Western Digital.

Solution Brief

Western Digital, Red Hat, and Mainsail Combine for Purpose-Built Zero-Trust Edge Computing Environments

Highlights

- A zero trust model confidential computing engine for cloud edge and tactical edge
- Cryptographic verification and authentication of hardware resources
- Encryption of data in-flight, at-rest, and in-use
- Human portable and Rackmount designs including MIL-STD compliant ruggedization for operation in harsh environments

Challenges

- Edge servers operate outside the protections of established secure data centers
- Cyber attackers' sophistication is evolving, making it increasingly difficult to defend
- Edge servers should not be trusted until they are cryptographically verified to be in a known good state

Solutions

- Western Digital Ultrastar Edge server is a Red Hat® Enterprise Linux® and OpenShift Certified, hardened server designed to TAA, FIPS 140-2 compliant encryption, and MIL-STD 810G and MIL-STD 461G ruggedization standards
- Mainsail Metalvisor is a Red Hat certified platform extending zero-trust principles down to the silicon embedded in the Western Digital Ultrastar Edge servers
- The combined solution delivers a higher standard for secure edge computing for the defense industry, and highly regulated industries such as Financial Services, Energy, and Healthcare

A Higher Level of Security is Needed for the Edge

Securing edge compute and data collection resources is a high priority given that edge devices operate outside of established secure data centers. Cyber attackers are growing more and more sophisticated in their tools and techniques, moving down the application stack, making it increasingly difficult to protect information assets. To better protect against these threats, a new approach is needed that involves "trusting nothing" and cryptographically verifying edge servers before they can be trusted.

A Zero Trust Environment

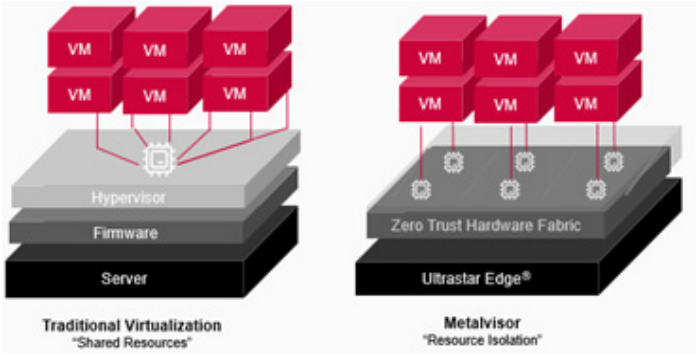
To protect the Western Digital Ultrastar® Edge servers outside the data center, Western Digital has partnered with Mainsail for their Metalvisor technology. Mainsail Metalvisor is a TypeZero Hypervisor, designed to protect systems from the silicon up through the application stack, using hardware-based isolation and cryptography to create immutable, tamper-proof environments. Mainsail Metalvisor works with Intel® processors to create additional security features to mitigate physical and cyber threats. A technology originally developed and used in United States Department of Defense programs, Mainsail Metalvisor is now commercially available and uses Red Hat Enterprise Linux as the foundation for industry leading workload compatibility. Zero Trust principles are built into the design by "never trust, always verify" starting with the Intel processor, where cryptographic verification of hardware leads to a secure hardware-based root of trust where higher-level software and application chains of trust are built. The entire system is constantly verifying the runtime of workloads, enforcing security policy, and protecting against advanced attacks.

Red Hat OpenShift for Safeguarding Edge Workloads

Red Hat OpenShift is a Kubernetes container based application platform that includes an enterprise-grade Linux operating system, container runtime, networking, monitoring, registry, and authentication and authorization solutions. Mainsail's Metalvisor brings hardware-based isolation to Red Hat OpenShift, ensuring separation between workloads and high-quality service. This helps to run demanding edge workloads that require high determinism and quality of service, like 5G and AI/ML workloads. Metalvisor also transparently encrypts memory so workloads can benefit from confidential compute and protect data in use. Metalvisor removes the virtualization overhead and allows you to use Red Hat OpenShift to build workloads without worrying about degraded performance experienced with traditional virtualization. Red Hat OpenShift workloads run with the same profile as a bare-metal machine with the benefits of virtualization and Red Hat Enterprise Linux compatibility.

Western Digital, Red Hat, and Mainsail combine for Purpose-Built Zero-Trust Edge Computing Environments

"Never trust, always verify" Unlike traditional systems that depend on implicit trust of either the hardware or virtualization layer, Mainsail Metalvisor implements isolated domains, launched from firmware siting below the Operating System level. A dedicated policy engine independent of the Operating System and designed to uniquely perform security policy & cryptographic verification for all resources in hardware & software. Per Mainsail, the solution meets and exceeds NIST 800-207 SP Zero Trust Architecture.



Confidential Compute

Mainsail Metalvisor ensures that all memory accessed from the Intel CPU is encrypted, to provide greater protection against software & hardware attacks protecting data in-use. Each domain is encrypted with unique private tenant keys which are derived and owned by the end user. Operating systems and applications can deploy without any code changes.

Trusted Compute Base

Mainsail Metalvisor is a lightweight, sub 200k lines of code, TypeZero Hypervisor that runs from firmware/UEFI.

Maximize Resource Performance

Mainsail Metalvisor isolates and dedicates hardware to domains where virtual machines have dedicated hardware CPU, Cache, Memory, Storage and Network enabling in 100% utilization of hardware, proper workload sizing, determinism and a guaranteed quality of service.

Hardened Specialized Servers

Western Digital Ultrastar Edge specialized servers can embed the zero-trust capabilities described above and add unique physical layer security and durability attributes.

Western Digital Ultrastar Edge servers can enable organizations to extend remote data capture, analytics, cloud services, virtualized infrastructure and containers, digital twin, machine learning and artificial intelligence beyond the reach of established global, regional, or local data centers. Processing data closer to where it is created eliminates the latency associated with wide area networks. Remote processing reduces the amount of traffic on network backbones while enabling real-time decision making. Low-latency processing capabilities in remote location enables a competitive advantage by delivering cloud-like services even when a network connection is intermittent or non-existent. Western Digital Ultrastar Edge specialized servers are vertically integrated with enterprise class Western Digital Ultrastar NVMe™ Solid State Disks, enabling IaaS environments to easily be run remotely.

In addition, the Western Digital Ultrastar Edge-MR is designed for operation in harsh environments. Western Digital Ultrastar Edge-MR's ruggedized shell with internal suspension protects the server from shock and vibration during transit. Western Digital Ultrastar Edge-MR is designed and tested in accordance with MIL-STD-810G-CHG-1 standards for limits of shock and vibration.

Furthermore, Western Digital Ultrastar Edge-MR is designed and tested to the MIL-STD-461G standard for electromagnetic interference. This reduces threat of detection by enemy forces of radiated electromagnetic emissions, and reduces susceptibility to interference from external electromagnetic interference.

Western Digital.

5601 Great Oaks Parkway
San Jose, CA 95119, USA
www.westerndigital.com

April 2023