Intel® Network Builders Insights Series

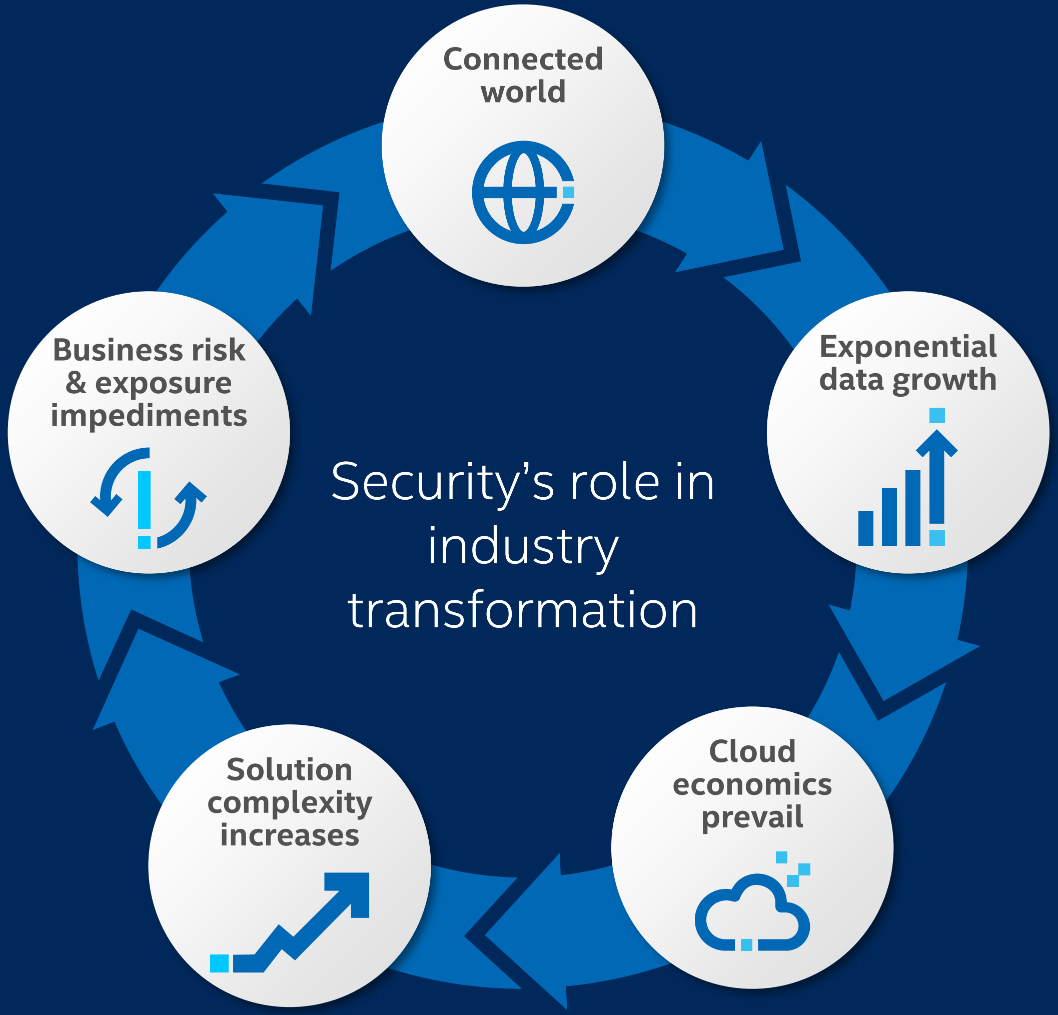
Security Features in 3rd Gen Intel® Xeon® Scalable Processors

- Xiaojun (Shawn) Li, Sales Director, Next Wave OEM & eODM
- Bill Carlson, Solutions Architect, Data Platforms Group, Network and Communications Sales Organization

Notices and Disclaimers

- Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
- Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.
- Your costs and results may vary.
- Intel technologies may require enabled hardware, software or service activation.
- © Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Data Center Security Landscape



