MOSAICS
2020 INDUSTRY DAY

BEDROCK Systems Inc

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

MOSAICS
2020 INDUSTRY DAY

The BedRock Systems Solution

BEDROCK Systems Inc

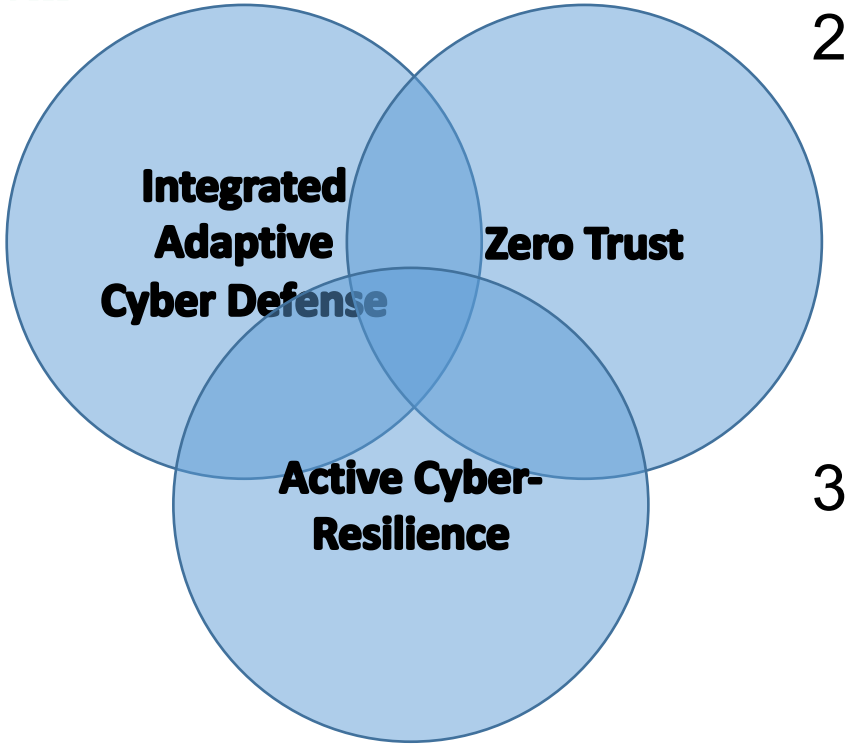
1. **BedRock HyperVisor™/BHV™ - A Trusted Computing Base (TCB) & Formally Verified Virtualization**
   a. Modularity, Composability, and Separation on a Trusted Computing Base – Enables Use Case Specifics
   b. Zero Trust Design on a top of a capability-based microkernel
   c. High Assurance VM/VMM isolation/separation 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

