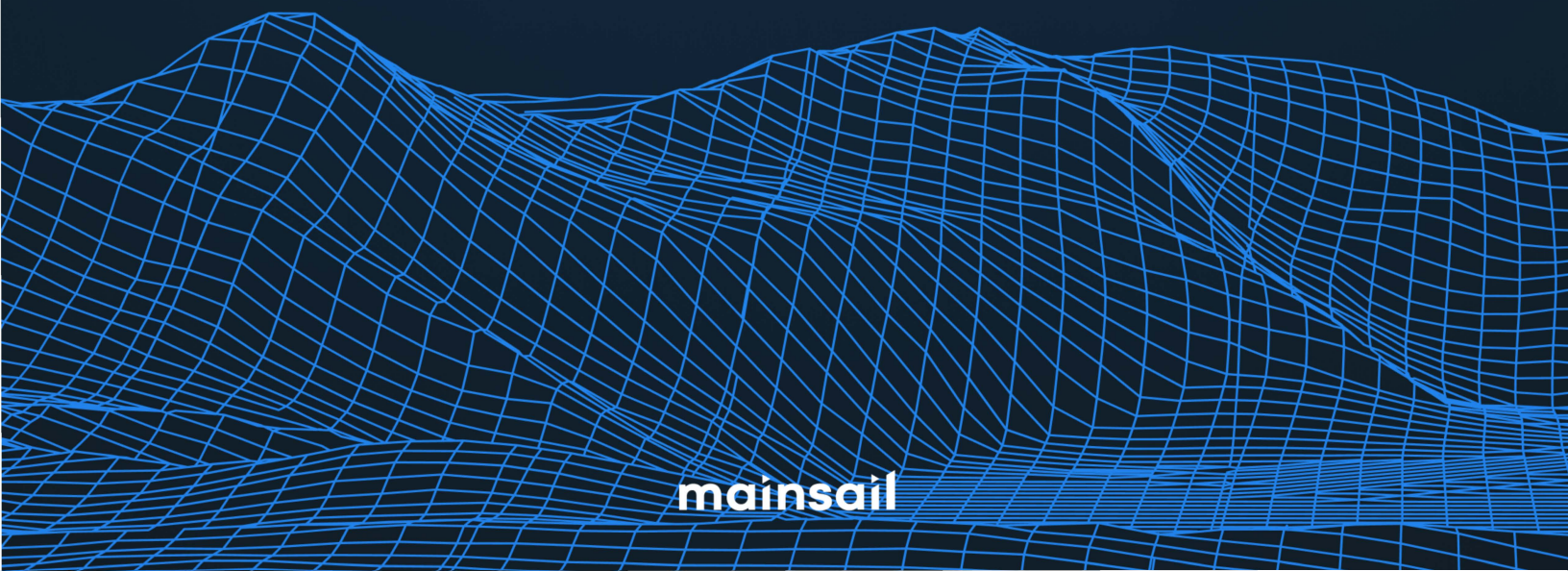
METALVISOR

Introducing the first TypeZero Hypervisor Workload Consolidation



mainsail

Edge computing is a distributed computing architecture that brings computation and data storage closer to the edge of the network, closer to the devices and end-users that generate and consume data. This approach aims to address the challenges of latency, bandwidth, and data privacy that arise when data has to be transmitted over long distances to centralized data centers.

Edge computing is expected to grow rapidly in the next few years due to the increasing demand for low-latency, real-time applications and services such as autonomous vehicles, augmented and virtual reality, and the Internet of Things (IoT). Edge computing also helps to reduce the load on centralized data centers, making them more efficient and scalable.

Use cases of edge computing are numerous and span across various industries such as manufacturing, healthcare, retail, and transportation. For example, in manufacturing, edge computing can be used to monitor and control production processes in real-time. In healthcare, edge computing can be used to process medical imaging and perform real-time patient monitoring. In retail, edge computing can be used to process customer data and provide personalized experiences. In transportation, edge computing can be used to process data from sensors on vehicles and support autonomous driving.

As the technology and infrastructure for edge computing continue to evolve, it is expected that new use cases will emerge and existing ones will expand into more industries. For example, edge computing can be used to support smart cities by processing data from sensors in real-time to manage traffic, energy, and other critical infrastructure.