Connected world

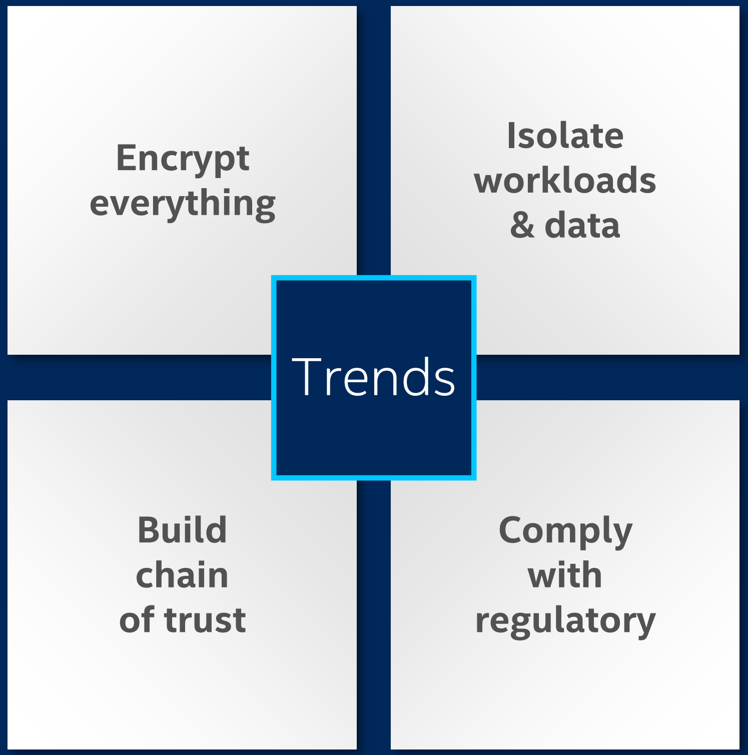
Exponential data growth

Cloud economics prevail

Solution complexity increases

Business risk & exposure impediments

Security's role in industry transformation



Trends

Encrypt everything

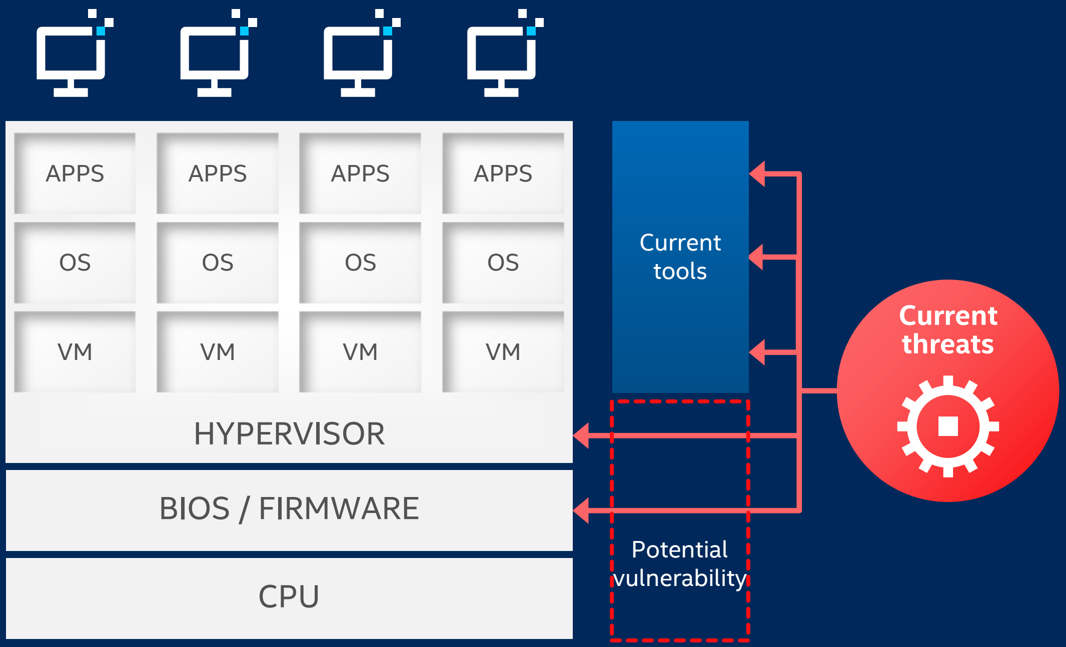
Isolate workloads & data

Build chain of trust

Comply with regulatory

Data Center Security Strategy

Effective security is built on a **foundation of trust**



Protect the **Data**

