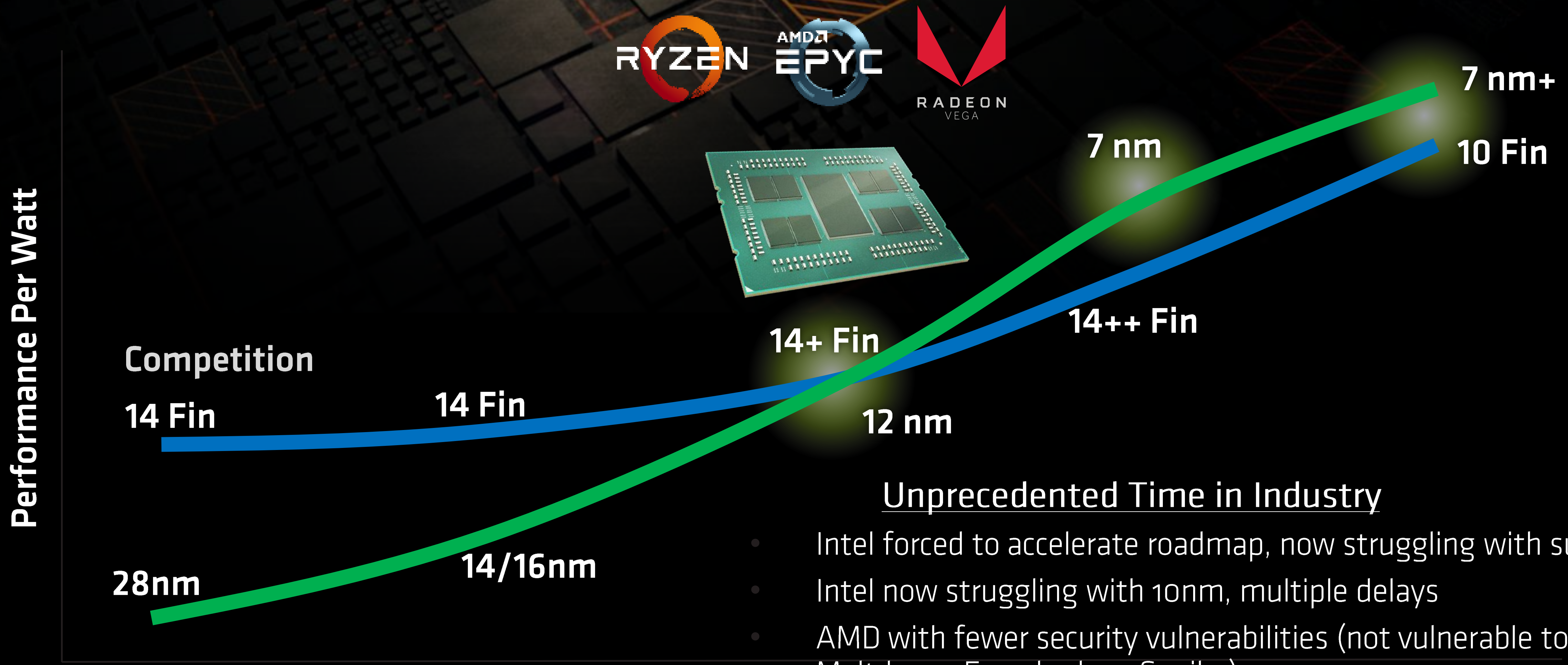
AMD Commercial solutions

AMD ROADMAP EXECUTION

LEADERSHIP LEVELS THE COMPETITIVE PLAYING FIELD



Unprecedented Time in Industry

- Intel forced to accelerate roadmap, now struggling with supply
- Intel now struggling with 10nm, multiple delays
- AMD with fewer security vulnerabilities (not vulnerable to Meltdown, Foreshadow, Spoiler)

Roadmap Subject to Change.

ELEVATE AMD

AMD WILL MAKE HISTORY IN 2019

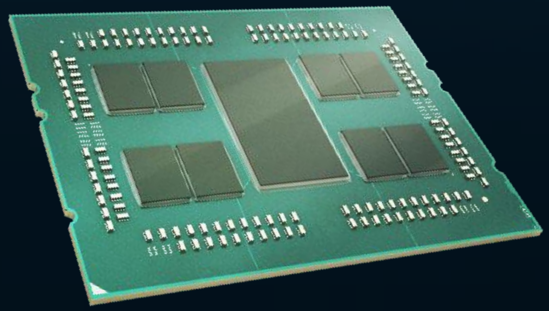
ZEN 2

RADEON NAVI

High Performance Processor Cores

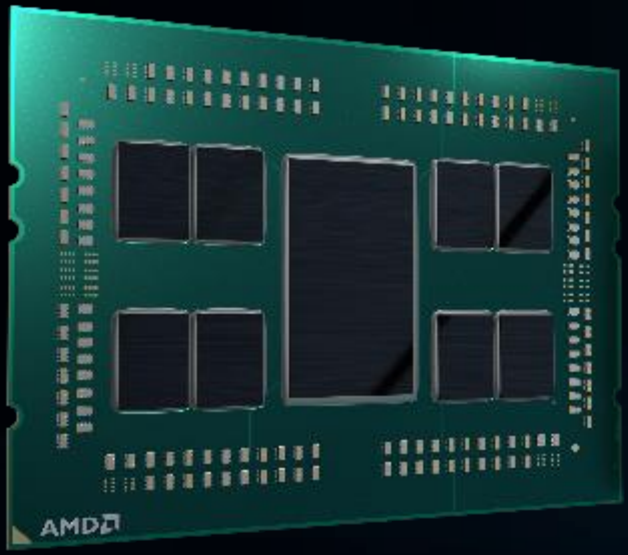
7nm

Leading Edge Manufacturing Technologies



New Approach to Chip Design

AMD EPYC™



WORLD'S HIGHEST PERFORMANCE x86 CPU

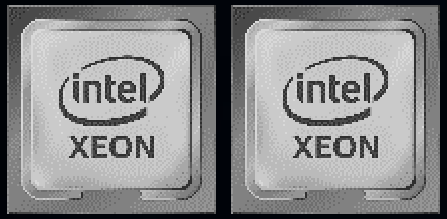
- 64 High Performance Cores, 128% More than Intel® Xeon®
- 97% More Performance than Xeon
- Up to 8TB of 3200 GHz Memory
- 128+ Full Bandwidth PCIe 4.0 Lanes
- No Compromise Single Socket
- Dedicated Secure Co-Processor

