NSA CYBERSECURITY

CNSA 2.0 and New Security Requirements

MORGAN STERN, PHD
MARCH 17, 2026

What is a National Security System?

The Director of NSA serves as the National Manager for US National Security Systems, giving NSA the authority to set requirements for cryptography across this area. This is a key part of NSA's Cybersecurity mission.

Most systems run by the Department of Defense or Intelligence Community fall under this "National Security System" classification.

- Department of Defense has well over a million employees who need secured communications with minimal downtime, with many deployed to locations across the world.
  - NIPRNet, which has been up since the original ARPANET
- Classified networks
- Industrial control systems owned by Department of Defense
- GPS
- Weapon systems

A little history of commercial standards in NSS

2001	CNSSP-11 lays out that commercial-off-the-shelf products intended to protect National Security Systems must be validated using the FIPS and NIAP processes
2005	Suite B announced, laying out the use of commercial standards for public key to be used to protect National Security Systems
2016	CNSSP-15 updated to address the quantum threat, and introducing CNSA 1.0
2022	National Security Memo 10 signed making it an aim of US to be off quantum vulnerable crypt by 2035 NIST announces specific quantum resistant algorithms they intend to standardize and NSA announces their future quantum resistant suite, CNSA 2.0
2025	CNSSP-15 updated to deprecate CNSA 1.0 and provide timelines for transition to CNSA 2.0
2026	Protection Profiles released and transition ramps up

Commercial National Security Algorithm (CNSA) 2.0 Suite

Quantum Resistant Cryptography approved to protect commercial National Security Systems

Algorithm	Purpose	Relevant NIST standards
General purpose algorithms		
AES-256	Block Cipher	FIPS 197
SHA-384 or SHA-512	Cryptographic Hash	FIPS 180-4
ML-KEM-1024	Public Key Establishment	FIPS 203
ML-DSA-87	Digital Signature	FIPS 204
Specific use case algorithms		
LMS or XMSS (LMS 256-192 recommended)	Software/Firmware Signature	SP 800-208
SHA3-384 or SHA3-512	Hashing in internal hardware (e.g. secure boot)	FIPS 202

We do not anticipate any major revisions to this list over the course of the quantum resistance transition

Additional guidance available at https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

CNSA 2.0 Quantum Resistance Timeline*

2022
CNSA 2.0 Released

2024
CNSA 2.0 Finalized

2027
New NSS acquisitions must be QR

2030
All equipment on NSS should be QR capable

2031
All NSS should be QR

2035
NIST proposed date disallowing quantum vulnerable public key

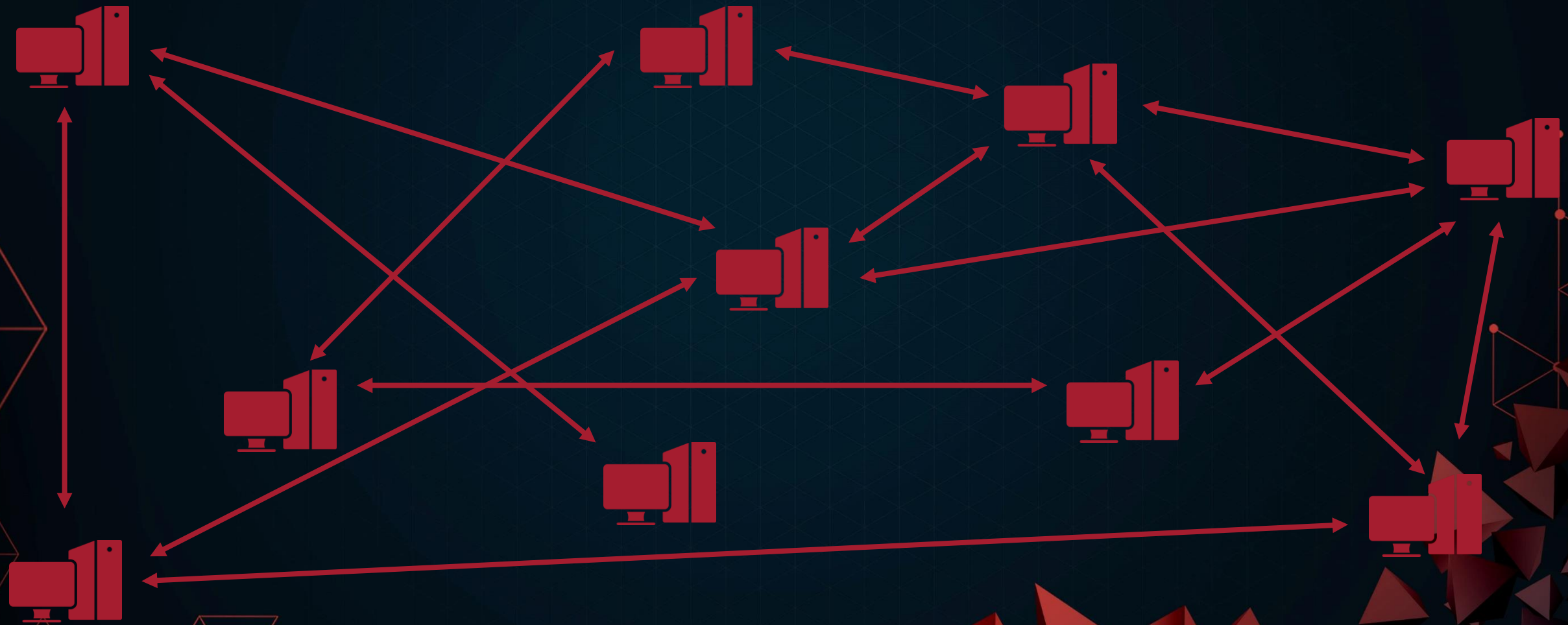
*Specific product lines or technologies and applications will possibly have their own timeline, but barring such separate guidance this is the default

