CLOUD COMPUTING SECURITY

Chris Hotchkiss (B.S. EE ’94, MBA ’99)

Vice President, General Manager

Platform Execution and Validation (PEV)

Data Center Group, Intel Corporation

Contributors: Jesse Schrater, Nikhil Deshpande and Naresh K. Sehgal

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

AGENDA / TOPICS

1. Background
2. Cloud Computing Security Concerns
3. Solutions in the market
4. Future Challenges
5. Summary

BACKGROUND

- Cloud Computing (CC) refers to
  - Providing IT Services, Applications and Data
  - Using dynamically scalable pool(s)
  - Remotely residing Resources
- Cloud provides financial benefits to users and providers
- But, Cloud presents Information security challenges

SECURITY IMPORTANCE

Top 5 Data Breaches of All Time

- Yahoo: 3 billion accounts in 2013.
- Yahoo: 500 million accounts in 2014.
- Marriott: 500 million guests in 2018.
- Friend Finder Networks: 412 million accounts in 2016.
- Equifax: 146 million accounts in 2017.

Security and TCO are top criteria for public vs. private cloud decision

-'17 Enterprise/SMB Survey

Top priority is security – second is operational support

-Major US CSP, 2018

Security is highest priority for enterprise using public cloud

-'17 Enterprise/SMB Survey

SECURITY PROBLEM STATEMENTS --→ CONSIDERATIONS / EXAMPLES

Access Control

Rightful access to a computer system

--→

Multiple users on same compute node
Integrity of run-time programs
Performance / Job Time Completion
Licensing control

Secure Communications

Data Transfer via open channels

--→

Large amounts of files transferred over public nodes
Large Transfer time will increase customer cost

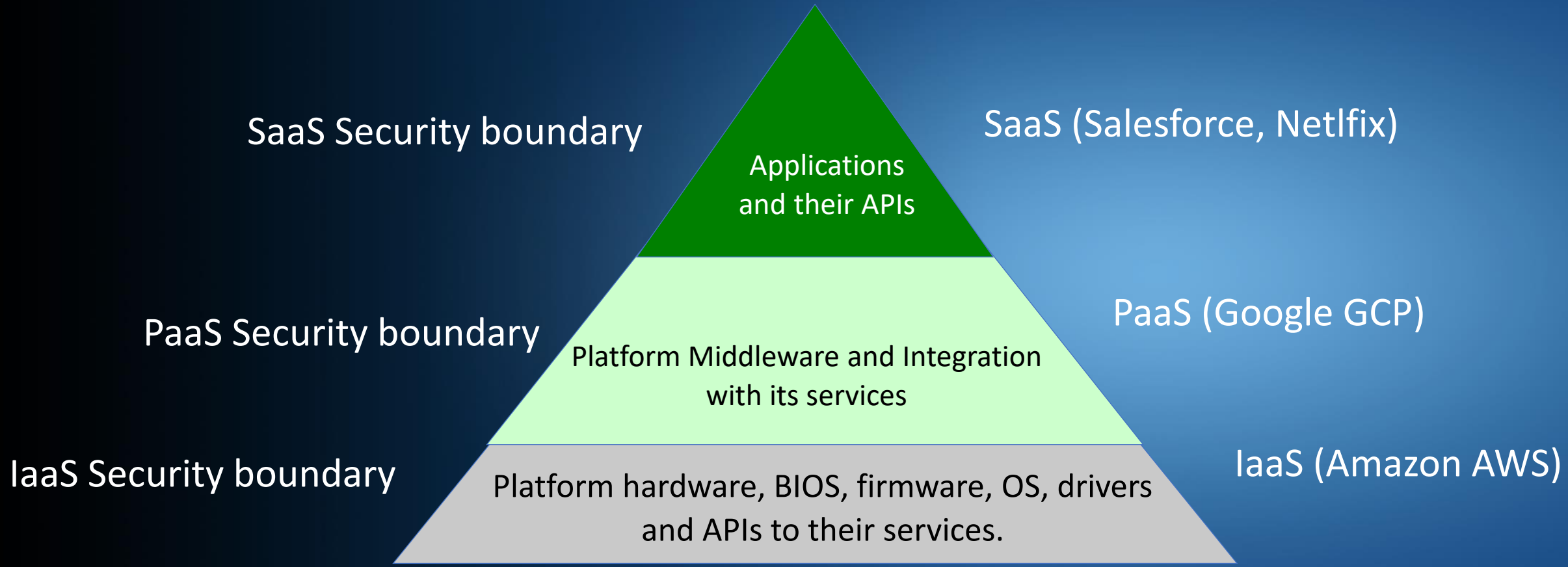
Data Protection in Cloud

Run-time and after job completion

--→

Information theft - Fake login or indirect access
Footprints after job is done
Balancing protection with cost & performance

