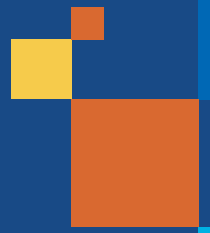
Intel® Network Builders Insights Series

Paradigm Shift in Edge to Core Security with 5G

- Xiaojun (Shawn) Li, Sales Director, Next Wave OEM & eODM
- Kapil Sood, Principal Engineer & Network Security Architect
- Chandresh Ruparel, Director, 5G/Wireless Core



intel®

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 does not control or audit third-party data. You should consult other sources to evaluate accuracy.
- Product plans, dates, and specifications are preliminary and subject to change without notice
-

Agenda

- Cloudification of the Network
- Security Requirements for Network and Edge Transformation
- Intel Platform Security
- Confidential Computing
- Summary & Key Takeaways

Network Cloudification

- Business Drivers
- Network Cloud Architecture

Network Security is more important than ever

The transition to 5G and intelligent connectivity will substantially increase the risk posed by cybersecurity attacks. This is due to the increase in the number of attack surfaces in the 5G architecture, which spans from edge to core to cloud. Therefore, security has become a top-of mind concern in the telecom industry.

Global System for Mobile Communications (GSMA)

According to one survey, more than half the respondents indicated they would be reluctant to do business with a firm that had experienced a data breach

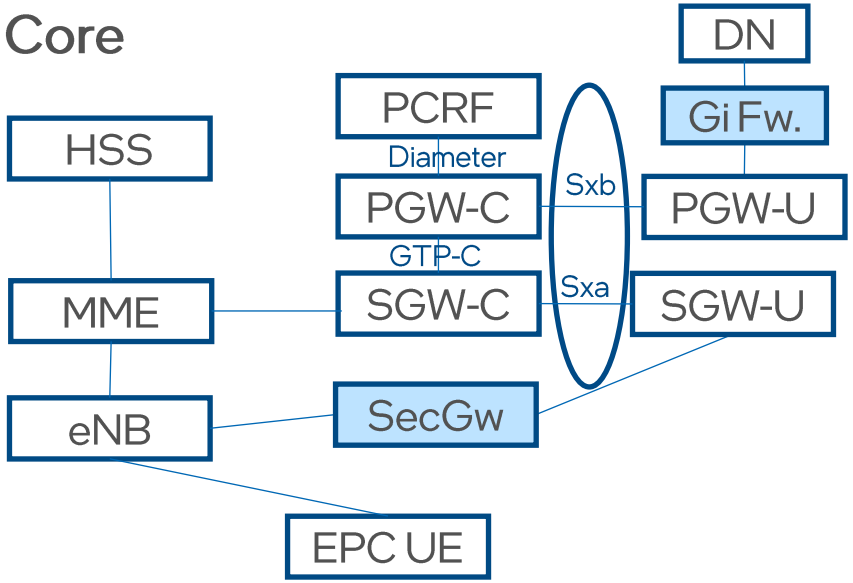
https://engagecustomer.com/data-security-key-to-customer-confidence-and-loyalty/

Cyberattacks are now considered the third highest global risk, according to the World Economic Forum (WEF)