*COMPARED TO INTEL 8280L

SEE ENDNOTES ROM-09, ROM-95 AND ROM-06

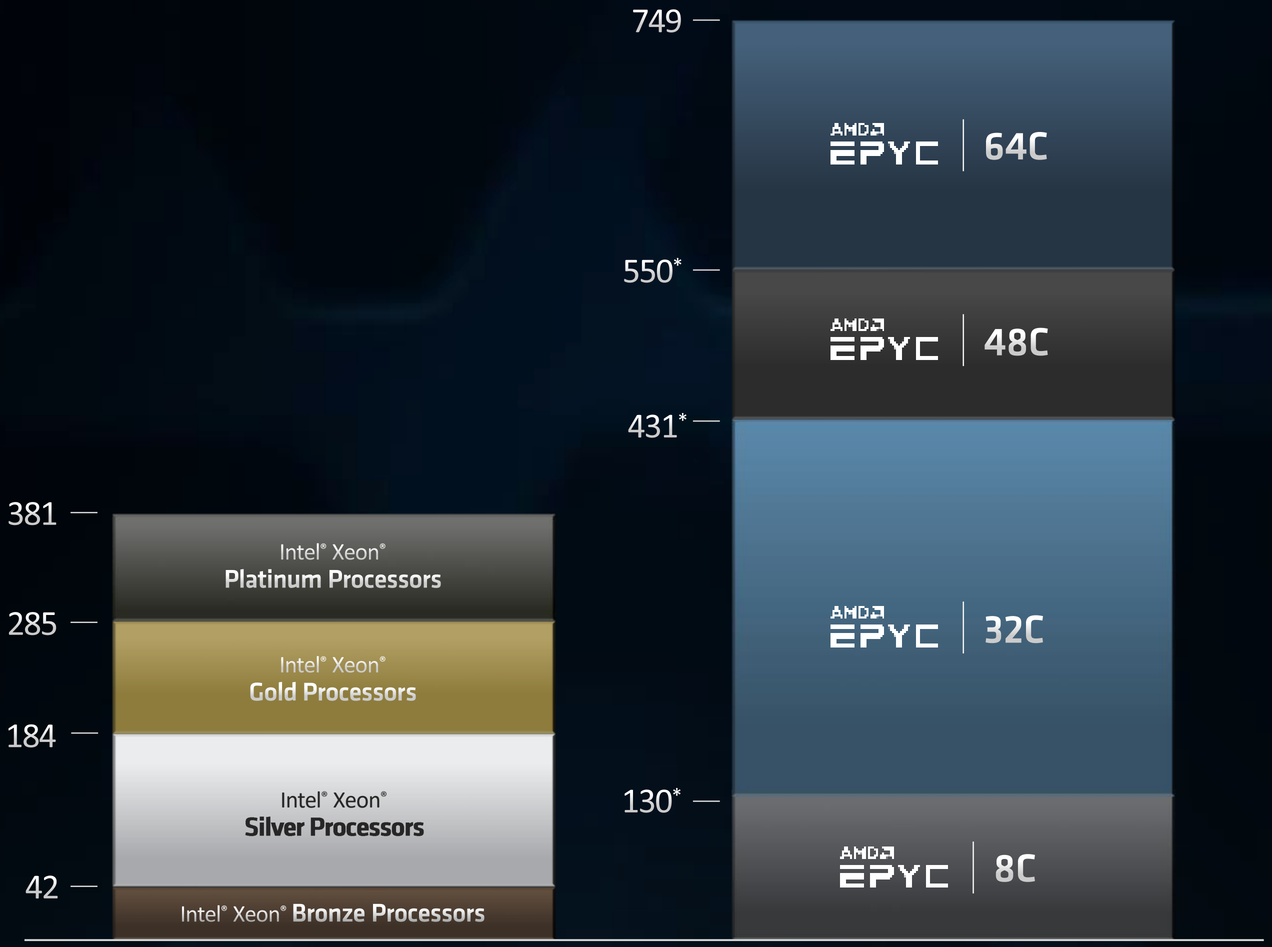
TWO SOCKET LEADERSHIP

2S INTEL® XEON® vs. 2S AMD EPYC™ SPEC CPU® 2017 PERFORMANCE



2S Intel® Xeon®

PRODUCT STACK



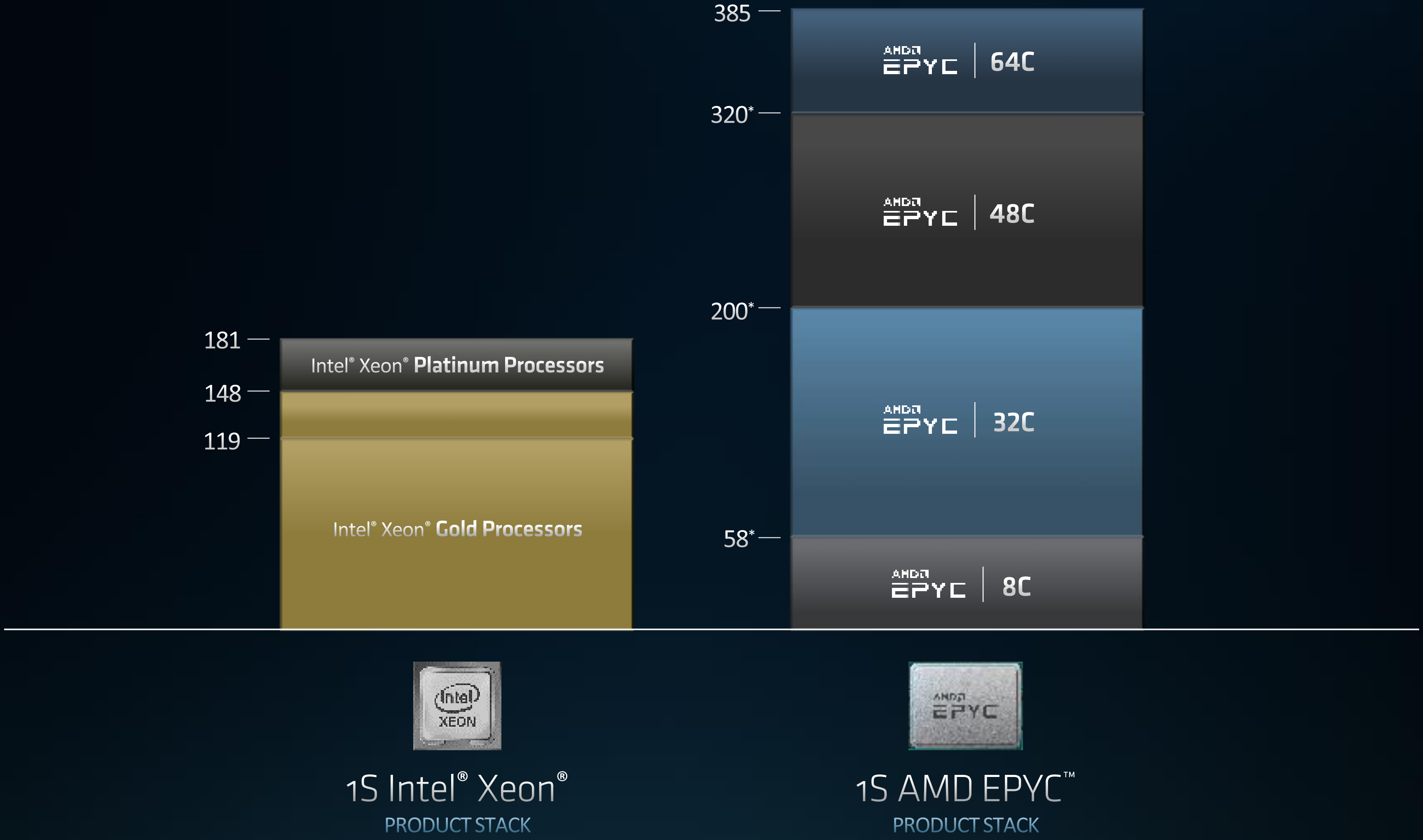
2S AMD EPYC™

PRODUCT STACK

*ESTIMATED; SEE ENDNOTE ROM-258 | SPECRATE®2017_INT_PEAK

SINGLE SOCKET LEADERSHIP

1S INTEL® XEON® vs. 1S AMD EPYC™ SPEC CPU® 2017 PERFORMANCE