Cybersecurity ramifications of quantum computing

Alice and Bob use the shared secret to key an efficient symmetric algorithm

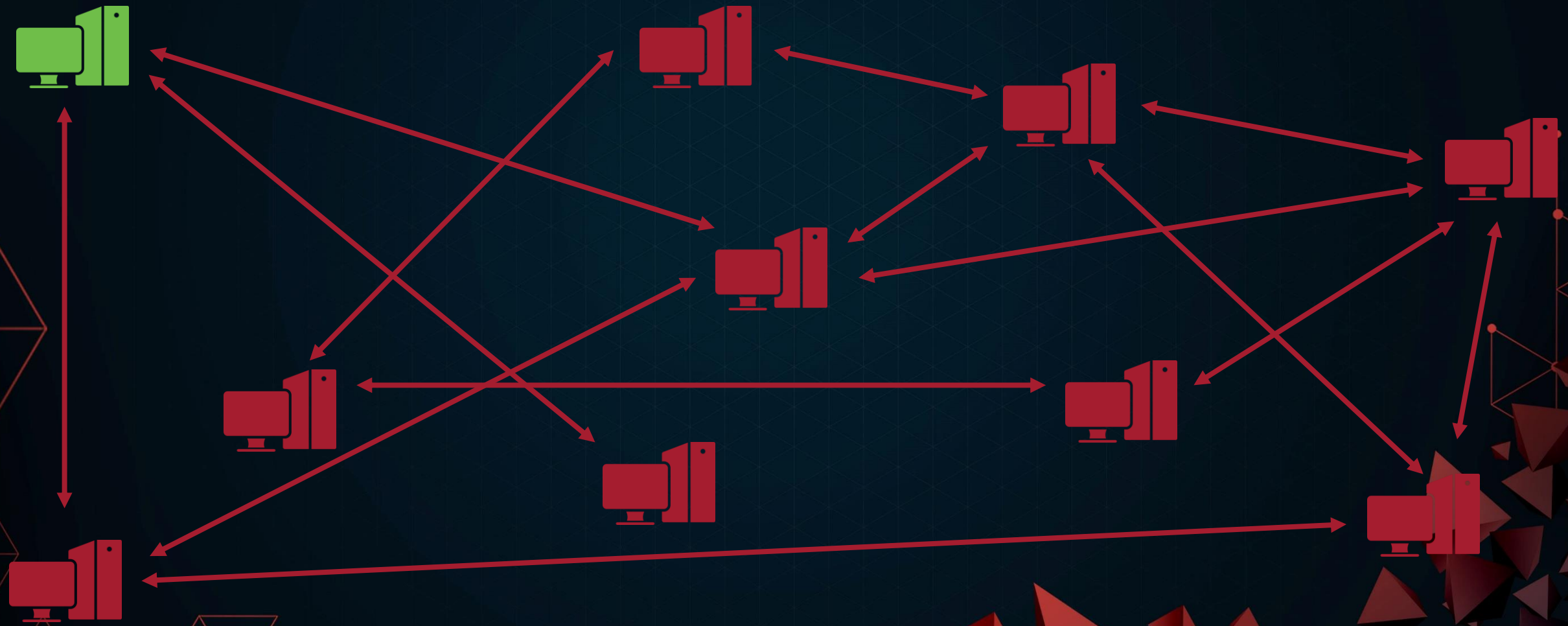
Implementing Quantum Resistance

Confidentiality: When no computers are quantum resistant, all links are quantum vulnerable



