ami | TruE®

With more than 35 years as the leader in BIOS and BMC firmware development, AMI has applied its deep understanding of firmware to the AMI TruE Trusted Environment Security Solution for cloud service providers and datacenter operators looking to ensure platforms and workloads are secure and can be trusted with sensitive data and workloads.

As security threats and attacks increase on a near daily basis, firmware security has come into sharper focus - along with the need to keep devices secure at the platform level. These growing threats are particularly critical for cloud service providers and data centers, who have a fundamental need to verify the trust status of every platform in the datacenter throughout its lifecycle.

To help combat these threats, AMI TruE enables confidential computing, easy to deploy workload attestation and protection of application keys without compromising confidentiality or adding cost. It delivers a holistic, secure datacenter solution that is scalable, extensible and built for cloud-to-edge applications. It establishes and tracks the servers' trusted compute status in the datacenter, complies with data sovereignty regulations, runs sensitive workloads on trusted servers and provides remediation measures for untrusted platforms.

AMI TruE isolates sensitive data in an encrypted CPU enclave during processing, using Intel® Software Guard Extensions (Intel® SGX) and Intel® Security Libraries for Data Centers (Intel® SecL-DC) found in the latest Intel® Xeon® Processors to provide a true trusted environment for confidential computing and secure cloud execution.

Key Features:

END-TO-END TRUST IN YOUR DATACENTER

Establish and track the trust status of all compute servers in the datacenter from installation, deployment and beyond.

COMPLY WITH DATA SOVEREIGNTY

Ensure compliance with regional data sovereignty regulations.

APPROVES SENSITIVE WORKLOADS ONLY ON TRUSTED SERVERS

Ensure workloads containing sensitive information run only on trusted nodes.

EXTENSIBLE SOLUTION WITH RESTFUL APIs

AMI TruE offers seamless integration with existing datacenter management infrastructure such as with KUBERNETES®.

AMI TruE helps datacenters secure platforms throughout the entire platform life cycle, by providing end-to-end firmware security and verification across the datacenter and integrating with other datacenter management and orchestration tools to provide a holistic view of platform firmware security for all servers in use. Supply chain attacks can be easily avoided by attesting the shipped firmware and software hash information of new platforms. After deployment, server trust validation continues to attest the integrity of the firmware and software running across the enterprise.

Trusted Hardware

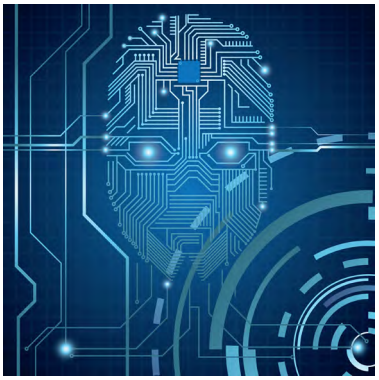
The future of trusted hardware is here now. Running sensitive workloads in a black box, such as in an Intel® SGX secure enclave, furthers data privacy, sovereignty and protection in the cloud by reducing the attack surface in the data center. Intel® Software Guard Extensions (Intel® SGX), Intel® Security Libraries for Data Centers (Intel® SecL-DC) and AMI TruE enables Platform Trust and Runtime Encryption.

Platform Trust

The AMI TruE trust agent operates 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 it to known trusted hashes. The attestation server maintains all the hash information collected across the data center and tracks the trust status of each. When a node is found to be untrusted, it can be scheduled for automatic firmware updates based upon datacenter policies.

Core Management Features

- Automatic Discovery
- Event Logging
- Alerts and Notification
- User Management
- Provisioning Framework for Remediation Actions
- Automation via RESTful APIs
- Redfish® -based out-of-band (OOB) management for security of all managed servers
- Generic Redfish features include hardware inventory, server health monitoring, platform BIOS configuration
- AMI TruE also supports Remote KVM and Remote Media Redirection (on specific platforms)



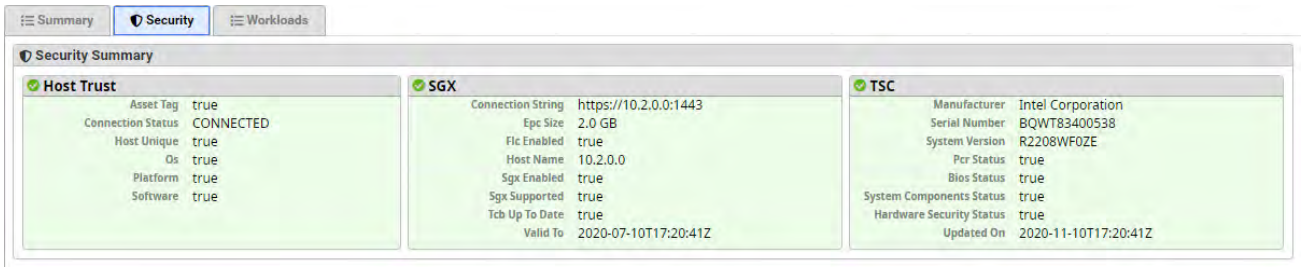
Intel® SGX + AMI TruE Deliver Confidential Computing

Leveraging Intel® SGX secure enclaves, AMI TruE enables secure computing, easy to deploy workload attestation and secure application keys without compromising confidentiality – to deliver a secure data center solution that is scalable, extensible and built for cloud-to-edge applications without compromise.

Privacy & Data Sovereignty

AMI TruE bolsters the ability of datacenters, cloud service providers and end users to comply with privacy laws and data sovereignty regulations by binding the server's geographic location to its asset tag information to create a geo-tag. AMI TruE identifies and separates protected data to ensure compliance with regional data sovereignty regulations such as GDPR and CCPA.

Customization with Flavors



Attest New Server Installations

Avoid supply chain attacks and other physical tampering with robust attestation and remediation.

For more information please visit: ami.com/true