MOSAICS

ABSTRACT

More Situational Awareness for Industrial Control Systems (MOSAICS)
Industry Days, 4 & 5 November 2020, Port Hueneme, CA

Title:

Trusted Compute Base and Active Security for ICS/Critical Infrastructure Protection

Submitted by:

BedRock Systems Inc.

Authors:

John Walsh
Osman Ismael

Point of Contact POC

John Walsh
(813) 508-6920
John@BedRockSystems.com

Submitted: September 15, 2020

Industrial controls systems and critical infrastructure are becoming increasingly dependent on IT/OT networks being perpetually connected. Infrastructure such as Public Transportation, Electrical Grids and the Smart City architecture are highly vulnerable and under attack. The increasing Nation State vulnerabilities (including Supply Chain) are becoming more well known as industry and Governments continue to collaborate to develop and implement solutions/countermeasures. Other countries like Ukraine has experienced Russia taking down major parts of their energy grid and this could happen in the US as well.

As the Nation State threat has pivoted to the cyber physical (OT) domain, so have many of the traditional approaches for asset management, monitoring, detection, and remediation. While attempting to adequately address the unique OT challenges associated with RTOS and software stacks not designed for the new intersection of Safety and Security, the reality of proprietary/multiple protocols, latency, compatibility with brownfield , make it very difficult to provide the end users a “single glass panel” in trusted operational support. The increasing use of virtualization and Software-Defined with the goal of achieving IT/OT convergence while reducing abstraction layers, is a key architectural decision to handle the growing complexity. Furthermore, our National Strategy and Cyber Frameworks are moving forward to address these challenges with methodologies requiring reducing the attack surface and implementing Active Resilience and Zero Trust Architectures - requiring authentication/authorization, continuous monitoring/detection, policy and rules enforcement including real time self-healing capabilities for remediation/restoration.

We will introduce the importance of establishing a mathematically correct Trusted Computing Base (TCB) implementing Virtualization that enables the eco-system to enhance Security, Safety, Supply Chain Risk Management with the flexibility to consolidate / isolate data, workflows and API’s in brownfield and greenfield environments. The presentation will include a reference architecture example illustrating the potential to reduce complexity and some options leveraging industry capabilities we were introduced to at the MOSAIC workshop #2 to achieve the objectives described above.

We will present a formally secure TCB with BedRock Active Security™ that integrates with the ICS eco-system in brownfield and greenfield scenarios leveraging Virtualzation to run unmodified virtual appliances and applications. Formal Verification is used as the underpinning to remove the TCB from the attack vector, while Active Security™ enables anomaly detection and remediation for critical applications and communication in a contested environment. This approach will offer a fail operational architecture based on industry standards, building a trusted infrastructure that allows the eco-system to innovate while under attack.

BEDROCK
Systems Inc

www.BedRockSystems.com

Challenge: Lack of a Verified Trusted Computing Base (TCB)

Solution: Formal Methods Proven Modular Compute Stack with Active Security^{TM}

Commercial Use

- **Wide applications across commercial domain**
  - Enterprise, Critical Infrastructure, Avionics, Autonomous, …
  - Legacy systems compatible – brownfield and greenfield
  - Critical Infrastructure: Energy, Water, Bldg. Automation & FinTech
  - Secure 5G Enclaves: for Smart Cities, Emergency Response, ..
  - Ultra secure mobile phones including Dual Persona
  - Secure IoT/IIoT Connected Devices: incl. nested VPN, Double DAR..
  - Automotive: Autonomous/Head Units
- **Secure Resilient and Zero Trust Systems; Meeting CMMC L4-5 Objectives**
- **Ubiquitous**: Open Source + Commercial market approach – Enables Upstreaming and Commercially Driven Roadmap

