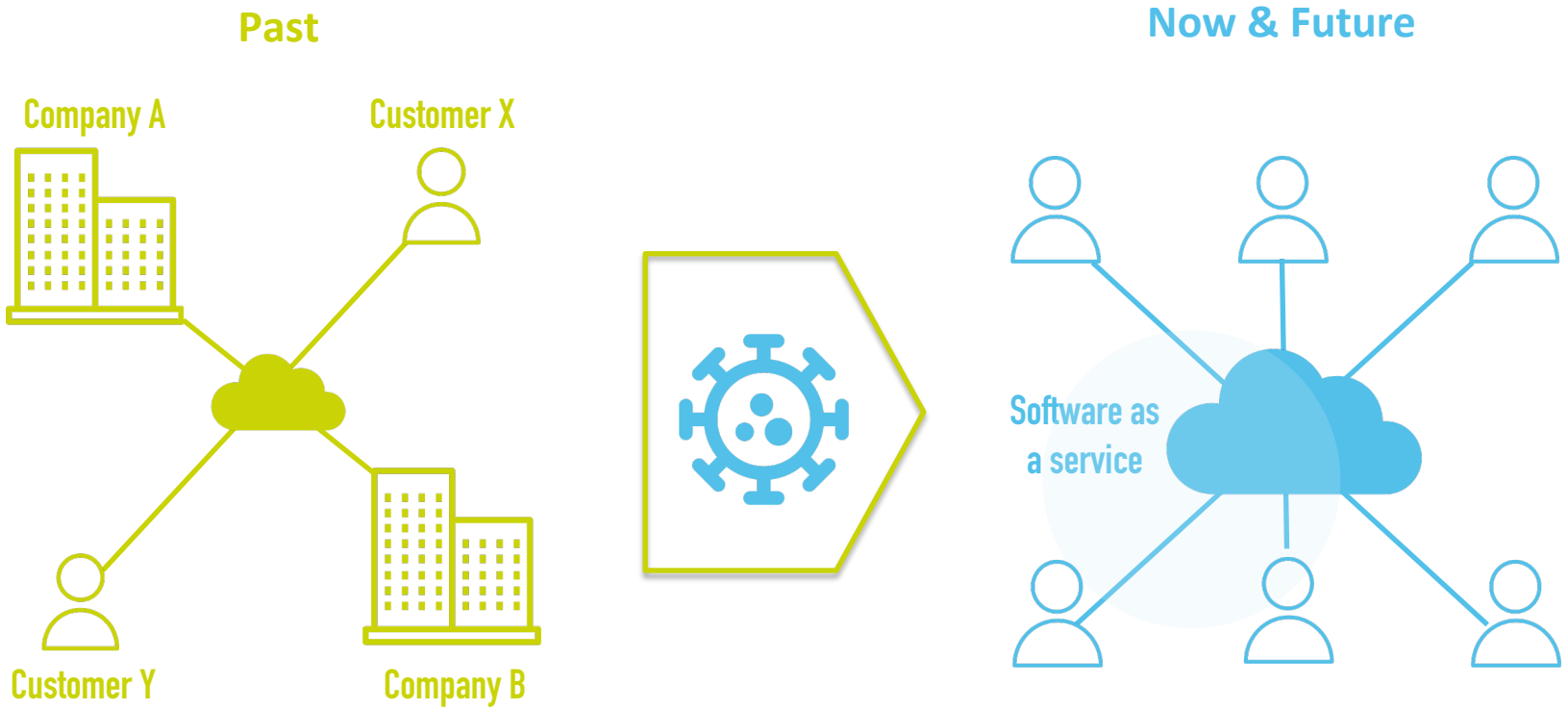
Data Risk Zone | **Initial Risk Zone** | **High Risk Zone**

QUANTUM-READY IDENTITY SOLUTIONS



- Q1 20 – Quantum-ready IDaaS platform built for Avaya
- Q2 20 - Now on AWS Connect virtual contact center:
- Q3 20 – Integration with Salesforce
- Highly scalable microservice modules
- “Register once, use many” Bring Your Own ID platform
- No app download required for easy multi-merchant interactions