SPECRATE®2017_INT_PEAK | *ESTIMATED; SEE ENDNOTE ROM-259

80

WORLD RECORDS

AND COUNTING

SEE ENDNOTE ROM-169

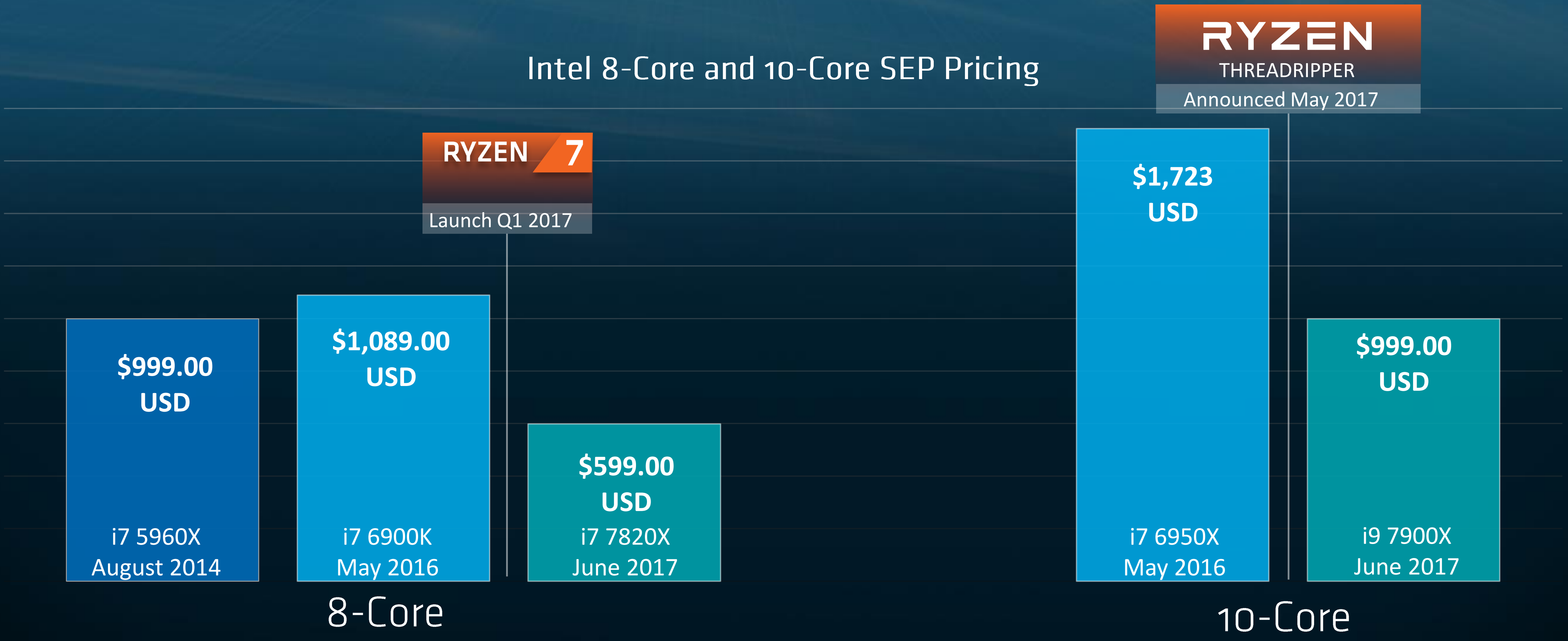
NEW LEADER, NEW RULES

80 WORLD RECORDS AND COUNTING

HPC	4	High Performance Computing Apps
	11	Floating Point Performance
SDI/ENTERPRISE	4	Integer Performance
	26	Java® Based Performance
	4	DB/ERP Business Applications
	7	Energy Efficiency
BIG DATA	18	Big Data and Analytics
CLOUD	6	Cloud and Virtualization

