미국 정부와 QuSecure, 정부 네트워크 통한 양자 후 암호화 통신 조정

2022년 7월 12일

SAN MATEO, Calif, 2022년 7월 12일 – PQC(Post-Quantum Cyber Security, 양자 후 사이버 보안)의 선두 주자인 QuSecure, Inc.는 오늘 미국 연방 정부가 현재 QuProtect PQC 솔루션을 활용하여 정부 네트워크를 통한 세계 최초의 포스트 양자 암호화 통신을 조정하고 있다고 발표했습니다. QuProtect는 양자 보안 채널을 사용하여 암호화된 통신 및 데이터를 양자 복원력으로 보호하도록 고유하게 설계된 업계 최초의 종단 간 PQC 소프트웨어 기반 솔루션입니다.

정부는 공군, 우주군 및 NORAD 위치에 있는 레거시 시스템에서 QuSecure의 고유한 양자 후 암호화 알고리즘을 활용하고 있습니다. 양자 탄력적 배포는 QuProtect의 양자 터널을 통해 대역폭이나 지연 문제가 증가하지 않고 이전에 표준 암호화를 사용했던 데이터를 100% 보호하는 가동 시간을 제공합니다. 현재 전송 중인 데이터는 QuProtect 시스템이 없으면 다른 사람이 해독할 수 없으며, 저장하기 위해 보호된 데이터를 수집하는 어떠한 상대도 양자 컴퓨터를 사용하더라도 미래에 해독할 가능성이 거의 없습니다.

“미국 정부가 이전에 온프레미스에서 양자 후 커뮤니케이션 채널을 사용하지 않았기 때문에 이는 매우 중요합니다." 라고 QuSecure 연방 운영 책임자인 Pete Ford는 말했습니다. ”QuProtect 플랫폼은 중단되지 않고 지속적인 양자 채널 가동시간으로 이전에 고전적으로 암호화되고 양자에 취약했던 비대칭 키를 보호하여 탁월한 성능을 발휘하고 있습니다."

이 역사적인 사건은 PQC 솔루션에 대한 SBIR(Small Business Innovation Research) 3단계 연방 정부 조달 계약에 대한 QuSecure의 평가 및 최종적으로 수주한 활동을 통해 가능했습니다. 지난달 발표된 QuSecure는 정부의 PQC 요구 사항에 대한 표준을 정립하면서 정부의 선도적인 PQC 솔루션 제공업체로 설립되었습니다. 이것은 포스트 퀀텀 위협에 대한 엔드 투 엔드 종합 솔루션을 다루는 것을 목표로 하는 정부의 최초이자 유일한 3단계 지정이며, 고전 및 미래의 양자 공격을 위해 PQC를 배포해야 하는 오늘날의 필요성을 더욱 강조합니다.

SBIR에 참여하는 연방 기관에는 다음 기관 및 부서가 포함됩니다: 중소기업청, 농업, 상업, 국방, 교육, 에너지, 보건 및 복지 서비스, 국토 안보, 교통, 환경 보호, 미국 항공 우주국(NASA), 국립 과학 재단.

정부의 QuSecure 배포는 레거시 장비 및 시스템에 대한 개방형 인터넷 네트워크를 통해 운영되고 있습니다. QuSecure는 사후 양자 암호화 표준화 경쟁에서 모든 NIST(National Institute of Standards and Technology) 최종 후보 알고리즘을 지원하는 암호화 민첩성을 사용하여 정부 시스템에서 작동함을 입증했습니다. NIST 대회의 우승자는 7월 5일에 발표되었다.

Ford는 "현재의 비즈니스, 상거래, 전쟁 및 일상적인 통신 속도를 통해 QuProtect는 기존 시스템 및 장치의 모든 데이터를 보호하고 시스템 속도를 늦추지 않습니다."라고 덧붙였습니다. "우리는 성공적인 초연에서 이를 입증했으며, 이는 정부와 SBIR 3단계 계약의 결과로 대규모 배포로 이어질 것입니다. 이 역사적인 순간을 통해 QuSecure는 매우 안전한 양자 미래를 보장한다는 우리의 비전을 실현하는 데 한 걸음 더 다가섰습니다."

QuProtect는 조직에서 처음으로 양자 복원력 기술을 활용하여 오늘날의 사이버 공격을 방지하는 동시에 네트워크의 미래를 보장하고 양자 이후 사이버 위협에 대비할 수 있도록 합니다. 그것은 언제 어디서나 모든 장치에서 양자 복원력있는 암호화를 제공합니다. QuProtect는 디지털 생태계의 가장 취약한 측면을 해결하는 종단 간 QSaaS(Quantum-security-as-a-Service) 아키텍처를 사용하여 제로 트러스트, 차세대 포스트 양자 암호화, 양자 강도 키, 고가용성, 손쉬운 배포 및 능동적 방어를 포괄적이고 상호 운용 가능한 사이버 보안 제품군으로 제공합니다. 종단 간 접근 방식은 데이터가 저장, 전달 및 사용되는 전체 데이터 수명 주기를 중심으로 설계되었습니다.

QuSecure 소개

QuSecure는 양자 및 고전 사이버 보안 위협으로부터 기업 및 정부 데이터를 보호하는 사명을 가진 포스트 양자 사이버 보안의 리더입니다. 특허 출원 중인 양자 안전 솔루션은 모든 조직에서 양자 내성으로 쉽게 전환할 수 있는 경로를 제공합니다. 회사의 QuProtect 솔루션은 양자 보안 채널을 사용하여 양자 복원력으로 암호화된 통신 및 데이터를 보호하도록 고유하게 설계된 업계 최초의 PQC 소프트웨어 기반 플랫폼입니다. QuSecure는 현재 은행/금융, 의료, 우주/위성, IT/데이터 기업, 데이터 센터 및 다양한 국방부 기관에 고객을 배치하고 있습니다. QuSecure는 투자자 지원을 받고 있으며 실리콘 밸리에 사무실을 두고 있습니다. 자세한 내용은 www.qusecure.com 을 방문하십시오.

[출처]
https://www.hpcwire.com/off-the-wire/us-gov-and-qusecure-orchestrate-post-quantum-encryption-communication/