SECURITY NEEDS IN A PUBLIC CLOUD AT EACH LEVEL



THREE FORCES Impacting DATA CENTER SECURITY

CHALLENGES IN IMPLEMENTING, MAINTAINING, AND EXECUTING PRODUCTS AND PROCESSES

Expansion
of attack surface

Billions of connected devices and the move to the cloud

INDUSTRIALIZATION
of hacking

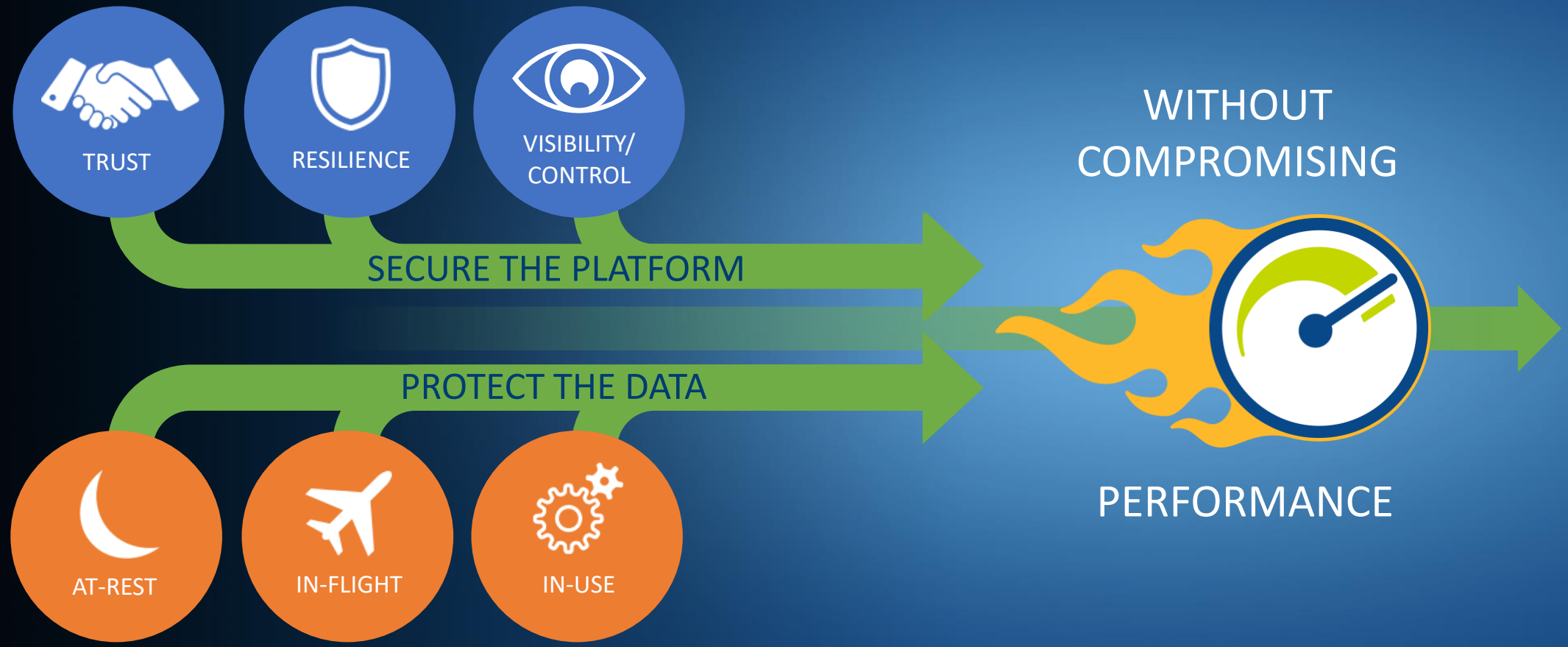
Criminal sophistication and evolving intent to get to your data