SEE ENDNOTE ROM-169

THE IMPACT OF AMD COMPETITION



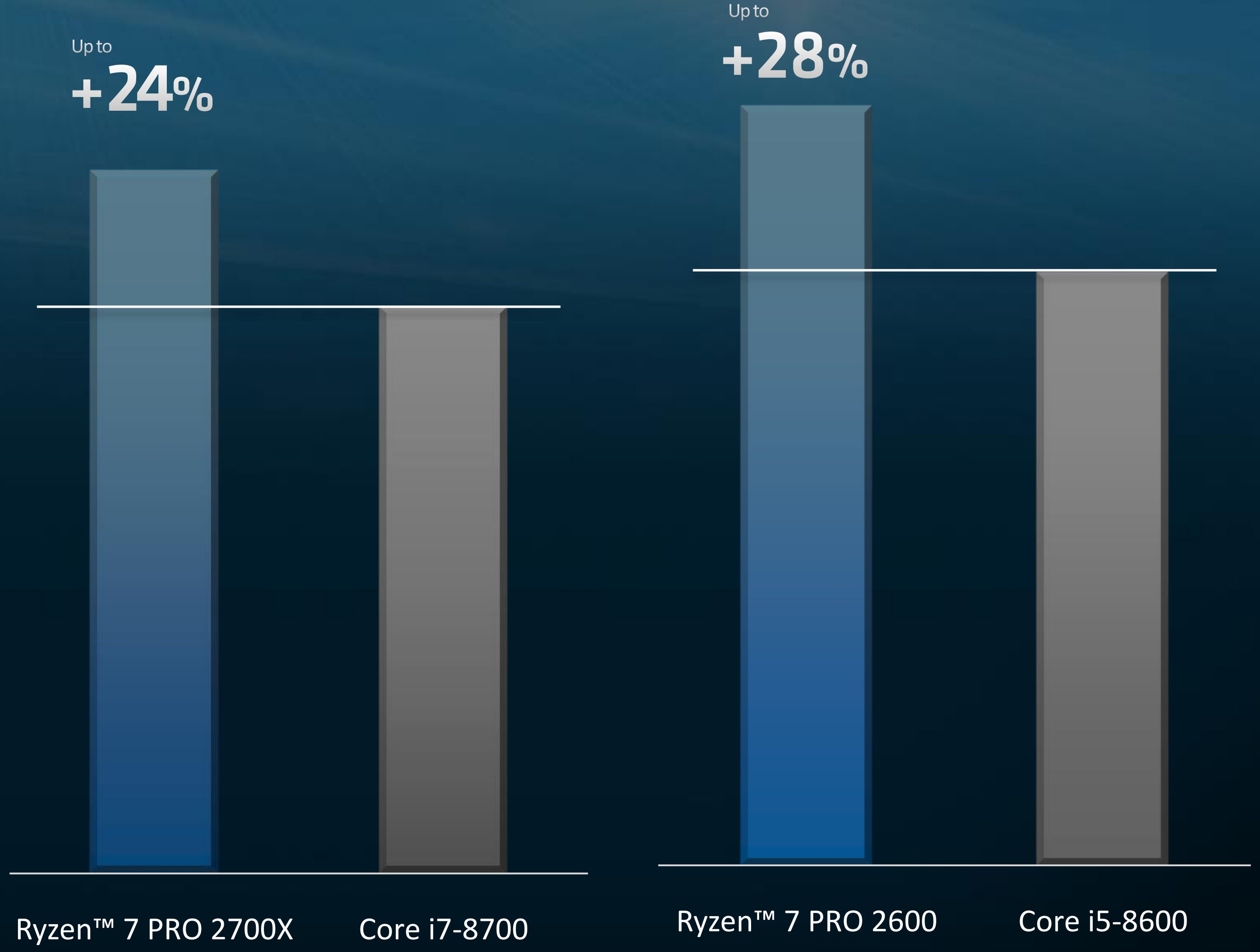
Intel 8-Core and 10-Core SEP Pricing

AMD RYZEN IS CHANGING THE LANDSCAPE

* See Footnote 1

GREAT DESKTOP PERFORMANCE VS 8TH GEN

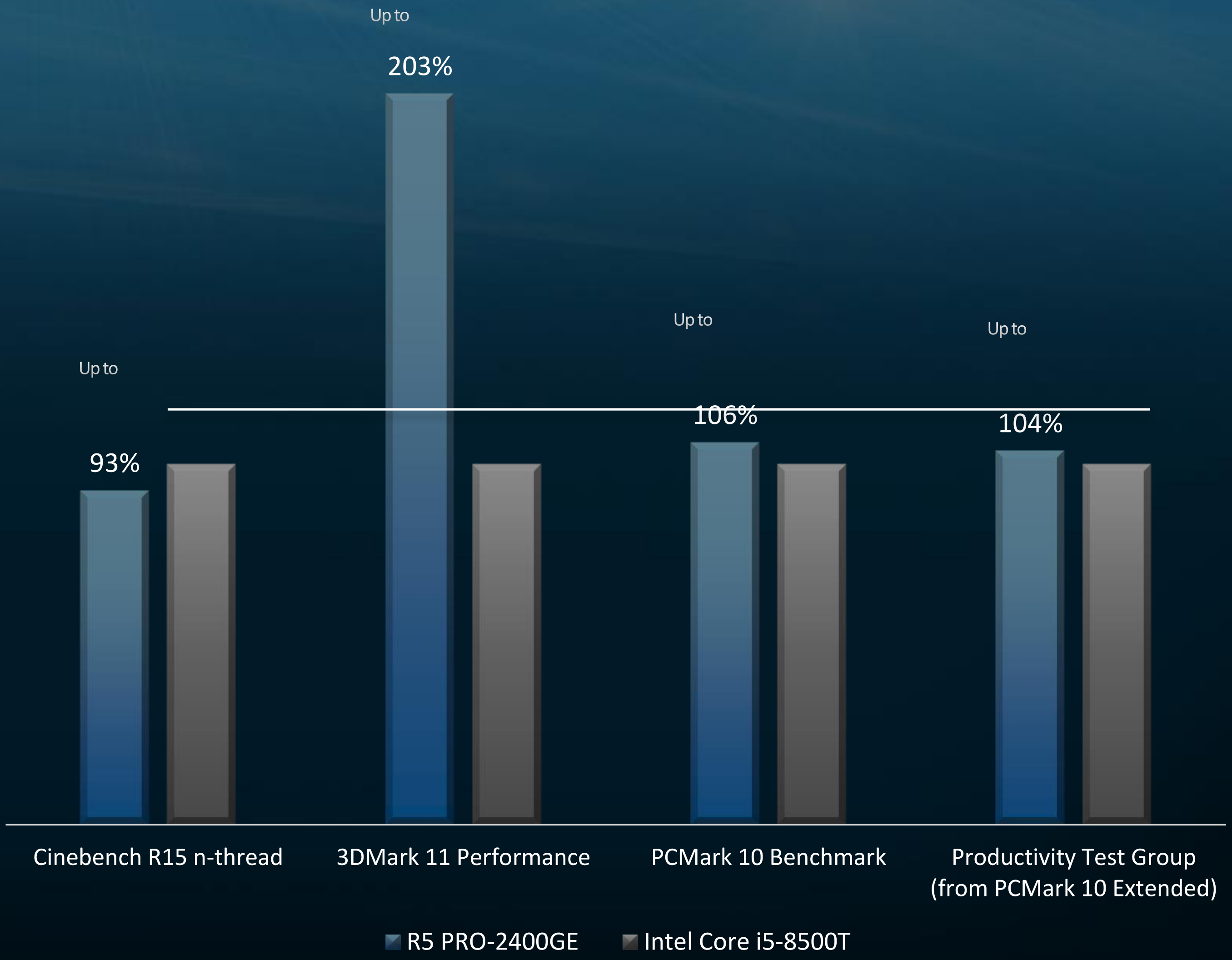
2nd GENERATION RYZEN PRO DESKTOP



* SEE ENDNOTES: PP-8, PP-12 RESULTS MAY VARY.

GREAT 1L DESKTOP PERFORMANCE VS 8TH GEN

2nd GENERATION RYZEN PRO DESKTOP



* SEE ENDNOTES: PP-8, PP-12 RESULTS MAY VARY.

‘Matisse’: 3rd Gen AMD RYZEN™ DESKTOP PROCESSOR TARGETS

DESIGNED FOR PERFORMANCE. BUILT TO WIN.

THE BEST

CORE

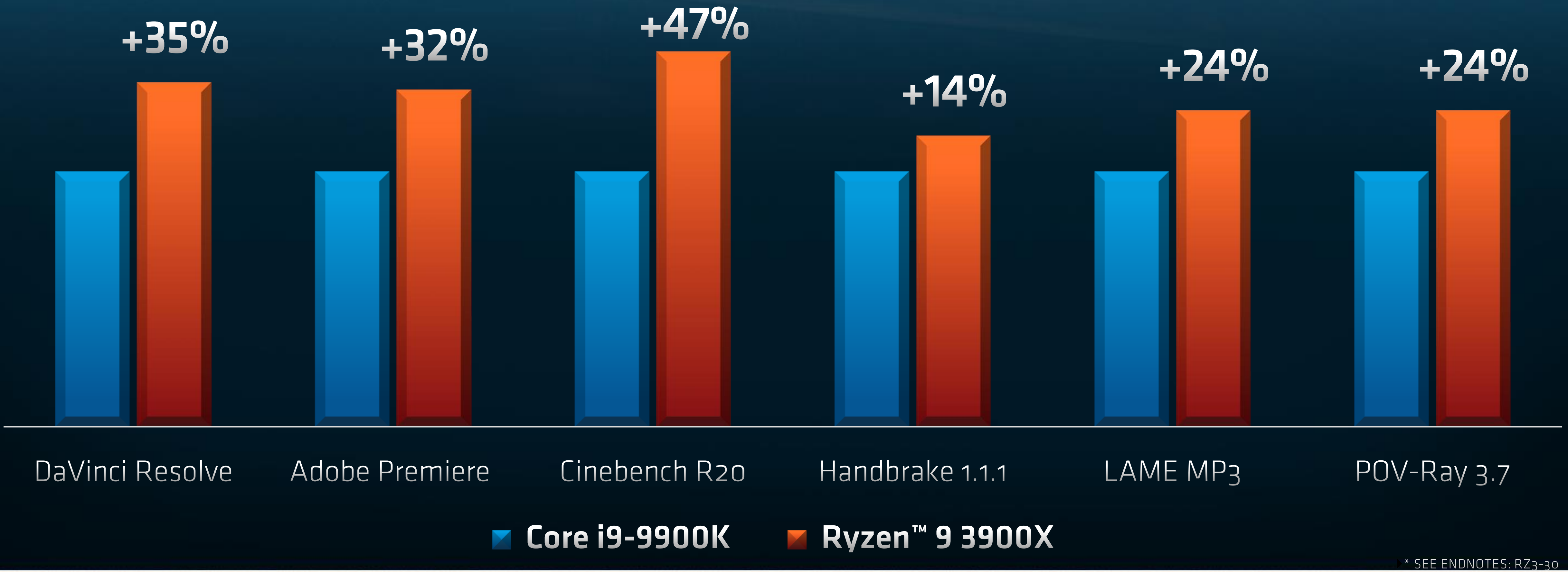
7NM EFFICIENCY

TECHNOLOGY LEADERSHIP:

- The World’s First 7nm Desktop Processor
  - Higher performance at the same TDP
- New ‘Zen2’ Core
  - Higher IPC Plus PCIe G4 Support
- Efficiency Leadership
  - Enhanced Power/Performance Metrics Driving to Achieve AMD’s 25x20 Goal
- Designed For Optimized Multitasking
  - Optimized for 1T Performance When it Matters, and nT