PROBLEM HAS BEEN FURTHER ACCELERATED BY COVID-19



Enterprise centric & cloud solutions for
INDIVIDUAL employees and customers

We are now all on our own as
BOTH employees and customers

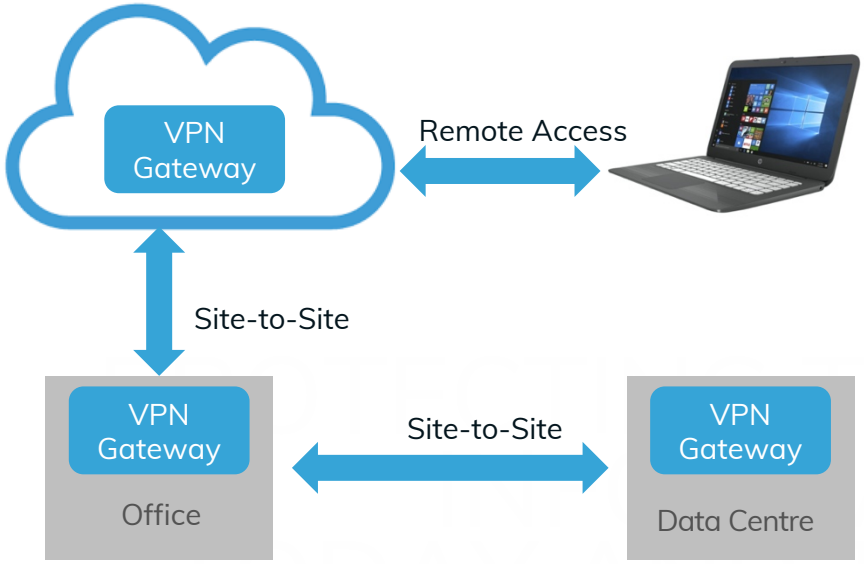
Problems are getting worse in:
End to end security, Authentication and Authorisation

Remote identity authentication and authorisation are key to everything:
Nomidio IDaaS is Post-Quantum's **first quantum-ready solution in Unified Identity**

