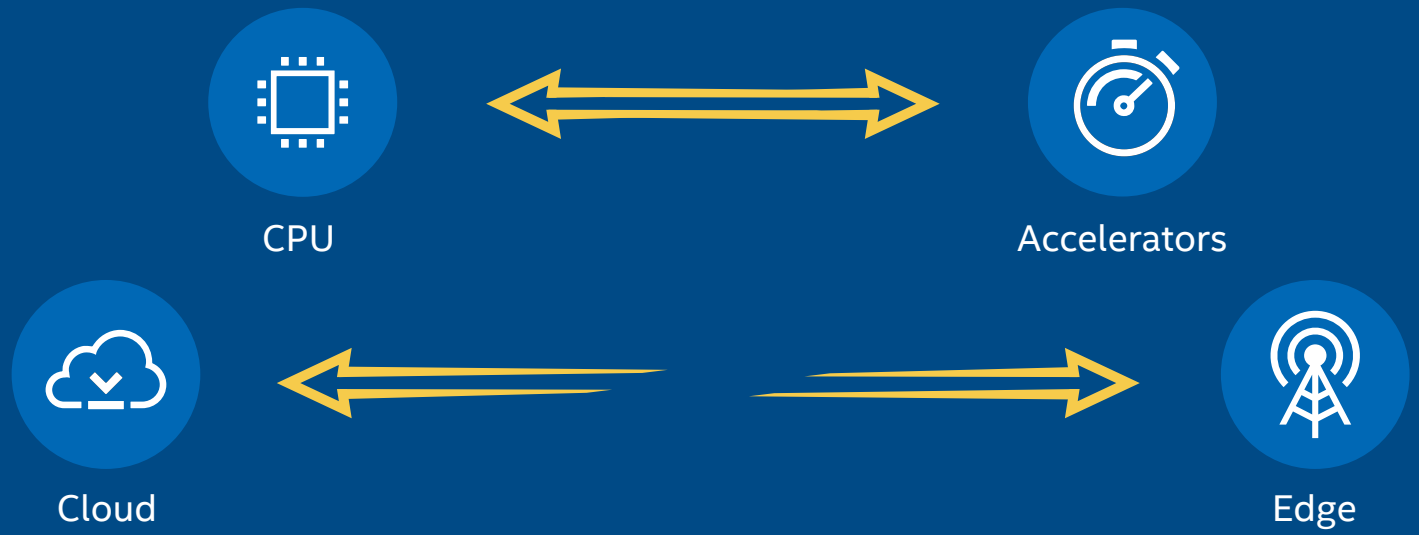
Designing Data Center Security for the Future

Anil Rao, Vice President & GM of Data Security, Systems and Architecture Group

Data Centric Security Strategy

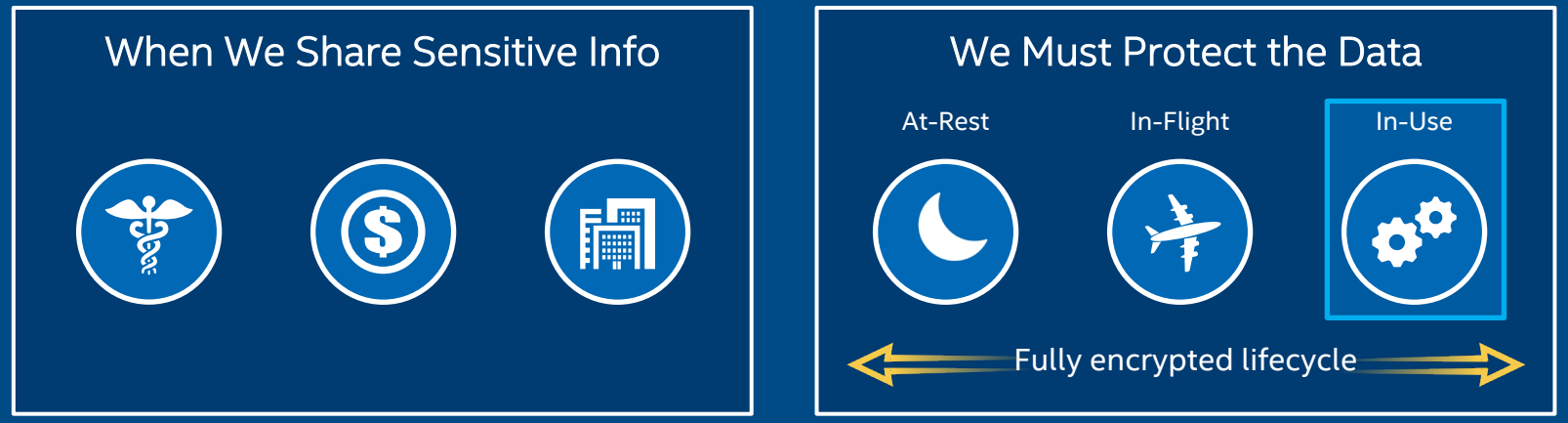
Rooted in silicon, Intel security technologies help create a trusted foundation

