Kyber Odyssey
Charting a course for secure innovation in a post-Crowdstrike world

Matt A. Porter, B.S[1], Marcheta J. Hill, DO[2], Dawn L. Laporte, MD[3], Amiethab A. Aiyer, MD[3]

[1]Qompass, Spokane, WA

[2]Arnot Ogden Medical Center Emergency Medicine Residency Program, Elmira, NY

[3]The Johns Hopkins University School of Medicine, Department of Orthopaedic Surgery, Baltimore, MD

ORTHOMENTOR

ArnotHealth
It's what we do

One faulty cybersecurity configuration

:(

Your PC ran into a problem that it couldn't handle, and now it needs to restart.

BANK

:(

11+ Hospitals −$1.94B

10+ Banks −$1.15B

20+ Airlines −$550M
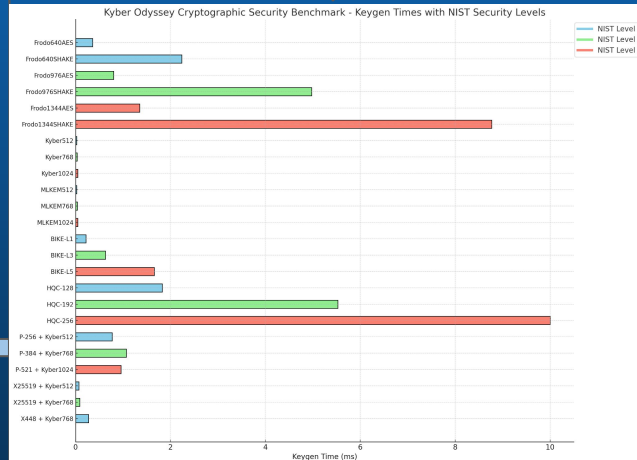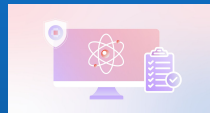
8.5 Million Computers affected

Post−Quantum Cryptography (PQC)

NIST

NSF

Reliable Security For All

We compiled and tested 24 NIST encryption algorithms on−device for $0

oqs

Open SSL

Kyber Odyssey Cryptographic Security Benchmark - Keygen Times with NIST Security Levels

NIST Level 1
NIST Level 3
NIST Level 5

Frodo640AES
Frodo640SHAKE
Frodo976AES
Frodo976SHAKE
Frodo1344AES
Frodo1344SHAKE
Kyber512
Kyber768
Kyber1024
MLKEM512
MLKEM768
MLKEM1024
BIKE-L1
BIKE-L3
BIKE-L5
HQC-128
HQC-192
HQC-256
P-256 + Kyber512
P-384 + Kyber768
P-521 + Kyber1024
X25519 + Kyber512
X25519 + Kyber768
X448 + Kyber768

Keygen Time (ms)

We recommend adoption of PQ/classical hybrid protocols like ML−KEM(Kyber)768+X25519, for their use in platforms familiar to healthcare professionals and NIST security level 3 rating.

Primary use cases include securing data at rest and authenticating sensitive communications.

zoom