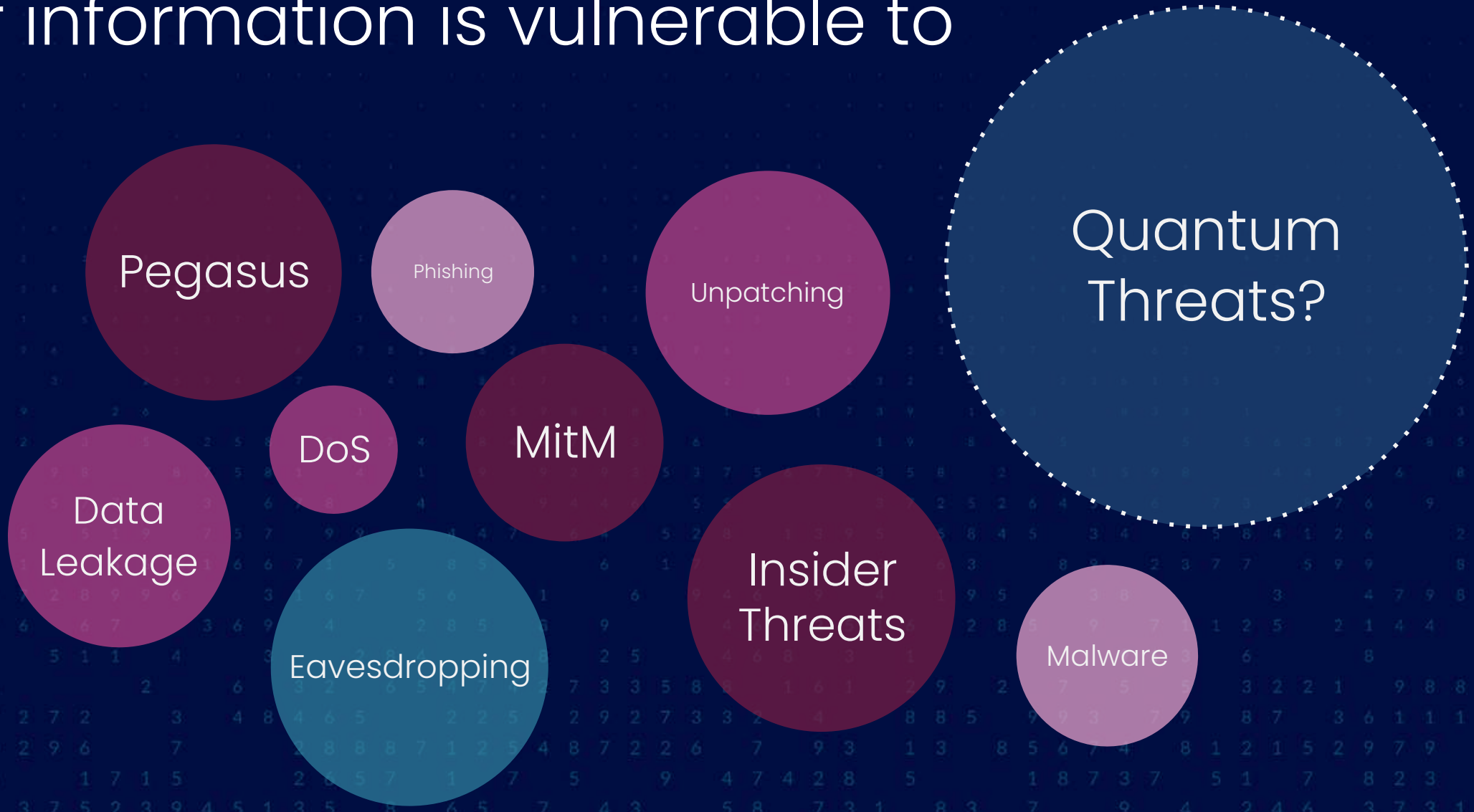
QuantPaths

The future of cybersecurity

POST QUANTUM, GLOBAL AND ULTRA-SECURED
COMMS, IN ONE SPOT

THE PROBLEM WITH UNENCRYPTED DEVICES

Your information is vulnerable to



DIFFERENCES BETWEEN SYSTEMS

Binary Computing

✓ Bit is the basic unit. A bit can only have one value at a time: 1 o 0.