- **at rest**
- **in flight**
- **in use**

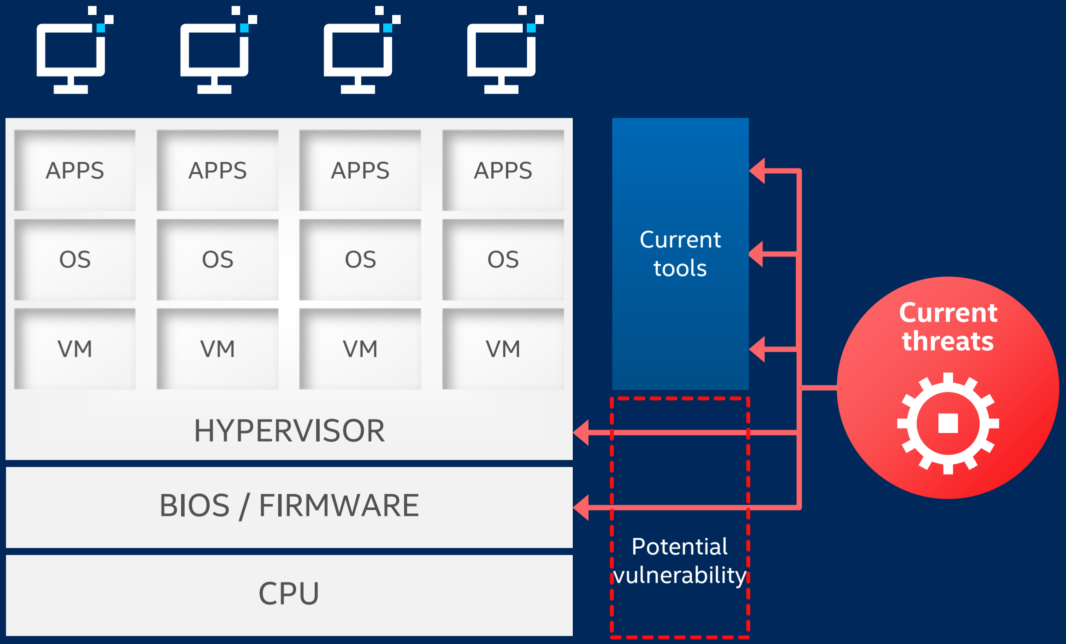
Protect the **Platform**

- **trust**
- **resilience**
- **visibility**

Enable **Performance**

Data Center Security Strategy

Effective security is built on a **foundation of trust**



Protect the **Data**

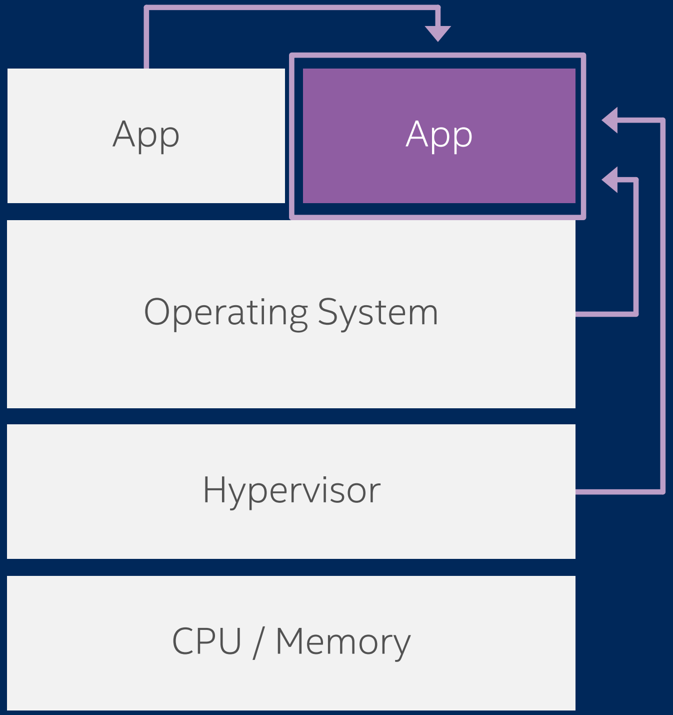
- at rest
- in flight
- in use

Protect the **Platform**

- trust
- resilience
- visibility

Enable **Performance**

Why protect data in use?