Fragmentation
of solutions

Thousands of products from hundreds of vendors

INTEL'S DATA CENTER Security Strategy

EFFECTIVE SECURITY IS BUILT ON A FOUNDATION OF TRUST



**No computer system can be absolutely secure

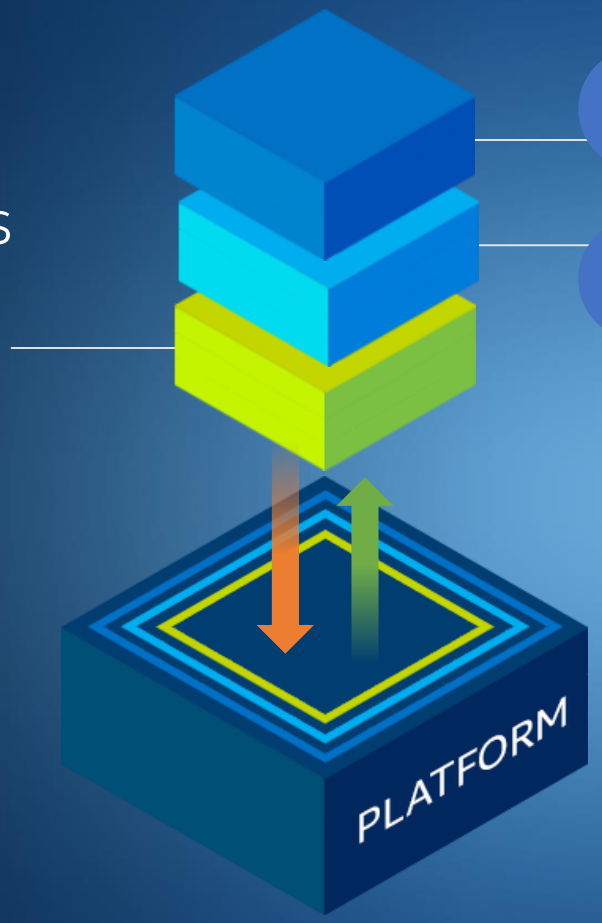
INTEL SECURITY TECHNOLOGIES ARE ROOTED IN SILICON

SECURE THE PLATFORM

TRUST

1 Build essential technologies into the platform

- Silicon-based Root of Trust
- Built-in instructions for measurement and verification
- Fast, high quality random number generator
- Firmware assurance



3 Partner for optimized ISV security solutions

2 ENABLE with Intel Security Libraries

- Enable advanced customer security protections and mitigations
  1. Workload Integrity
  2. Data Sovereignty
  3. Threat Detection

ROOTED IN SILICON, OUR SECURITY TECHNOLOGIES HELP CREATE A TRUSTED FOUNDATION

HARDWARE-ENHANCED SECURITY

INTEL enables TRUSTED INFRASTRUCTURE

DATA PROTECTION & KEY MANAGEMENT

INTEL® XEON® PROCESSOR E5 V3 FAMILY (2014)

Previous features

General Crypto Assists
Asymmetric/Symmetric Crypto Assists
Intel® Trusted Execution Technology (TXT)
Execute Disable (XD) Bit
Intel® Data Protection Technology (Secure Key)
BIOS Guard (WS)
PCH-Dynamic Random Number Generator (RDRAND)
Intel® Platform Protection Technology (OS Guard) - SMEP

- Intel® AES-NI enhancements (from E5 v2)
- Trusted Platform Module (TPM) 2.0 support

INTEL® XEON® PROCESSOR E5 V4 FAMILY (2016)

- Crypto Speedup (ADOX/ADCX)
- New Random Seed Generator (RDSEED)
- Supervisor Mode Access Prevention (SMAP)
- Virtualization exception (#VE)

Intel® Xeon® Scalable Processor (2017)

- Intel® Advanced Vector Extensions 512
  - (SHA Multi-Buffer performance)[1]
- Intel® QuickAssist Technology (QAT) – Enhanced + Integrated
- Intel® Key Protection Technology (KPT)[2]
- Intel® Platform Trust Technology (PTT)

2nd Generation Intel® Xeon® Scalable Processor (2019)

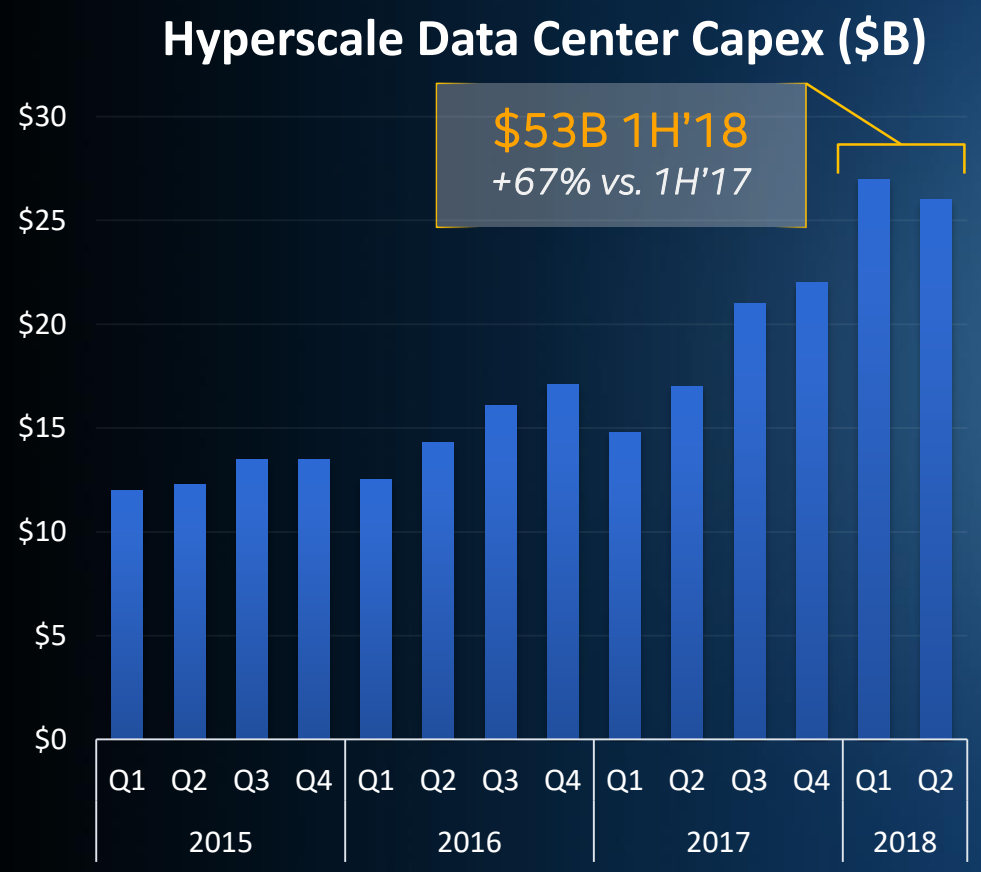
- **Intel® Security Libraries for Data Center (Intel® SecL-DC)**
- **Intel® Threat Detection Technology (Intel® TDT)**
- **Intel® Security Essentials**