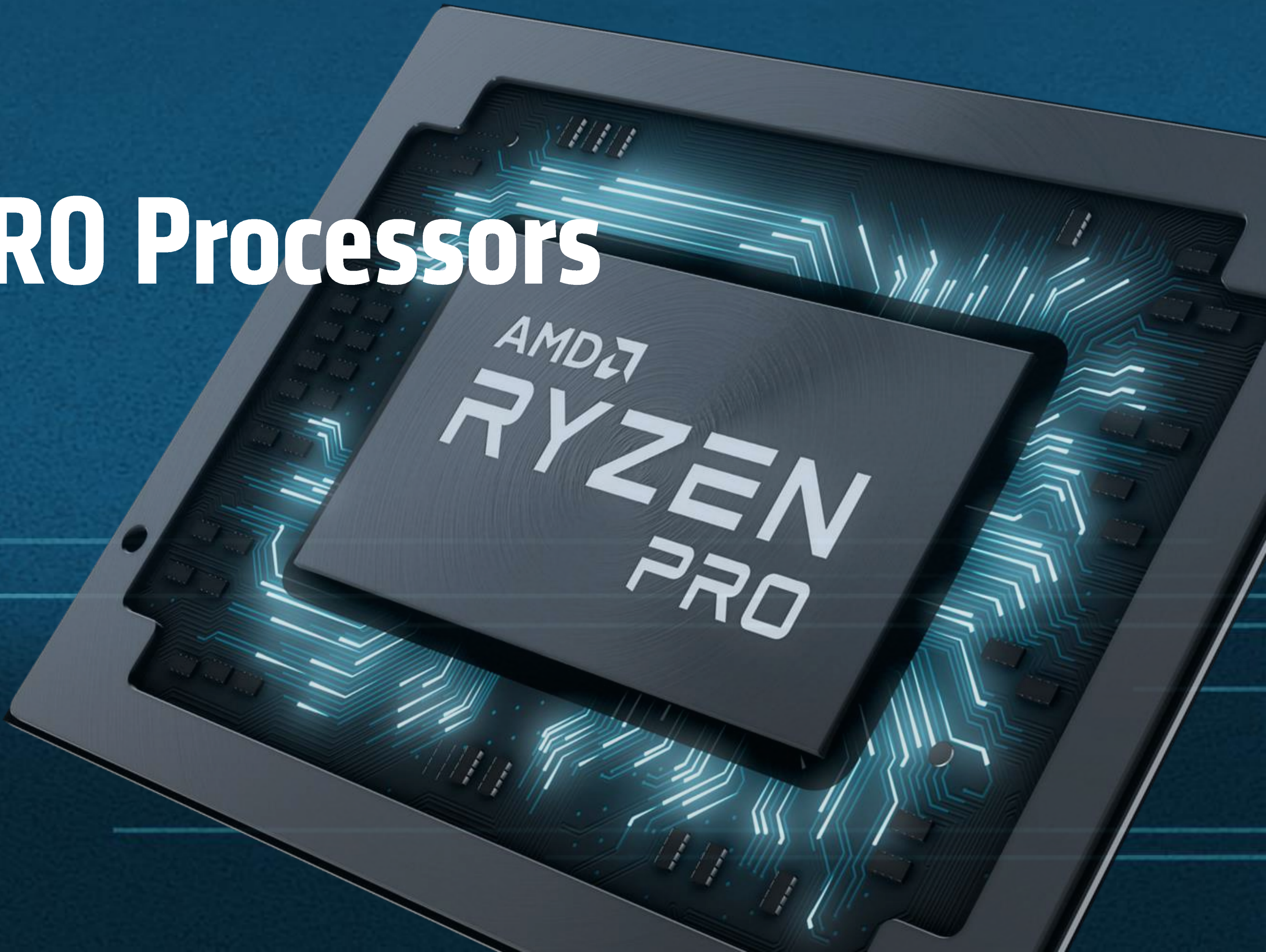
3RD GEN AMD RYZEN™ 9 PROCESSORS

WINNING FOR CREATORS AT $499



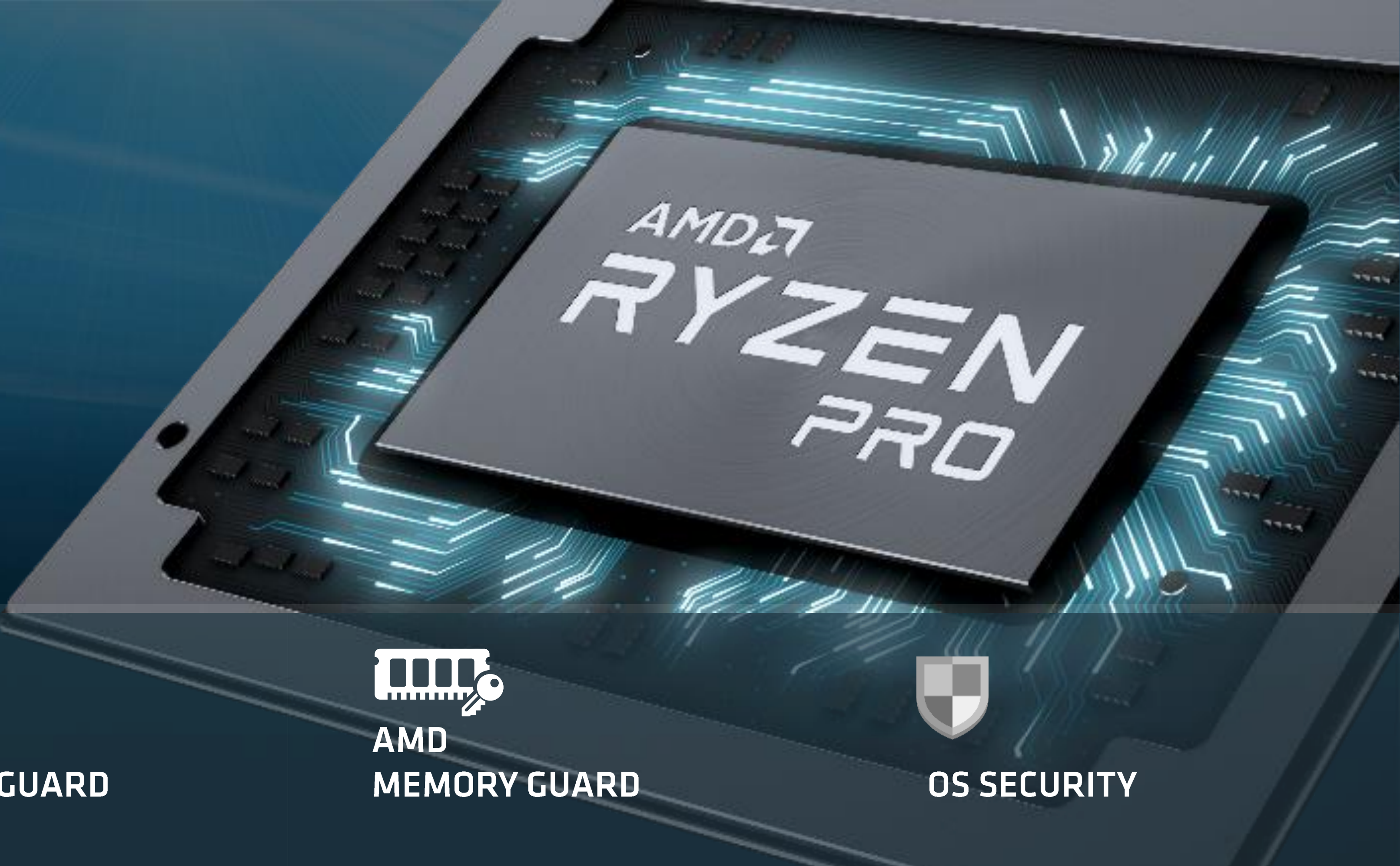
* SEE ENDNOTES: RZ3-30

AMD Ryzen™ PRO Processors



PRODUCTIVITY
PROTECTION
PROFESSIONAL

PRIME DIRECTIVE: PROTECT THE BUSINESSES



Security at the Silicon Level with AMD GuardMI Technology

Ryzen™ Pro Platforms takes full advantage of OEM security offerings

AMD BOOT GUARD

Helps secures BIOS from power on

Helps prevent threats from reaching critical software

Hardware-based root of trust

AMD MEMORY GUARD

OS and application-independent memory encryption

No software modifications

Helps mitigate Cold Boot Attacks

OS SECURITY

Support important Windows 10 security features

Device Guard, Credential Guard, TPM 2.0 , VSB, Level 2 security and beyond with Microsoft

Cost of data loss is up

Easy physical access to sensitive information stored on PCs

Every 53 Seconds
One laptop is stolen

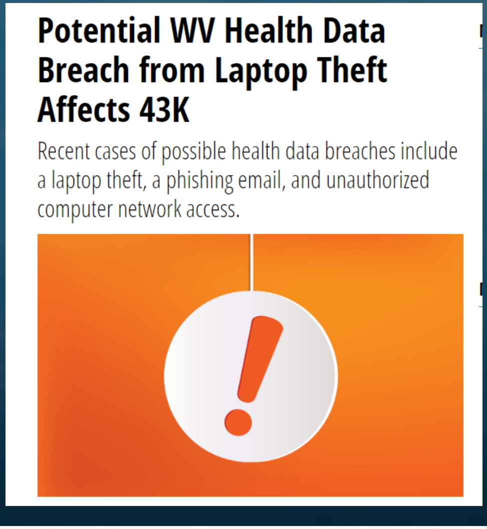
52%
Devices stolen from workplace

80%
Avg cost of the lost of the laptop is from data breach

3X
Data breach is up from 2018

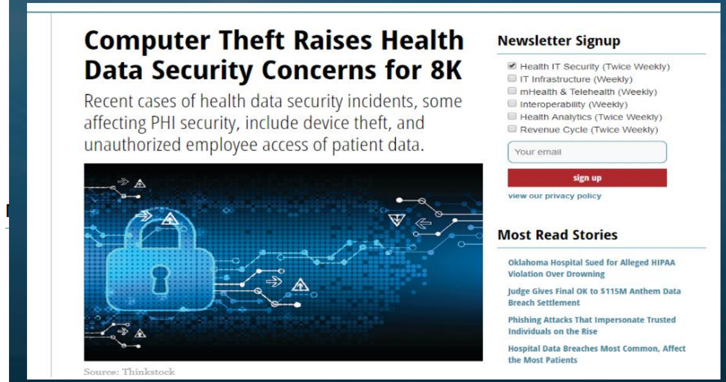
24%
Laptops are stolen from conferences

6%
Cost of data breach is up from 2017



Potential WV Health Data Breach from Laptop Theft Affects 43K

Recent cases of possible health data breaches include a laptop theft, a phishing email, and unauthorized computer network access.



