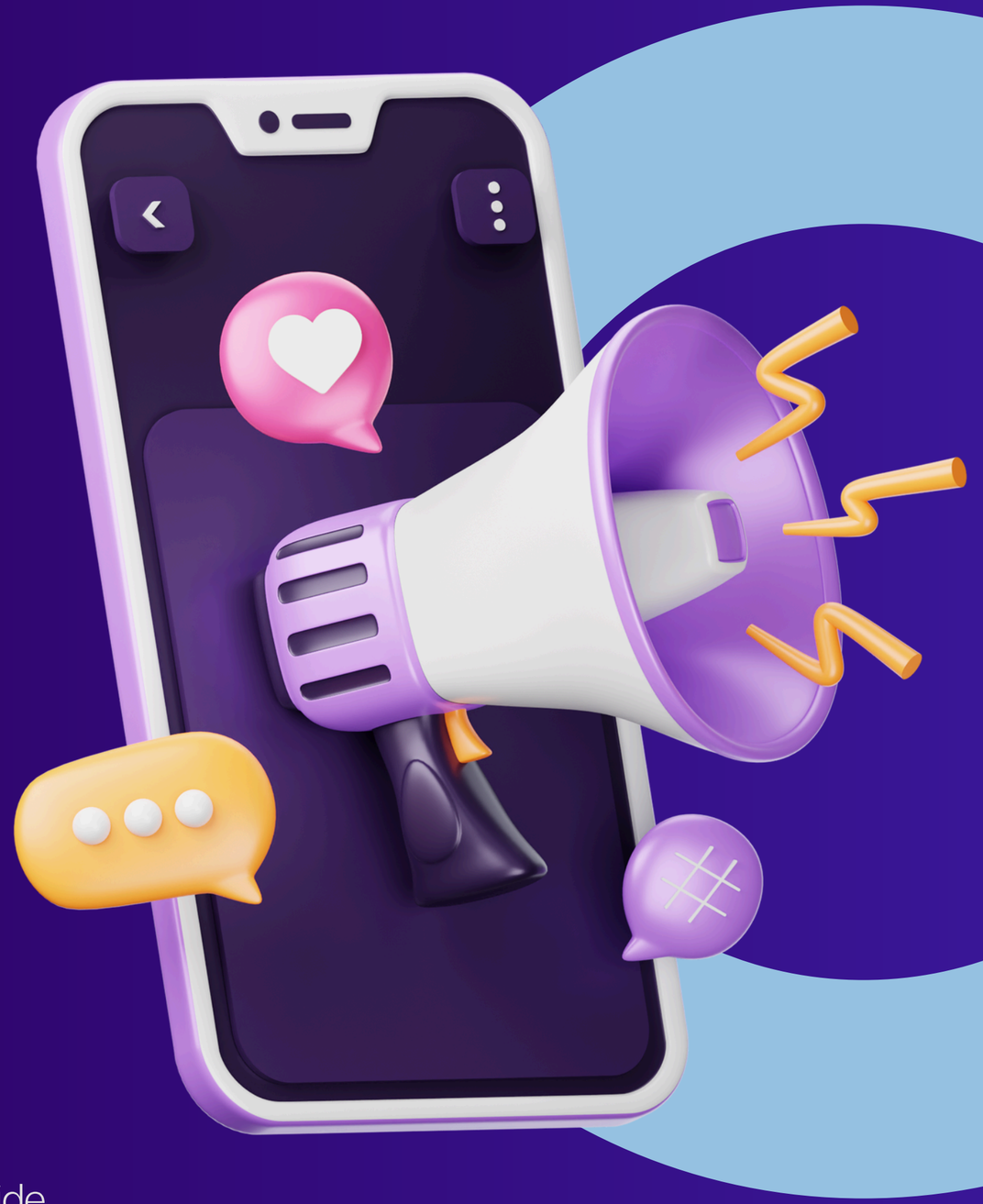
QUEVATECH

ON-PREM* CRYPTOGRAPHIC BASED ON RANDOMNESS SECURITY

AT THE HEART OF CRYPTOGRAPHY: WE PROVIDE SCALABLE UNPREDICTABILITY.