✓ Classic computers have components like CPU, RAM memory and a screen.

✓ The binary coding is adequate for usual and complex tasks in varied spheres such as scientific and business.

Quantum Computing

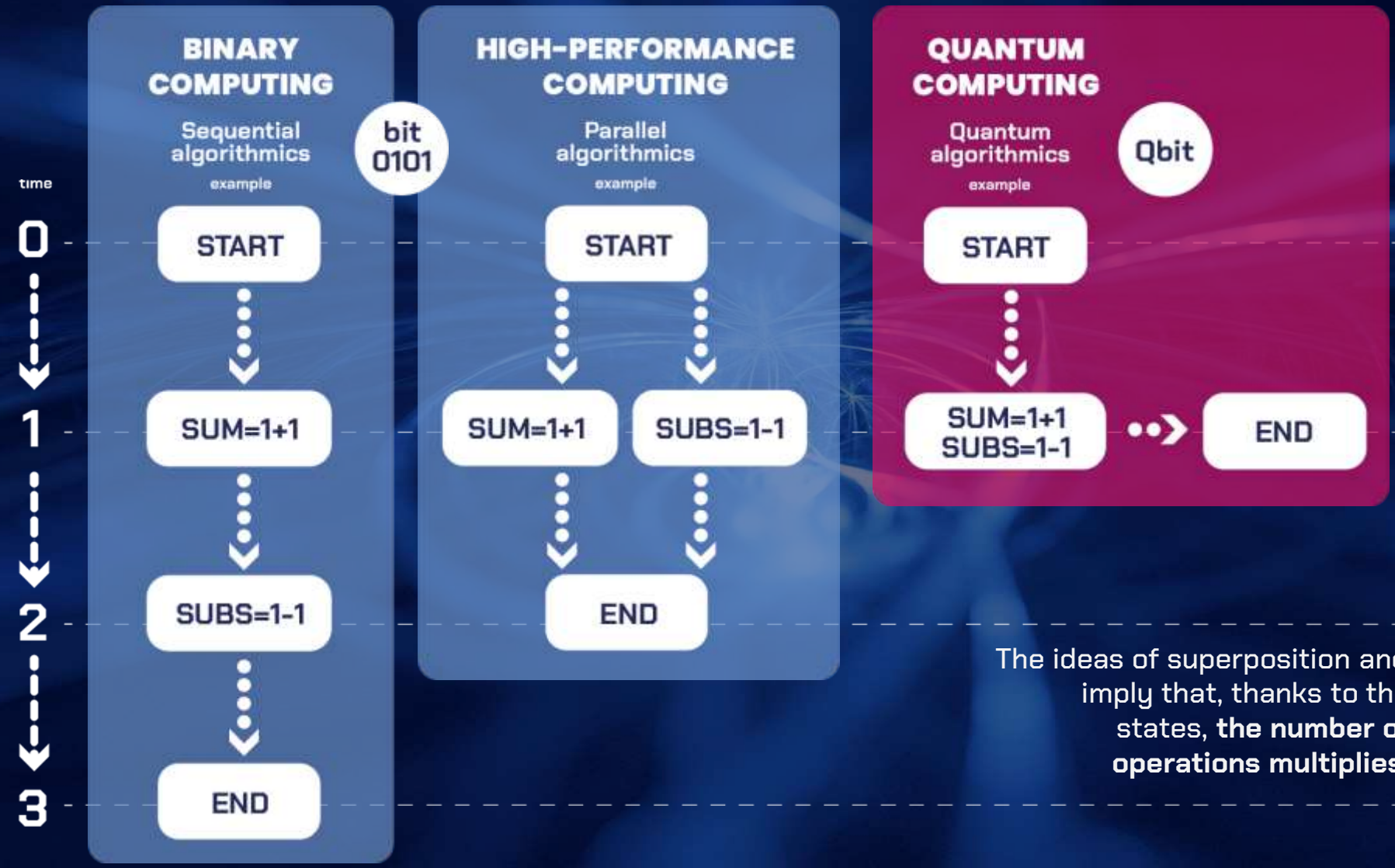
✓ Qubit is the unit of reference. it is expressed in qubits.