DOD Value

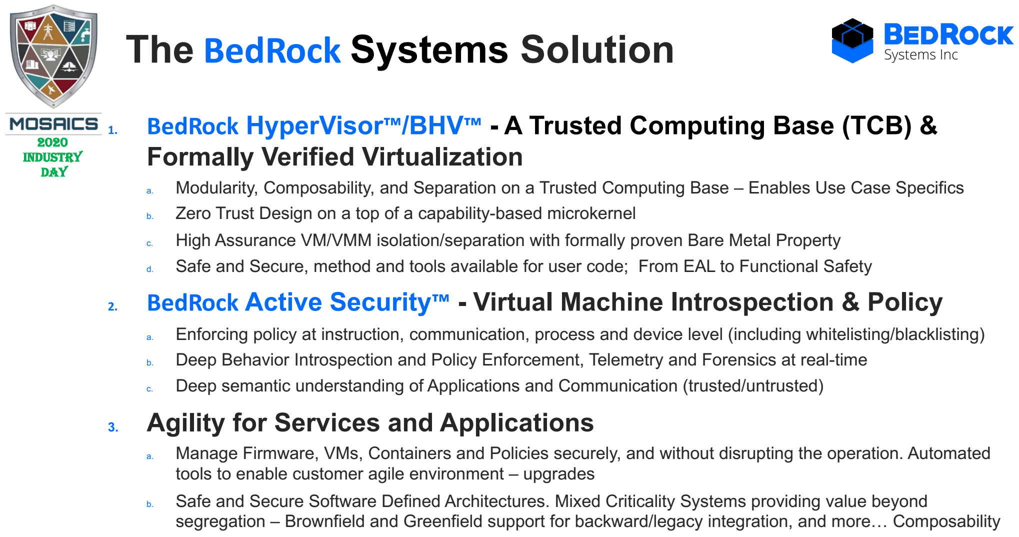
- **Supports current DoD initiatives including Zero Trust, Active Resilience, Cyber Maturity Model Levels 4-5, enhances High Assurance, Supply Chain Integrity and reduces the attack surface.**
- **Secures IoT on COTS for DoD connected device use cases**
- **Enables active resilience and the ability to remediate / restore**
- **Continuous Monitoring/Compliance "up and down the stack" with a capability to isolate and consolidate workloads/abstraction layers**
- **Enables the ability to provide secure enclaves at a larger scale due to the larger Trusted Computing Base….from the Edge to the Cloud**
- **First FM proven TCB with the flexibility to integrate with legacy systems and infrastructure resilience – path forward to the future.**

Technology

- **Type 1 BedRock Hypervisor^{TM} (BHV^{TM})**
  - Virtualization with the Bare Metal Properties
  - BHV based upon NOVA Micro Kernel
  - Supports Multi-Core: ARMv8; X86
- **Formal Methods – extensible beyond the hypervisor "up stack"**
  - Modular Design, API's, and Autonomous FM Tools
- **Isolation/Segregation – VMM per VM with highly scalable Virtual Switch**
  - Capabilities Based Model – bare metal resource allocation/policy
  - Enables forensics at a per VM level
  - Full-Stack verification including concurrency
- **Active Security^{TM}**
  - Continuous Monitoring, Detection, and Response is efficient with our Capabilities Based System
  - VM Introspection – "looking glass vs the Bare Metal"
  - Ability to integrate and look "up the stack and down the stack"

Company Background

- **BedRock Systems Inc.:** brings to market a revolutionary platform – an unbreakable Foundation for Formally Secured Computing and Active Defense
  - Provide the tools for enabling Formal Methods at Scale
  - Deliver software with strong guarantee using Formal Method Verification
- **Founded in 2017:** global leaders in type 1 trusted hypervisor, virtualization, continuous monitoring, detection, response, formal methods at scale, and systems.
- **Experienced Senior Team:** FireEye, Mobile Iron, Citrix, WindRiver, Intel, ADI, and Government Advisory Board
- **Strong Financial Backing:** Wing Capital Ventures, Kleiner Perkins, and others