BUILT-IN SECURITY TO PROTECT DATA (IP & CUSTOMER PRIVACY) + SYSTEM RESILIENCE

1. per-core improvements
2. with Integrated Intel® QAT + Intel® PTT

CLOUD SERVICE PROVIDER INVESTMENT GROWING

Depending on Intel



Source: Synergy Research

Google tripled [capex] to $7.3B in Q1'18 – and the CFO says its not a 'one-off'

-Business Insider, 4/23/18

It's a Tech War, and It Costs a Fortune.

Alphabet, Amazon, Microsoft, and Facebook collectively boost capital spending by 68% in first quarter.

-Bloomberg, 4/27/18

Google, FB, and Other Tech Giants' Capex Is Going Sky High

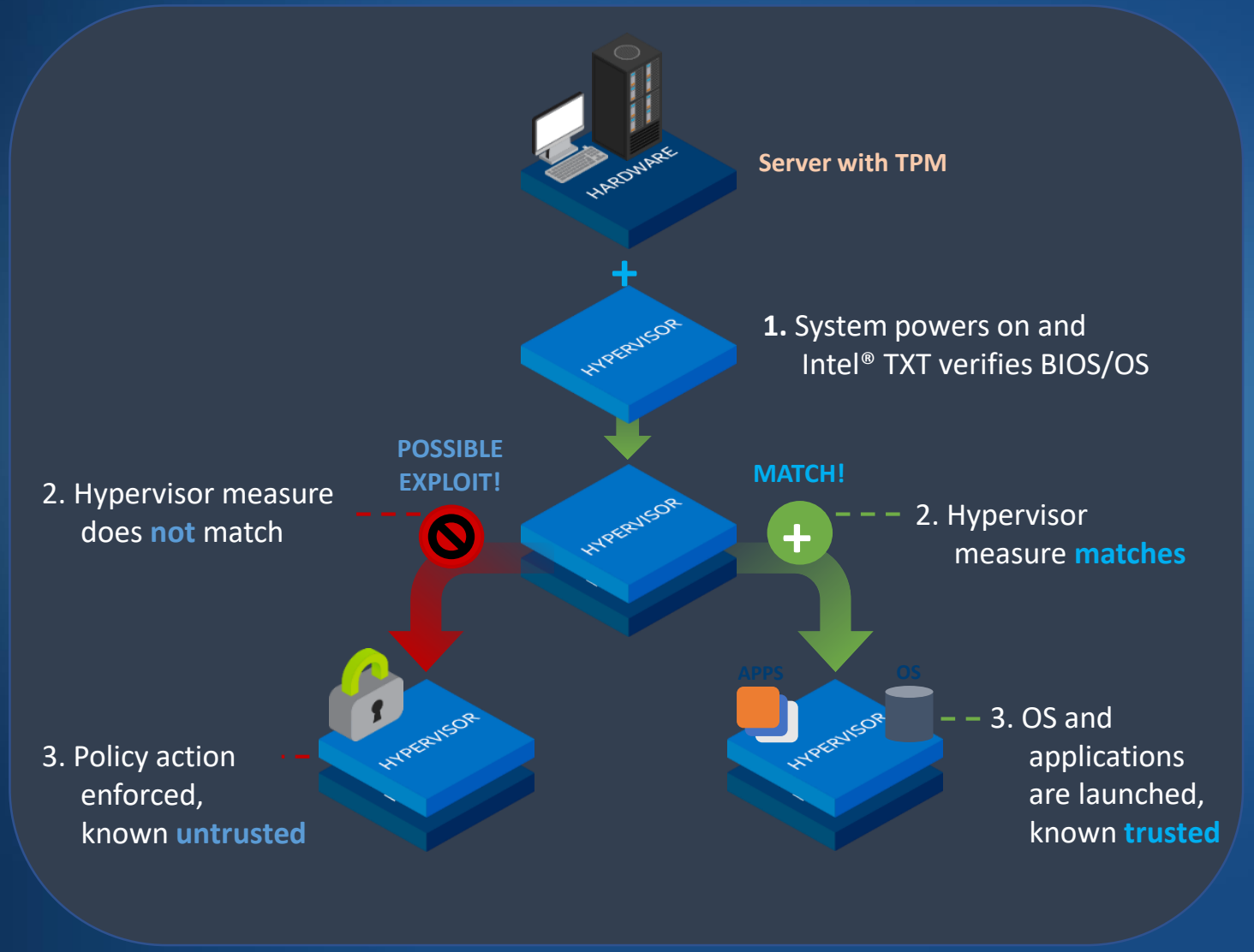
-The Street, 4/24/18