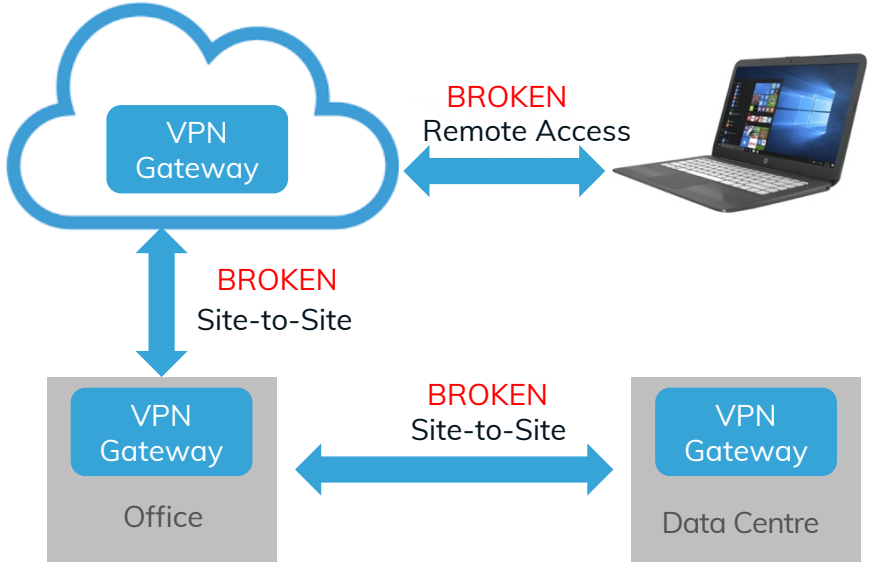
NomiDio

WE ARE ALL ON OUR OWN NOW, AND ALSO IN THE FUTURE

Now



Later

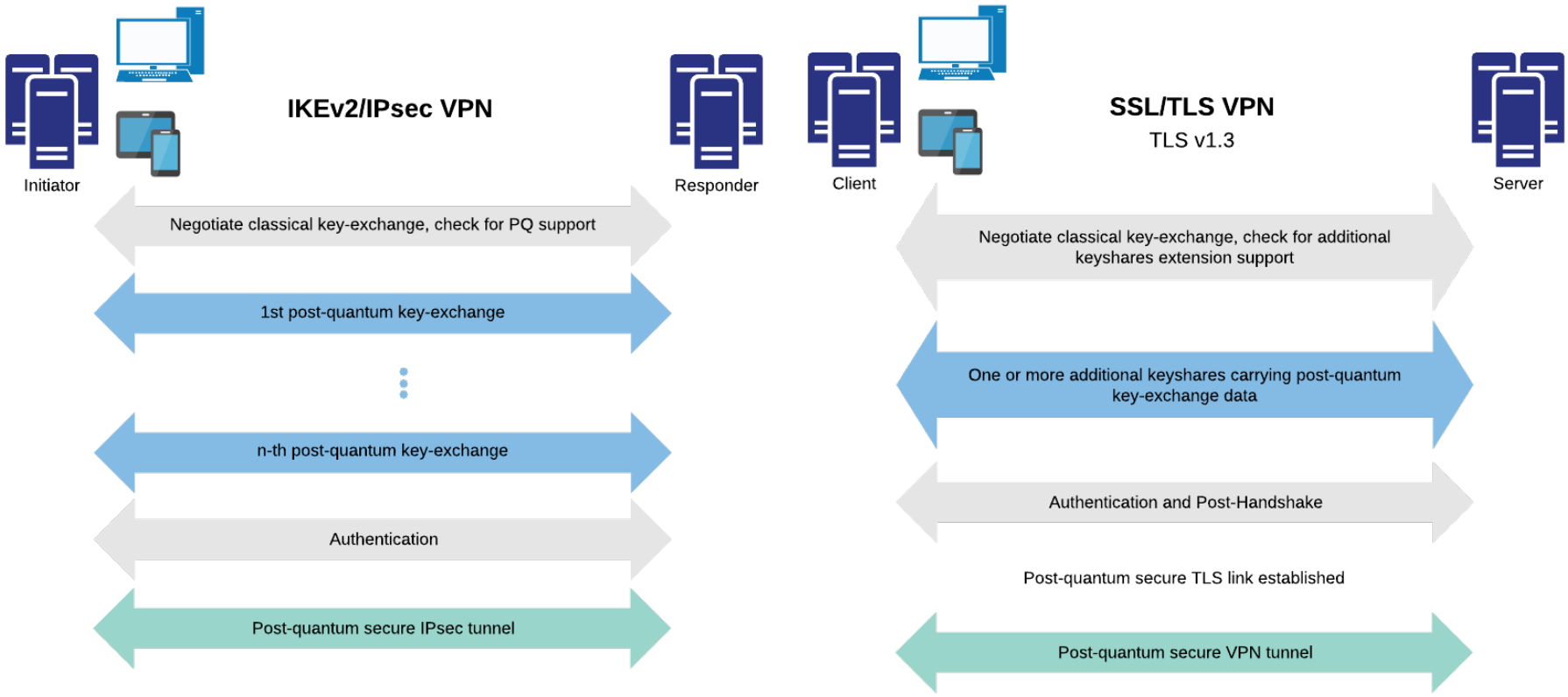


WHERE DO WE GO NEXT → PQ VPN

COVID-19 PARADIGM SHIFT HAS ACCELERATED THE NEED FOR A PQ SECURE VPN

- Remote working is the “New Norm”
- Increasing use of clouds means more and more data will be intercepted and harvested for future cracking
- No employer can afford to install security individually at each house
- We need a new way to secure our data transmission
- Our Hybrid PQ VPN fully protects data - today and tomorrow
- → The market size is the entire remote working world

IETF PQ VPN


Initiator
IKEv2/IPsec VPN
Responder
Negotiate classical key-exchange, check for PQ support
1st post-quantum key-exchange
n-th post-quantum key-exchange
Authentication
Post-quantum secure IPsec tunnel
Client
SSL/TLS VPN
TLS v1.3
Server
Negotiate classical key-exchange, check for additional keyshares extension support
One or more additional keyshares carrying post-quantum key-exchange data
Authentication and Post-Handshake
Post-quantum secure TLS link established
Post-quantum secure VPN tunnel