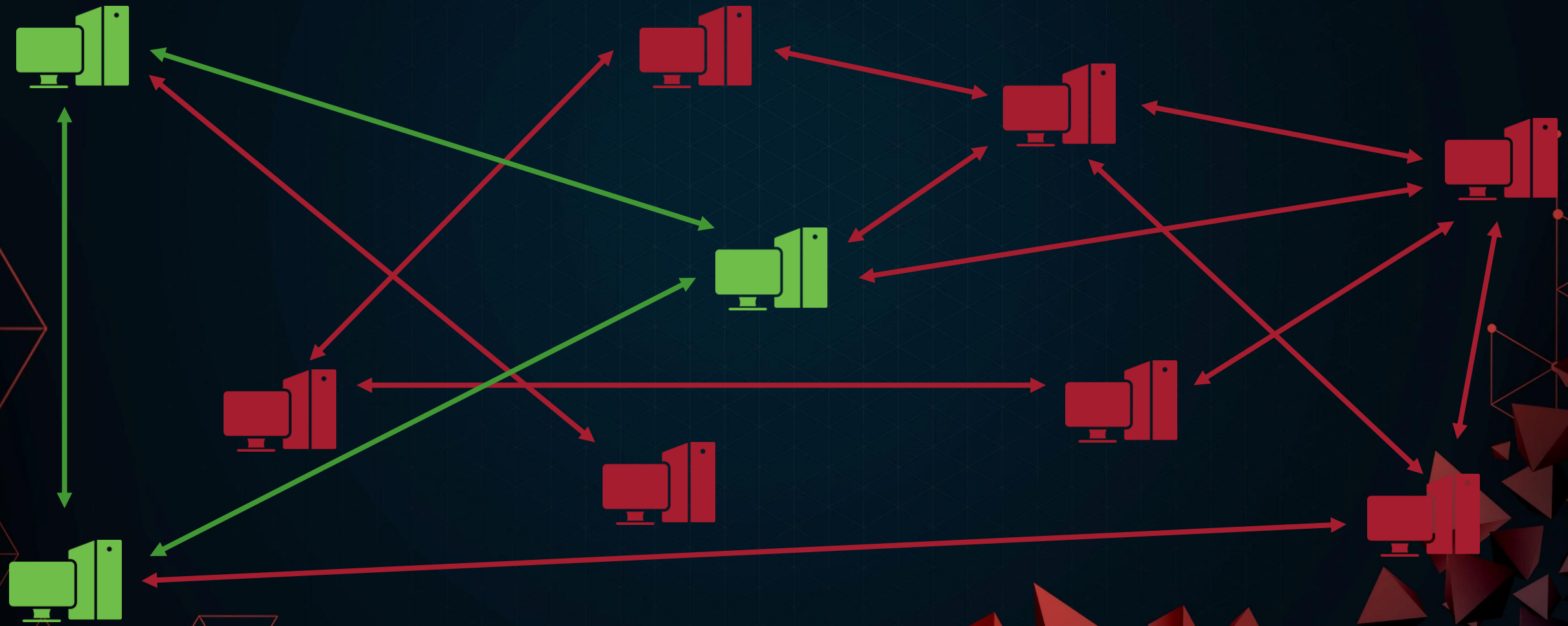
Implementing Quantum Resistance

Confidentiality: A single quantum resistant computer is still quantum vulnerable



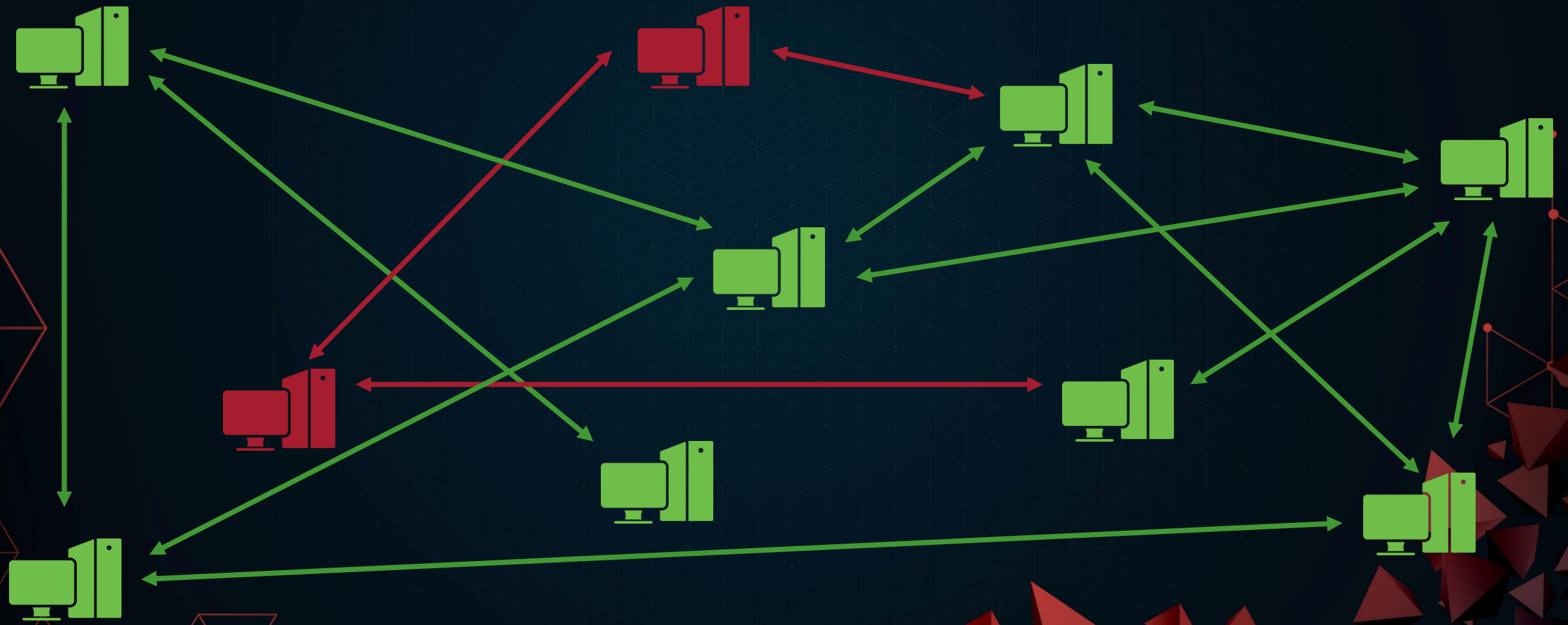
Implementing Quantum Resistance