A TRUSTED PLATFORM BEGINS IN SILICON

ENSURING A MEASURED ENVIRONMENT BASELINE WITH INTEL® TRUSTED EXECUTION TECHNOLOGY (INTEL® TXT)

SECURE THE PLATFORM

- System boot stack gets crypto-hashed before execution
- Hash values get stored in a Trusted Platform Module (TPM)
- Match to known-good values determines system trust status
- One-Touch Activation: OOB TXT/TPM remote discovery, enablement, activation independent of OEM/OS

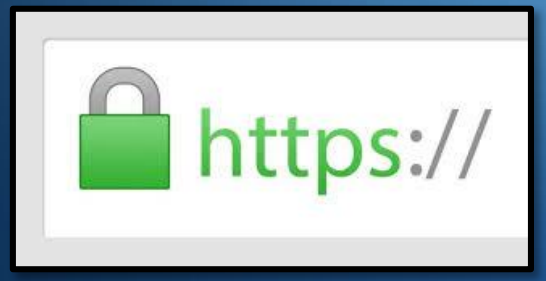


Encrypting Data Throughout its Lifecycle

Existing | New Frontier

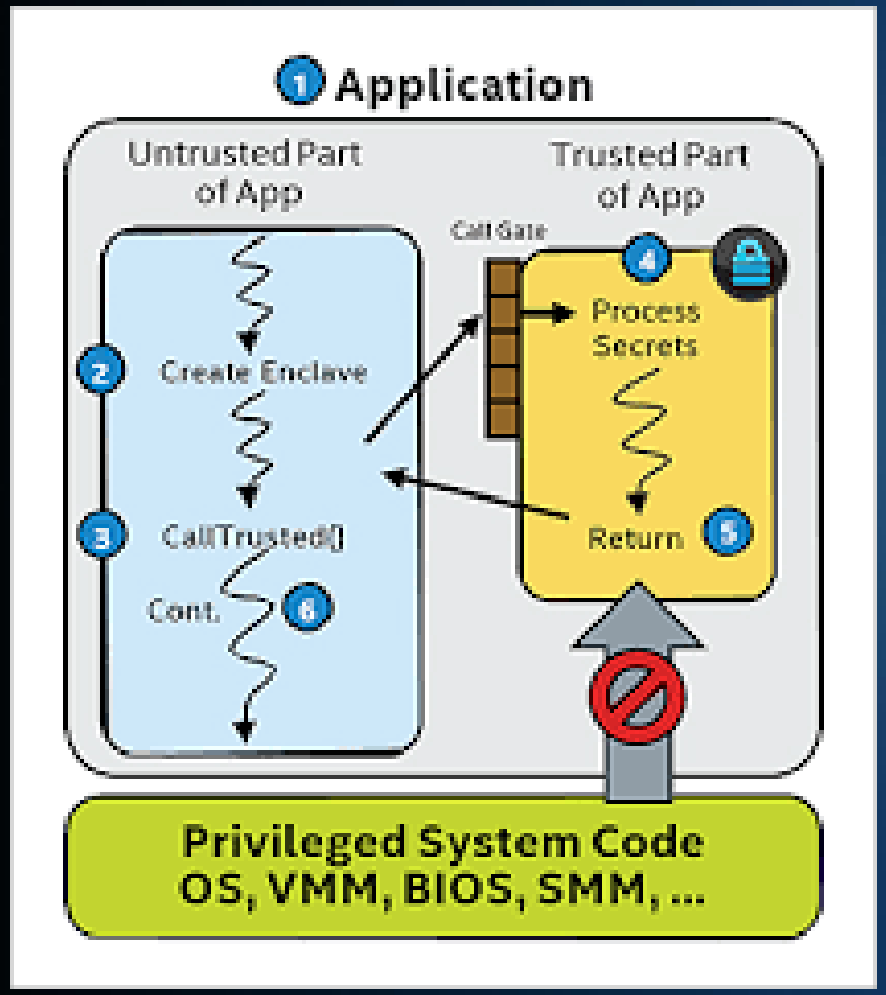
Encrypt inactive data when in storage, database, etc