EXPERIENCED ENTREPRENEURS IN SECURITY & FINANCIAL SERVICES

Andersen Cheng
Founder & CEO
+ Director of L3-TRL and Honeywell Satamatics
+ Founder member of LabMorgan, London
+ European Head of Credit Risk, JP Morgan
+ COO of Carlyle European Venture Fund
+ FCA, ICAEW
+ MSc – Imperial College

CJ Tjhai
Founder & CTO
+ Inventor of PQ crypto protocols being standardised by NIST/IETF
+ Government grade mission critical solutions
+ Expert at translating and optimising inventions for commercial use
+ 30+ patents
+ PhD – Plymouth

Martin Tomlinson
Founder & CSO
+ Director of L3-TRL and Honeywell Satamatics
+ Critical satellite comms at RSRE (now QinetiQ)
+ Inventor of PQ crypto protocols being standardised by NIST/IETF
+ 55+ patents
+ PhD – Birmingham

James Matthews
CFO/COO
+ 20 years' experience working with tech startups
+ Senior finance and operations roles at Universal Music Group
+ Adjunct Professor at Hult Business School
+ ACMA/CGMA
+ MBA - INSEAD
+ MA - Oxford

Ben Todd
VP Worldwide Sales
+ 25+ years in sales
+ Sales Director of cyber security at Cisco
+ Sales Director at Lancope (acquired by Cisco)
+ Sales Director of Central Telecom and Touchbase
+ BA – Cardiff

Philip Black
Commercial Director
+ Senior sales and business development roles at Huntsman Security, Brainstorm, Netname
+ Security program management roles at Oracle and Logica
+ BSc – Hull

Brian Snow
Technology Adviser
+ Ex-NSA Technical Director
+ Head of Cryptology and Information assurance
+ Security and ethics adviser
+ Advocate in quantum computing threats
+ PhD - Colorado

Tom Glocer
Business Adviser
+ Ex-CEO of Thompson Reuters
+ Chairman of Bluevoyant
+ Board member:
  - Morgan Stanley
  - Merck
  - Linklaters
+ BA – Columbia
+ JD - Yale

TRL Technology
one step ahead
satamatics
J.P.Morgan
THE CARLYLE GROUP
Goldman Sachs
UNIVERSAL
Morgan Stanley
CISCO
Imperial College London
UNIVERSITY OF OXFORD
INSEAD
THOMSON REUTERS
NATIONAL SECURITY AGENCY
GCHQ

JOURNEY OF POST-QUANTUM

- Top secret grade heritage through TRL & Satamatics
- Highly scalable and “Cannot Fail” security following 10 years’ R&D
- End-to-end architecture that will become the new core of commerce
- Pioneers in quantum-safe enterprise security technology – PQChat, Nato, NCSC
- Nomidio IDaaS is the first quantum-ready solution
- PQ VPN will bring PQ security to post-COVID-19 “New Norm”

BARCLAYS

NATO OTAN

National Cyber Security Centre
a part of GCHQ

NIST

HITACHI

AVAYA

amazon

SUMMARY

- Quantum supremacy no longer a science problem but an engineering problem
- Post-quantum protection essential for critical systems and long term data storage
- Government urgency completely changed in the past 2-3 years
- Protocol standards will be set in the next 2-3 years
- Must start future proofing systems now
- Crypto-agile approach(hybridisation) the best for smooth migration to counter Cyber Armageddon

FINALLY

- We were lucky enough to have trademarked “Post-Quantum” and “PQ” before anyone else was remotely interested
- Industry publications and research firms such as Gartner have formalised these two terms as a standalone category and standard web search keywords
- This means “post-quantum” is already seen and used in the same way as “hoover”, “google” and “photoshop” as both brand and generic reference term
- We have always come top in all the search engines without having spent any money on SEO
- The following is potentially a new business line and our competitors will then be Nike and Adidas! ;-)

LET'S JOURNEY TOGETHER INTO THE POST-QUANTUM WORLD!

Andersen Cheng, CEO
ac@post-quantum.com

post-quantum.com
Nomidio.com