https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf

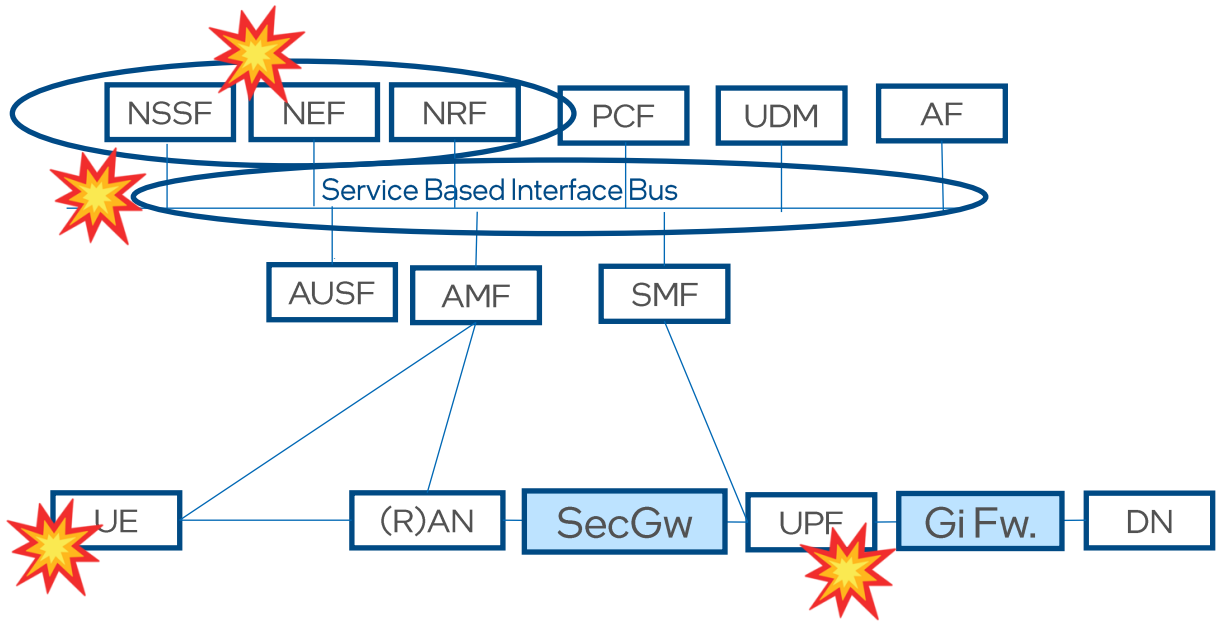
5G: Many New Security Exposures

4G/Evolved Packet Core



Network perimeter security, point-to-point comms with Core, single vendor proprietary interfaces.

