ami | TruE™

Features

TRUST IN YOUR DATA CENTER

Establish and track the trust status of all compute servers in the data center.

COMPLY WITH DATA SOVEREIGNTY

Ensure seamless compliance with various regional data sovereignty regulations.

RUN SENSITIVE WORKLOADS ON TRUSTED SERVERS

Ensure workloads containing sensitive information run only on trusted nodes with KUBERNETES® integration.

EXTENSIBLE SOLUTION WITH RESTFUL API

Elect to use AMI TruE out-of-the-box or integrate AMI TruE with your existing data center management infrastructure.

ATTEST NEW SERVER INSTALLATIONS

Avoid supply chain attacks and other physical tampering.

With more than 35 years as the leader in BIOS/BMC firmware development, AMI® leverages its deep understanding in firmware to bring a suite of trusted firmware security products to enterprise clients and data center operators.

The need to secure firmware is growing at an exponential rate according to NIST, the National Institute of Standards and Testing. This is a result of the amount of firmware in the data center increasing over the years as platforms become more complex and components require their own firmware. With security issues becoming more common at the firmware level, organizations must be able to assure the integrity of their platform firmware. AMI TruE™ delivers holistic data center security solutions using Intel® Security Technologies and Intel® Security Libraries for Data Centers to provide a **Tru**sted **E**nvironment for cloud execution.

Platform Trust

AMI TruE uses a trust agent running at the OS level to collect firmware and software hash information from the Trusted Platform Module (TPM), which is used to determine platform trust by comparing this hash information to known trusted hashes. A customer installed and managed attestation server will keep all the various hashes collected across the data center and track which ones are trusted or untrusted. When a node is found to be untrusted, it can be scheduled for automatic firmware updates based upon data center policy.

ami®
power • manage • secure

Core Management Features

- Automatic Discovery
- Event Logging
- Alerts and Notification
- User Management
- Provisioning Framework for Remediation Actions
- Automation via RESTful APIs

Privacy & Data Sovereignty

AMI TruE enables data centers and businesses the ability to comply with privacy laws and data sovereignty regulations by binding the server's geographic location to its asset tag information – creating what is called a geo-tag. With AMI TruE, protected personal data can be identified and separated, and compliance with data sovereignty regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), can be assured.

Customization with Flavors

Combine platform requirements in any combination to create flavors. Flavors help determine whether a particular compute node is suitable for certain workloads. Apply one or more flavors to any subset of your managed environment to enforce platform trust requirements, operating system requirements, geographic location requirements, and more. AMI TruE even gives you the ability to create custom attributes for your flavors.

Integration with Cloud Orchestration

By assuring that your environment is running only trusted firmware and software, integration with popular industry cloud orchestration software, such as KUBERNETES®, allows AMI TruE to ensure that workloads containing sensitive information or data requiring data sovereignty compliance are run only on trusted compute nodes in the required geographic location. KUBERNETES® integration allows for the enforcement of flavors to be automated by the data center workload orchestration environment.

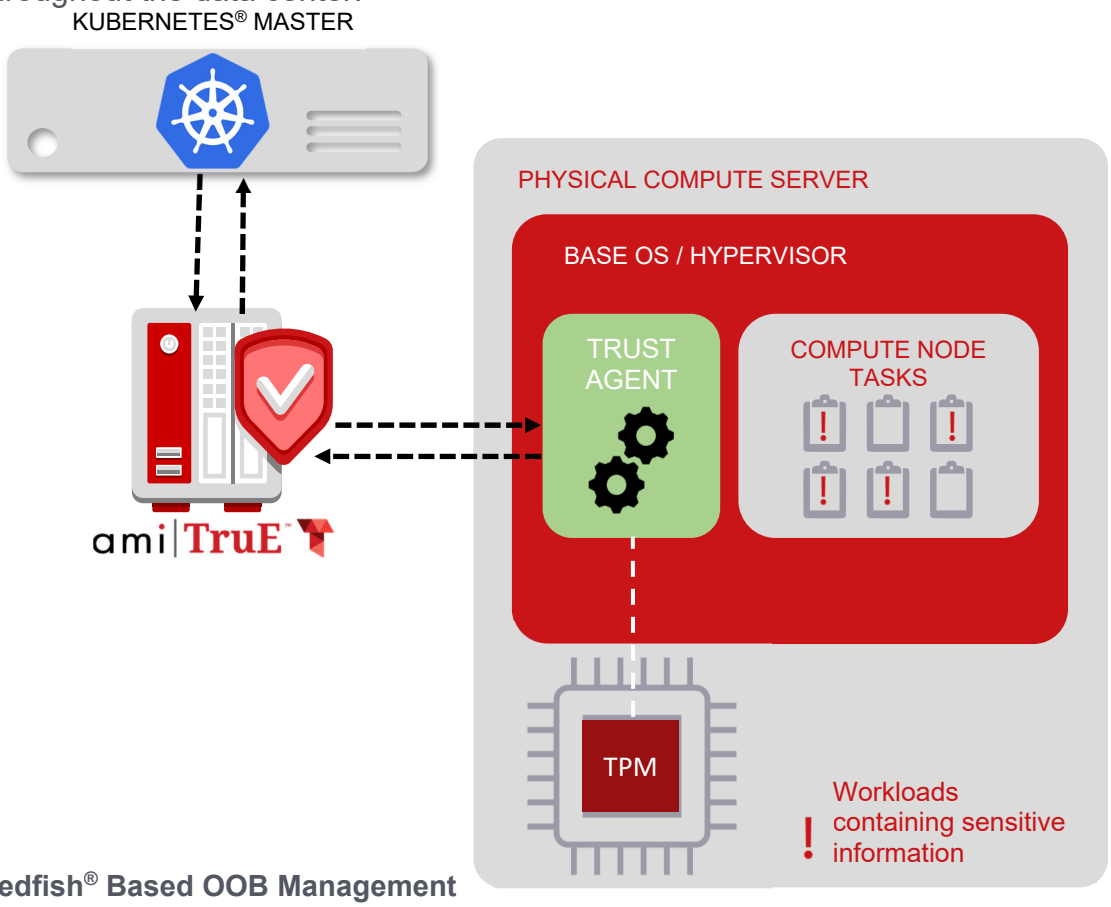
Designed with Extensibility in Mind

AMI TruE comes as an out-of-the-box product of the AMI Composer® product line, that focuses on platform security features, and uses RESTful APIs for ease of integration into other data center management environments.

ami®
power • manage • secure

End-to-End Security with AMI TruE

AMI TruE helps data centers secure platforms throughout the entire product life cycle. Supply chain attacks can be easily avoided by attesting the shipped firmware and software hash information with the attestation server upon installation into an existing trusted environment. After deployment, server trust validation continues to attest the integrity of the firmware and software running throughout the data center.



Redfish® Based OOB Management

AMI TruE features includes Redfish based out-of-band management capabilities. Redfish based management leverages platform security features that ensure all managed servers are secure. Redfish features include hardware inventory, server health monitoring, platform BIOS configuration as generic redfish features. AMI TruE also supports Remote KVM and Remote Media Redirection on specific platforms.

For more information, please visit:
ami.com/true

ami®
power • manage • secure