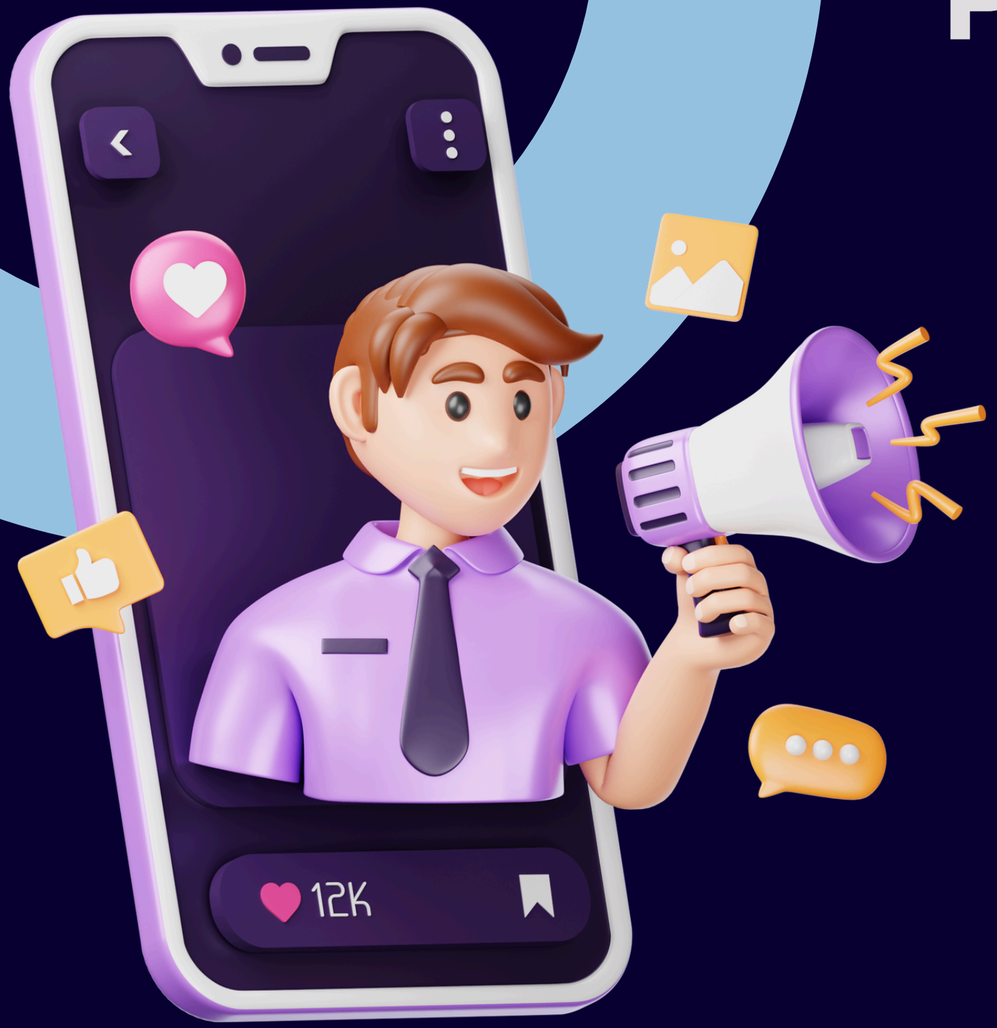
Presented by:
Hasan Yiğit

Email:
hasan@queva.tech

*On-prem: An on-premise device, a device not connected to the outside.