5G SA Core

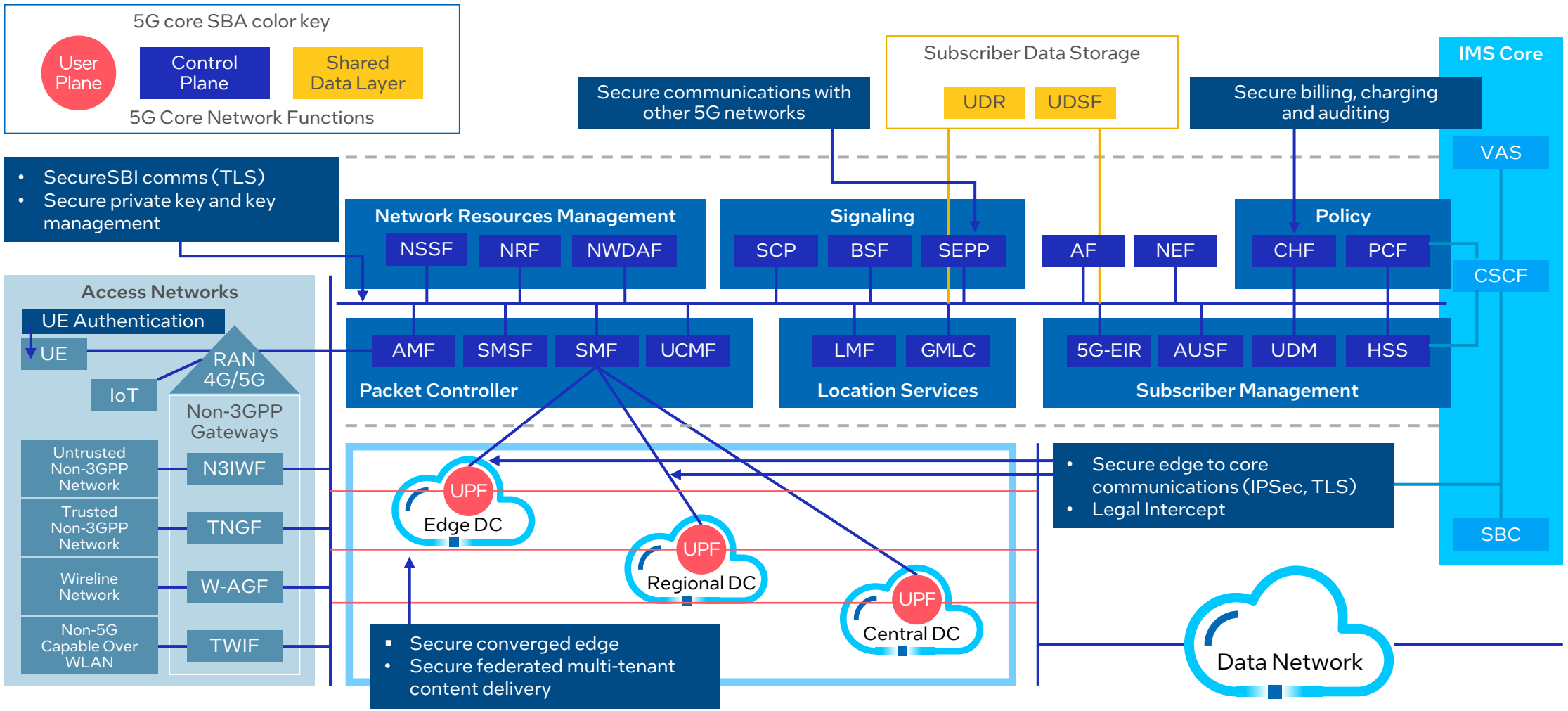


Network Perimeter Security insufficient.

New Exposures: Microservices, multi-vendors in SBA, multi-tenancy, open web-based APIs, highly distributed user plane, multi-domain deployments...

Security for 5G Core Use Cases)

5G System with 5G Core Service-based Architecture (SBA) + IMS Core



5G Core and Edge Top Security Use Cases

Control Plane

Private Key Management and Protection for Inter-Network Function Communication on 5G SA Service Based Interface Bus

Edge-to-Core

More security of data in flight from unsecure edge locations to the 5G Core via high performance IPSec, VPP, etc.

Regulatory Compliance

Enforcement of regulatory requirements such as more secure access to Lawful Intercept channels, Billing CDR audits, etc. in a trusted execution environment

IP Protection

Customer code and more data security and protection at rest and in execution such as AI models, malware signature files, etc.

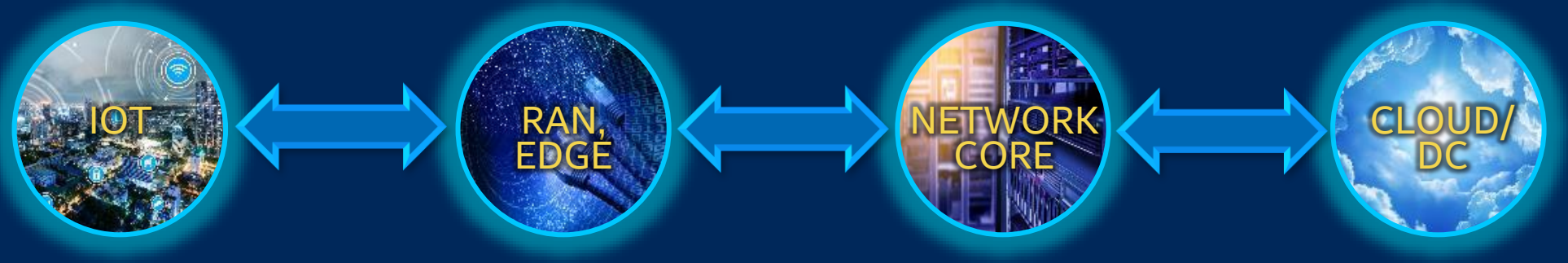
Trusted Multi-Tenancy Compute

Help enable multiple untrusting parties hosted on shared platform while keeping sensitive data confidential.

