QCOR ZERO TRUST STORAGE™ (ZTS) STOPS MORE THAN RANSOMWARE

Prevents data extortion, sabotage, and theft in real time.

UNHACKABLE DATA SECURITY

Explosive data growth and complexity increase your cyber risk daily, making every organization around the globe susceptible to a cyber event. For example, in 2021, the average ransomware event took 21-days to recover and cost $1.8million. Cyber measures are not keeping up with this new generation of ransomware.

Qcor's ZTS data security platform ensures that any cyber threats, including ransomware, cannot hack your data. Our patented ZTS software powered by AI protects any size or type of data workload, including your legacy storage. Finally, we inject NIST Zero Trust into the physical data layer of your cybersecurity, giving you the highest level of protection globally.

ZTS FEATURES

On-Premises, Cloud, or Software (SaaS)

Deploy Qcor ZTS as an on-premises appliance, in the cloud, or as software. Simple to set up and scalable, supporting up to as many Petabytes as needed.

Neuron™ AI Software

Automated configuration and integration with Neuron cyber defense control. Neuron AI performs continuous integrity, auditing and intrusion checking alerting you when anything is out of the ordinary.

Hardware & Software Immutability

Tamper-proof storage with proprietary WORM firmware automated by AI-powered software (Neuron) secures data at a physical (partition or block) level resulting in the world's most secure data storage.

WORMdisk™ Security

Partition level WORM protection for data workloads like VMs, SaaS apps, databases, Linux and Windows files. Integrates with your on-site encryption, authentication, and access control cybersecurity.

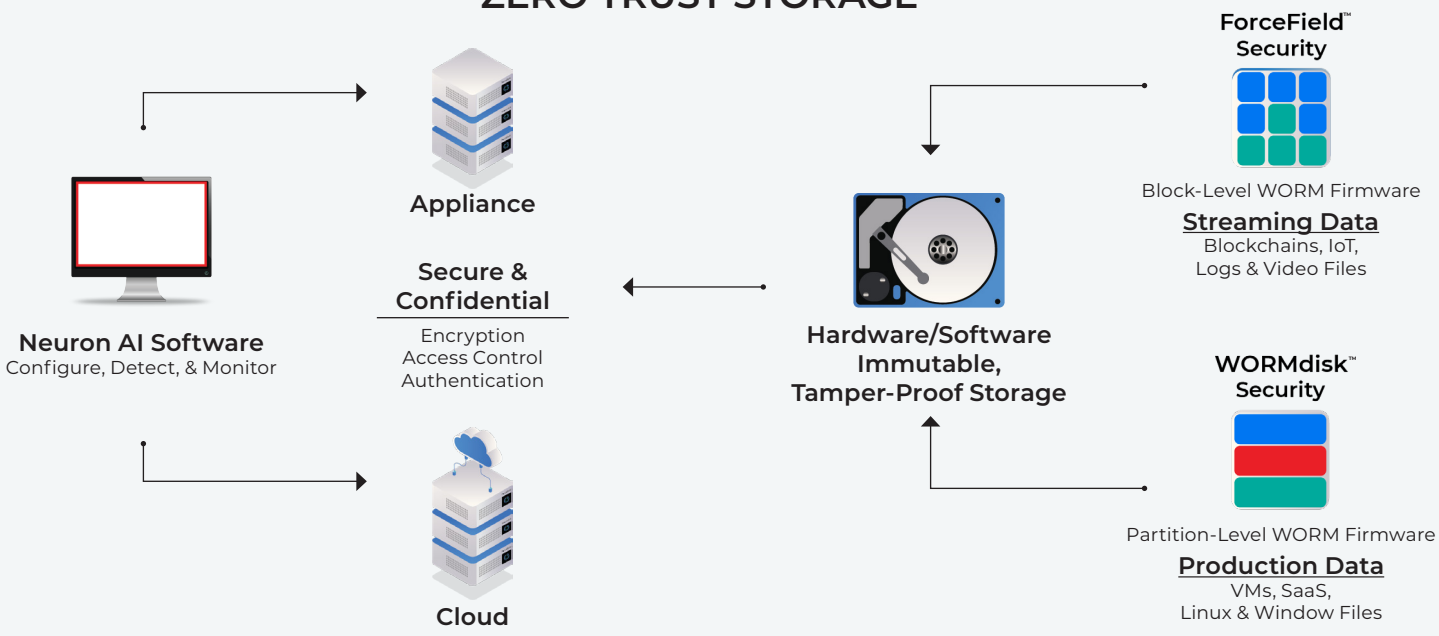
ForceField™ Security

Block-level WORM for streaming data workloads like blockchains, transactions, logs, IoT, and video data. Built in encryption, authentication, and access control easily integrates into your systems.