QUEVATECH

PROBLEM AREA



Weak Random Number

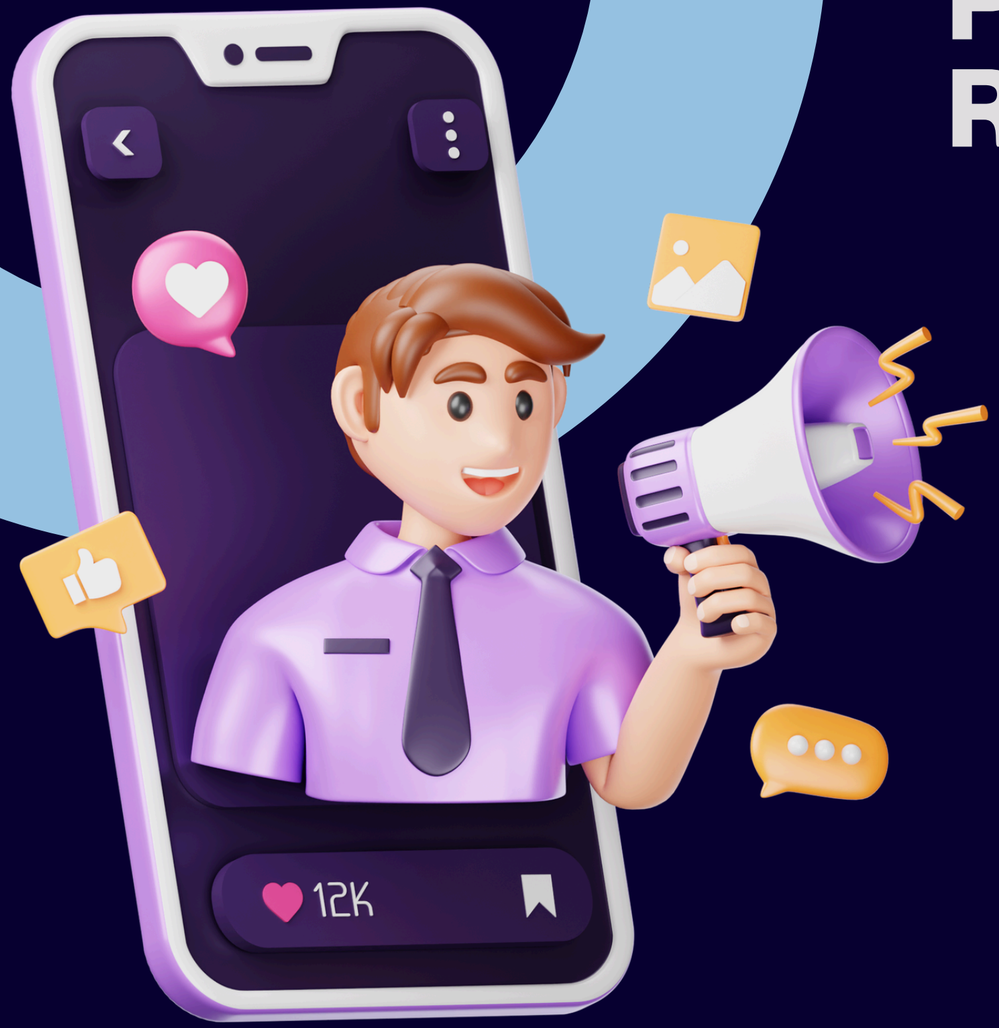
Weak Random Number Generator

Predictiable Password

Results in a security risk

The result is a silent open door.

QUEVATECH



PROBLEM AREA REAL EXAMPLES

- Debian OpenSSL (2006-2008) - Predictable keys
https://nvd.nist.gov/vuln/detail/cve-2008-0166

- Juniper NetScreen (2012-2015) - Silent decryption of VPN traffic

- CVE-2015-7755 https://hovav.net/ucsd/dist/juniper.pdf
RSA BSAFE default (2007-2013)

- Dissemination of Suspicious RNG
https://www.securityweek.com/nist-pulls-dualecdrbg-algorithm-random-number-generator-recommendations/

- Android SecureRandom bug (2013) - Draining of Bitcoin wallets

- YubiKey FIPS series (2019) - Low entropy on first use

QUEVATECH

SOLUTION SUMMARY

WHY IS IT IMPORTANT?

A stronger seed means stronger encryption keys. This protects everything from your personal data to national cybersecurity. It's like an invisible seatbelt you add to your infrastructure; it quietly and continuously increases security.

WHERE IS IT USED?

- **Encryption and Security: In all systems that use standards like OpenSSL and PKCS#11.**
- **Network Security: VPNs and SSL/TLS certificates.**
- **Hardware Security: HSMs (Hardware Security Modules).**
- **Operating Systems: Operating systems' own random number generators (RNG).**
- **Corporate Processes: CA (Certificate Authority) and SOC (Security Operations Center) processes.**

QUEVATECH

SOLUTION SUMMARY

SUMMARY NOTE

We increase the overall security of the digital infrastructure by increasing the quality of randomness that systems use for encryption. Simply put, a better starting point (seed) means a more robust result and processes.