Encrypt data moving across untrusted public/private networks



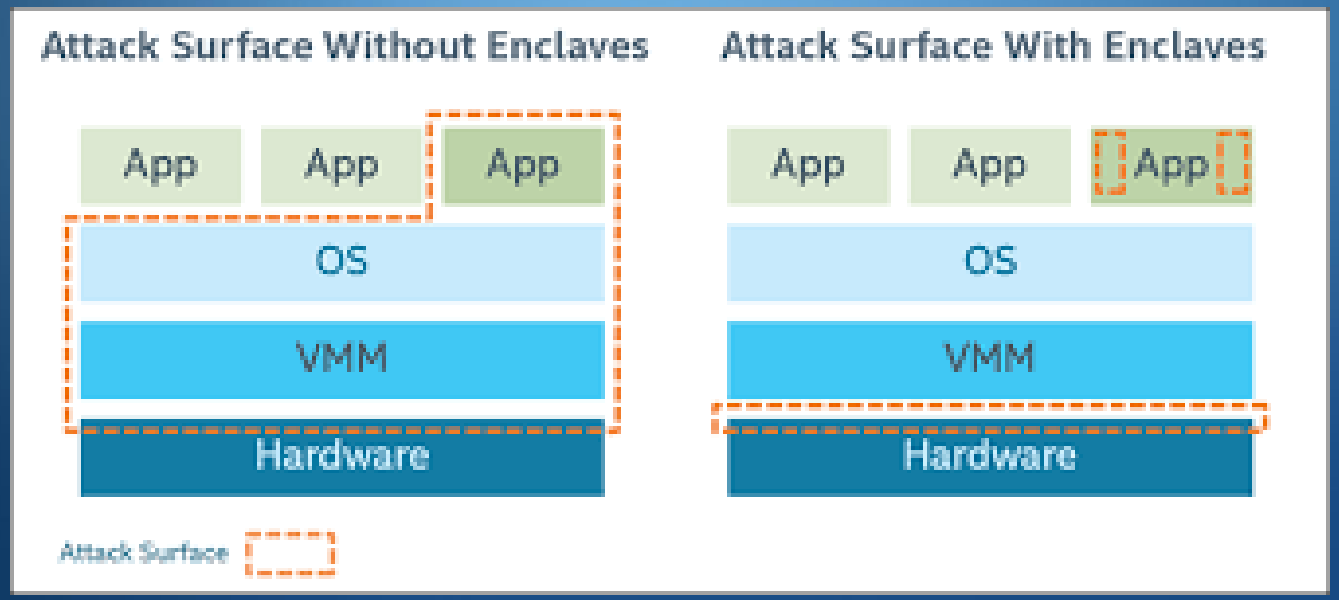
Protect/Encrypt data while being held in memory and processed for computation

INTRODUCTION TO INTEL SGX



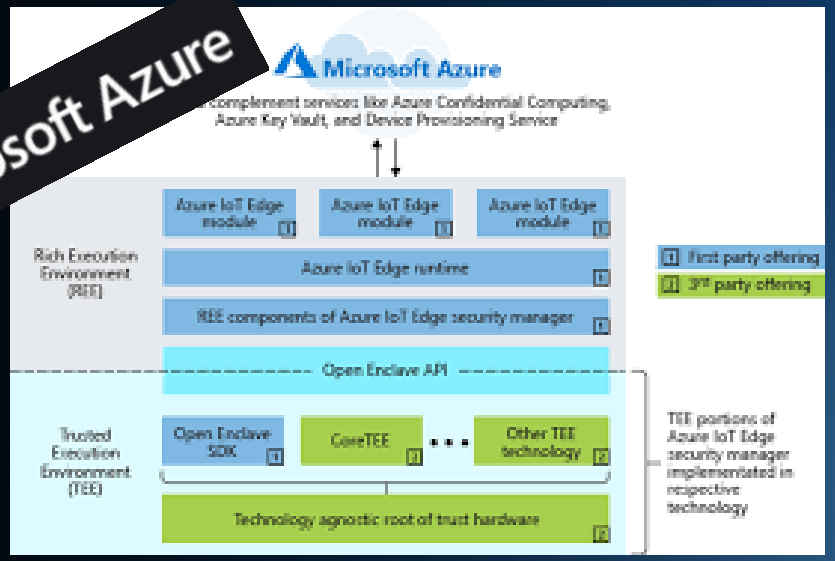
Went from concept to deployment within 12 months:

- Avoided NIH syndrome
- Technology reuse from another domain
- Adapt and run, to skip the crawl-walk stage☺.