Secure Key Management

Protecting keys for Cloud Native, Service Mesh, and Comms, VMs, scalable cloud KMS

Intel Hardware Security For Networking Infrastructure



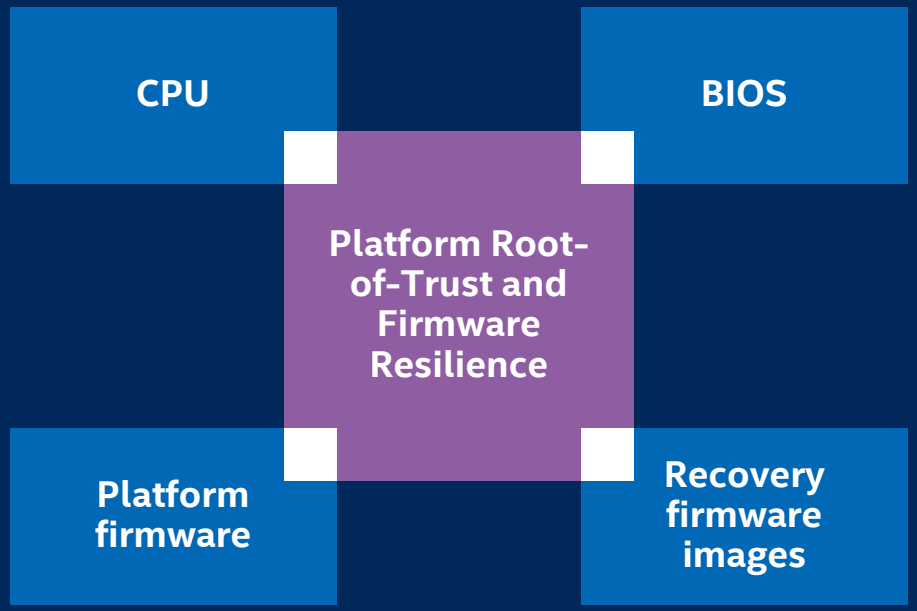
		Intel Security and Research
NETWORKING SOFTWARE	Virtual Machines ➔ Containers ➔ Service Mesh ➔ Micro-Services	Intel Reference Security Solutions, Open Source
REGULATORY	DATA PROVENANCE & SOVEREIGNTY; IDENTITY; PRIVACY; ANALYTICS	Attestation AI Acceleration
WORKLOAD SECURITY	Confidential Computing PROTECT SENSITIVE DATA & CODE	Intel SGX Intel Key Protection Technology
ESSENTIAL SECURITY	High Performance Security CRYPTO & COMPRESSION ACCELERATION + KEY PROTECTION	Intel QAT, vectorized AES
	Platform Root of Trust & Resilience	Intel Platform Firmware Resilience