Expanding Protections Across Domains



In a data-centric world, security is an end-to-end imperative

The New Frontier of Data Protection



Confidential Computing:

Focuses on protecting data during computation, especially when it takes place in a platform or environment, we do not directly control

Data Protection Innovations Coming

Working to bring new innovations to make data protections scalable and provide more choice

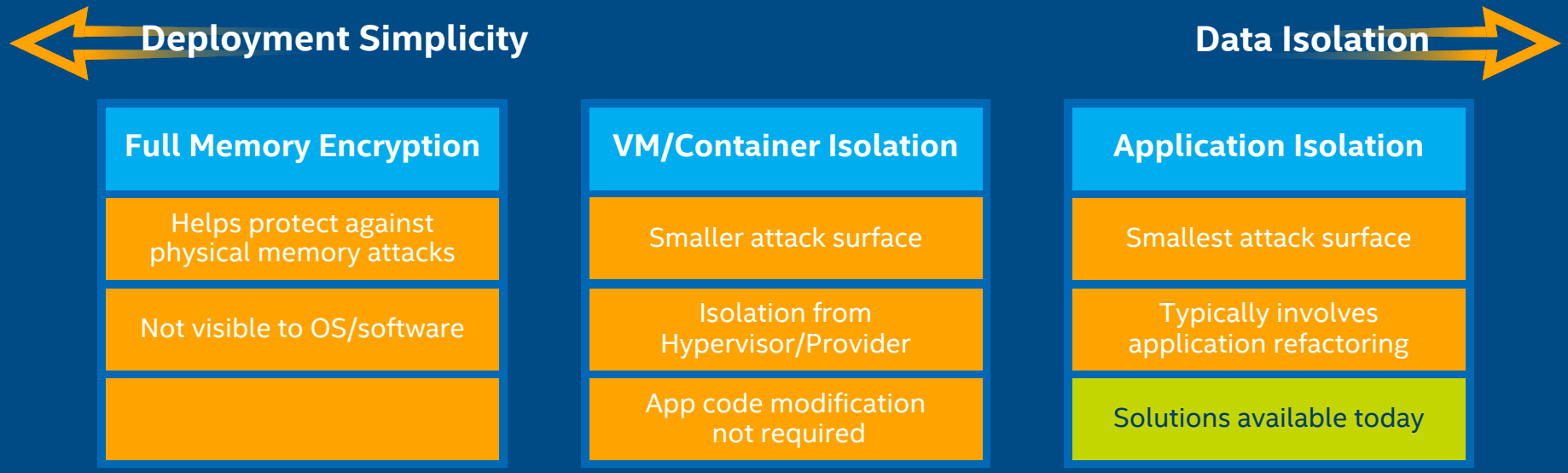
Full Memory Encryption

VM/Container Isolation

Application Isolation

Data Protection Innovations Coming

Working to bring new innovations to make data protections scalable and provide more choice



Customers choose level of protection required within the spectrum of end-to-end security

Expanding Confidential Computing Usages

Cloud Infrastructure
Protect the confidentiality and integrity of customer data in-use in the multi-tenant public clouds

Federated Learning
Enable parties to securely conduct machine learning across broader data sources while keeping algorithms and data sets confidential

Native Application Hosting
Run even native unmodified applications inside enclaves with the benefits of virtualization and enhanced security

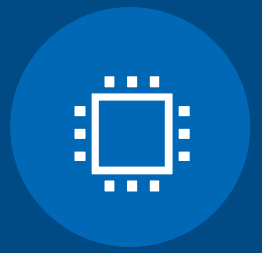
Blockchain
Keep private data and transactions secure for authorized network participants and improve scalability capabilities

Trusted Multi-Party Compute
Enable multiple untrusting parties to interact on shared data while keeping sensitive data confidential

Secure Key Management
Provide unified HSM and key management capabilities on a scalable distributed architecture