Synergies This Brings to MOSAICS

Building a Foundation/Chain of Trust

MOSAICS 2020 INDUSTRY DAY

BEDROCK Systems Inc



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

MOSAICS
2020 INDUSTRY DAY

BEDROCK Systems Inc

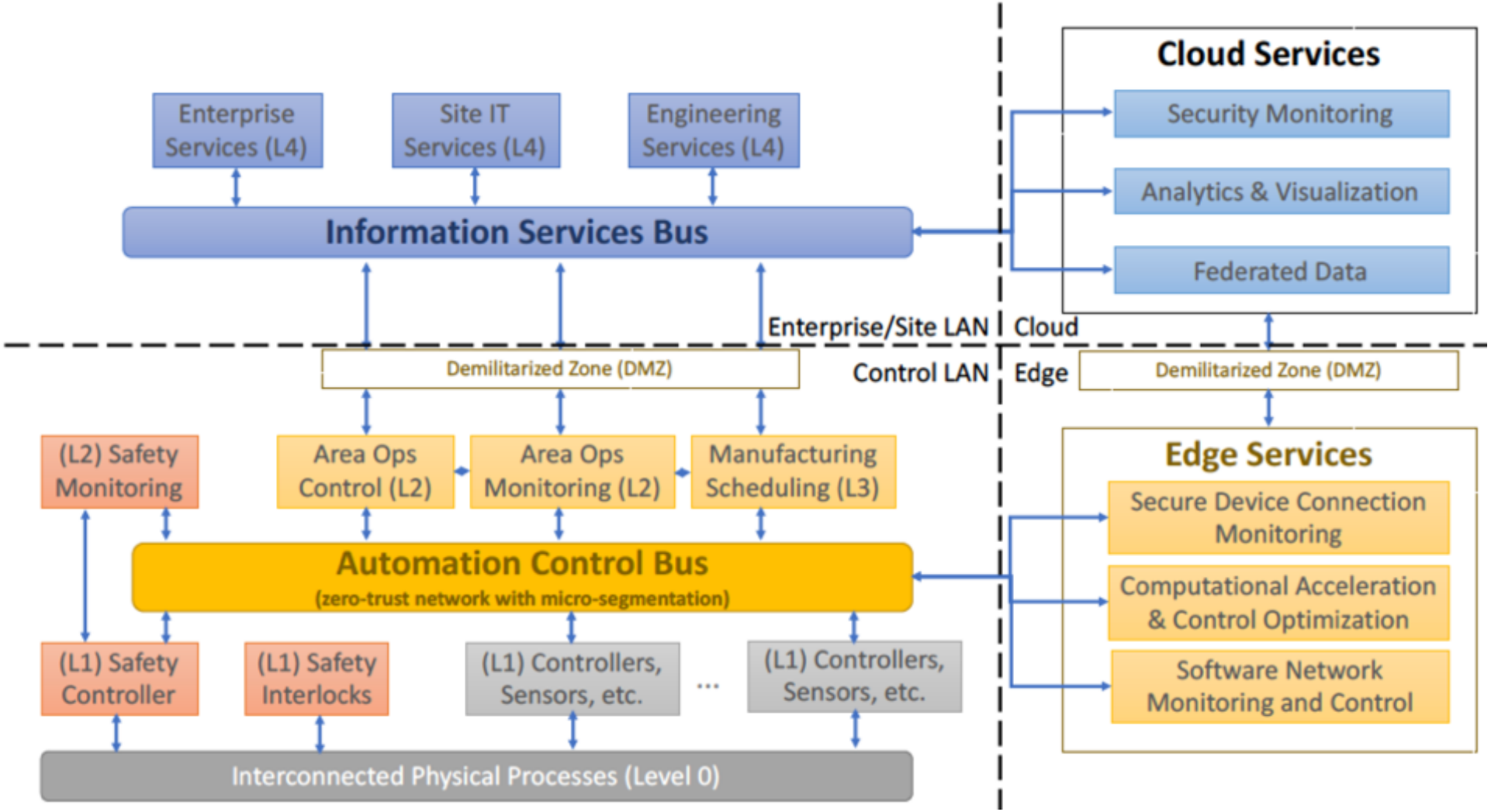
What Gap Does This Fill In MOSAICS?

"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.