Confidentiality: As more computers transition, more of the network is secure



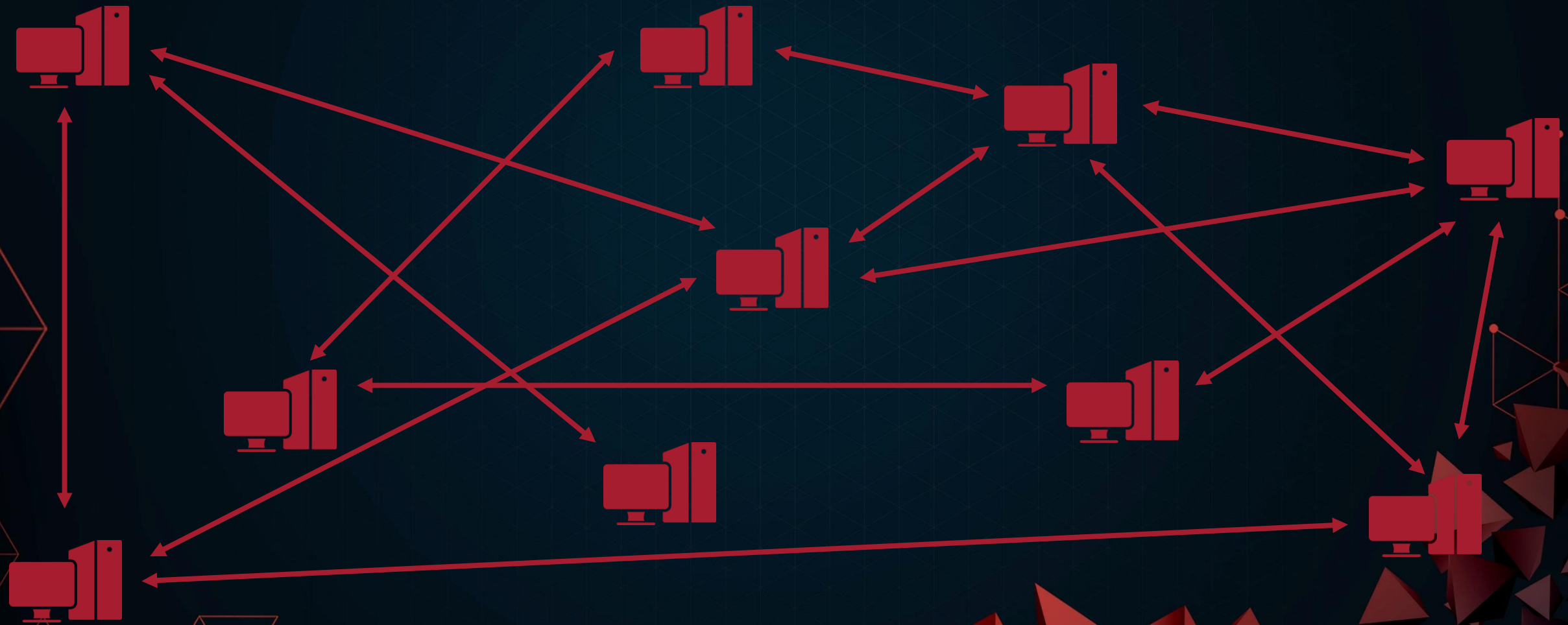
Implementing Quantum Resistance

Confidentiality: When most are quantum resistant, most users' communications are fully secure