MANY CUSTOMERS USING INTEL SGX.....

Microsoft Azure



IBM Cloud

Baidu 百度

Alibaba Cloud

https://confidentialcomputing.io/

intel

FUTURE CHALLENGES: EDGE COMPUTING SECURITY PROBLEMS

- Definition of a Cloud has been expanding
- Perimeter defence is insufficient
- Fixed protocols for boundaries of security fail
- A fixed universal security policy is inadequate
- Components on Edges need to be adaptive

THE ENVIRONMENT

Today's Brutal DDoS Attack Is the Beginning of a Bleak Future

-- Gizmodo

CLOUD SERVICE PROVIDERS ENCRYPT EVERYTHING

DISTRIBUTED COMPUTING CREATING NEW ATTACK SURFACES

USERS AND HOSTERS WANT TO MAINTAIN OWNERSHIP BOUNDARY

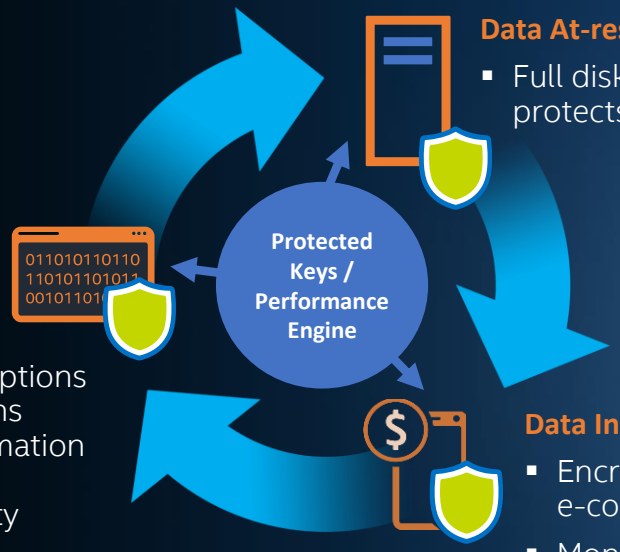
SUPPLY CHAIN PROTECTION ACROSS BORDERS

Protect the Data THROUGHOUT ITS LIFECYCLE

ENCRYPTION AT EVERY STAGE

PROTECT THE DATA

PERFORMANCE



Data At-rest

- Full disk encryption protects data at rest

Data In-use

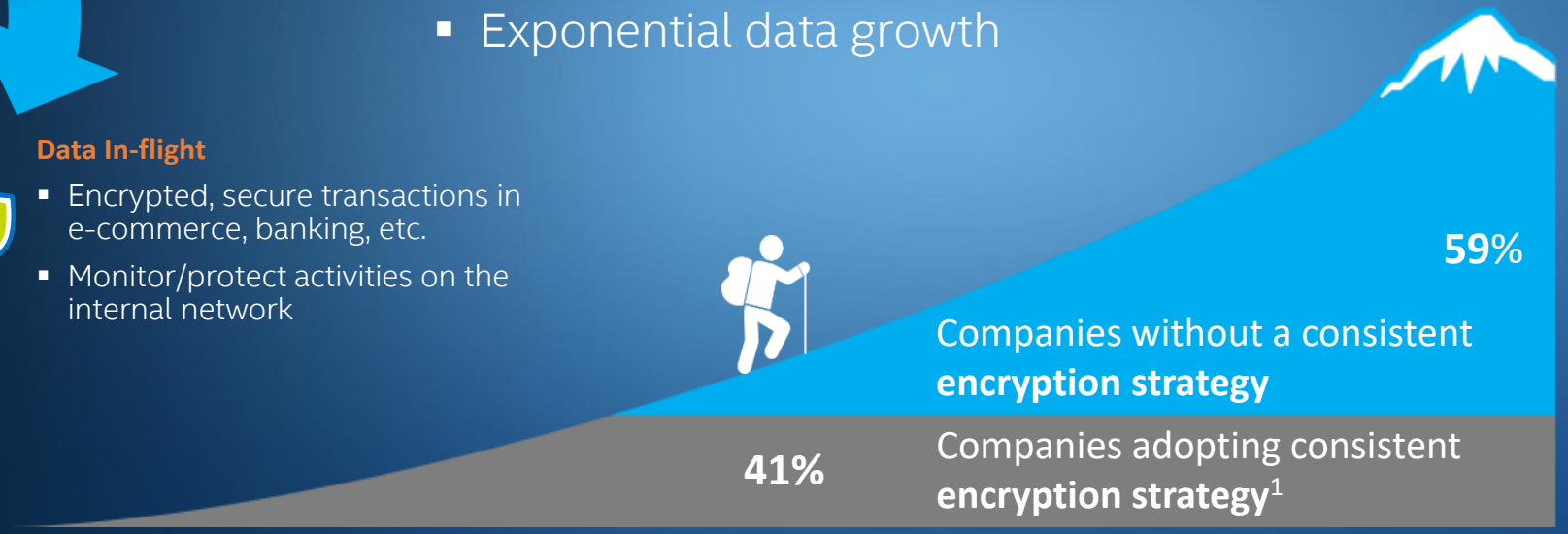
- Encryption options in applications secure information and protect confidentiality