MOSAICS
2020
INDUSTRY
DAY

The BedRock Systems Solution

BEDROCK
Systems Inc

1. **BedRock HyperVisor™/BHV™ - A Trusted Computing Base (TCB) & Formally Verified Virtualization**
   a. Modularity, Composability, and Separation on a Trusted Computing Base – Enables Use Case Specifics
   b. Zero Trust Design on a top of a capability-based microkernel
   c. High Assurance VM/VMM isolation/separation with formally proven Bare Metal Property
   d. Safe and Secure, method and tools available for user code; From EAL to Functional Safety
2. **BedRock Active Security™ - Virtual Machine Introspection & Policy**
   a. Enforcing policy at instruction, communication, process and device level (including whitelisting/blacklisting)
   b. Deep Behavior Introspection and Policy Enforcement, Telemetry and Forensics at real-time
   c. Deep semantic understanding of Applications and Communication (trusted/untrusted)
3. **Agility for Services and Applications**
   a. Manage Firmware, VMs, Containers and Policies securely, and without disrupting the operation. Automated tools to enable customer agile environment – upgrades
   b. Safe and Secure Software Defined Architectures. Mixed Criticality Systems providing value beyond segregation – Brownfield and Greenfield support for backward/legacy integration, and more… Composability

The BedRock Systems solution can be summarized as a:

1. A formal methods mathematically proven Trusted Computing Base (TCB) and Virtualization architecture that provides modularity, composability, and high assurance separation between VM's that are capable of running unmodified guest applications.

2. The Active Security^{TM} layer provides network and data integrity by employing Virtual Machine introspection within the boundaries of trust providing fine grain monitoring for verification and enforcement of software and data integrity. For example: continuous monitoring and enforcement of network traffic that both ingress and egress the VM's - providimg the ability for deep inspection: or enforcing the concept of least functionality in the control systems and detecting attempts to bypass policies; or data fusion for telemetry and analytics. We provide mechanisms that define trust and can implement policies at the binary or instructions level to determine whether things are operating trusted and apply constraints in the case they are not. There are many examples of what can be done within this Active Security and VM environment.

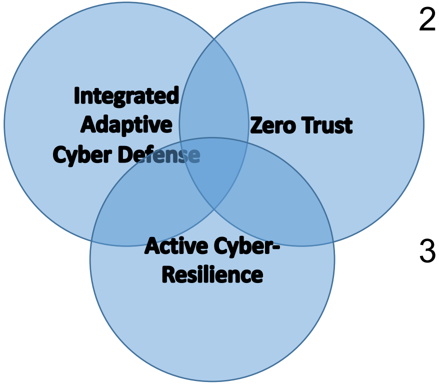
3. Finally, working with the MOSAICS eco system partners, provide the tools and capabilities to configure for use case specific implementations easing modernization, consolidation, and integration of both legacy brownfield and greenfield system with new safety and security capabilities.

MOSAICS
2020
INDUSTRY
DAY

Synergies This Brings to MOSAICS

Building a Foundation/Chain of Trust

BEDROCK
Systems Inc



Integrated Adaptive Cyber Defense

Zero Trust

Active Cyber-Resilience

1. Trusted Computing Base – Formal Method Automation
2. Leverage Trusted Virtualization to Consolidate Work/Data Flows and Abstraction Layers:
    a. Modularity and Composability
    b. Modernization of Brownfield
    c. Enable Software Defined
    d. Reduced Attack Surface
3. Real Time Monitoring, Detection, Telemetry, and Response at a Granular Behavior Level Including:
    a. Black/White Listing; integrating AI/ML and deep Semantics
    b. Supply Chain Risk Management
    c. IACD/Active Resilience in Contested Environment
4. Integrate / Interactive with up stack layers

Some of the synergies BedRock brings to MOSAICS are summarized on this chart. Working with partners such as those participating in the MOSAICS industry day event, we can integrate the specific capabilities necessary to establish a foundation of trust, integrity, and the ability to achieve the objectives of INTEGRATED ADAPTIVE CYBER DEFENSE, ACTIVE RESILIENCE, AND ZERO TRUST.

For example – operating in a contested environment we can detect changes in behavior or performance to trigger a response such as the reallocation or rebooting of resources using contingent VM's, telemetry information up the stack, and implement behavior constraints to limit adversarial actions or ensure safe operations.

MOSAICS
2020
INDUSTRY
DAY

BEDROCK
Systems Inc

What Gap Does This Fill In MOSAICS?