HOW DOES IT WORK?

- **Source: It collects data from the system's entropy sources (e.g., hardware noise).**
- **Conditioning with Artificial Intelligence (AI): It processes the collected raw data using Artificial Intelligence algorithms and improves its quality.**
- **Byte Stream Generation: This process results in a high-quality random byte stream that passes standard tests.**
- **Usage: This strong seed is then used in the production of random data for VPN sessions, certificate keys, or other encryption purposes.**

QUEVATECH

INTEGRABLE ENTROPY DEVICE

WHAT DO WE OFFER?
We provide an on-premise randomness device and test software that measures its quality.

WHY IS IT IMPORTANT?
It objectively increases the RNG/key quality of your organization. You create and distribute it.

QUEVATECH

ENTROPY PROXY ASSISTANT SOFTWARE

WHAT ARE WE SAYING?

We inject a mix of TRNG into the key/session generation of servers and applications.

WHY IS IT IMPORTANT?

It works automatically within daily operations ; it reduces human error and prevents the use of weak RNG.

HOW DOES IT WORK?

It is a proxy service at the API or socket level ; it is a lightweight integration into existing systems. It is open-source software.

WHERE IS IT USED?

Corporate servers, VPNs, identity providers, and signing services.

We are installing an invisible and lightweight seatbelt in the middle of the operation.

QUEVATECH

KEY KIOSK SECRET SHARING TASK TRANSFER SECURITY

Human processes are fragile; other methods are not reliable ; this module binds them to a procedure.

WHAT ARE WE SAYING?

It is a single-use, traceable key generation and secure storage/recovery of a fragmented secret during task changes.

WHY IS IT IMPORTANT?

Access continuity and auditability are preserved in situations such as personnel changes. The kiosk generates a secure key ; it divides the secret into parts using the Shamir method ; the secret cannot be revealed without an authorized meeting.

WHERE IS IT USED?

Critical area accesses, CA ceremonies, highly privileged accounts.

QUEVATECH

ARCHITECTURE AND SECURITY BOUNDARIES

YOUR DATA STAYS IN YOUR ORGANIZATION:

Our system runs entirely on-premise. This means your sensitive data never leaves the physical and virtual boundaries of your organization. All audit records are stored in a signed and chained structure.

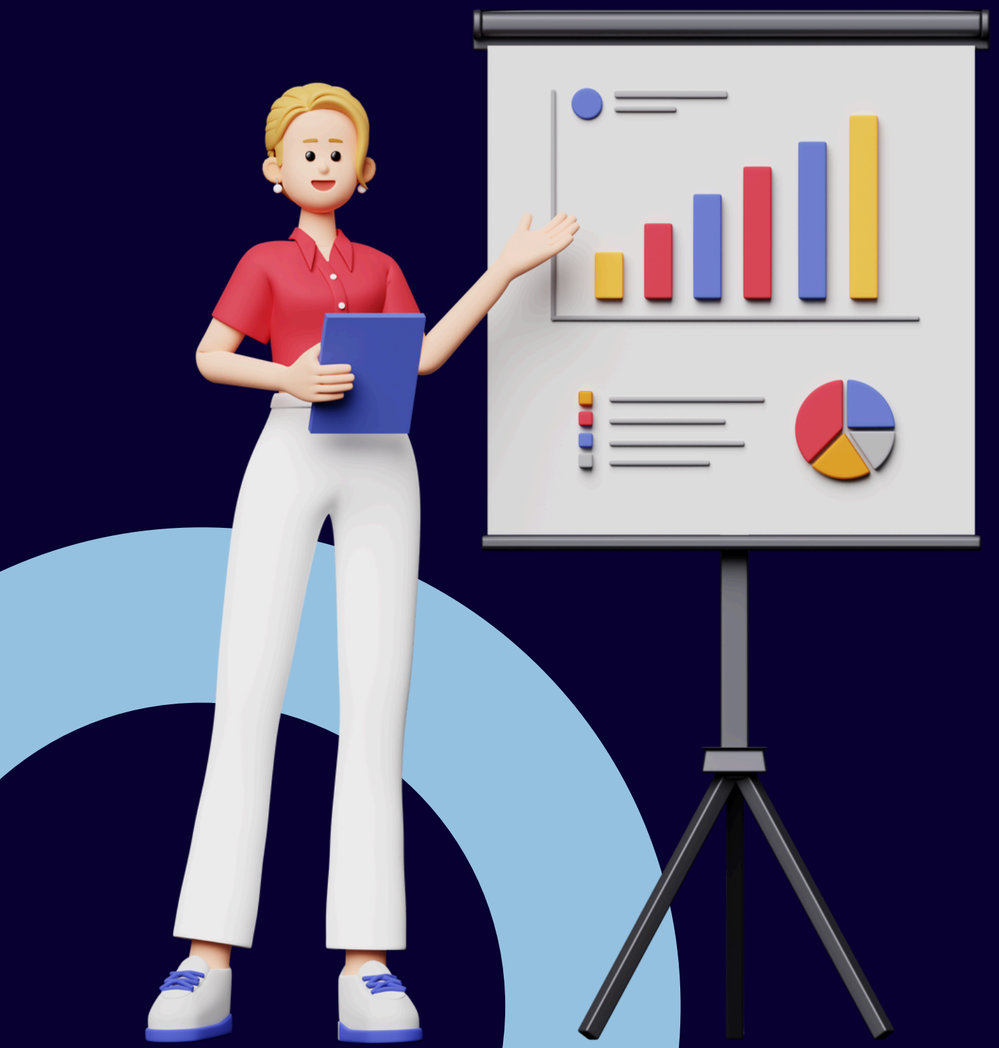
NO EXTERNAL DEPENDENCE:

Like Cloudflare's inspiration from natural noise sources, we feed from our own internal sources. Special measures have been taken against side-channel attacks, and our artificial intelligence models have been cleansed of known backdoors.

OPERATIONAL SECURITY

The system is based on a multi-source structure that eliminates external dependence. Thus, no single component can break the entire product. We keep our operational security at the highest level with continuous model updates and regular maintenance.

QUEVATECH



EVIDENCE: MEASURABLE RESULTS, NOT TRUST

WE DON'T SAY "BELIEVE US", WE PROVE IT.

The reliability of our system is supported by scientific research and concrete tests. This approach is the foundation of building transparency and trust.

- Scientific Verification: We openly present our working principles and methods to the scientific world. You can access our detailed article at arxiv.org/abs/2507.00145.
- Superior Performance: The random data we produce performs 2-3% better than the randomness output of standard CPUs. These results were obtained on 100 x 1Mb datasets using internationally accepted methods such as NIST SP 800-22 tests (see Table 2).
- High Entropy: Our random byte stream offers almost perfect randomness with a minimum entropy value as high as 7.94 out of 8 bits.
- Transparency and Auditing: The data we obtain is open to all non-commercial audits. Every claim we make is backed by a concrete method and report. These reports are reliable files that you can use in your decision-making processes.
- In short, the quality of our randomness is not just a claim, but a measurable and demonstrable fact.

QUEVATECH

WHY SHOULDN'T YOU DEVELOP IT YOURSELF?

BUILDING A CRYPTO INFRASTRUCTURE FROM SCRATCH WITHIN THE INSTITUTION IS NOT JUST A SOFTWARE PROJECT; IT IS A HIGH-COST, MULTI-DISCIPLINARY, AND LONG-TERM EFFORT.

This takes both your time and valuable resources away from your main business.

Broad Areas of Expertise: You need to bring together and continuously manage many different areas of expertise at the same time, such as cryptography, physical entropy engineering, security tests, and legal regulations. This is very difficult to manage with a single team.