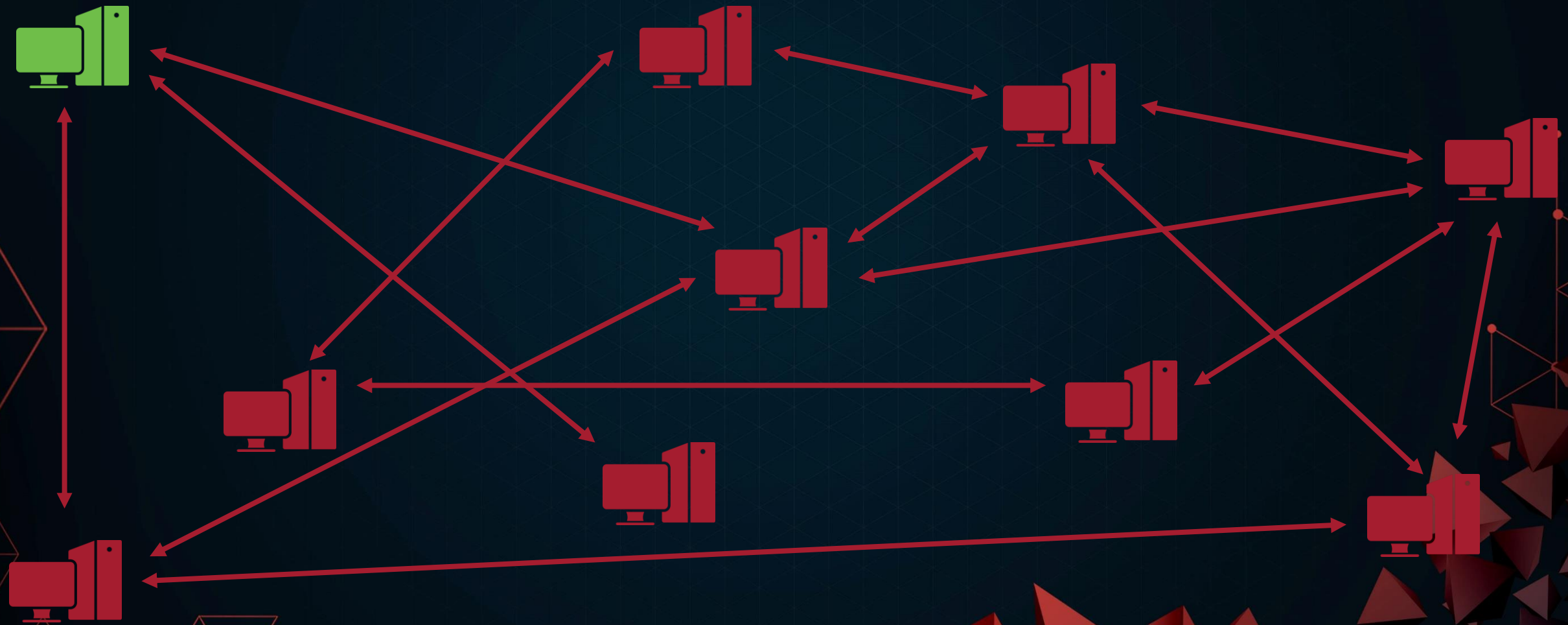
Implementing Quantum Resistance

Authentication: When no computers are quantum resistant, the whole network is vulnerable



