PRODUCT BRIEF

RES Trust with BuiltSECURE Rugged Secure Servers: Maintain Data Integrity and Safeguard IP at the Edge

mercury

Features

- Latest data center caliber processors with built-in hardware security
- Proven cryptography, secure boot and advanced physical protection options
- U.S. designed, tested and manufactured motherboards in award-winning, trusted IPC-1791-certified and DMEA-accredited facilities
- Root of Trust (RoT) enforced boot and configuration management
- Cyber-resilient BIOS
- Secure virtualization and data-at-rest protection options

Benefits

- Mitigate reverse engineering, bolster cybersecurity and safeguard critical IP with Mercury's proven BuiltSECURE™ technology
- Reduce cost and preserve security development with extendable architecture proven across multiple processor generations
- Safeguard against present and emerging threats with secure processing and end-to-end system security engineering (SSE) services
- Minimize risk of back doors, counterfeits and trojans with secure manufacturing and supply chain integrity

Proven BuiltSECURE Technology options:

- access control
- key management
- non-volatile memory write protection
- data-at-rest protection
- sanitization
- secure firmware management
- physical protection mechanisms
- sensors
- cryptographic offload engine capabilities

System Security Engineering (SSE) Services and Support

- 12-month warranty for service/repairs and continuous support included
- Cybersecurity partner pre-integration
- Program Protection Planning Assistance
- Red team/Blue team vulnerability analysis

Available Deliverables

- RES Trust XR5 1U / 2U RIO
- RES Trust XR6 1U / 2U RIO

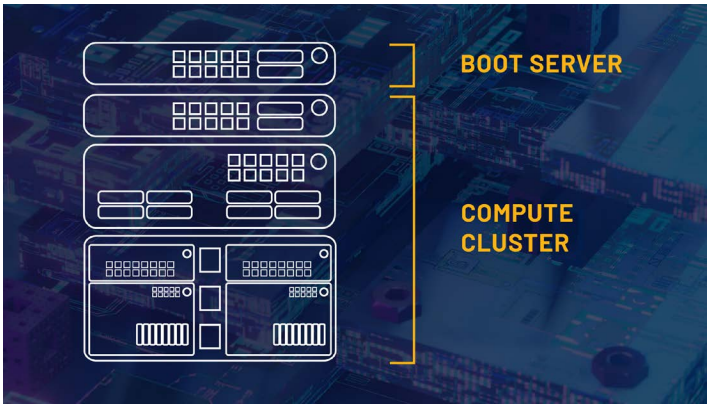
Standards Compliance

- MIL-STD: 810G, 901D, 167-1, 461

Sensitive technology, critical intellectual property and confidential data are vulnerable when deployed at the edge and must be protected from local or remote attacks. Mercury's RES Trust servers are designed specifically to address this challenge. Our RES Trust rugged secure servers maintain system-wide integrity and protect critical data and technology from loss or compromise.

Secure Your Server Cluster

When configured as a boot server, RES Trust ensures only authorized personnel can modify the cluster. Built-in cryptography and physical security delivers assurance and maintains data integrity even when the stack is offline or remotely accessed, making it ideal for edge applications.



Lower Your Total Cost of Ownership

Systems exposed to classified information in the field must be physically guarded or properly sanitized. Our built-in board volatility features ensure no classified data is unintentionally stored on the hardware, avoiding the need for expensive handling.

Mitigate Future Threats

Our extensible BuiltSECURE security architectures are built to evolve against current and future threats. Architectures can be utilized across processor generations, preserving security development to reduce overall cost and program risk.

Security Services and Analysis

Mercury's experienced system security engineers and customer support teams deliver affordable, end-to-end product security services including vulnerability assessments, technical training, classified capabilities and product-specific protection schemes.

Maintain System-Wide Integrity with BuiltSECURE

Deployed on over four generations of Intel® microarchitectures, RES Trust servers can be configured with a variety of nation-state level security features that mitigate reverse engineering and deliver cyber resiliency. A hardware-based Root of Trust and cyber-resilient BIOS mitigate multiple security threats to the application by reducing attack surfaces and minimizing boot devices. Built-in interfaces allow servers to participate in platform-wide security architectures.

System security features enable customer Foreign Military Sales (FMS) or Direct Commercial Sales (DCS) program success. Detailed security capability offerings can be requested.

Supply Chain Integrity for Trusted Performance

Board support packages, BIOS, and network stacks are maintained by U.S. personnel and are available for inspection by government agencies. Motherboards are manufactured and tested in DMEA-accredited facilities; minimizing the risk of back doors, counterfeits, and trojans.

A trusted supply chain is utilized for both hardware and software to deliver assurance that commercial IP will be protected. This design also helps system integrators meet Defense industry trust objectives including DoDI 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks."

Protect Sensitive Data & Operate through Cyber Attacks

Our optional FIPS 140-2, NIAP-certified, rugged secure solid state drives protects data at rest for NSA's CSfC program, even if the system is compromised, with key purge, fast erase, sanitization and self-destruct protocols. An optional secure hypervisor efficiently manages resources and minimizes attack surfaces so systems can efficiently respond and recover from compromise.

Field-Proven, Approved Design

To further enhance reliability, the system removes socketed components and solders processors and memory directly to the motherboard—eliminating disconnect during shock events. Advanced thermal and mechanical design features provide superior resilience to vibration, shock, dust, sand, and temperature extremes.With over 30 years of technical expertise Mercury Systems works closely with customers to design trusted computing solutions that are easy to integrate, affordable, and reliable for years to come. Mercury's MIL-PRF-38534 Class H/K, MIL-PRF-38535 Class Q, ISO 9001:2015 and AS9100 facilities maintain quality and inspection compliance.

Mercury Systems • 50 Minuteman Road • Andover, MA 01810 USA • (978) 967-1401 • Fax (978) 967-3330
Mercury Systems International • Regus Center, 26 Avenue Jean Kuntzmann • Montbonnot • 38330 France • +33 608 419949