“Single Pane of Glass”

Situational Awareness

Policy/Rules Enforcement

Data Stream Integrity & Threat Detection

Asset/Config Mgmt & Threat Assessment

Identity

1. Cyber-attacks are moving down the computing stack exploiting vulnerabilities to gain access then traversing virtualization, software, and devices to compromise the entire system of systems architecture... evading the cyber systems that protect us.
   a. The platforms, devices, and virtualization that are the foundation of our cyber security applications, sensors, et al must be on a trusted computing base and operating in a trusted environment.
2. Defense in depth: Foundational/Multiple Layer Defense/Resilience
3. Modernization of legacy systems and next generation software defined require trusted virtualization for composability, introspection, consolidation, ease of integration.
4. IACD/Active Resilience – i.e. TCB, threat monitoring/detection, supporting fail safe (black/white listing) response, self-healing with contingent VM/VMM’s and software.

Trust starts at the foundation of the applications and analytics that we rely on within the architecture itself. Being closer to the silicon, we can provide separation of duty via segmentation and fine grain monitoring to detect behavior and enforce only those that are permited via policy. Including the detection of abnormal behavior indicative of a potential supply chain threat.

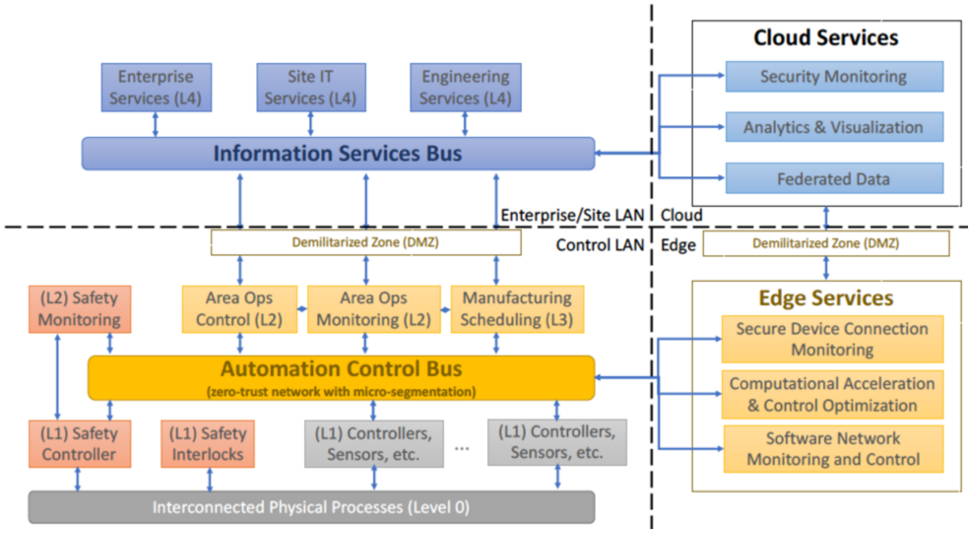
As part of the MOSAICs team, BedRock can work with the OEM solutions architects to focus on the high priority gaps and close them.

