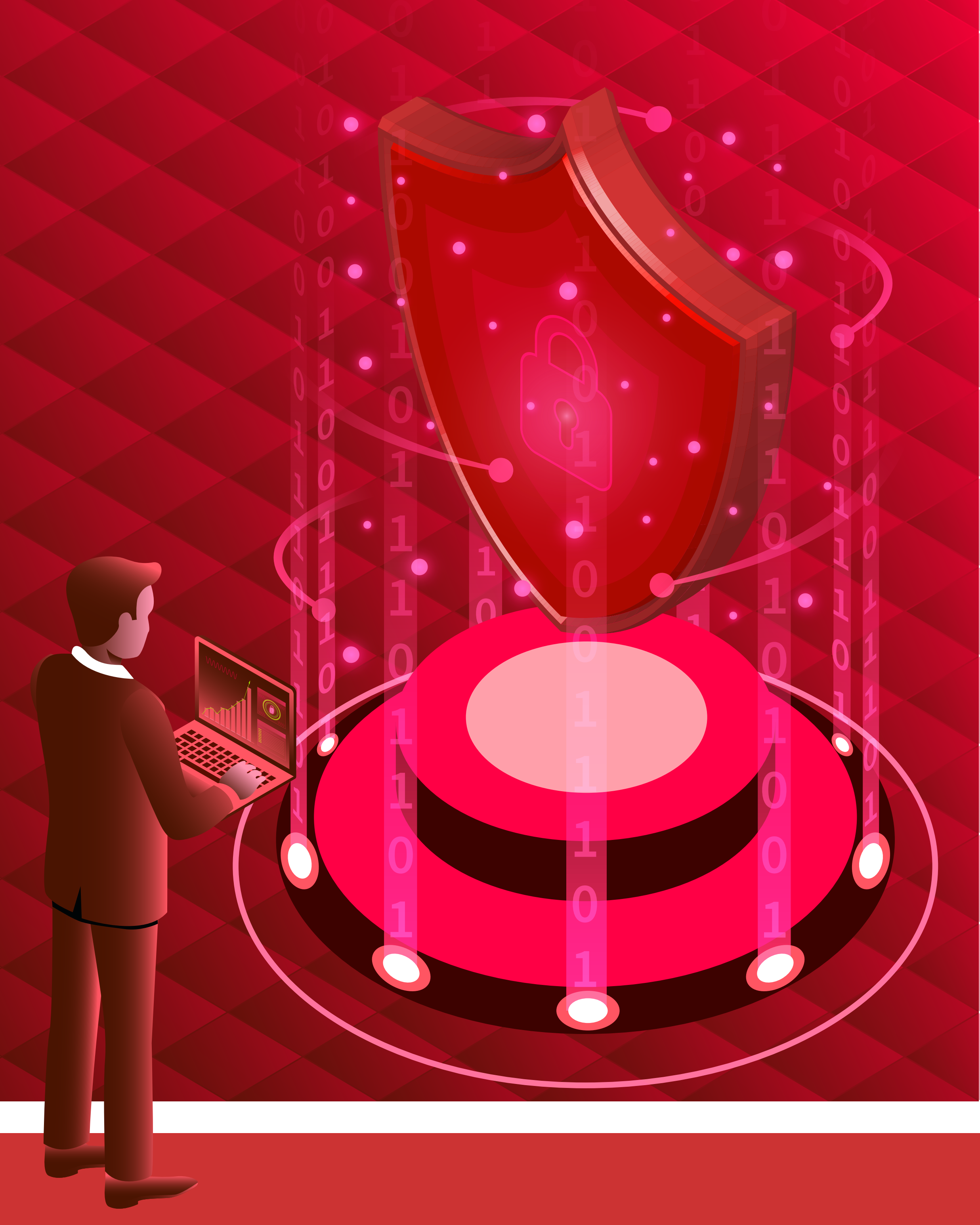
ami
power · manage · secure

ami | TruE™
TRUSTED ENVIRONMENT



Confidential Computing

*is an **industry initiative** focused on*

- **Securing data-in-use** by enabling encrypted data to be processed in memory.
- Addresses the challenge of **protecting data-in-use**.
- Because data-in-use needs to be decrypted before it gets processed by a workload, it is exposed in RAM during processing, making it vulnerable.

Powering **Confidential Computing** with **AMI TruE™** and **Intel's Software Guard Extensions (SGX)** and **Secure Key Caching (SKC)** Library

FEATURES AND BENEFITS

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.

