INTEL® XEON® SCALABLE PLATFORM

SECURITY WITHOUT COMPROMISE: ONGOING COMMITMENT TO DATA CENTER SECURITY

Every month brings news of another major data breach. And as more enterprises move applications to hybrid and public clouds, the need for data center security only increases. The **Intel® Xeon® Scalable platform** delivers the next generation of features to secure the platform, increase trust, and protect data without compromising performance.

THREE FORCES IMPACTING DATA CENTER SECURITY

Securing data centers has never been easy. And today, three forces are making it more challenging than ever.

EXPANSION OF ATTACK SURFACE

Billions of devices are connected and moving to the cloud—with more added every day.

INDUSTRIALIZATION OF HACKING

Criminals are becoming more sophisticated and finding new ways to get to data.

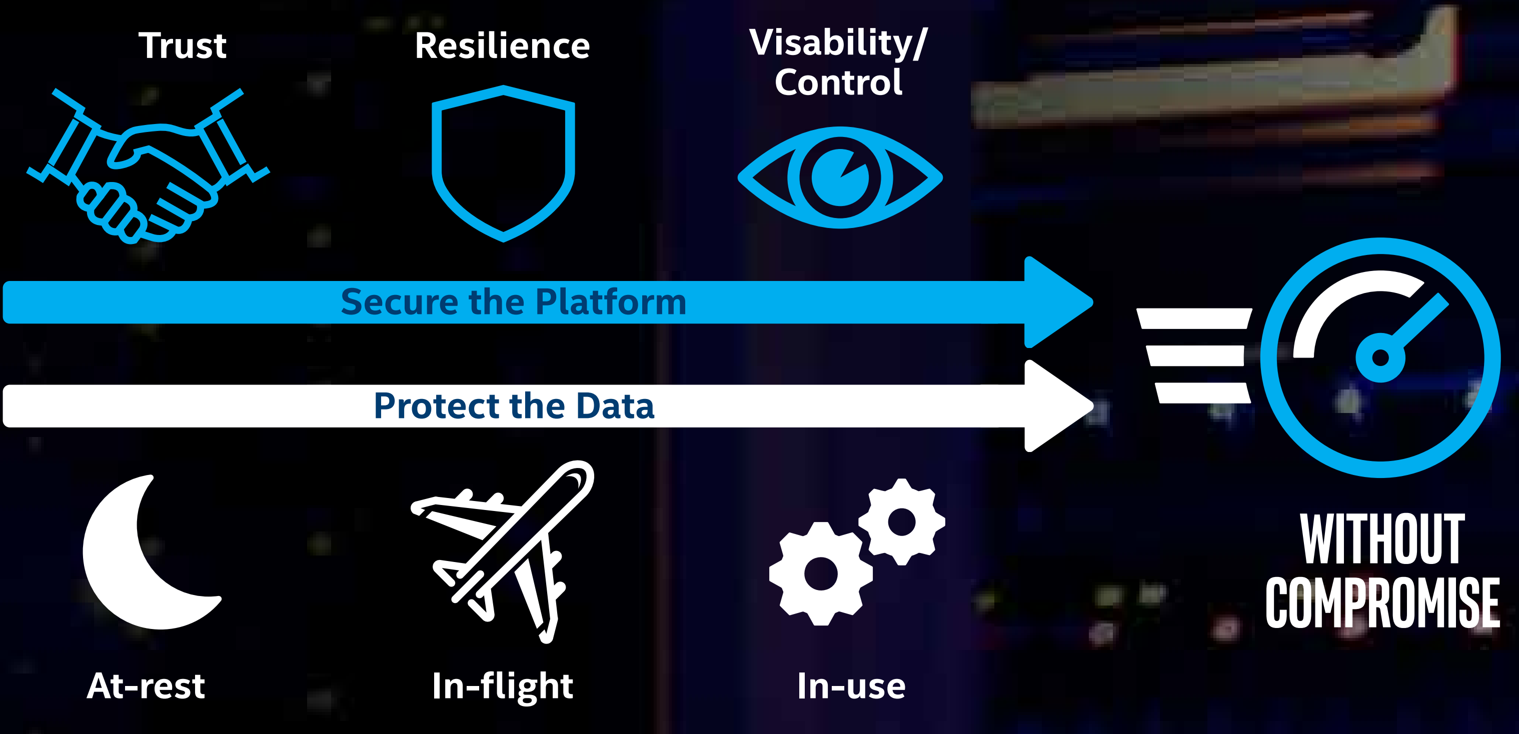
SOLUTION FRAGMENTATION

Data centers may contain thousands of products from hundreds of vendors.

TRUSTED INFRASTRUCTURE: SECURITY ROOTED IN THE HARDWARE

To address evolving threats to the data center, Intel believes in a comprehensive security strategy. First, the platform must be secured with the latest features designed to build trust, resiliency, visibility, and control. Second, data must be protected at rest, in flight, and in use.

TRUSTED INFRASTRUCTURE FOR THE DATA CENTER



Trust

Resilience

Visability/ Control

Secure the Platform

Protect the Data

At-rest

In-flight

In-use

WITHOUT COMPROMISE

SECURE THE PLATFORM

A trusted infrastructure is fundamental to data center security, providing a reliable foundation for a variety of advanced security solutions.

Intel® Trusted Execution Technology (Intel® TXT) with

ONE-TOUCH ACTIVATION

Intel TXT defines platform-level enhancements that provide the building blocks for creating trusted platforms. With one-touch activation, **Intel TXT** is now faster and easier to deploy.

Intel® Platform Trust Technology (Intel® PTT)

TRUSTED PLATFORM MODULE

Intel PTT is a trusted platform module (TPM) integrated directly into the firmware on the chipset.