MOSAICS 2020 INDUSTRY DAY

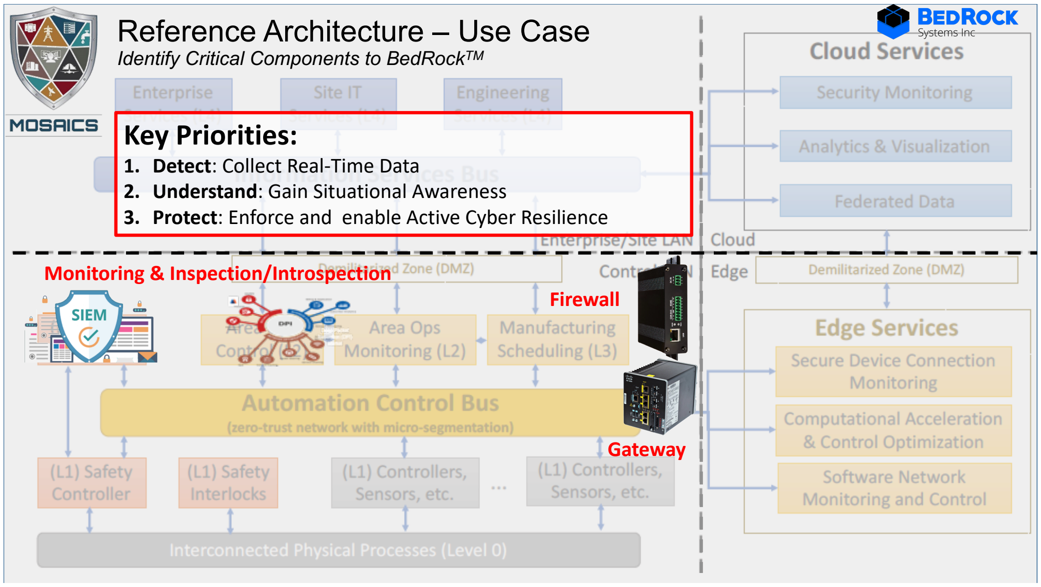
Reference Architecture – Use Case

Identify Critical Components to BedRock™

BEDROCK Systems Inc



Let's take a typical Industrial Control System Architecture consisting of the enterprise, automation, and services provided both at the edge and via cloud.



Reference Architecture – Use Case

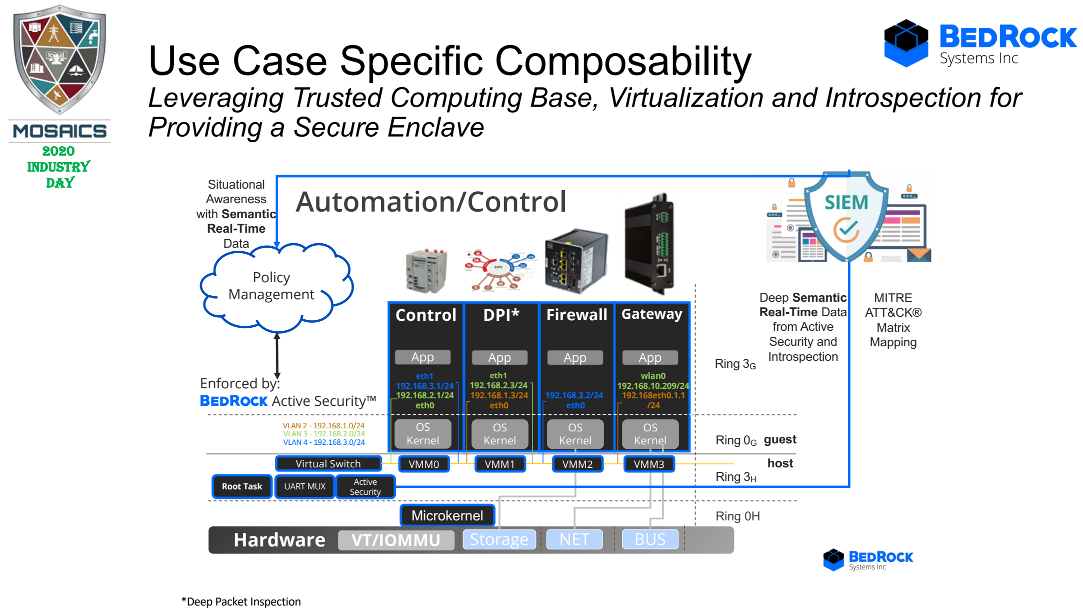
Identify Critical Components to BedRock™

Key Priorities:

1. **Detect**: Collect Real-Time Data
2. **Understand**: Gain Situational Awareness
3. **Protect**: Enforce and enable Active Cyber Resilience

MOSAICS
BEDROCK Systems Inc
Enterprise
Site IT
Engineering
Cloud Services
Security Monitoring
Analytics & Visualization
Federated Data
Enterprise/Site LAN
Cloud
Monitoring & Inspection/Introspection
Demilitarized Zone (DMZ)
Control LAN
Edge
Demilitarized Zone (DMZ)
SIEM
Firewall
Area Ops Control (L2)
Area Ops Monitoring (L2)
Manufacturing Scheduling (L3)
Edge Services
Secure Device Connection Monitoring
Computational Acceleration & Control Optimization
Software Network Monitoring and Control
Automation Control Bus
(zero-trust network with micro-segmentation)
Gateway
(L1) Safety Controller
(L1) Safety Interlocks
(L1) Controllers, Sensors, etc.
...
(L1) Controllers, Sensors, etc.
Interconnected Physical Processes (Level 0)