3rd Party Extensible

Scalable and extensible allowing fast connection with most 3rd party cyber security services. Tested and validated by leading authentication, access control, backup, cloud, encryption, and detection providers.

ZERO TRUST STORAGE™



QCOR UNHACKABLE DATA SECURITY

ZTS BENEFITS

Impenetrable Storage

Your data cannot be read, manipulated, or deleted by a cyber attack. The only patented hardware and software immutable storage platform that stops ransomware infections at the physical partition or block level.

True Zero Trust

NIST Zero Trust standards are engineered into our hardware and software WORM technologies. Competitive worm solutions are software-based and hackable.

Dynamic Workloads

Dynamically scales to support growth and performance for all data workloads or legacy storage systems. Loaded with storage to match your multi-year growth needs, with the ability to expand as your requirements grow.

Always-On Live Data

Since Ransomware cannot damage your data, it remains online and live even after an attack, which means you have 100% availability to your data for real time applications or fast data recovery.

AI-Powered Control

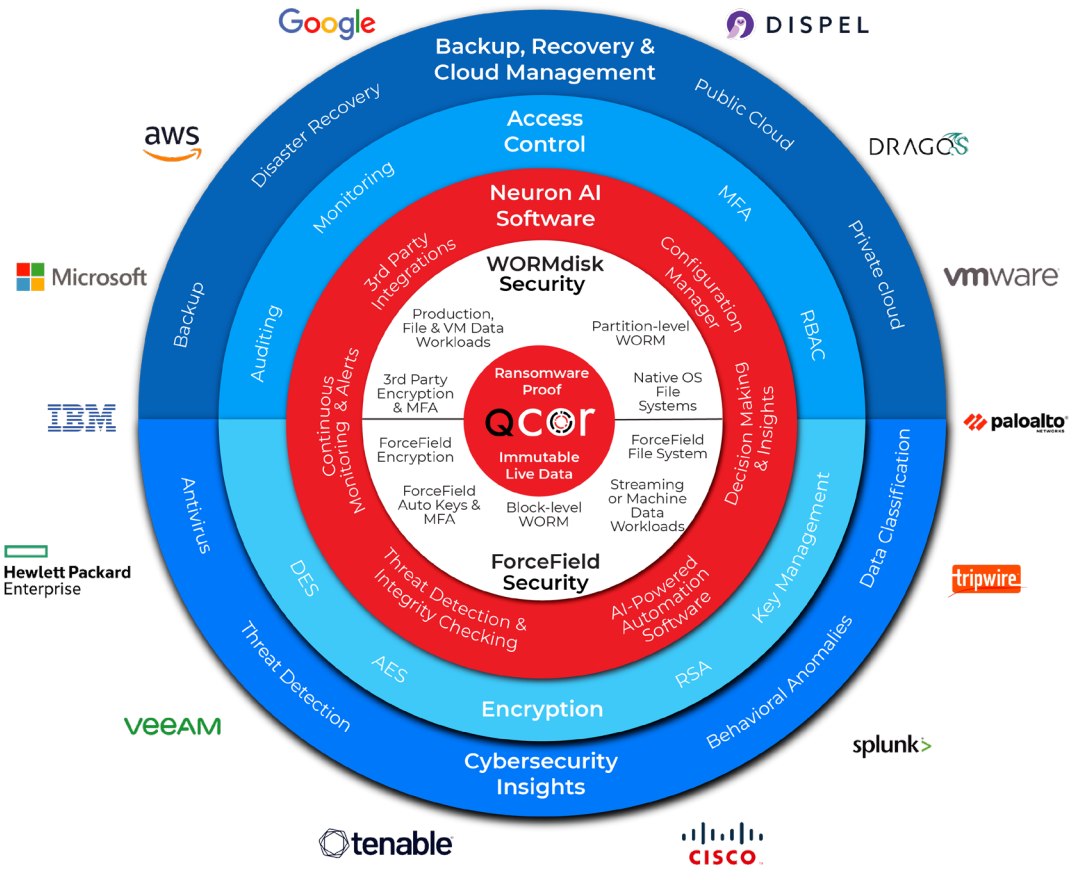
Automated AI software provides for a quick setup, monitoring, and integration with current cyber security, backup, recovery, and cloud management systems.

Lower Total Costs

Lower total costs due to our pricing model, less redundant storage, and automation requiring fewer people.

QCOR'S ZTS MULTI-LAYERED DATA SECURITY PLATFORM

Easily Integrates with your existing cybersecurity ecosystem



Validated by U.S. cybersecurity experts

DISA DEFENSE INFORMATION SYSTEMS AGENCY The IT Combat Support Agency

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST National Institute of Standards and Technology U.S. Department of Commerce

Raytheon Technologies