Intel Platform Security

- Platform Firmware Resilience

Infrastructure Security Assurance

Address NIST SP800-193 platform firmware resiliency Requirements



Protect

Helps monitor and filters malicious traffic on system buses

Detect

Designed to verifies integrity of platform firmware images before executing

Correct

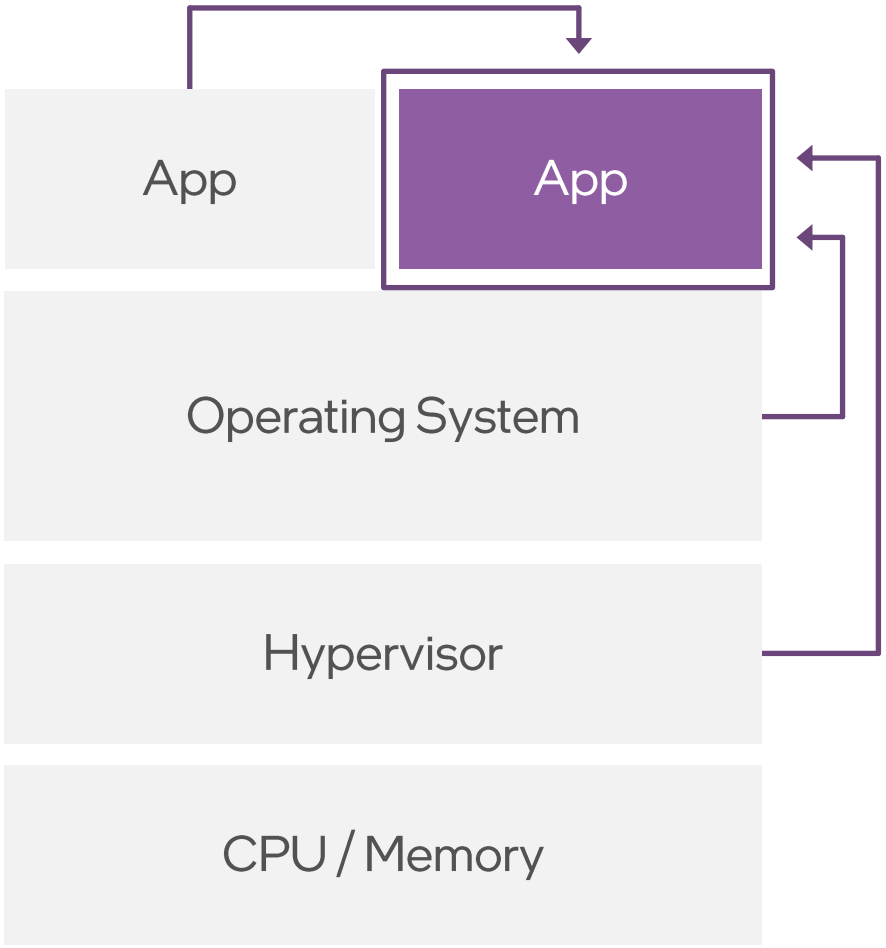
Supports automatically restoring corrupted firmware from a protected gold recovery image

Provide more Supply Chain Security and establish trust through Verification and Attestation

Confidential Computing

- Intel® Software Guard Extensions (Intel® SGX) for Networking
- Network Security Acceleration

Confidential Computing: Why Protect Code/Data in Use?