Edge computing

Edge computing is expected to bring several benefits to the U.S. government and the Department of Defense (DoD). Some of these benefits include:

1. **Improved security:** Edge computing allows sensitive data to be processed and stored closer to the edge of the network, reducing the risk of data breaches and unauthorized access. This is particularly important for the U.S. government and the DoD, where the protection of sensitive information is of paramount importance.
2. **Increased efficiency:** Edge computing reduces the amount of data that has to be transmitted over long distances, leading to improved network efficiency and reduced latency. This can help improve the performance of critical systems and applications that are used by the U.S. government and the DoD.
3. **Real-time data processing:** Edge computing allows for real-time data processing and decision-making, which can be crucial in time-sensitive situations such as military operations.
4. **Enhanced situational awareness:** Edge computing can be used to process data from sensors and other sources in real-time, providing enhanced situational awareness and enabling faster decision-making in the field.
5. **Lower cost:** Edge computing can help reduce the cost of data processing and storage by reducing the load on centralized data centers. This can help the U.S. government and the DoD to more efficiently allocate their resources.

Edge computing has the potential to improve the efficiency, security, and performance of critical systems and applications used by the U.S. government and the DoD, and to support their mission-critical operations.

AI/ML

Artificial Intelligence (AI) and Machine Learning (ML) can bring several benefits to the Department of Defense (DoD). Some of these benefits include:

1. **Improved decision-making:** AI and ML can be used to analyze vast amounts of data and provide insights that can help improve decision-making in complex and time-sensitive situations.
2. **Enhanced situational awareness:** AI and ML can be used to process data from sensors and other sources in real-time, providing enhanced situational awareness and enabling faster decision-making in the field.

3. **Predictive maintenance:** AI and ML can be used to predict equipment failures and schedule maintenance in advance, reducing downtime and increasing the efficiency of military operations.
4. **Automated tasks:** AI and ML can be used to automate repetitive and time-consuming tasks, freeing up personnel to focus on more complex and critical tasks.

Edge computing can help to enhance the benefits of AI and ML for the DoD in several ways:

1. **Low latency:** Edge computing reduces the amount of data that has to be transmitted over long distances, leading to improved network efficiency and reduced latency. This can help improve the performance of AI and ML applications and enable real-time decision-making.
2. **Improved security:** Edge computing allows sensitive data to be processed and stored closer to the edge of the network, reducing the risk of data breaches and unauthorized access. This is particularly important for the DoD, where the protection of sensitive information is of paramount importance.
3. **Enhanced processing power:** Edge computing allows for the deployment of powerful computing resources closer to the edge of the network, improving the performance of AI and ML algorithms.

The combination of AI and ML with edge computing can help the DoD to more effectively and efficiently process and analyze vast amounts of data, and to support their mission-critical operations.

Confidential computing

Confidential computing is a technology that protects data and computations in-use, while they are being processed. It provides an isolated and secure environment for data processing and can be used to protect AI and ML models at the edge. Confidential computing uses hardware-based security features, such as secure enclaves, to isolate sensitive data and computations and prevent unauthorized access or tampering.

Here's how confidential computing can help protect AI and ML models at the edge:

1. **Data privacy:** Confidential computing ensures that sensitive data, such as personal or financial information, is protected from unauthorized access or tampering, even when it is being processed by AI or ML models.

2. **Model protection:** Confidential computing can protect AI and ML models from reverse engineering, tampering, or theft. This is important for organizations that have invested in developing proprietary models and do not want to risk their intellectual property being compromised.
3. **Compliance:** Confidential computing can help organizations meet regulations and standards, such as GDPR, that require the protection of sensitive data.
4. **Improved performance:** By processing data and computations in a secure and isolated environment, confidential computing can help improve the performance of AI and ML models by reducing the overhead of encryption and decryption.

Confidential computing provides an essential layer of security for AI and ML models, protecting sensitive data and computations and helping organizations to meet regulatory requirements while improving performance and protecting intellectual property.

Metalvisor provides physical protection by using confidential compute and hardware-based isolation. Confidential compute protects data and processing in memory, storage, and communication paths by encrypting all data in use. Hardware-based isolation uses virtualization technology to isolate workloads from each other, providing physical protection from external threats, malicious actors, or accidental access.

Zero Trust

Metalvisor provides Zero Trust at the CPU level by using cryptographic verification of hardware, extending it to the runtime of applications. Metalvisor provides advanced security measures that meet and exceed the guidelines set forth by NIST 800-207 for Zero Trust. This high level of security helps protect the DOD against cyber threats by providing a secure environment for running critical applications and workloads. The cryptographic verification of hardware helps to ensure the integrity of the system and the authenticity of the hardware, preventing any unauthorized access or tampering. This advanced level of security can provide peace of mind to the DOD and help to minimize the risk of security breaches, data loss, and other cyber threats.

Immutable Workloads

Metalvisor provides a feature called "Immutable Workloads", which adds an extra layer of security for multi-tenant edge computing environments. It does this by cryptographically signing and locking down workloads, making them tamper-proof and ensuring that the code running on the edge device is always in its intended state. With this feature, Metalvisor provides an assurance that the code cannot be altered by unauthorized third parties, even in a shared environment. This helps prevent malicious attacks, such as

malware injection or unauthorized code changes, which can compromise the security and reliability of the edge device. In addition, the cryptographic signing process provides an audit trail, allowing administrators to track changes to the code and easily detect any unauthorized modifications. Overall, the immutability feature of Metalvisor helps to ensure that workloads run securely and reliably, even in multi-tenant environments.