Protect against…

Malicious insiders with escalated admin privileges

Hackers exploiting bugs in the hypervisor/OS

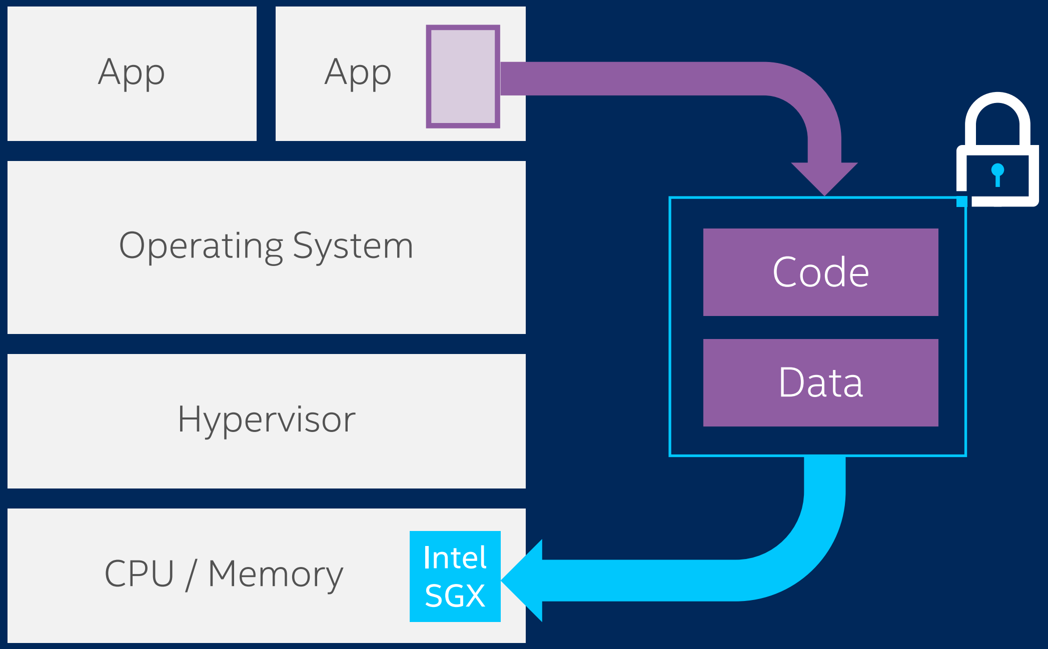
Third parties accessing data without owner's consent

Data & computation exposed to…

- **Guest OS**
- **Host OS**
- **Hypervisor**
- **Physical hardware access**
- **Host admin**
- **VM admin**

Intel® Software Guard Extensions (Intel® SGX)

The most researched, updated, and battle-tested hardware-based Trusted Execution Environment (TEE) for the data center



Delivers the smallest potential attack surface of any TEE available for the data center

Already available today on Intel® Xeon® E processors

Coming on 3rd Gen Intel® Xeon® Scalable Processors

- Up to 1TB protected enclaves for code and data
- Protected offload from enclaves to HW accelerators
- Broad software ecosystem support

Intel® SGX Software Partner Ecosystem

Most control ⟷ **Fastest path**

New App Development

Trusted portion of applications utilize enclave for code and data

- Open Enclave (OE) SDK
- Intel SGX SDK
- Enarx SDK
- MesaTEE
- …more…

Lift and Shift

Existing applications run **natively** within protected containers inside an enclave

- Graphene
- Anjuna
- Fortanix
- Scone
- …more…

Confidential Computing: A Security Game Changer

Intel is a **founding member** of the Confidential Computing Consortium

Focus is on **securing data while in use** using hardware-based controls

Emerging as a **key growth driver** for cloud and multi-party compute

https://confidentialcomputing.io

Premier

intel. accenture Microsoft HUAWEI
ANT GROUP FACEBOOK arm Google Red Hat

General

AMD anjuna Anqlave Bai du 百度
ByteDance cosmian decentriq Fortanix
KINDITE NVIDIA OASIS LABS swisscom
r3. Tencent 腾讯 vmware iExec

and growing…

Intel® SGX in Action

Trusted Multi-party Compute

Cloud Infrastructure

Azure uses Intel SGX to help protect the confidentiality and integrity of its customers' data and code while it's processed in the public cloud