Any number of methods can be used to determine what applications and data are highest priority for establishing a trusted computing base and leveraging the virtualization for consolidation and the use of active security for achieving the kind of objectives discussed previously. In this case we establish our key priorities as specific gateways, servers and boxes that are used for the routing or aggregating Real Time Data, Authentication of Identity for Access,Providing Situational Awarenenss or Analytics, and Enforcing Rules/Policies.



MOSAICS 2020 INDUSTRY DAY

Use Case Specific Composability

Leveraging Trusted Computing Base, Virtualization and Introspection for Providing a Secure Enclave

BedRock Systems Inc

Automation/Control

Situational Awareness with **Semantic Real-Time** Data

Policy Management

Enforced by: BedRock Active Security™

SIEM

Deep **Semantic Real-Time** Data from Active Security and Introspection

MITRE ATT&CK® Matrix Mapping

Control | DPI* | Firewall | Gateway

App | App | App | App

eth1 192.168.3.1/24 192.168.2.1/24 eth0 | eth1 192.168.2.3/24 192.168.1.3/24 eth0 | 192.168.3.2/24 eth0 | wlan0 192.168.10.209/24 192.168eth0.1.1 /24

OS Kernel | OS Kernel | OS Kernel | OS Kernel

VLAN 2 - 192.168.1.0/24
VLAN 3 - 192.168.2.0/24
VLAN 4 - 192.168.3.0/24

Virtual Switch | VMM0 | VMM1 | VMM2 | VMM3

Root Task | UART MUX | Active Security

Microkernel

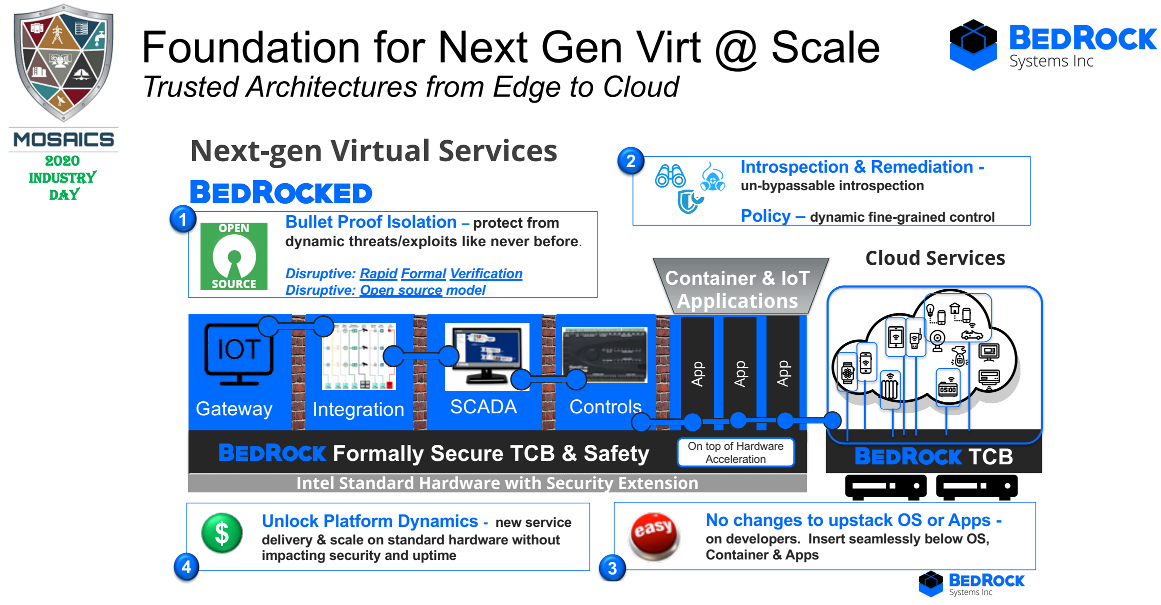
Hardware | VT/IOMMU | Storage | NET | BUS

Ring 3_G
Ring 0_G guest
host
Ring 3_H
Ring 0H

*Deep Packet Inspection

This illustrates leveraging the trusted virtual environment for system composability for consolidatation and segregation using multiple VM’s to monitor and enforce integrity locally, enable trusted communication and telemetry situational awareness for policy enforcement.