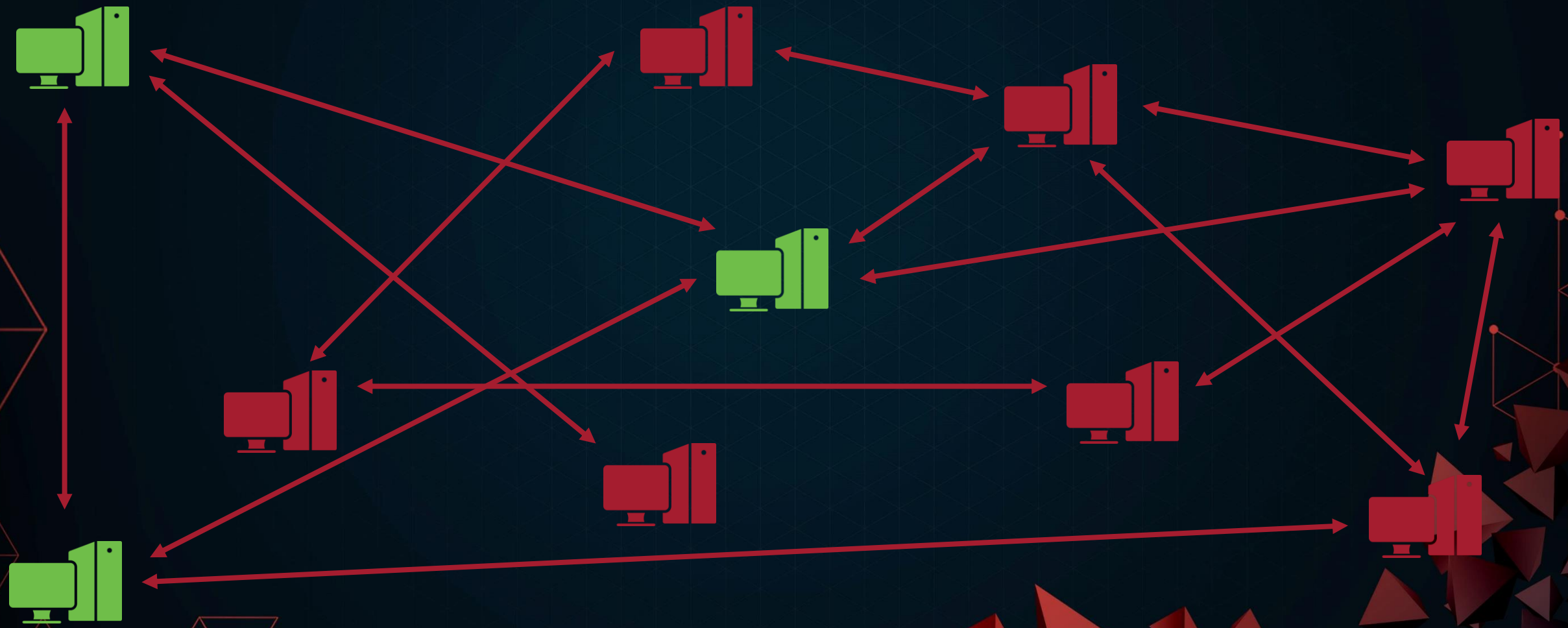
Implementing Quantum Resistance

Authentication: A single quantum resistant identity is still quantum vulnerable



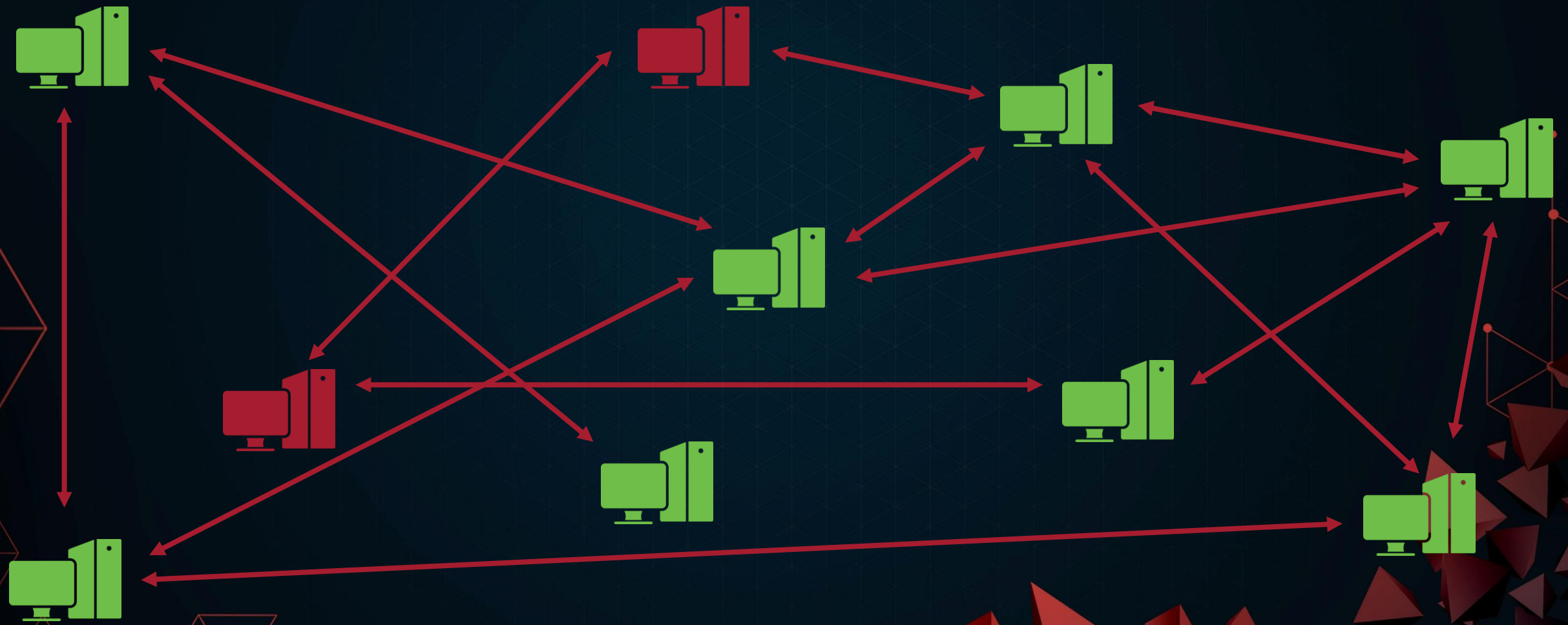
Implementing Quantum Resistance