✓ A quantum computer is a sealed cubicle with a metallic structure and a web of cables, operated from external conventional computers

✓ It is **designed for significative complex operations**, such as cybersecurity and big data.

✓ It is extremely sensitive to environmental conditions, requiring temperatures close to -273 °C and isolation from the Earth's magnetic field to work properly.

DIFFERENCES BETWEEN SYSTEMS



The ideas of superposition and entanglement imply that, thanks to the multiplicity of states, **the number of simultaneous operations multiplies exponentially.**

IMPLICATIONS OF

Quantum Computing

Quantum computing offers significant economic and scientific opportunities.

Nevertheless, it also accelerates the emergence of new security risks, especially the possibility of breaking public-key encryption, which is essential for the security of the financial sector and government comms.

The consequence of not being prepared for the quantum technology is leaving your secrets exposed.

RISKS & OPPORTUNITIES

Quantum Computing

40% of organizations are taking proactive measures to understand quantum threats*.

Quantum risk evaluation

40% of organizations have started to take measures.

Surveillance against threats

Many organizations are vigilant against threats like "Harvest now, Decrypt Later".

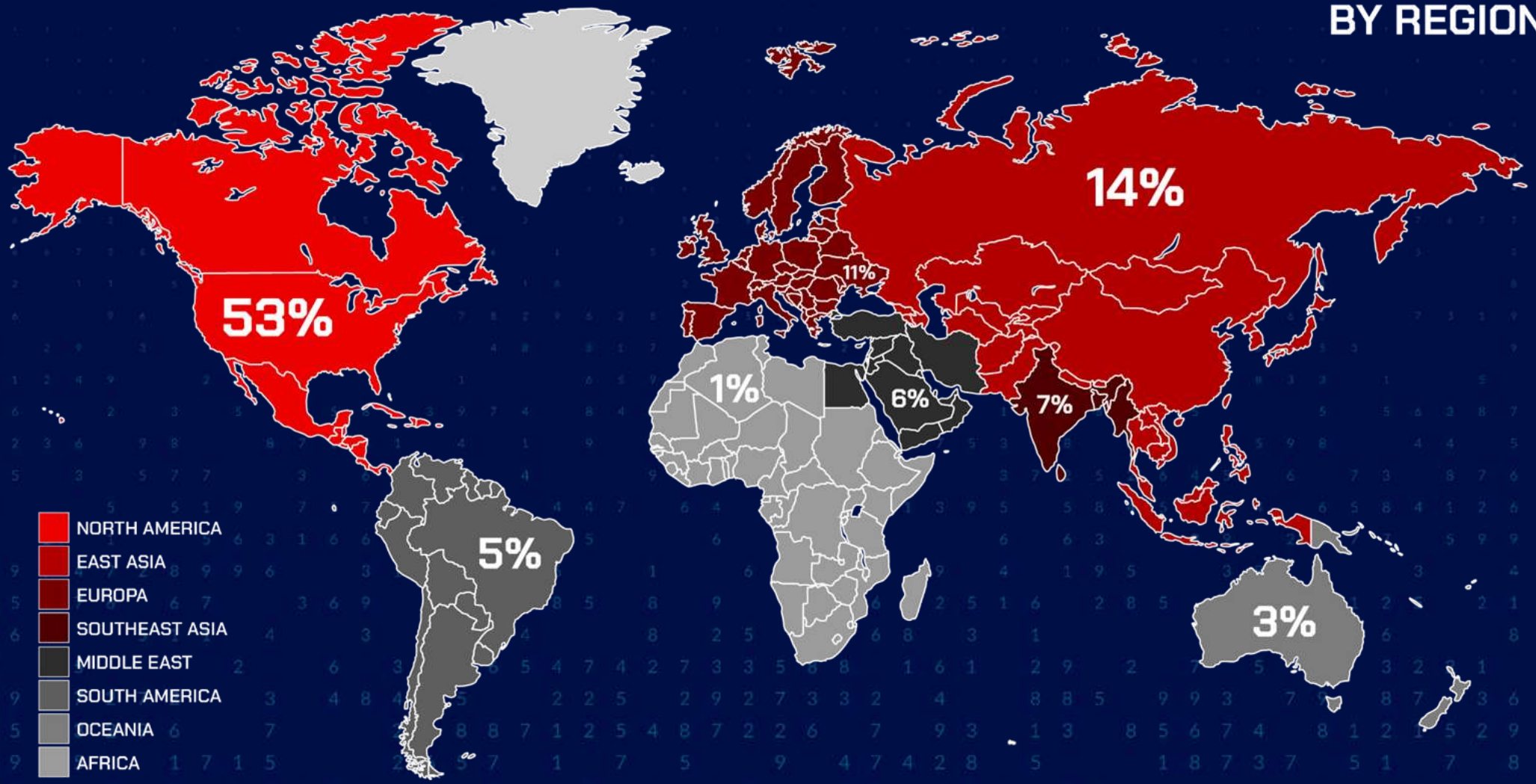
Recommendations & standards

Multiple efforts have been made to drive action, including recommendations from the G7 Cyber Security Expert Group and the publication of post-quantum cryptography algorithm standards by NIST.

*Source: Global Cybersecurity Outlook 2025, WEF & Accenture

STATE OF THE ART IN CYBERSECURITY 2025

INTERACTIVE INTRUSIONS BY REGION



Source: Repositorio Europeo de Accidentes Cibernéticos

STATE OF THE ART IN CYBERSECURITY 2025

Present and future of quantum computing

All major tech companies are involved in the development of this technology, from **IBM** to **Google** to the point of prototyping 'desktop models'.

However, the 'real' world is still very far off, as the prototypes are very basic and the drawbacks of their sensitivity to environmental conditions greatly limit their practical application.

Although it seems clear that the application of quantum computing will be limited to specific areas of our world that, due to their complexity, require super powerful computer equipment, it is positioned as a **mighty ally in cybersecurity**, as demonstrated by data encryption developments, such as **Quantum Key Distribution (QKD)**.