Intel® Software Guard Extensions Application Isolation Available Today

Hardware assists in establishing trust



Intel SGX is data center ready

Intel SGX ecosystem is 100+ strong

Research community helps strengthen Intel SGX

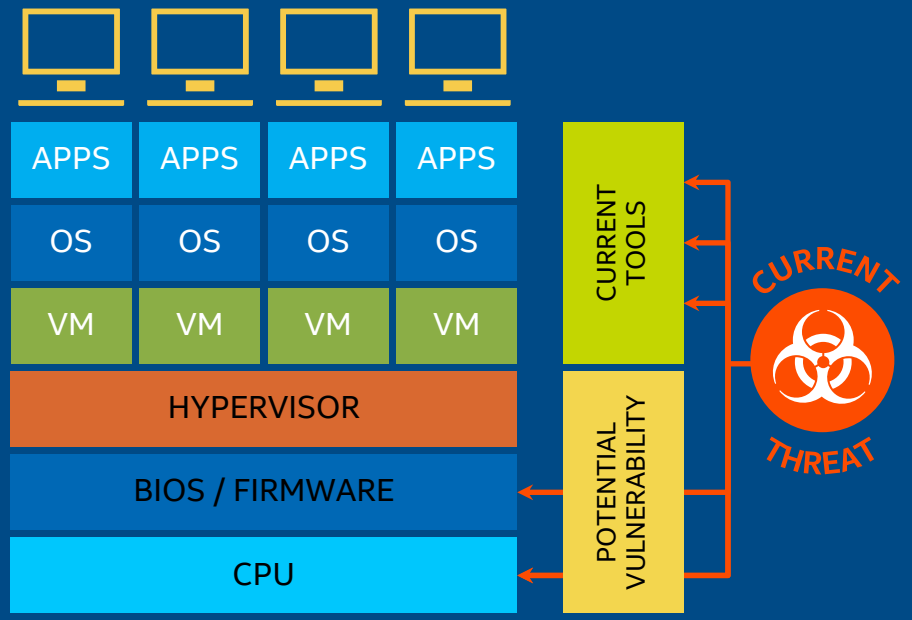
Production deployments in cloud, sensitive workloads

Solutions in-market today protecting sensitive workloads

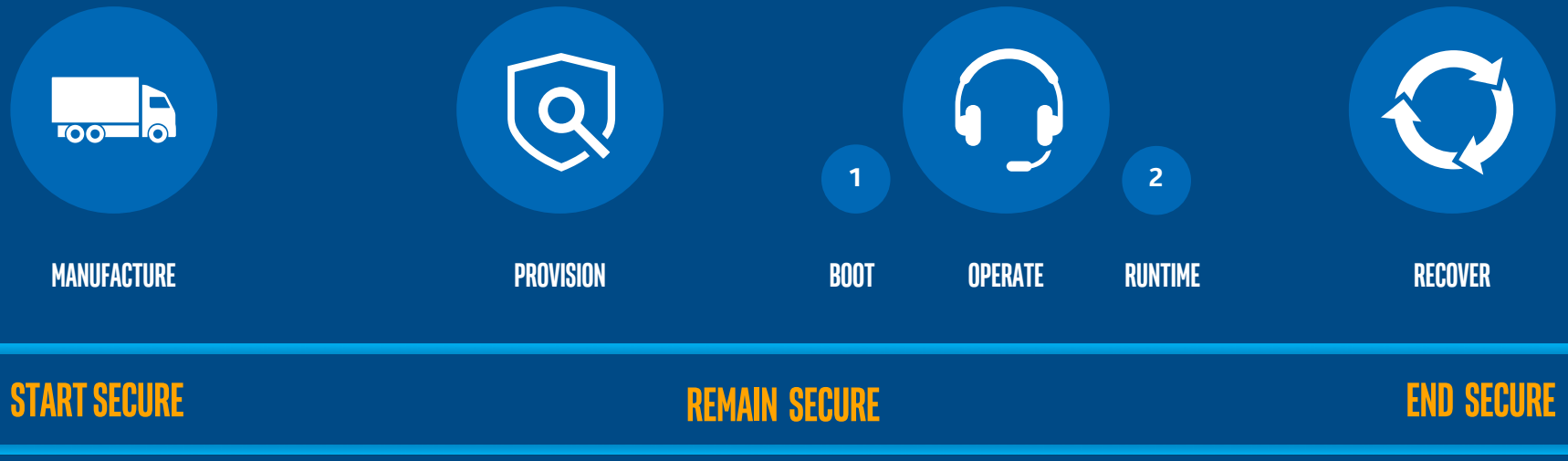
Security is Built on a Foundation of Trust

Hardware Root of Trust

- Foundation for data center security solutions
- Begin with a secure source in silicon
- Establish a chain-of-trust up the boot stack all the way to the application
- Enable ecosystem solutions with software libraries for streamlined integration