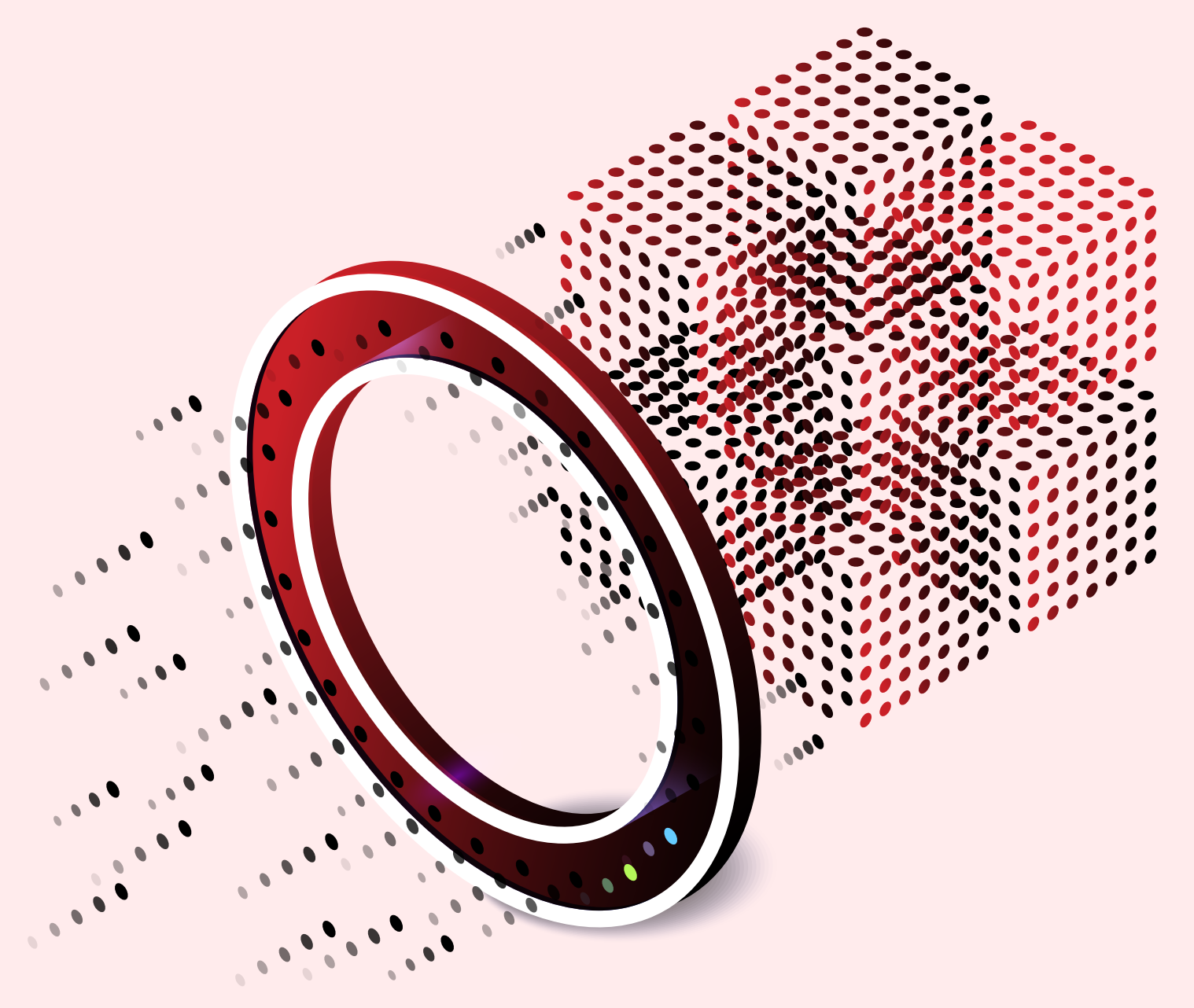
ATTEST
NEW SERVER INSTALLATIONS
Avoid supply chain attacks and other physical tampering.

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.

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.

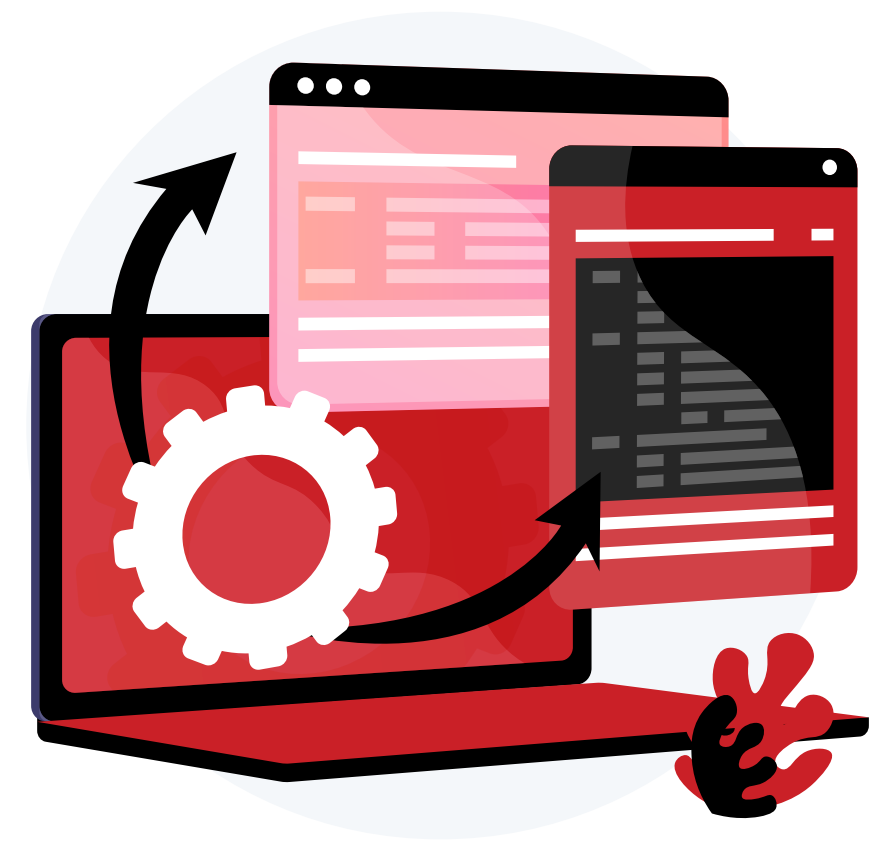


PRIVACY AND DATA SOVEREIGNTY

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.



DESIGNED WITH EXTENSIBILITY IN MIND

While AMI TruE comes as an extension to our **AMI Composer™** data center management software for an out-of-the-box product, it uses **RESTful APIs** for ease of integration into other data center management environments.

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.

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.

ami.com/**true**