Computer Theft Raises Health Data Security Concerns for 8K

Recent cases of health data security incidents, some affecting PHI security, include device theft, and unauthorized employee access of patient data.

Source: Thinkstock

Newsletter Signup

☑ Health IT Security (Twice Weekly)
☐ IT Infrastructure (Weekly)
☐ mHealth & Telehealth (Weekly)
☐ Interoperability (Weekly)
☐ Health Analytics (Twice Weekly)
☐ Revenue Cycle (Twice Weekly)

Your email

sign up

view our privacy policy

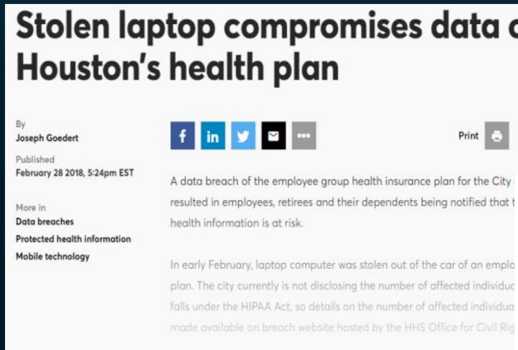
Most Read Stories

Oklahoma Hospital Sued for Alleged HIPAA Violation Over Drowning

Judge Gives Final OK to $115M Anthem Data Breach Settlement

Phishing Attacks That Impersonate Trusted Individuals on the Rise

Hospital Data Breaches Most Common, Affect the Most Patients



Stolen laptop compromises data of Houston's health plan

By
Joseph Goedert

Published
February 28 2018, 5:24pm EST

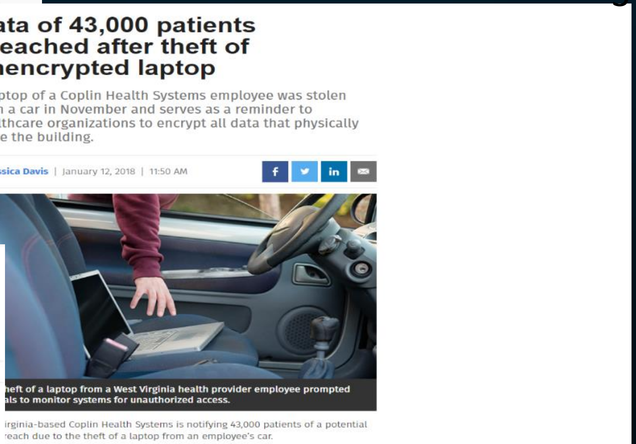
More in
Data breaches
Protected health information
Mobile technology

Print Reprint

A data breach of the employee group health insurance plan for the City resulted in employees, retirees and their dependents being notified that t health information is at risk.

In early February, laptop computer was stolen out of the car of an emplo plan. The city currently is not disclosing the number of affected individu falls under the HIPAA Act, so details on the number of affected individua made available on breach website hosted by the HHS Office for Civil Rig

3



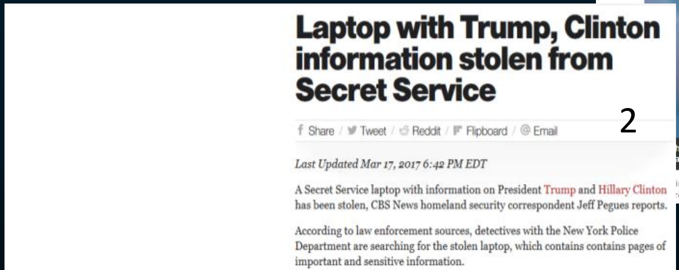
Data of 43,000 patients breached after theft of unencrypted laptop

A laptop of a Coplin Health Systems employee was stolen from a car in November and serves as a reminder to healthcare organizations to encrypt all data that physically leave the building.

By Jessica Davis | January 12, 2018 | 11:50 AM

heft of a laptop from a West Virginia health provider employee prompted als to monitor systems for unauthorized access.

irginia-based Coplin Health Systems is notifying 43,000 patients of a potential reach due to the theft of a laptop from an employee's car.



Laptop with Trump, Clinton information stolen from Secret Service

2

Share / Tweet / Reddit / Flipboard / Email

Last Updated Mar 17, 2017 6:42 PM EDT

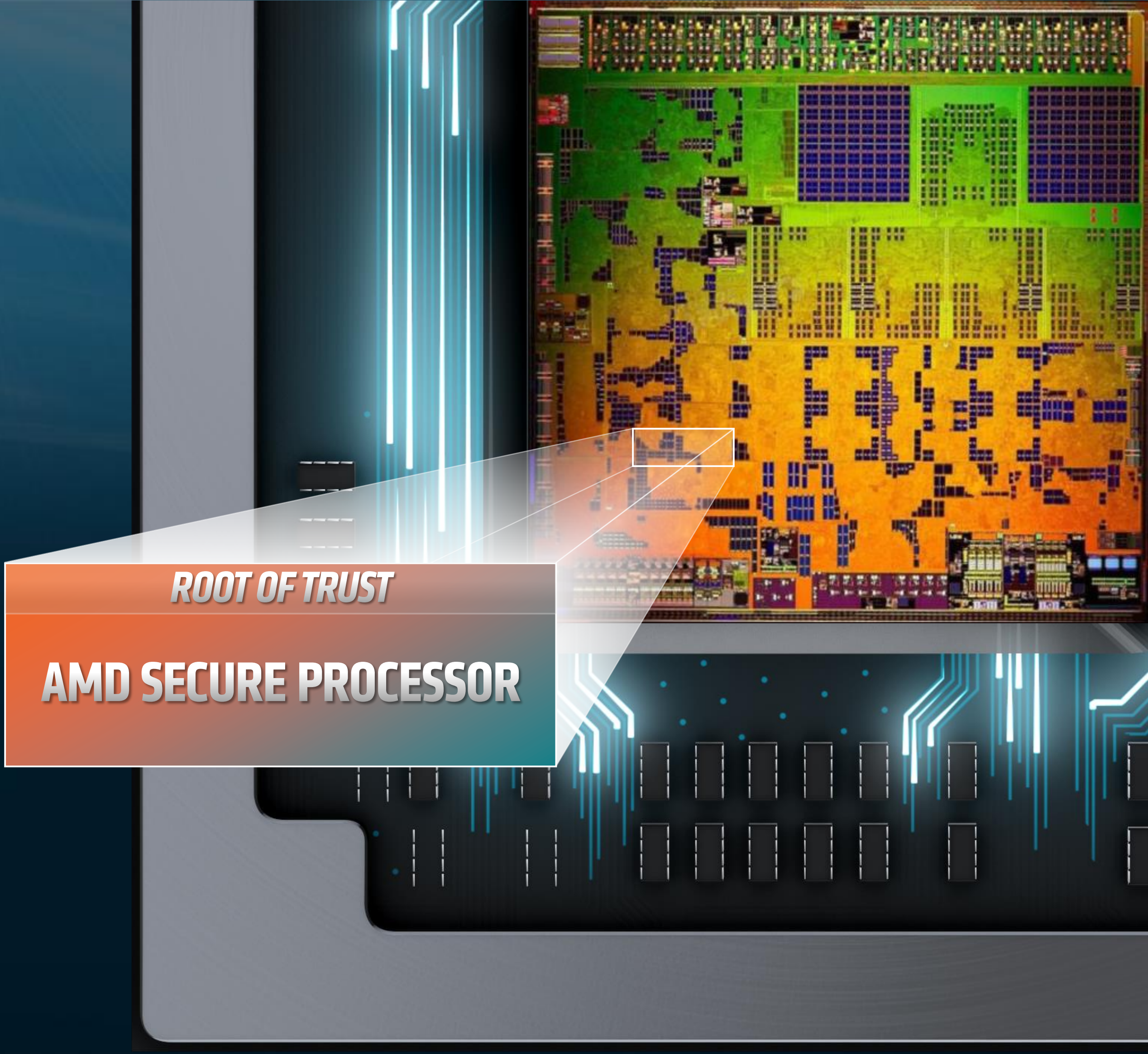
A Secret Service laptop with information on President Trump and Hillary Clinton has been stolen, CBS News homeland security correspondent Jeff Pegues reports.