Key Management

Secure Database

Blockchain

Network Virtualization

Native Application Hosting

Federated Learning

FSI uses Intel SGX to allow parties to more securely conduct machine learning across data sources to combat criminal activity in AML

Intel® Total Memory Encryption (Intel® TME)

Encrypts full system memory for added protection against physical attacks

- Helps protect platform memory against hardware attacks such as cold boot/freeze spray/DIMM removal
- Enabled in system BIOS with single CPU-generated key
- Compatible with Intel® SGX enclave solutions
- Small performance overhead

Broad

Encrypts the entire memory using a NIST standard “storage-class” algorithm for encryption: AES-XTS

Transparent

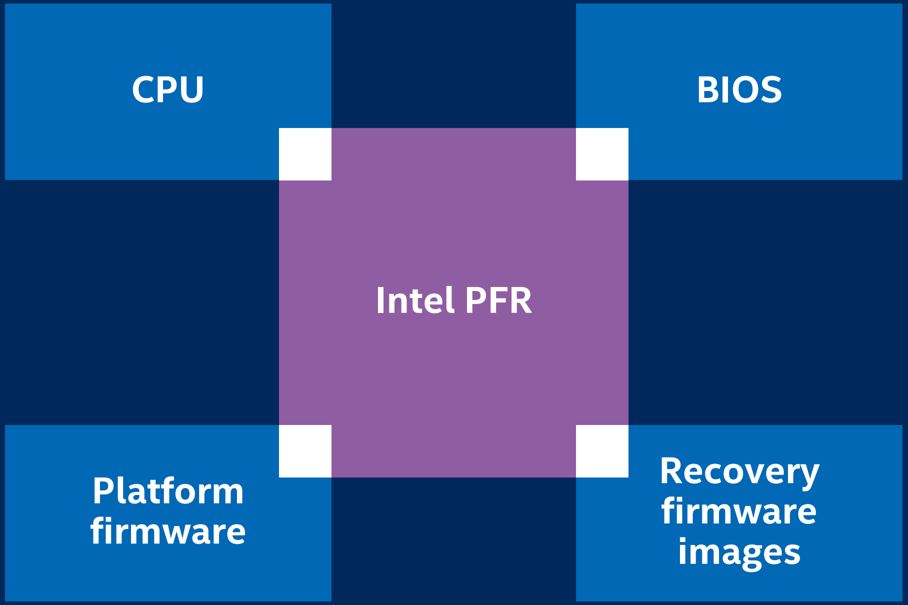
Encrypts data before writing to platform memory and then decrypts on read

Easy

Requires no OS or application enabling; Applicable to all OS and VMM

Intel® Platform Firmware Resilience (Intel® PFR)

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

Pushing the Boundaries of Crypto Acceleration

3rd Gen Intel® Xeon® Scalable processor delivers significant crypto performance improvements

- Reduced compute cycles spent on cryptographic security
- Improved performance and SLA

Public Key	AES	SHA extensions
Up to 5.6x faster* public key encryption and decryption Asymmetric-Key Cryptography for HTTPs (RSA, ECDHE, ECDSA)	**Up to 3.3x faster* with Vector AES encryption** Symmetric-Key Cryptography: Network (GCM, CMAC, CTR) and Storage (XTS)	**Hardware acceleration for common hashing algorithms** Hashing (SHA-1, SHA-256)

https://edc.intel.com/content/www/us/en/products/performance/benchmarks/3rd-generation-intel-xeon-scalable-processors/see references [70, 71]

- Security is foundational to business transformation
- Solutions start with hardware
- 3rd Gen Intel® Xeon® Scalable processor is a revolutionary step forward

Questions?

Xiaojun (Shawn) Li, Sales Director, Next Wave OEM & eODM

Xiaojun.Li@intel.com

Bill Carlson, Solutions Architect, Data Platforms Group, Network and Communications Sales Organization

Bill.Carlson@intel.com

Join Us Next Time

November 3rd @ 8am PDT

Intel® Network Builders Insights Series

Analyze & Optimize FlexRAN, DPDK and Other Network Workloads Using Intel® oneAPI

- Xiaojun (Shawn) Li, Sales Director, Next Wave OEM & eODM
- Abhinav Singh, Software Technical Consulting Engineer
- Ashish Gupta, Business Development Manager

intel®