Micro To The Max

MicroV is an open source hypervisor built from the ground up, designed specifically to execute Micro VMs (i.e., tiny virtual machines with no emulation needed to execute them). Assured Information Security (AIS) developed MicroV to support its U.S. Government and commercial customers with everything from basic research to operational environments with strict requirements on performance, security, reliability, disaggregation, isolation and a small trusted computing base.

MicroV

Open Source Hypervisor

UNPRECEDENTED FLEXIBILTY

AIS has nearly two decades of hypervisor experience ranging from basic research like the **MoRE hypervisor**, to operational hypervisors like **SecureView®**. To support our wide range of customer requirements, AIS uniquely designed MicroV to support as many use cases as possible. MicroV's design supports both type 1 and type 2 configurations, while simultaneously supporting any root OS of your choice including Windows, Linux and UEFI. MicroV could even be easily modified to support more esoteric environments like ThreadX, FreeRTOS or even a custom operating system. In addition, MicroV has been designed with AUTOSAR compliance in mind to support critical systems applications like automotive, medical, space and aviation. No other hypervisor currently available provides this same level of flexibility.

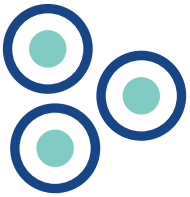
To support mobile, embedded, IoT and even cloud computing, performance and power efficiency was a priority in MicroV's design. To accomplish this, MicroV is designed to run everything, including the root OS, in a virtual machine while delegating scheduling and power management. This design choice not only ensures MicroV has a small trusted computing base with strong security and isolation, it provides exceptional performance and battery life by allowing the operating system that was designed for a device to manage the device.

AIS leveraged its experience with **SecureView®** to ensure MicroV was designed with security in mind. Unlike most other hypervisors, MicroV's internal design includes a small microkernel, executing the majority of the hypervisor in a deprivileged environment, complete with SELinux style enforcement of the hypervisor's internal communications. Whether you need a hypervisor for research, cloud computing, embedded/IoT, government or critical systems, MicroV was designed for you.

AIS WEBSITE PAGE | FIND US ON GITHUB | JOIN US ON SLACK

Assured Information Security
315.336.3306 WWW.AINFOSEC.COM

Features



Isolate Everything

Everything, including the root operating system, runs on a virtual machine. This allows MicroV to protect the root operating system from Micro VMs, as well as protecting Micro VMs from the root operating system.

Cross-Platform

MicroV can support any root operating system. Currently MicroV supports Windows, Linux and UEFI, but support can easily be added for any operating system including an RTOS as MicroV is implemented as a self-contained binary.

Performance

MicroV removes the need for emulation by requiring each Micro VM to execute a fully enlightened kernel (or unikernel). By default MicroV provides support for Linux, but MicroV's APIs can be leveraged to support any guest operating system of your choice.

Power and Scheduling

MicroV leverages the scheduler in the root operating system to schedule Micro VMs, improving both performance and battery life dramatically. Unlike KVM, MicroV accomplishes this without running the entire Linux kernel in the hypervisor.

AUTOSAR Compliance

MicroV was written in C++ using the AUTOSAR standards, enabling MicroV's use in critical systems including automotive, medical and government spaces.

Open Source

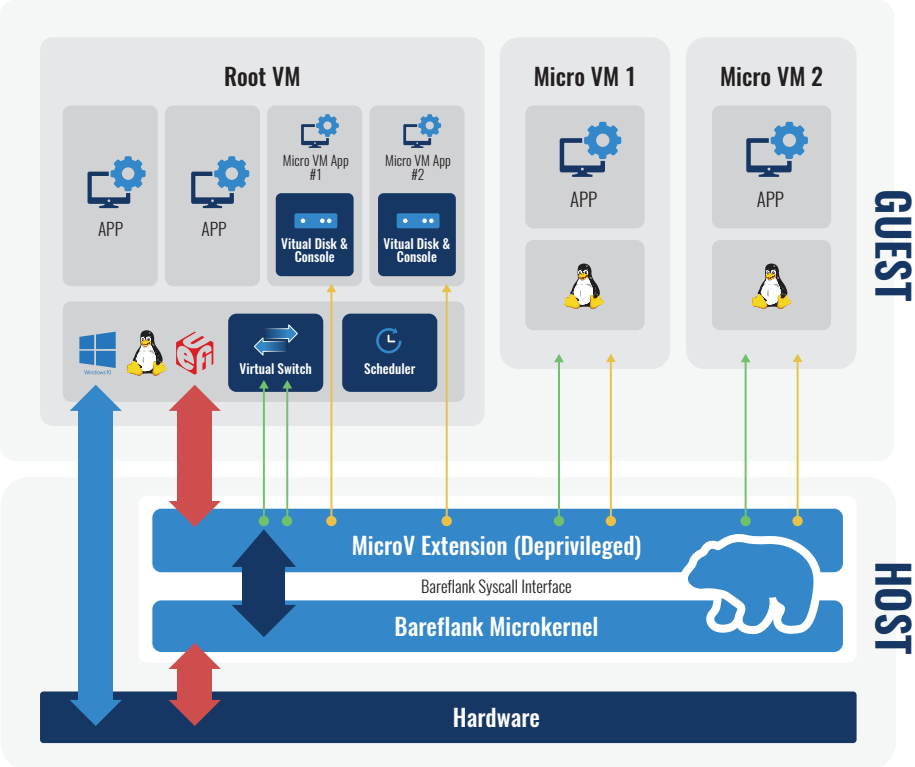
Unlike most other hypervisors, MicroV is open sourced under the MIT license. Feel free to use MicroV in your own commercial products. If you find a bug or want to add a feature, **contact AIS today**.

Under The Hood

MicroV's hypervisor is built using the Bareflank SDK.

Running on top of the Bareflank Microkernel, MicroV is a deprivileged Bareflank extension designed specifically to execute small, fully enlightened virtual machines called Micro VMs. MicroV can either start directly from the root operating system, demoting it into a virtual machine or it can start from UEFI and boot the root operating system inside a virtual machine. From there, additional Micro VMs can be created and executed. Unlike other hypervisors, MicroV gives the root operating system full access to most of the hardware on the device, while still executing under MicroV inside a virtual machine.

This allows MicroV to protect the Micro VMs in addition to the root operating system. MicroV uses the root operating system's scheduler and power management routines to execute each Micro VM. Not only does this improve performance and battery life, it also provides support for any scheduling algorithm you might need including real-time. MicroV removes the need for emulation by requiring each Micro VM to use a fully enlightened kernel (or unikernel), meaning the Micro VM doesn't have access emulated hardware. MicroV accomplishes this by providing its own, custom virtual interface that is designed to further reduce the need for emulation (even more so than existing PV interfaces like virtio). As a result, the entire architecture is dramatically simplified. Addition technical details about MicroV can be found on our **GitHub page**.



The MicroV hypervisor model

FOR MORE INFORMATION

bd@ainfosec.com

Assured Information Security
315.336.3306
WWW.AINFOSEC.COM

About Assured Information Security (AIS)

AIS is a cyber and information technology company that plays a leading role in supporting critical cyber operations for the United States Department of Defense and Intelligence Community. AIS employs expert engineers and research scientists across the United States.