According to law enforcement sources, detectives with the New York Police Department are searching for the stolen laptop, which contains contains pages of important and sensitive information.

1 - https://www.ibm.com/security/data-breach
2- http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches
https://healthitsecurity.com/news/potential-wv-health-data-breach-from-laptop-theft-affects-43k
https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop
https://www.healthdatamanagement.com/news/as-is-common-in-recent-data-breach-incidents-the-city-is-reinforcing-security-measures
https://healthitsecurity.com/news/computer-theft-raises-health-data-security-concerns-for-8k
https://www.cbsnews.com/news/laptop-trump-clinton-information-stolen-secret-service/

AMD Secure Processor

- AMD Secure Co-Processor integrated within SoC
- Available on all AMD Ryzen™ PRO SKUs
- Secure off host NV storage for firmware and data (i.e., SPI ROM)
- Provides cryptographic functionality for secure key generation and key management
- Independent from x86



AMD SECURE PROCESSOR

Secure Processor is integrated within SOC and available on all AMD Ryzen Processor

HARDWARE ROOT OF TRUST

FIRMWARE PROTECTION

TRUSTED EXECUTION ENVIRONMENT

PROTECTS DATA INTEGRITY & CONFIDENTIALITY

FIRMWARE TPM

PROTECTS CRYPTOGRAPHIC KEYS

PROTECT DATA

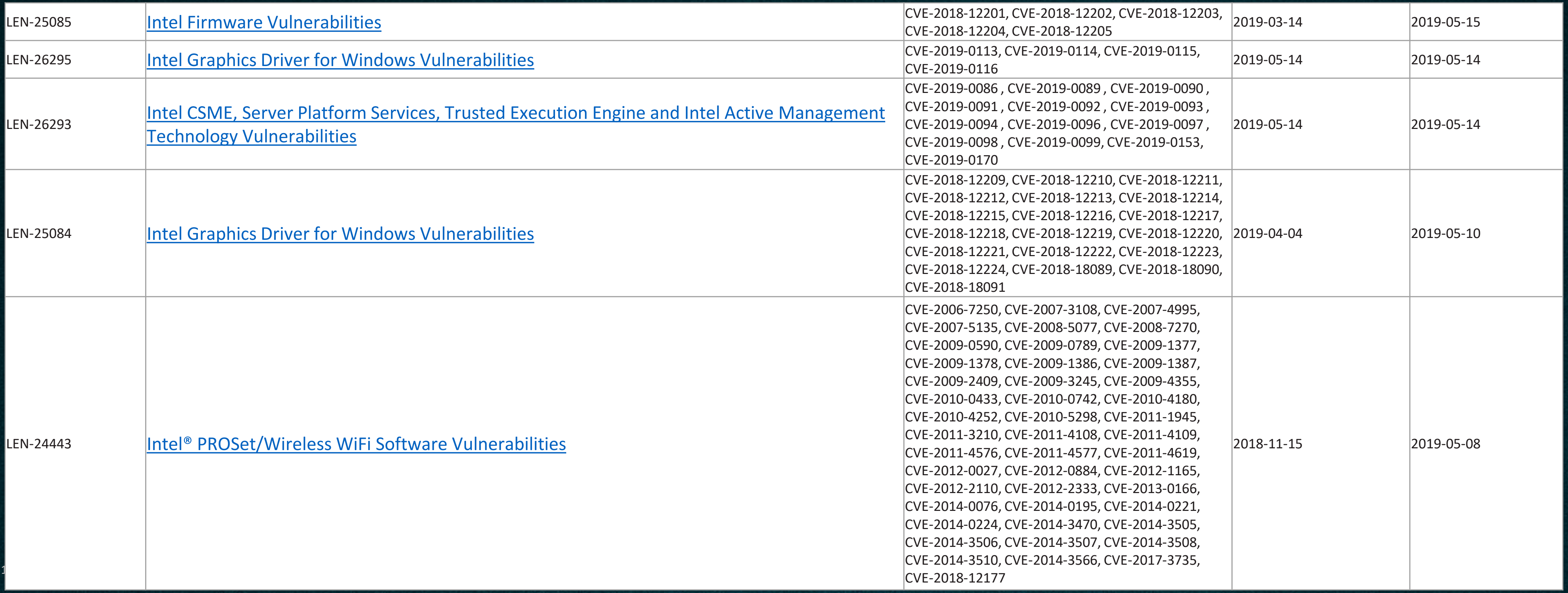
ENCRYPT MEMORY TO PREVENT COLD BOOT ATTACK

HARDWARE DRM

CONTENT PROTECTION

SECURITY VULNERABILITIES ARE CHURNING OEMS & CUSTOMERS

- Reference OEM Security Advisory Summaries to See Magnitude of Security Mitigations
  - Lenovo : https://support.lenovo.com/de/en/product_security/home
    - 30+ Intel security vulnerability/mitigations listed for 2018
  - HPi : https://support.hp.com/us-en/security-bulletins
    - 2 AMD security issues mentioned, 20+ Intel security mitigations listed in 2018



LEN-25085	Intel Firmware Vulnerabilities	CVE-2018-12201, CVE-2018-12202, CVE-2018-12203, CVE-2018-12204, CVE-2018-12205	2019-03-14	2019-05-15
LEN-26295	Intel Graphics Driver for Windows Vulnerabilities	CVE-2019-0113, CVE-2019-0114, CVE-2019-0115, CVE-2019-0116	2019-05-14	2019-05-14
LEN-26293	Intel CSME, Server Platform Services, Trusted Execution Engine and Intel Active Management Technology Vulnerabilities	CVE-2019-0086 , CVE-2019-0089 , CVE-2019-0090 , CVE-2019-0091 , CVE-2019-0092 , CVE-2019-0093 , CVE-2019-0094 , CVE-2019-0096 , CVE-2019-0097 , CVE-2019-0098 , CVE-2019-0099, CVE-2019-0153, CVE-2019-0170	2019-05-14	2019-05-14
LEN-25084	Intel Graphics Driver for Windows Vulnerabilities	CVE-2018-12209, CVE-2018-12210, CVE-2018-12211, CVE-2018-12212, CVE-2018-12213, CVE-2018-12214, CVE-2018-12215, CVE-2018-12216, CVE-2018-12217, CVE-2018-12218, CVE-2018-12219, CVE-2018-12220, CVE-2018-12221, CVE-2018-12222, CVE-2018-12223, CVE-2018-12224, CVE-2018-18089, CVE-2018-18090, CVE-2018-18091	2019-04-04	2019-05-10
LEN-24443	Intel® PROSet/Wireless WiFi Software Vulnerabilities	CVE-2006-7250, CVE-2007-3108, CVE-2007-4995, CVE-2007-5135, CVE-2008-5077, CVE-2008-7270, CVE-2009-0590, CVE-2009-0789, CVE-2009-1377, CVE-2009-1378, CVE-2009-1386, CVE-2009-1387, CVE-2009-2409, CVE-2009-3245, CVE-2009-4355, CVE-2010-0433, CVE-2010-0742, CVE-2010-4180, CVE-2010-4252, CVE-2010-5298, CVE-2011-1945, CVE-2011-3210, CVE-2011-4108, CVE-2011-4109, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619, CVE-2012-0027, CVE-2012-0884, CVE-2012-1165, CVE-2012-2110, CVE-2012-2333, CVE-2013-0166, CVE-2014-0076, CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470, CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3510, CVE-2014-3566, CVE-2017-3735, CVE-2018-12177	2018-11-15	2019-05-08

Cold Boot Attack

Problem with hard drive encryption, passwords and login protection

- Security keys remain in RAM until the computer is shutdown - Yet most users leave notebook in **SUSPEND** state[1]
- A 2017 IEEE Paper[2] and a 2018 Demonstration[3] researchers were still able to by-pass protections to access encryption keys and login information
- Threat of these attacks make users tradeoff security for features like modern standby

⚠ **Due to the design of modern computers, nearly all the data manipulated during a session is temporarily written to RAM. This can include texts, saved files, passwords, and encryption keys! Data from more recent activities has a greater likelihood of still residing in RAM[1]**