PROTECT THE DATA—ENCRYPT EVERYTHING

Data security and management is vital throughout the lifecycle of data, including when it is in flight, in use, and at rest.

LESS THAN

1% PERFORMANCE OVERHEAD

to encrypt 100 GB of data with **Intel® Advanced Encryption Standard (Intel® AES-NI)**[1]

UP TO

2.49X HIGHER TLS WEB SERVER (Gbps)

to encrypt data communications with **Intel® QAT accelerator**[2]

Intel® Advanced Vector Extensions 512 (Intel® AVX-512)

Intel AVX-512 delivers accelerated per-core performance for workloads such as cryptography.

Intel® QuickAssist Technology (Intel® QAT)

Intel QAT improves performance and efficiency across the data center by making it possible to accelerate workloads such as cryptography and data compression.

Intel® Key Protection Technology (Intel® KPT)

Data should be protected with encryption in all its phases: at rest, in use, and in flight. The single most critical piece of data is the private key used for decryption, so keys likewise need to be protected.

Intel KPT leverages **Intel PTT** as the keystore and **Intel QAT** as the encryption engine, both of which are integrated into the Lewisburg chipset. This allows the keys to be stored and processed without ever exposing them to main system memory—thus providing an extra layer of security.

DEFEND YOUR DATA CENTER

Find out how the **Intel Xeon Scalable platform** and other Intel® technologies can help you secure your data center. Visit **www.intel.com/xeonscalable** for details.

Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/benchmarks

[1] Time to write 100 GB of data on Intel(R) Xeon(R) processor E5-2697 v3 (https://software.intel.com/en-us/articles/intel-aes-ni-performance-enhancements-hytrust-datacontrol-case-study).

[2] Up to 2.49x TLS 1.2 download throughput: Intel(R) Xeon(r) processor E5-2699 v4 (55M Cache, 2.2GHz), Intel(R) DH895XCC (Coleto Creek), SuperMicro(r) X10DRX vs. Intel(R) Xeon(r) Platinum 8180 processor (39M Cache, 2.5GHz), Intel Lewisburg in x16 link mode, Neon City.