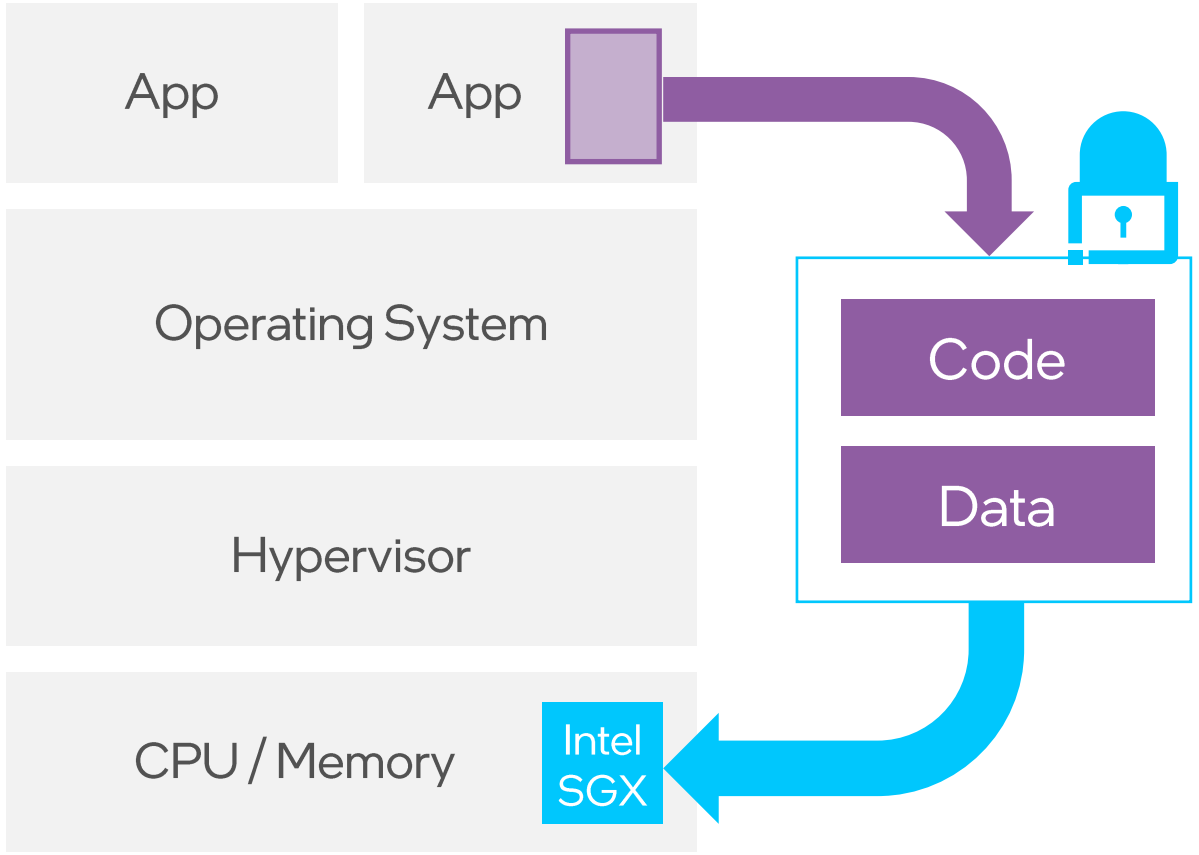
Designed to protect against…

- **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

Confidential Computing with Intel® Software Guard Extensions (Intel® SGX)



Helps deliver one of the smallest potential attack surface

- Protects Apps Code/Data from OS, VMM, Admins
- SGX requires appl. re-factoring & performance tuning, and customers' Attestation setup

Now on 3rd Gen Intel® Xeon® Scalable Processors

- Up to 1TB protected enclaves for code and data
- Broad ecosystem support

Reference Architecture and Libraries for Ease of Adoption

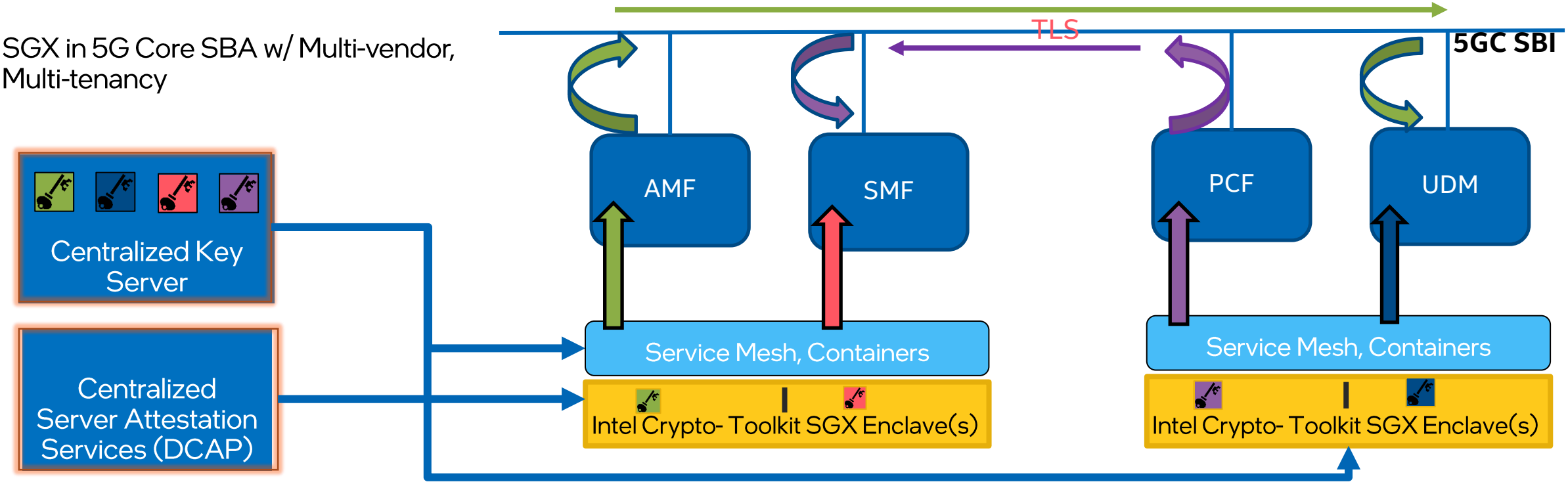
Intel® Software Guard Extensions (Intel® SGX)