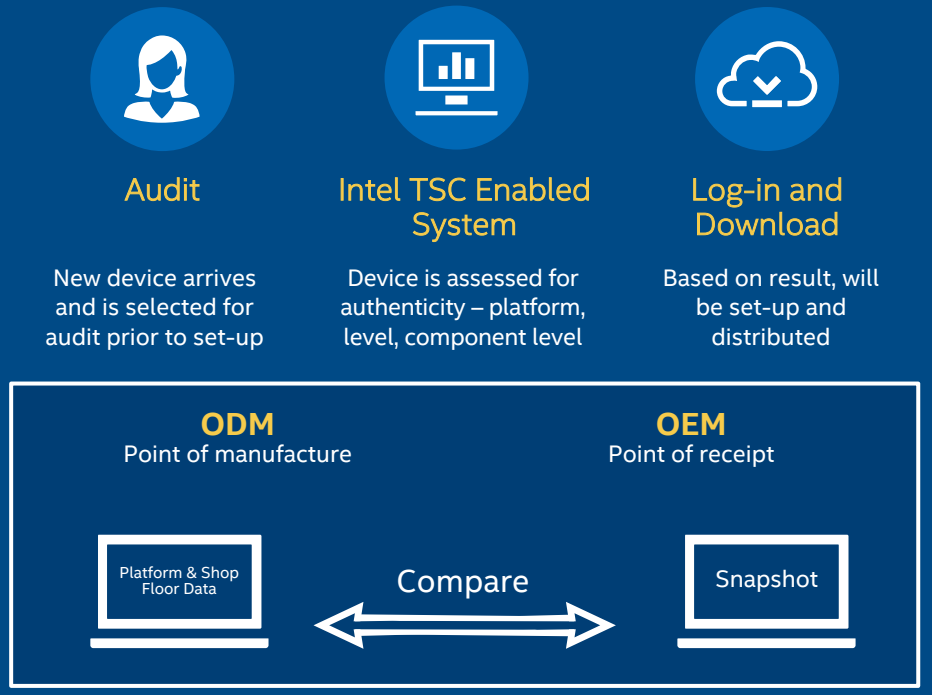
Platform Provenance and Supply Chain Security



New Intel Technologies Addressing:

Transparent Supply Chain | Trusted Boot | Firmware Resilience

Intel® Transparent Supply Chain



Know Exactly What You Get

Better quality, performance, lifespan

Detect Tampering

Review current inventory for suspect parts and attest to authenticity of the platform

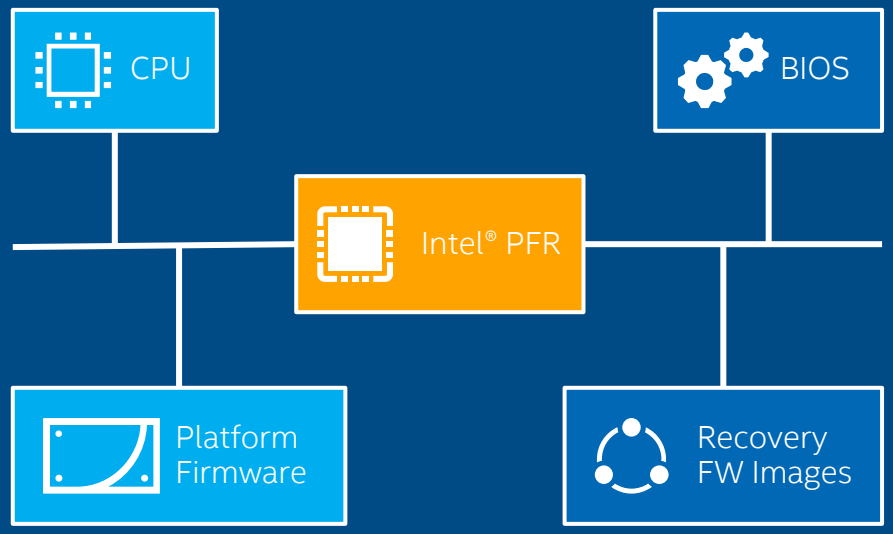
Helps Meet Procurement Guidelines

DFARS – two levels of component transparency

TOOLS AND METHODOLOGY FOR ENSURING AUTHENTICITY

Intel® PFR Helps Protect Platform Firmware

Intel® FPGA-based platform root of trust delivers NIST* SP800-193 Firmware Resiliency



PROTECT Monitors and filters malicious traffic on system buses

DETECT Verifies integrity of platform firmware images before executing

CORRECT Automatically restores corrupted firmware from a protected gold recovery image

Confidential Computing Consortium

Intel is a founding member of this open source community dedicated to defining and accelerating the adoption of confidential computing

Alibaba Cloud
facebook
intel
swisscom
arm
Fortanix
Microsoft
Tencent 腾讯
Bai 百度
Google
ORACLE
vmware
decentriq
HUAWEI
Red Hat
and growing...

Learn and Engage With Us

We encourage you to engage with us in dialogue and can also provide more information on programs we've developed for our customers and partners

intel® select solution

- Simplified evaluation
- Fast and easy to deploy
- Workload optimized
- Visit www.intel.com/selectsolutions

SECURITY BUILDERS

- Technical training
- Access to pre-launch and NDA Intel® technologies
- Reference architectures and technical documentation
- Visit https://builders.intel.com/

www.intel.com/securityinnovations


intel