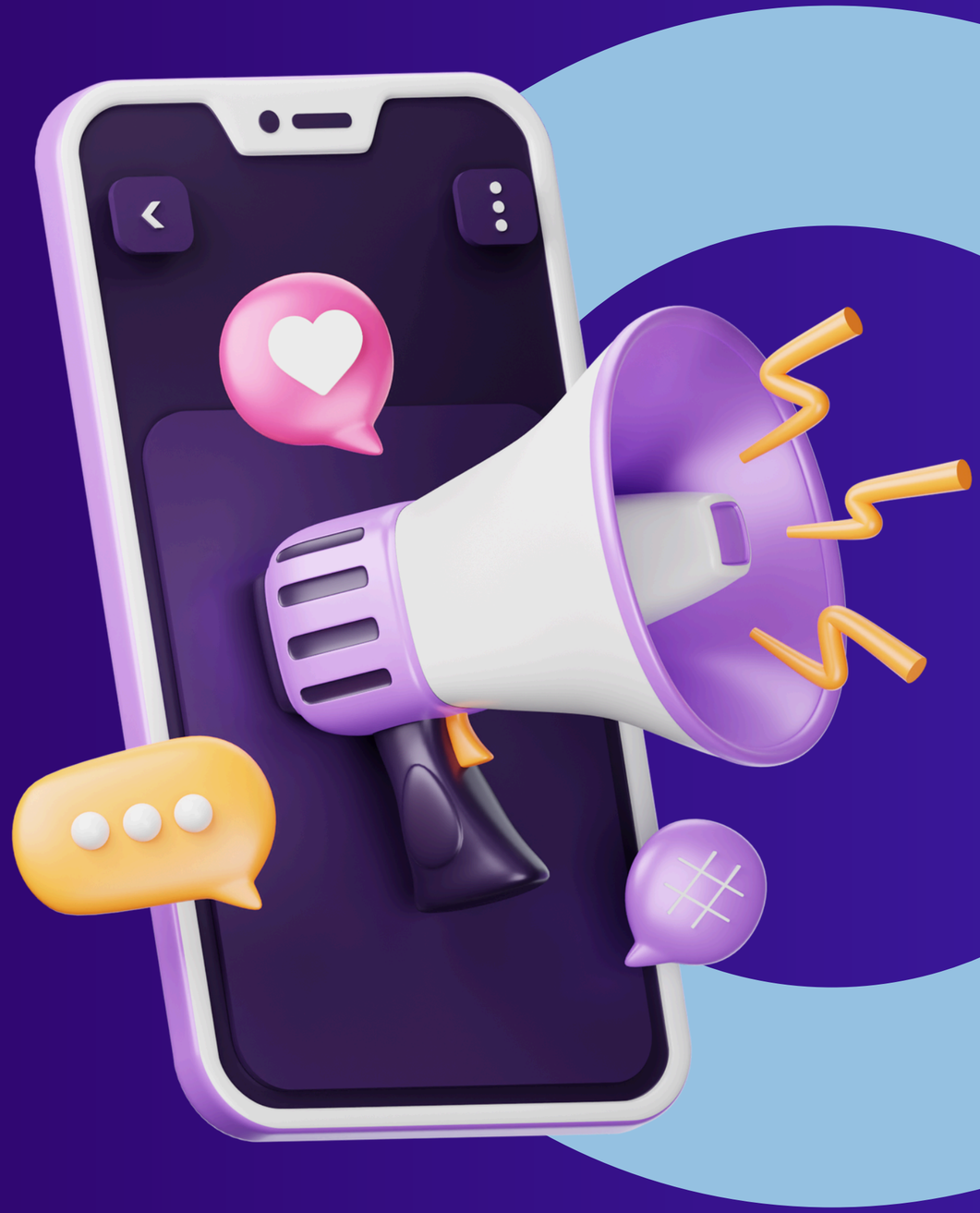
Hidden Costs: There are many costs that are not visible from the outside. The R&D phase of the project requires a team of 8-10 people working for 6-9 months, test labs, automation systems, and comprehensive audit documentation. Add to this the annual maintenance and update cycles.

Loss of Time and Opportunity: These processes cause institutionalized organizations to allocate resources away from their main operational tasks. Decision-making and system deployment can take months, which puts you behind your competitors.

QUEVATECH

THANK YOU FOR BOLDLY LOOKING TO THE FUTURE AND INVESTING IN SECURITY RATHER THAN TAKING RISKS.

LET'S CLARIFY THE DATE WE WILL COMMISSION THE FIRST DEVICE TODAY. 45 DAYS LATER, YOU WILL SEE OUR PROMISES IN A CONCRETE PROOF FILE.



Email (for everything):
hasan@queva.tech

Website:
www.queva.tech