Authentication: As more identities transition, the network remains insecure



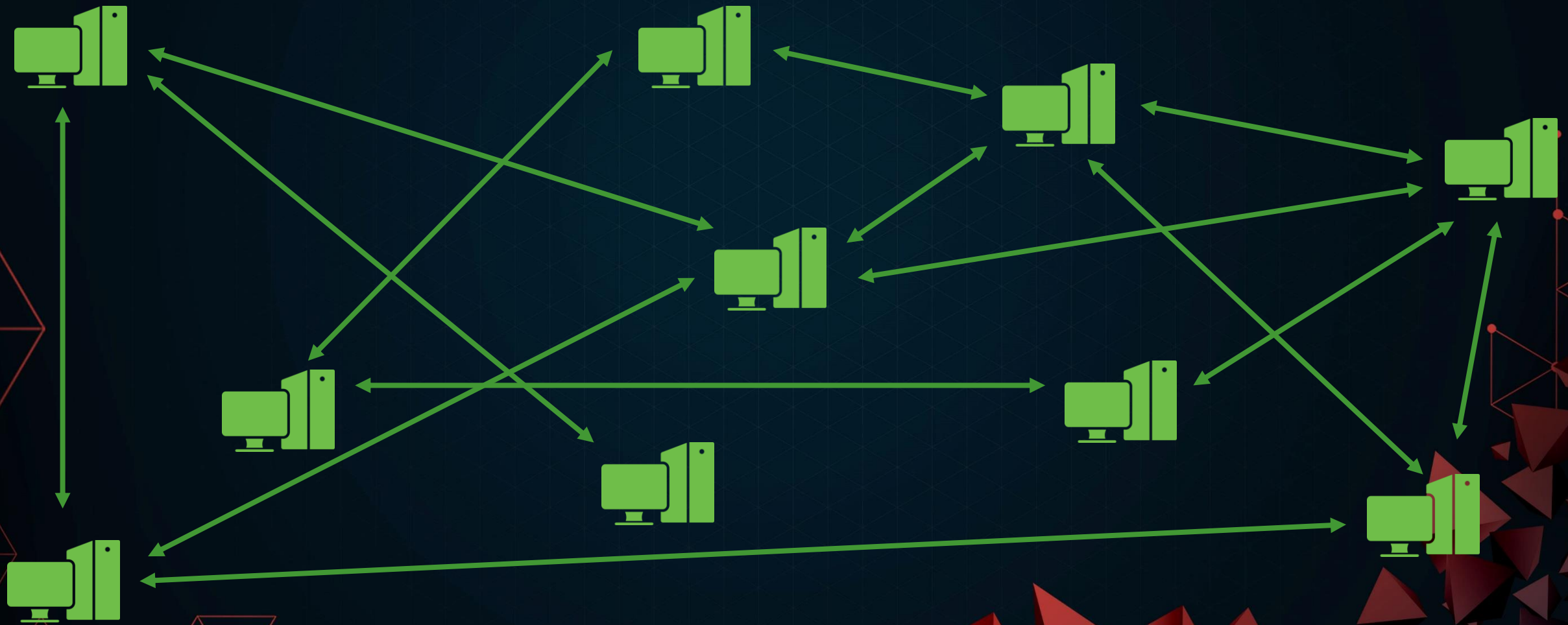
Implementing Quantum Resistance

Authentication: If even a single identity is quantum vulnerable, the whole network is