As ICS solutions are being re-architected BedRock brings the opportunity to do platform consolidation on both ARM and x86. Hardware platform and Boards can be shared with full isolation, enabling leveraging COTS, simplifying deployment topology and optimizing security – all at the same time with very significant cost savings. This approach will also provide velocity in deploying new versions of software as well as new solutions integrated on the same platform alongside existing solutions.



MOSAICS 2020 INDUSTRY DAY

Foundation for Next Gen Virt @ Scale

Trusted Architectures from Edge to Cloud

BedRock Systems Inc

Next-gen Virtual Services

BEDROCKED

1 **Bullet Proof Isolation** – protect from dynamic threats/exploits like never before.
Disruptive: Rapid Formal Verification
Disruptive: Open source model

OPEN SOURCE

2 **Introspection & Remediation** - un-bypassable introspection
Policy – dynamic fine-grained control

Container & IoT Applications

Cloud Services

IOT Gateway | Integration | SCADA | Controls | App | App | App

BedRock Formally Secure TCB & Safety | On top of Hardware Acceleration

Intel Standard Hardware with Security Extension

BedRock TCB

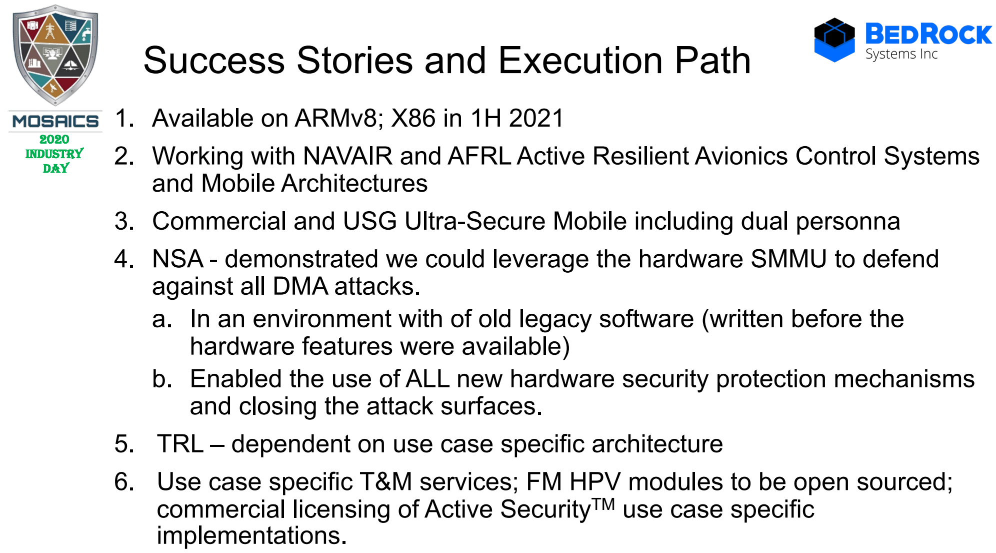
4 **Unlock Platform Dynamics** - new service delivery & scale on standard hardware without impacting security and uptime

3 **No changes to upstack OS or Apps** - on developers. Insert seamlessly below OS, Container & Apps

easy

This illustrates using the same features and the next level of virtualization and integration which some of the eco-system partners are looking at.