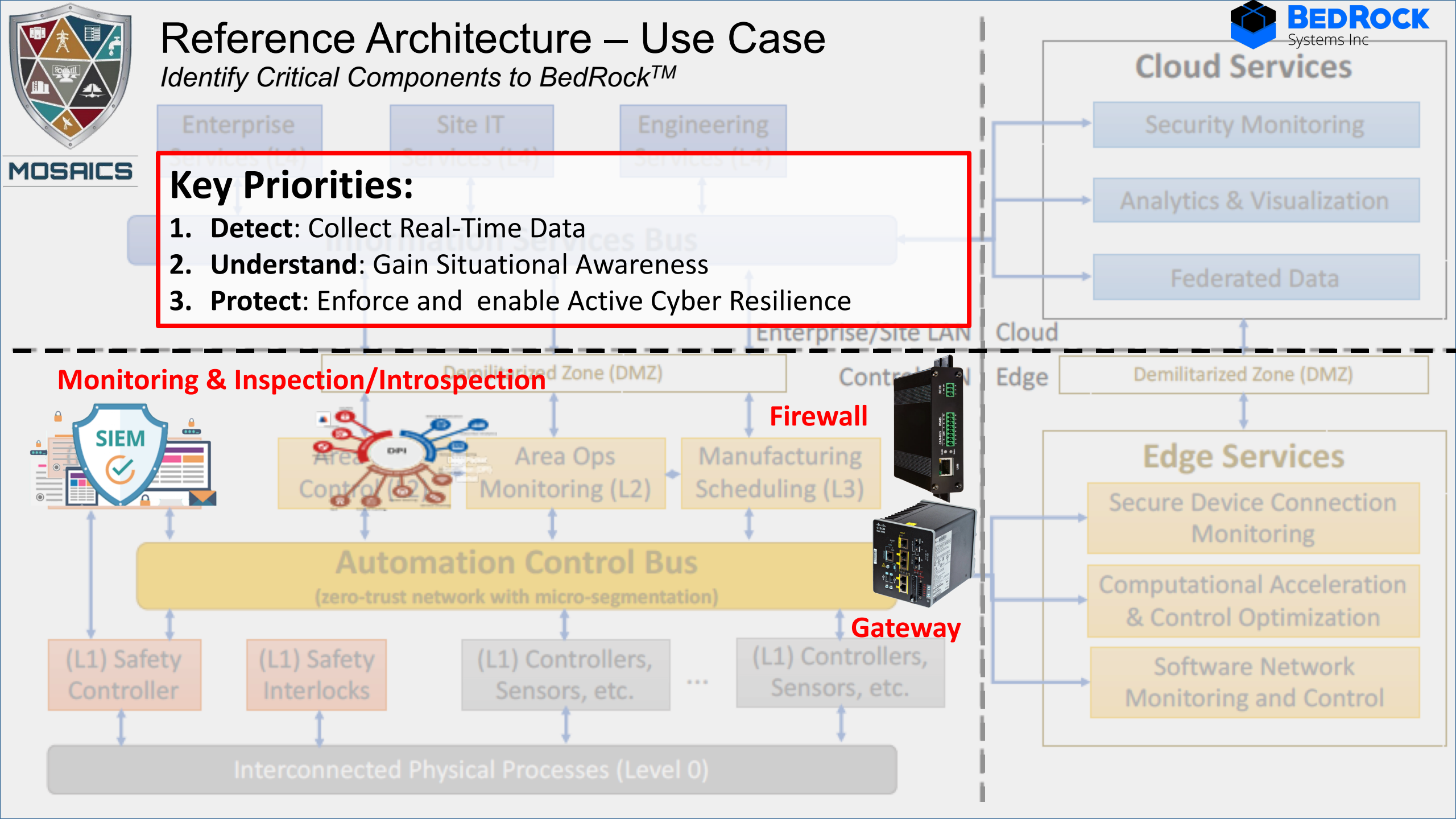
Reference Architecture – Use Case

Identify Critical Components to BedRock™



Reference Architecture – Use Case

Identify Critical Components to BedRock™



Key Priorities:

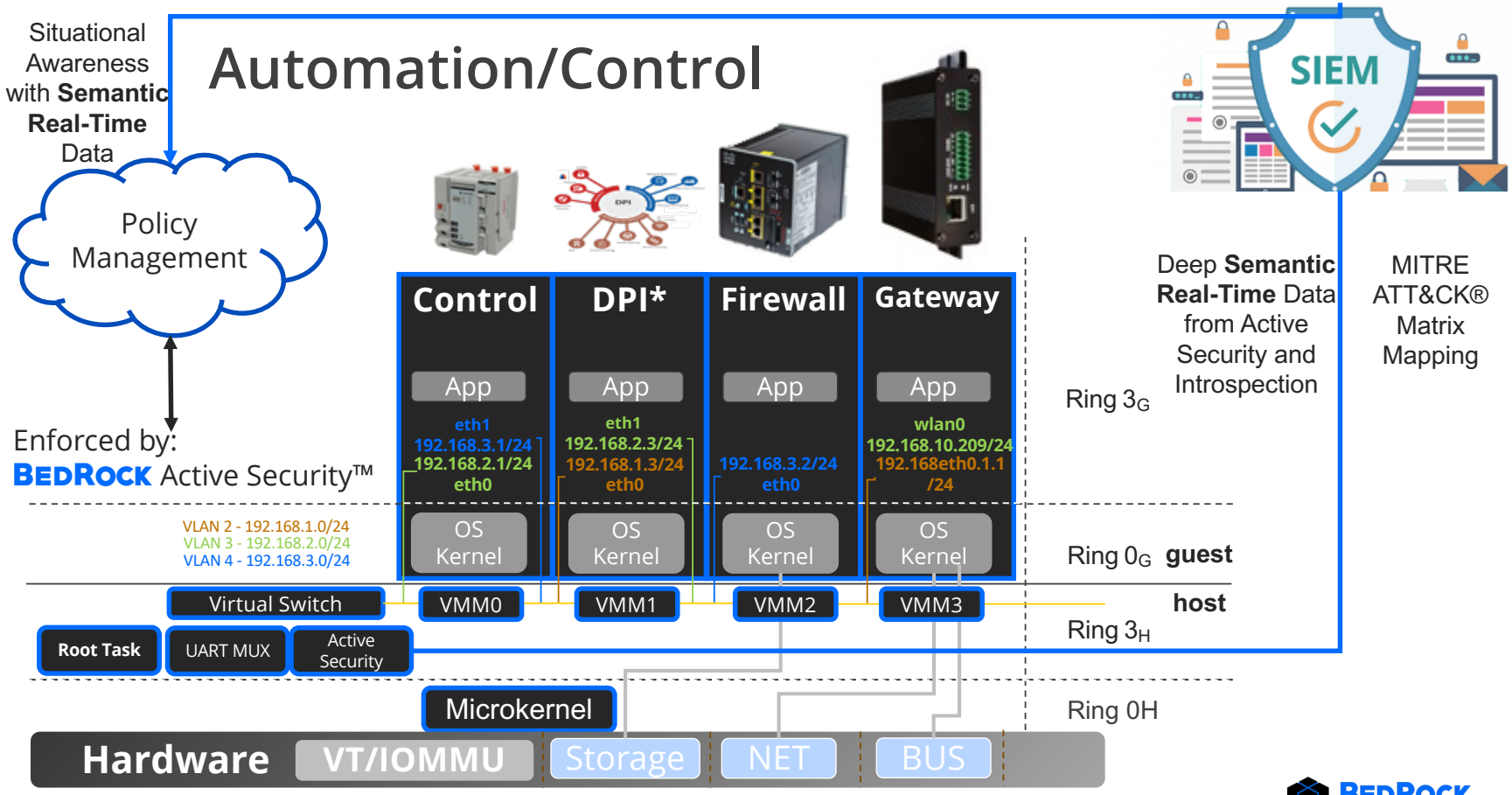
1. **Detect**: Collect Real-Time Data
2. **Understand**: Gain Situational Awareness
3. **Protect**: Enforce and enable Active Cyber Resilience