Implementing Quantum Resistance

Authentication: Only complete transition brings quantum security to the network



Key Takeaways

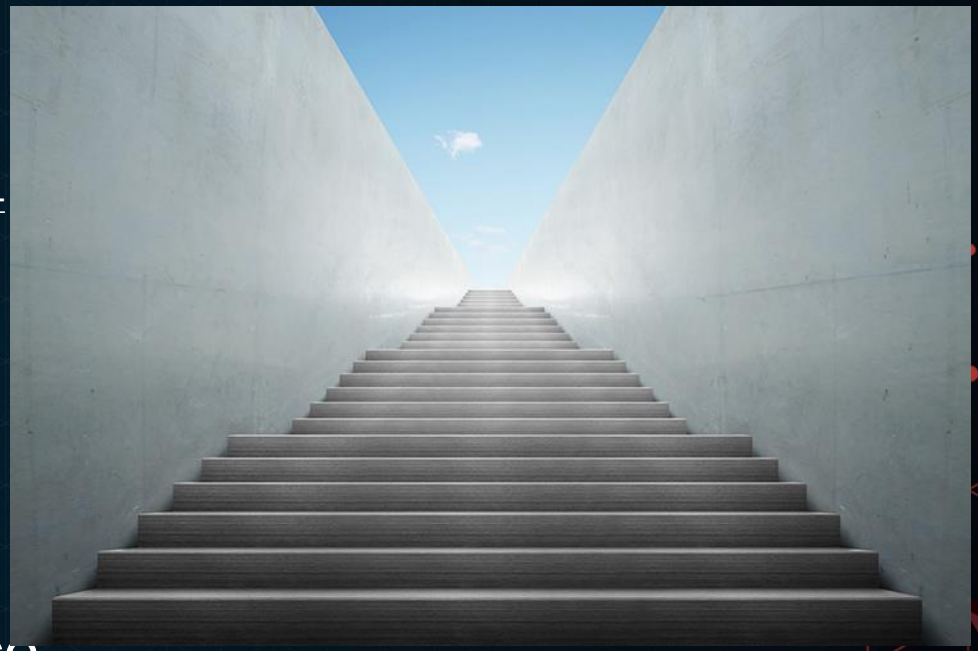
- There are great benefits to starting a quantum resistant transition for encryption, the more devices you transition today the more secure you are in the future
  - When you transition 99% of your devices then 98% of communications are secured*
- Identity management systems are only as secure as their weakest link and if we want to ensure we have any security in a quantum world, we need to begin today.
  - If you have transitioned 99% of a large network, there is still a large number of devices one can masquerade as to any other device on your network.
  - Little short of revoking/expiring quantum vulnerable credentials will bring you quantum resistance

A notional transition schedule

- Year 0:
  - Commit to ensuring all new acquisitions are capable of quantum resistance
  - All new gear has a quantum resistant hardware root of trust
- Year 1:
  - Stand up a quantum resistant root for your infrastructure
  - New devices opportunistically encrypt with quantum resistant key agreements
- Year 2:
  - Issue quantum resistant credentials to all new devices
  - Continue to issue traditional credentials to devices as needed
- Year 3:
  - Switch to fully quantum resistant protocols via software updates as needed
  - Begin to deliberately retire old equipment that cannot be upgraded
- Year 4+: Consider turning off your traditional PKI root

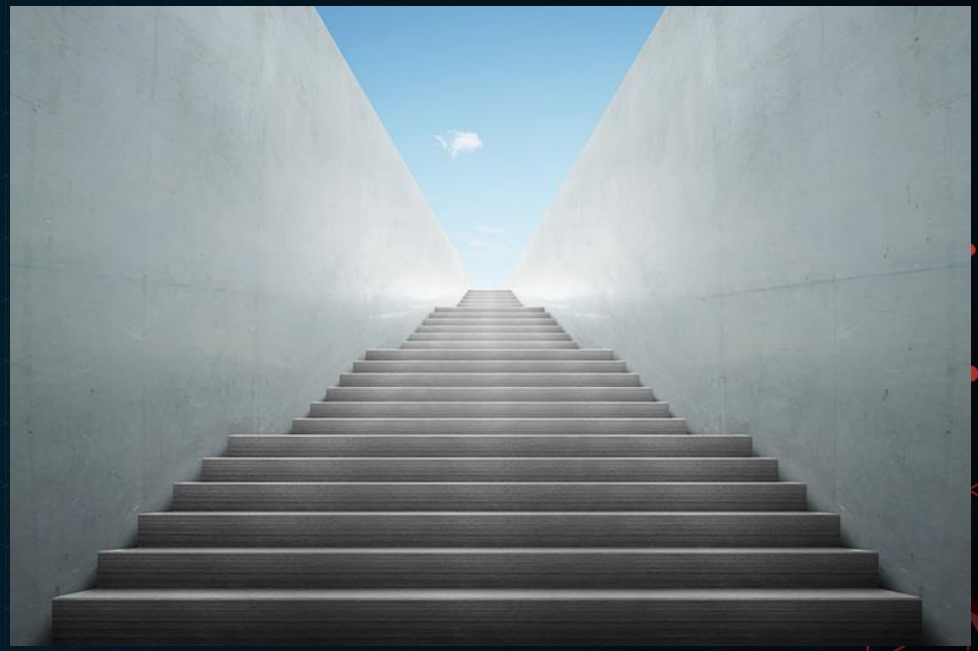
Concrete Steps Today

- Enable us to hit our 2027 acquisition requirements: commit to transition roadmaps
  - Help fill in CISA's PQ product categories https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards
- Ensure all new hardware can at least be upgraded to full QR
  - Likely requires a QR signature for the root of trust
- Update standards to support quantum resistance
  - Ensuring ML-KEM-1024 supported
  - CNSA supports ML-DSA-87, not HashML-DSA-87
- **Set up quantum resistant Certificate Authorities**



NSA's steps

- DoW PKI plans to stand up an quantum resistant root in 2027
- Published 6 RFCs to support CNSA 2.0
- All NSA-authored Protection Profiles will be rewritten by the end of this year.
  - At a minimum, all require quantum resistant update functionality, and many will achieve full quantum resistance



Questions?