CHALLENGES TO SOLVE

Low Security in Data

✓ Encryption methods are increasingly **vulnerable.**

✓ There is only one way to be safe in the **post-quantum era.**

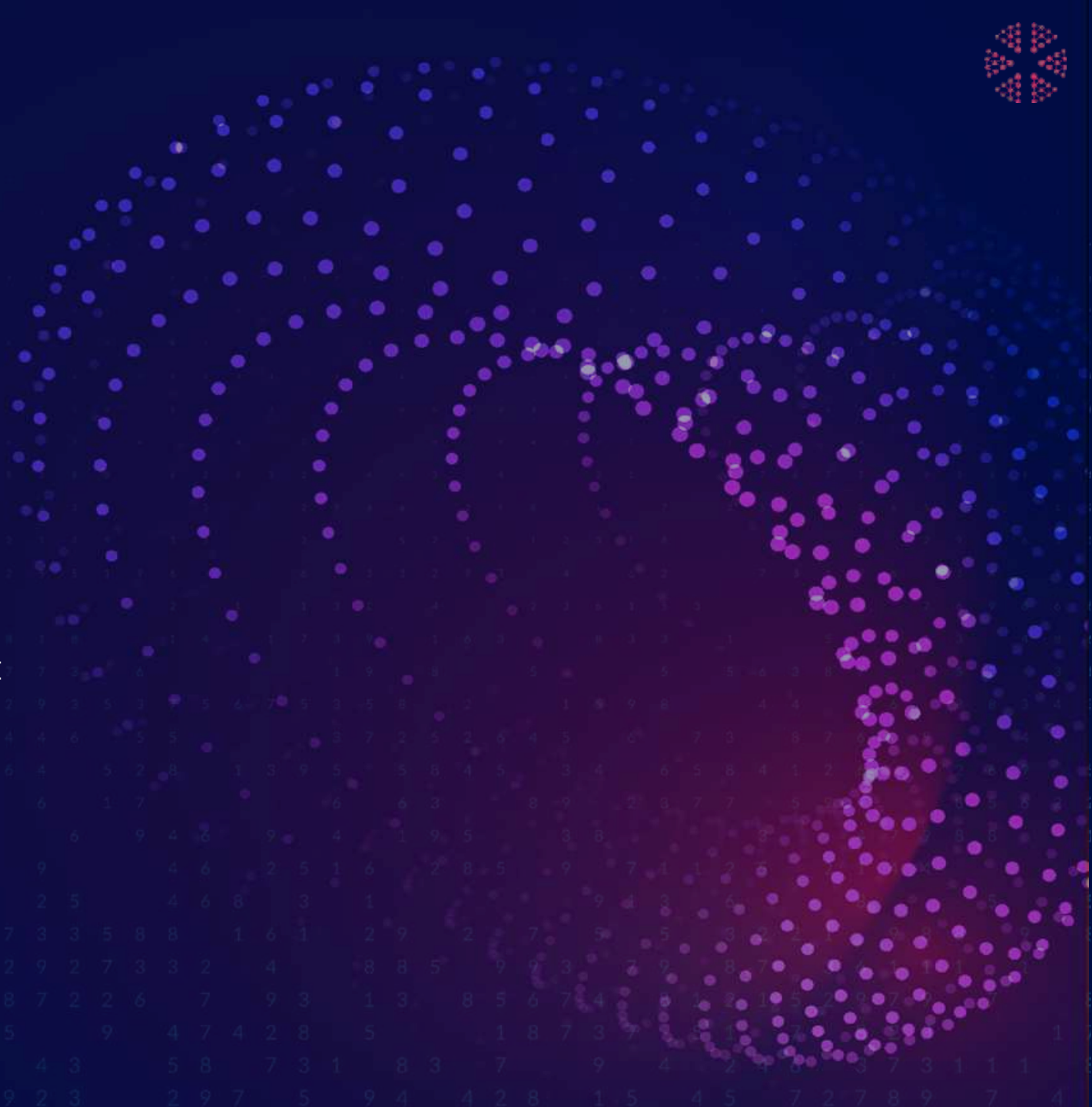
✓ The current offering is in its **early stages.**

CHALLENGES TO SOLVE

Security Challenges

✓ **Basic cybersecurity systems**. You get what you pay for.