Data In-flight

- Encrypted, secure transactions in e-commerce, banking, etc.
- Monitor/protect activities on the internal network

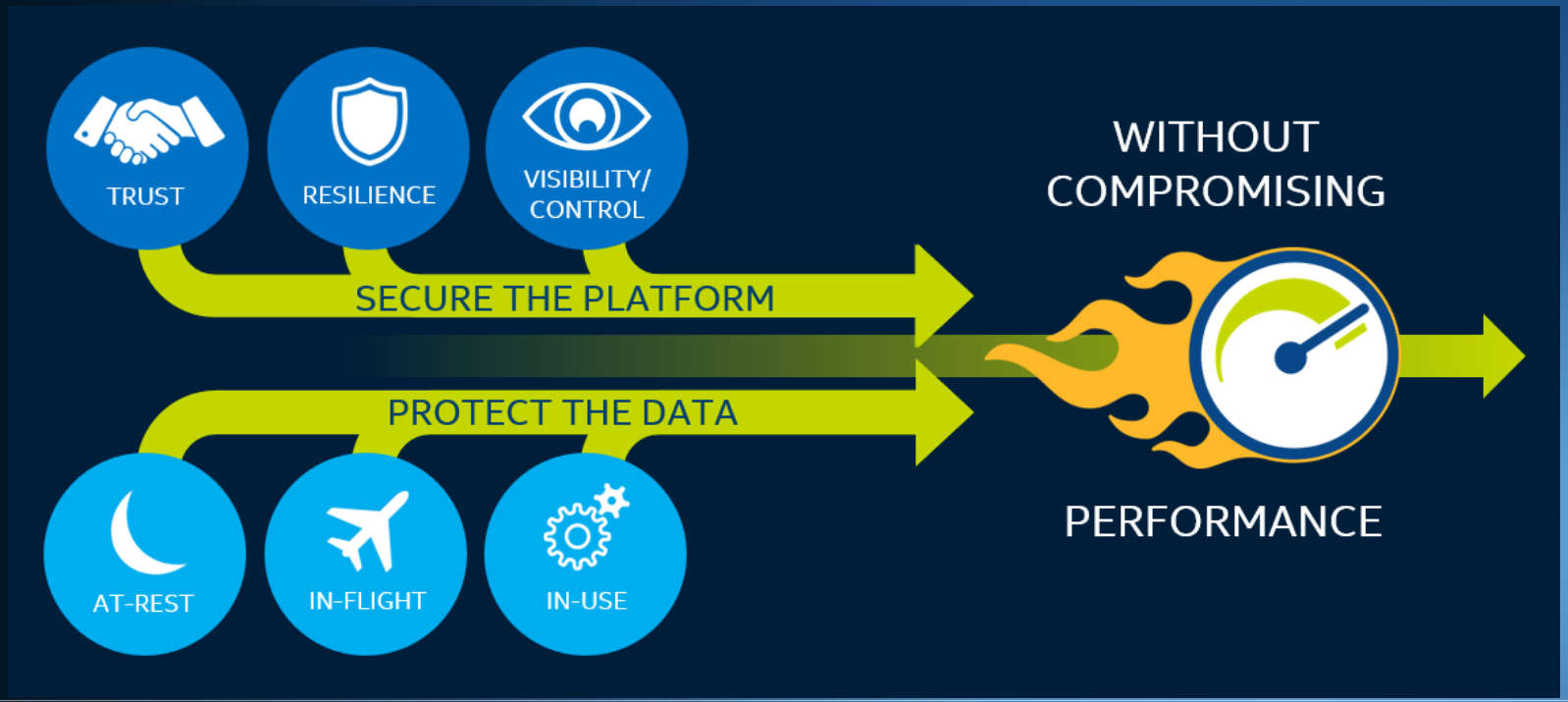
Performance issues are a chief factor in encryption adoption

- Longer keys
- Complex algorithms
- Exponential data growth



1Source: Thales e-Security Web Encryption Trends, 2017
(http://enterprise-encryption.vormetric.com/rs/480-LWA-970/images/2017-Ponemon-Global-Encryption-Trends-Study-April.pdf)

KEY TAKEAWAYS



All workloads should be secured on a trusted platform

All data should be protected through encryption throughout its lifecycle

Trust and encryption without compromising performance are possible with Intel Inside®