- Available since 2015
- Broad deployment/global adoption
- Most independently researched hardware-based trusted execution environment in the market
- Smallest attack surface for a Trusted Execution Environment, less vulnerable to data breach

Intel's Security Advantages	Intel SGX
Bare metal (non-virtualized) workloads	☑
Protections for virtualized environments	☑
Granular developer controls	☑
Proven with the most real-world deployments	☑
Most battle hardened (researched, tested, updated)	☑
Cloud-scale attestation (integrity verification)	☑
Full cloud stack outside of the trust boundary	☑
Unlimited per-enclave data encryption keys	☑

Intel® Software Guard Extensions (Intel® SGX) Key Management for 5G Core, Service Mesh

SGX in 5G Core SBA w/ Multi-vendor, Multi-tenancy



- The Private Keys are securely provisioned into the SGX Enclave
- All Private Key operations (e.g. Service Mesh Signing, mTLS) occur inside the enclave
- The Private key never leaves the enclave

3rd Generation Intel® Xeon® Scalable processor Crypto Performance for 5G Edge-To-Core Security

- Substantial improvements in crypto performance, compared to the previous-generation of Intel Xeon Scalable processors[1].

Up to 5.6x higher OpenSSL RSA Sign 2048 performance

Up to 4.2x higher TLS encrypted connections per second

Up to 3.3x higher IPSec AES-GCM performance

Up to 2.3x Data Integrity (CRC64)

[1] https://edc.intel.com/content/www/us/en/products/performance/benchmarks/3rd-generation-intel-xeon-scalable-processors/
Testing by ***Intel as*** of August 2020. Performance comparisons relative to 2nd Gen Intel® Xeon® Scalable processors using a single buffer algorithm versus multi-buffer algorithms for 3rd Gen Intel Xeon Scalable processors. Results have been estimated based on pre-production tests at iso core count and frequency as of August 2020. Performance gains are shown for individual cryptographic algorithms.

For workloads and configurations visit www.Intel.com/PerformanceIndex.

Summary

- Frequency and impact of cyberattacks are continuing to increase
- Security breaches affects customer confidence with both immediate and long-term impact
- 5G SA with Cloud Native, multi-vendor and high distributed framework, has significantly increased attack surface and security risks
- A highly secure hardware + software framework that is consistent across the 5G network end-to-end is a critical requirement
- Intel provides a highly secure, hardware rooted solution stack with capabilities that allow smallest attack surface.
- Key Technologies include:
  - Intel® Software Guard Extension (Intel®SGX)
  - Intel® Platform Firmware Resilience (Intel® PFR)
  - Intel® Xeon® Scalable processor instruction set for crypto acceleration

References

These can be found in the attachments tab below your viewing screen

- https://www.intel.com/content/www/us/en/communications/5g-edge-to-cloud-security-guide.html
- KMRA Source Code & White Papers on 01.org: Here
- Intel® Software Guard Extensions (Intel® SGX) - NGINX* Private Key on 3rd Generation Intel® Xeon® Scalable Processor User Guide
- Intel® Software Guard Extensions (Intel® SGX) - Key Management on the 3rd Generation Intel® Xeon® Scalable Processor Technology Guide

Questions?

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

Xiaojun.Li@intel.com

Kapil Sood, Principal Engineer & Network Security Architect

Kapil.Sood@intel.com

Chandresh Ruparel, Director 5G/Wireless Core

Chandresh.Ruparel@intel.com

Join Us Next Time

September 1st @ 8am PDT

Intel® Network Builders Insights Series

Intel IPUs Fundamental Role In Your Cloud Strategy

- Xiaojun (Shawn) Li, Sales Director, Next Wave OEM & eODM
- Brian Niepoky, Director Connectivity Group Marketing
- Sabrina Gomez, Director Programmable Solutions Group Marketing


intel