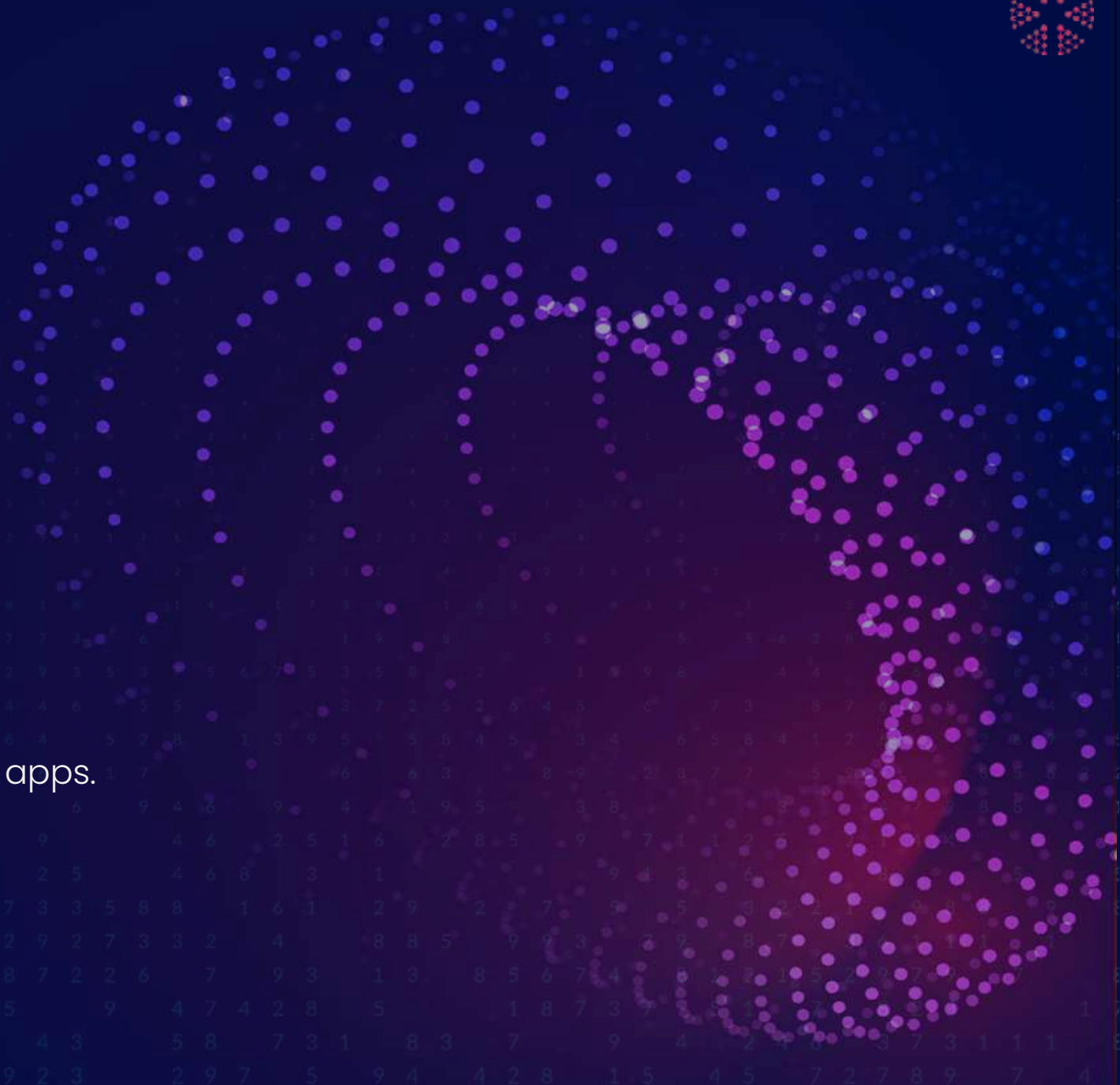
✓ **Corrupted, non-debugged encryption systems** by various actors(Open Source)**.**



CHALLENGES TO SOLVE

Lack of trusted offering

- ✓ **Reduced offerings** of systems and devices.
- ✓ Lack of support and **consulting** services**.**
- ✓ **Limited options** from certified cyber security apps.