Unclassified
09/15/2020

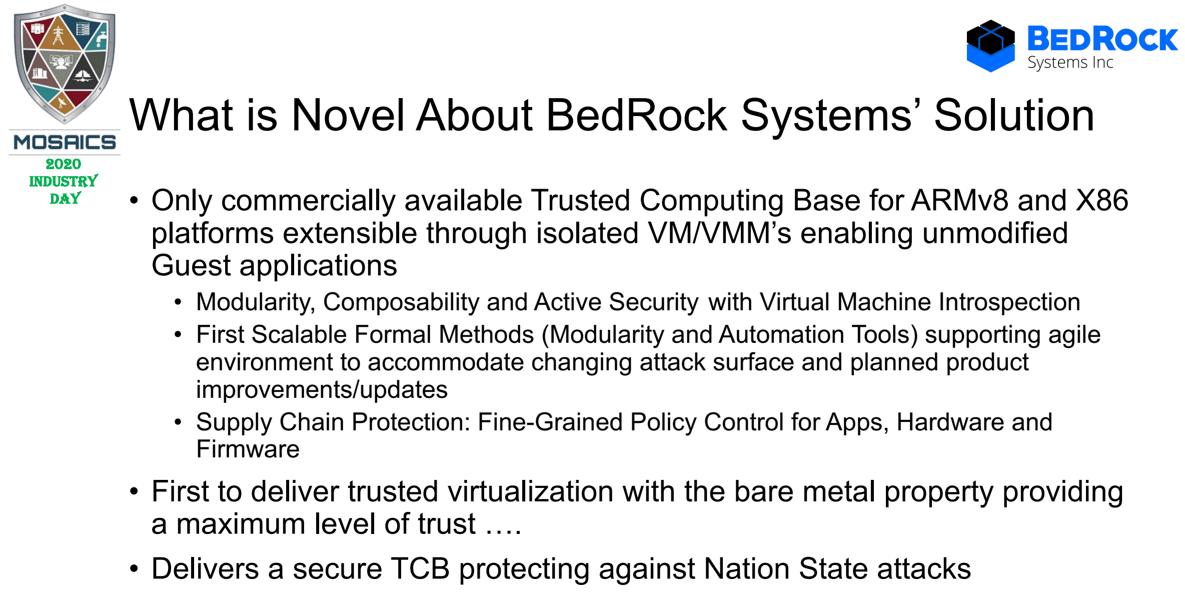


Success Stories and Execution Path

MOSAICS
2020
INDUSTRY
DAY
BEDROCK
Systems Inc

1. Available on ARMv8; X86 in 1H 2021
2. Working with NAVAIR and AFRL Active Resilient Avionics Control Systems and Mobile Architectures
3. Commercial and USG Ultra-Secure Mobile including dual personna
4. NSA - demonstrated we could leverage the hardware SMMU to defend against all DMA attacks.
   a. In an environment with of old legacy software (written before the hardware features were available)
   b. Enabled the use of ALL new hardware security protection mechanisms and closing the attack surfaces.
5. TRL – dependent on use case specific architecture
6. Use case specific T&M services; FM HPV modules to be open sourced; commercial licensing of Active Security^{TM} use case specific implementations.

Some of our success stories and use cases are listed. Specific relationship to MOSAICS will be the work we are doing on resilient controls architectures and our successful defense of a brute force attack on legacy hardware and software implementing BedRock.



What is Novel About BedRock Systems' Solution

MOSAICS
2020
INDUSTRY
DAY
BEDROCK
Systems Inc

- Only commercially available Trusted Computing Base for ARMv8 and X86 platforms extensible through isolated VM/VMM's enabling unmodified Guest applications
  - Modularity, Composability and Active Security with Virtual Machine Introspection
  - First Scalable Formal Methods (Modularity and Automation Tools) supporting agile environment to accommodate changing attack surface and planned product improvements/updates
  - Supply Chain Protection: Fine-Grained Policy Control for Apps, Hardware and Firmware
- First to deliver trusted virtualization with the bare metal property providing a maximum level of trust ….
- Delivers a secure TCB protecting against Nation State attacks

In summary, what is novel about BedRock"s Solution is it is the first commercially available Trusted Computing Base with Virtualization and Active Security to provide the feature capabilities described.

BedRock is the first introduce automated tools and modularity to enable the extension and scale-ability of formal methods to the Guest VM and supporting an agile design and product lifecycle.

We provide trust to the mechanisms that define trust. We can provide and implement policies at fine grain to determine the trustworthiness of software and data running BedRocked^{TM} platforms.