Threat Protection & Active Response

Metalvisor has built-in Endpoint Detection and Response (EDR) and active response capabilities ARC, which help organizations to detect, respond to, and prevent cyber threats, including zero-day exploits. Metalvisor uses heuristic analysis to stop zero-day exploits and other cyber threats. Heuristic analysis is a method of detecting malicious activity by using patterns of behavior that are indicative of a threat. This allows Metalvisor to identify and respond to threats that are not yet known or documented by security vendors.

Here's how Metalvisor uses heuristic analysis to stop zero-day exploits:

1. **Zero-day exploits:** A zero-day exploit is a type of cyber attack that takes advantage of vulnerabilities in software or hardware that are unknown to the vendor or the users. Metalvisor's EDR and ARC capabilities provide organizations with real-time visibility into endpoints allowing them to detect and autonomously respond to threats quickly and effectively.
2. **Real-time monitoring:** Metalvisor monitors endpoint activity in real-time, allowing it to detect and respond to potential threats quickly. This enables Metalvisor to identify and stop zero-day exploits before they can cause harm.
3. **Threat detection and response:** Once Metalvisor has identified a potential threat, it can respond in a number of ways, including isolating the affected endpoint, blocking malicious activity, and providing detailed information about the threat.

Metalvisor's heuristic analysis capabilities help organizations to detect and respond to zero-day exploits and other cyber threats quickly and effectively, reducing the impact of cyber-attacks and improving their overall security posture.

Bare-metal Performance

Metalvisor provides bare-metal-like performance by leveraging Metalvisor's Type-0 hypervisor operating under the operating system. The Metalvisor hypervisor is launched from the firmware UEFI, providing a trusted and secure foundation for virtualized workloads. This architecture enables Metalvisor to provide new levels of determinism and Quality of Service (QoS) for workloads, just like bare-metal, but with the added benefits of virtualization.

The Metalvisor hypervisor provides hardware-level virtualization, which offers improved performance and resource management, allowing for more efficient use of system resources and better performance for workloads. By providing a more secure, reliable, and performant virtualization layer, Metalvisor enables customers to run their workloads with confidence, even in demanding edge environments.

Modern Workloads

Metalvisor provides support for running modern workloads, including Kubernetes, OpenShift, Rancher, and other Kubernetes platforms. This is achieved through the integration of Metalvisor, which is a type-0 hypervisor that operates below the operating system. The combination of Metalvisor's advanced security features provides a secure and robust platform for running modern workloads at the edge, ensuring that the workloads are protected against both cyber threats and physical threats. Additionally, Metalvisor's support for Kubernetes platforms and other modern workloads provides customers with a flexible and scalable solution that can meet their changing needs as their workloads evolve over time.

High Performance Workloads

Metalvisor can run low latency, latency-sensitive and real-time workloads effectively due to its bare-metal-like performance, providing new levels of determinism and Quality of Service (QoS) for workloads. The Metalvisor, as a type-0 hypervisor, operates directly on the hardware, providing a direct path to the physical resources and bypassing the overhead of traditional virtualization. This allows the consolidation of previously unconsolidated workloads and provides the benefits of virtualization with the performance of bare metal. Additionally, the use of confidential computing and hardware-based isolation helps protect the workloads from physical threats outside the data center, ensuring that the low latency, latency-sensitive and real-time workloads can run securely and reliably.

Requirements for the Secure Edge

The DoD handles sensitive data and needs to ensure that AI and ML workloads are secure from unauthorized access and tampering. By using a hardware and software solution that provides end-to-end security, the DoD can reduce the risk of data breaches and protect sensitive information. The DoD is subject to various regulations and standards that govern the use of AI and ML workloads. By using a hardware and software solution that is designed to meet these requirements, the DoD can ensure that it is in compliance with applicable regulations and standards. The DoD needs to be able to run AI and ML workloads in a cost-effective manner, especially in remote locations where infrastructure may be limited. By using a hardware and software solution that is designed for harsh environments, the DoD can reduce costs by eliminating the need for additional infrastructure and support. Overall, the DoD needs a hardware and software solution to securely run AI and ML workloads at the edge to support real-time decision-making, improve network connectivity, enhance data security, meet compliance requirements, and reduce costs.

