

Zero Trust Platform for the Secure Edge

Introducing the first TypeZero Hypervisor for Secure Edge

Decision Dominance at the Edge

Artificial intelligence, machine learning, human-machine teaming, advanced visualization, data analytics, and machine-to-machine coupling work in concert to optimize the command and control C2 cycle. The potential value is an ability to provide DoD with secure edge computing as a means to underpin All Domain Operations, including the envisioned Joint All Domain Command and Control (JADC2) concept for managing complex, information-centric warfare in the air, land, sea, space and cyberspace domains simultaneously.

Hardware-based Zero Trust model from Mainsail

Mainsail's Metalvisor is a security platform that protects edge workloads that are outside of the enterprise data center or cloud. Metalvisor defends edge workloads against sophisticated cyber attacks by utilizing separation enforced by security functions in hardware and protecting data in all forms: at-rest, in-transit, and in-use.

It uses a custom separation kernel at the Firmware layer to provide a secure environment below the Operating System. By implementing security at this level, it is able to restrict threats and adversaries that would otherwise be able to bypass traditional security measures and thus offers robust protection against sophisticated cyber attacks. A technology initially developed and used in the United States Department of Defense, Metalvisor is now commercially available.

What are the threats at the edge?

Devices at the edge are outside the physical controls of the enterprise datacenter/cloud and attacks are getting more sophisticated by going down the application stack (bootkits/rootkits). Attackers are finding it harder to exploit and maintain access in the application and OS levels due to better software controls and 3rd party security products.

This is why attackers are looking to exploit external supply chains and move their attacks lower in the stack (like firmware and BIOS) to avoid detection. Mainsail believes that you have to go to the lowest point (the silicon) and make sure that it is cryptographically secure.


Edge workloads

- ▶ Real-Time & Low Latency
- ▶ 5G & Open Radio Access Network (ORAN)
- ▶ AI/ML Inference & Models
- ▶ High Performance Computing (HPC)
- ▶ Multi-Level Security (MLS)
- ▶ Mission Critical & SCADA
- ▶ Containers & VMs

About Mainsail

Mainsail is a US security company focused on advancing customers' missions and bringing advanced technology to the warfighter. We are engaged in the research, design, development, and integration of advanced technology systems, products & services across Defense, Public Sector, Enterprise, and Critical Infrastructure.

NORTH AMERICA
386-748-4404
mainsailindustries.com

 @mainsail-industries

Features

Introducing the first TypeZero Hypervisor for Secure Edge

Secure edge

▶ Zero Trust

“trusting nothing, always verify” Cryptographic verification, authentication, and signing of all hardware & software resources. Metalvisor meets and exceeds NIST 800-207

▶ Immutability

Unique domain entropy and customer-owned encryption keys are used to lockdown and cryptographically sign multi-tenant workload environments at the edge. Preventing unauthorized changes in hardware or software

▶ Simple Management

Workloads can be cryptographically signed and deployed via Cockpit or Ansible. Metalvisor is integrated with Cockpit a familiar web interface for managing Linux. Metalvisor has certified platform support with Red Hat

▶ Modern Workloads

Metalvisor has been tested and verified to run modern Containers, Kubernetes, and Virtual Machine workloads without the overhead of traditional virtualization

▶ Workload consolidation

Consolidate Real-time, low-latency, and traditional workloads with guaranteed quality of service. Reduce Space, Weight, and Power (SWaP) and use DevOps principles to manage workloads

▶ Physical Protections

Protect workloads from physical threats outside the data center by protecting data in all forms at-rest, in-transit, in-use

▶ Confidential Compute

End-to-End data protection by encrypting data in-flight, at-rest, and in-use. No additional software or app refactoring

▶ Bare-metal Like Performance

New levels of determinism and QoS for workloads, just like bare metal, but the benefits of virtualization

▶ Autonomous Threat Protection

The entire system is constantly verifying the runtime of workloads, enforcing security policy, and protecting against advanced attacks. Even in disconnected environments

Schedule a demo of Mainsail Metalvisor

Email info@mainsailindustries.com