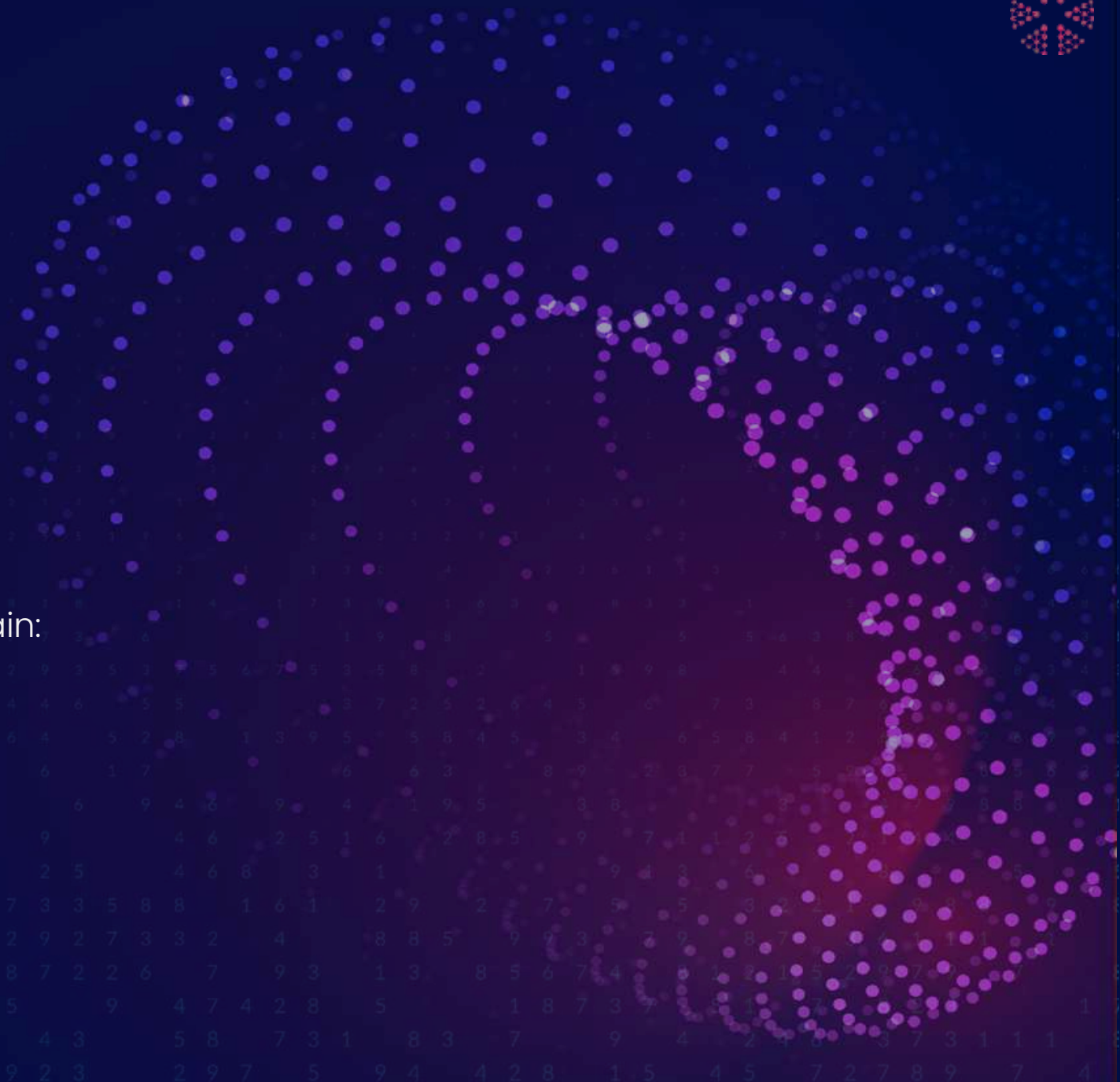
CHALLENGES TO SOLVE

System vulnerabilities

Cyber resilience is increasingly harder to sustain:

✓ The attacks shows progressively greater sophistication.

✓ Lack of resources and capabilities to implement effective security measures.



WHO WE ARE

QuantPaths

The cybersecurity organization that provides consulting services, develops and offer solutions to implement **data** security with post quantum encoding protection.

Devices

Compatible under MSQuantum license (encrypted messaging) included in the phone.

Applications

Improve the security with secure comms like encrypted mail and storing.

IT Environment

Consulting in best practices in security and implementation of post quantum encryption, working globally with your IT Department.

OUR RANGE OF

Solutions

Our portfolio includes cybersecurity consulting, enablement of AI-based post-quantum algorithms and security product development.

ADVANTAGES OF

Our offering

Our approach is based on layers of security that enable:

- Exclusive user control of all data
- De-risk unauthorized access
- Specialized IT team and direct client support.

OUR

Product

An unparalleled device, certified by:

BlackBerry

Encrypted with **post-quantum infrastructure** that protects mobile communications, with global coverage

- ✓ No current certified competitors
- ✓ Intuitive and simple interface
- ✓ Infrastructure under post-quantum certified network
- ✓ Communication with encrypted apps without risk of cyber attacks

OUR ALLIES IN

Academia

DE MONTFORT UNIVERSITY LEICESTER

Thanks on behalf of

QuantPaths

¿Do you like to see a demo?
Write us:

info@quantpaths.com

Phone:
+57 321 225 00 10

www.quantpaths.com

Access the presentation