MOSAICS
2020 INDUSTRY DAY

BEDROCK Systems Inc

Use Case Specific Composability

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



BEDROCK Systems Inc

*Deep Packet Inspection

Foundation for Next Gen Virt @ Scale

Trusted Architectures from Edge to Cloud

MOSAICS 2020 INDUSTRY DAY

BEDROCK Systems Inc

Next-gen Virtual Services

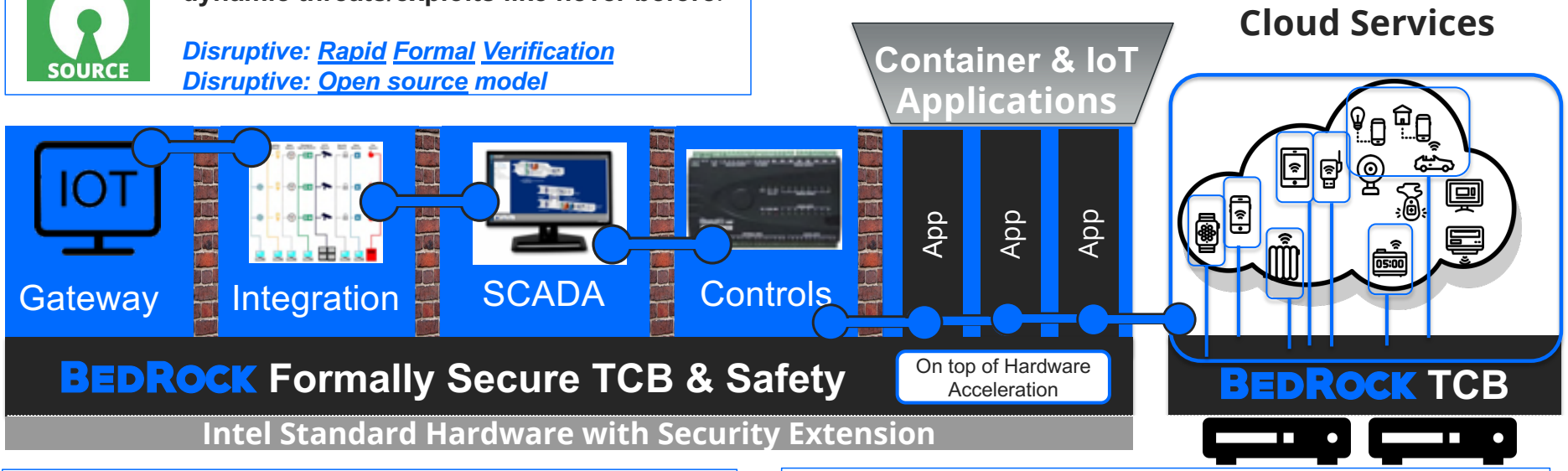
BEDROCKED

1 **Bullet Proof Isolation** – protect from dynamic threats/exploits like never before.

Disruptive: Rapid Formal Verification
Disruptive: Open source model

2 **Introspection & Remediation -** un-bypassable introspection

Policy – dynamic fine-grained control



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

BEDROCK Systems Inc

MOSAICS
2020 INDUSTRY DAY

BEDROCK Systems Inc

Success Stories and Execution Path

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™ use case specific implementations.

MOSAICS
2020 INDUSTRY DAY

BEDROCK Systems Inc

What is Novel About BedRock Systems' Solution

- 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

MOSAICS
2020
INDUSTRY
DAY

BEDROCK
Systems Inc

Point of Contact: John Walsh
BedRock Systems Inc.
John@BedRockSystems.com
813-508-6920