Purpose Built Edge Solution

Metalvisor is an excellent solution for secure edge computing for the Department of Defense (DOD). The Metalvisor provides a secure, isolated environment for data processing at the edge. This solution offers several benefits for the DOD, including

1. **Security:** The Metalvisor provides hardware-based security, isolating sensitive data and computations and making it difficult for attackers to access or tamper with the data.
2. **Performance:** Metalvisor provides high-performance data processing, making it well-suited for edge computing scenarios that require real-time data processing and low latency.
3. **Compliance:** The Metalvisor provides a secure environment for data processing, helping the DOD to meet regulations and standards that require the protection of sensitive data.

Metalvisor provides a secure, high-performance platform for edge computing, helping the DOD to protect sensitive data, meet regulatory requirements, and provide fast and reliable data processing at the edge.

Red Hat Certified

Being certified with Red Hat provides customers with the assurance of compatibility and support from a well-established and trusted technology company. Having Red Hat certification means that the hardware and software have been thoroughly tested and verified to meet the necessary standards for enterprise-level performance and security.

Having support through Red Hat also provides customers with access to Red Hat's extensive support network, including their technical support team and the ability to leverage their knowledge base. Customers can also benefit from Red Hat's commitment to ongoing updates and improvements, which helps to ensure that the hardware and software continue to function optimally over time. Additionally, Red Hat's certifications often help to streamline the procurement process, as it can provide assurance to customers that the hardware and software they are purchasing meet necessary standards. Overall, having Red Hat certification helps to give customers peace of mind, knowing that their technology investments are supported and secure.

Metalvisor, being certified with Red Hat, provides several benefits to customers, particularly those in the Department of Defense (DoD) who need secure and reliable solutions for their edge computing needs. Red Hat is a leading provider of open source software solutions and services, and its certification program ensures that hardware and software products have been rigorously tested and are compatible with Red Hat's solutions. By having Metalvisor certified with Red Hat, customers can be assured that they have been tested and are compatible with Red Hat's software solutions.

This certification provides several benefits to the customer, including

1. **Support:** Red Hat provides world-class support to its certified partners, which ensures that customers have access to the resources and expertise they need when they need it.
2. **Compatibility:** With certification, customers can be assured that Metalvisor is compatible with Red Hat's solutions and can work together seamlessly.
3. **Interoperability:** Certified products have been tested for interoperability, which means that customers can easily integrate them with other solutions and systems they may already be using.
4. **Reliability:** Certified products have been tested and approved by Red Hat, which provides customers with confidence that they can depend on these solutions for their edge computing needs.

Certification with Red Hat provides customers with a level of assurance and support that is crucial for mission-critical systems in the DoD.

Summary

Metalvisor is an excellent solution for secure edge computing for the Department of Defense (DOD) and meets and exceeds the National Institute of Standards and Technology (NIST) 800-207 for Zero Trust. This combination offers several security features to help protect sensitive data and ensure the integrity of the system

1. **Confidential Compute:** The Metalvisor provides hardware-based security, isolating sensitive data and computations in a secure, isolated environment, known as confidential compute. This helps to prevent unauthorized access to sensitive data and ensures that computations are performed securely.
2. **Zero-Day and Malware Protection:** Metalvisor provides advanced threat protection to prevent zero-days, rootkits, and bootkits from compromising the system. This provides a strong defense against attacks that attempt to bypass software-based security measures.
3. **Secure Boot:** Metalvisor provides secure boot functionality, ensuring that the system starts with a trusted, verified boot process. This helps to prevent unauthorized software from running on the system and ensures that the system is secure from the start.
4. **Encryption:** Metalvisor supports encryption at-rest, in-transit, and in-use, providing an additional layer of security for sensitive data.
5. **Compliance:** Metalvisor helps organizations to meet regulatory requirements and standards that require the protection of sensitive data, such as NIST 800-207 for Zero Trust.

In summary, the Metalvisor provides a secure platform for edge computing that meets and exceeds the NIST 800-207 standard for Zero Trust. The hardware-based security features of the Metalvisor and the secure boot and encryption capabilities provide a strong defense against attacks and ensure the confidentiality, integrity, and availability of sensitive data at the edge.

Metalvisor is a security solution that is built into the server and provides enhanced security features such as zero trust, confidential computing, and protection against zero-day exploits and malware. Metalvisor offers a highly secure solution for the DOD to run AI and ML workloads at the edge with confidence.

Thank you for downloading this Red Hat brief! Carahsoft is the Master GSA and SLSA Dealer and Distributor for Red Hat Enterprise Open Source solutions available via GSA, SLSA, ITES-SW2, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Red Hat's solutions, please check out the following resources and information:

For additional resources:
carah.io/RedHatResources

For upcoming events:
carah.io/RedHatEvents

For additional Red Hat solutions:
carah.io/RedHatPortfolio

For additional Open Source solutions:
carah.io/OpenSourceSolutions

To set up a meeting:
redhat@carahsoft.com
877-RHAT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/RedHatContracts