1. Attacker has access to a company laptop and steals it

2. Attacker changes firmware settings

3. Attacker performs cold reboot from a USB key

4. Attacker gets encryption keys from memory

New cold boot attack affects 'nearly all modern computers'

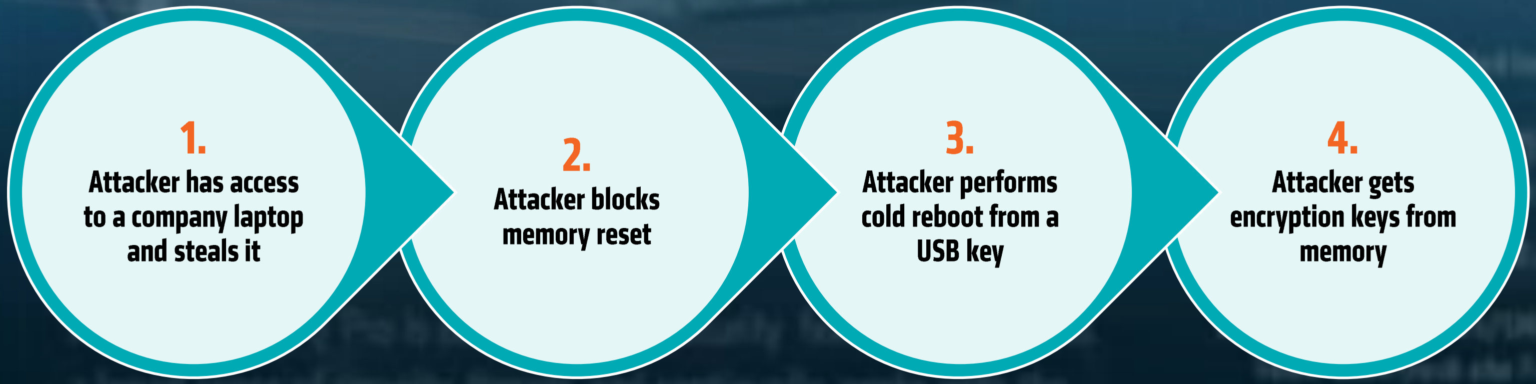
Security researchers find a new way to disable current cold boot attack firmware security measures to steal sensitive data from high-value computers.

By Catalin Cimpanu for Zero Day | September 13, 2018 -- 08:30 GMT (01:30 PDT) | Topic: Security

[1] - https://www.whonix.org/wiki/Protection_Against_Physical_Attacks#cite_note-5
[2] - https://www.eecs.umich.edu/eecs/about/articles/2017/HPCA17-coldboot.pdf
https://www.youtube.com/watch?v=E6gzVVjW4yY
[3] - https://blog.f-secure.com/cold-boot-attacks/

AMD Designs In Security Features To Help Address Cold Boot Attacks

Anatomy Of A Cold Boot Attack:



1. Attacker has access to a company laptop and steals it

2. Attacker blocks memory reset

3. Attacker performs cold reboot from a USB key

4. Attacker gets encryption keys from memory

- Security keys remain in RAM until the computer is shutdown - Yet most users leave notebook in suspend state[1]
- A 2017 IEEE Paper[2] and a 2018 Demonstration[3] researchers were still able to by-pass protections to access encryption keys and login information
- Threat of these attacks make users tradeoff security for features like modern standby

Security Approaches

4. User must shut PC completely off

Poor user experience

Greater Risk

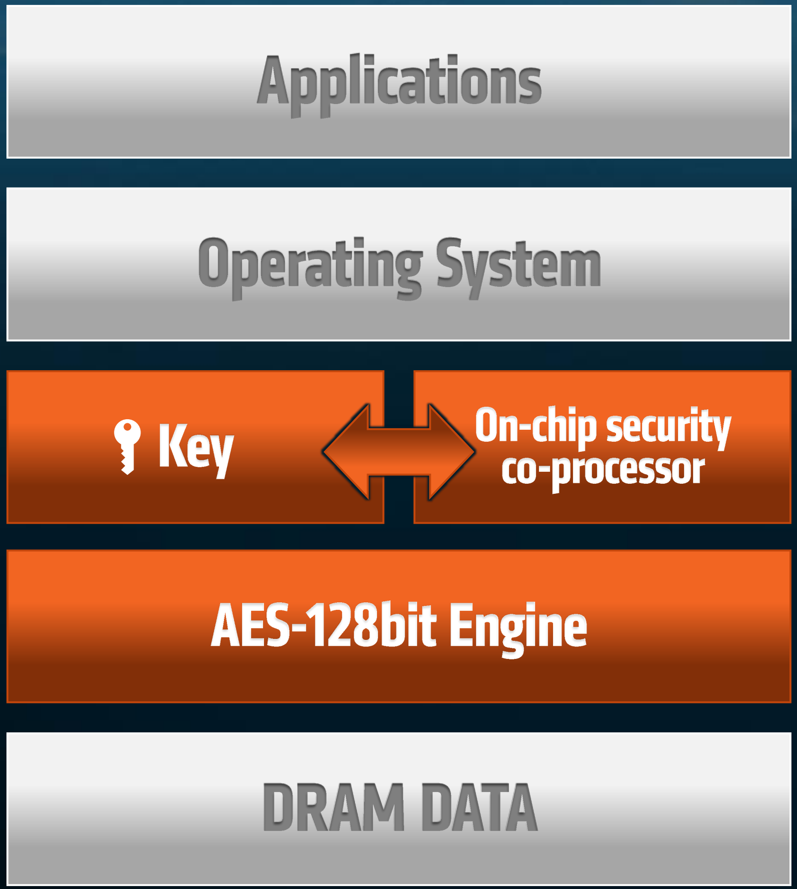
Current Approach

4. ~~Attacker gets encryption keys from memory~~

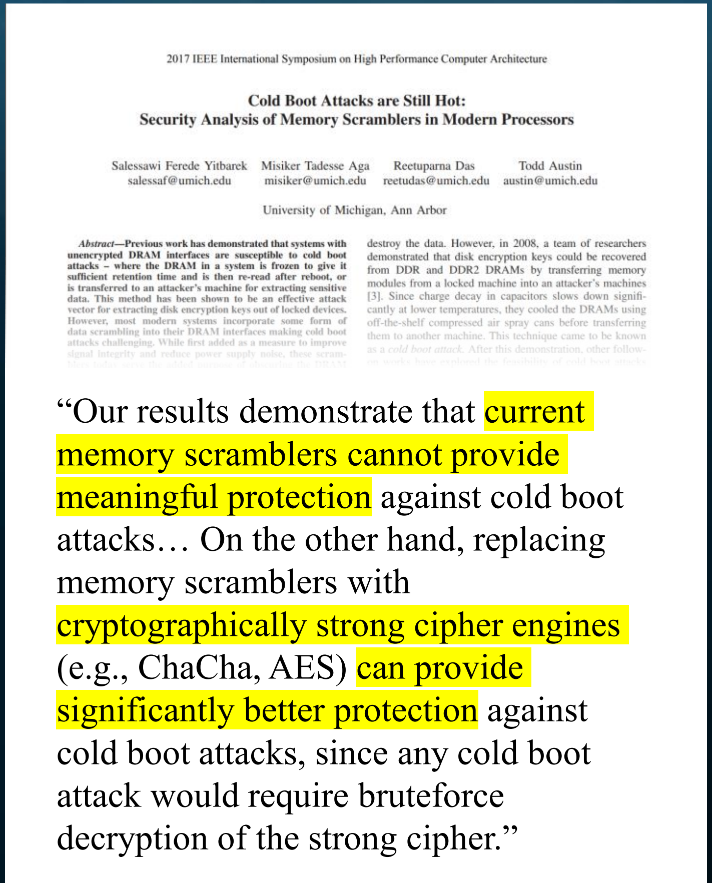
User leaves PC in Standby

AMD Memory Guard Helps Mitigate Attack And Allows Full User Experience

AMD Memory Guard



- OS and Application Independent
- Included on All Ryzen PRO and Athlon PRO Processors
- AES Encryption Key Managed by Security Co-Processor and is Not Accessible by x86 Cores and OS/App Software
- Key is generated by a onboard NIST SP 800-90 compliant hardware random number generator on each boot
- Real-Time Encryption/Decryption of System RAM* with negligible performance Impact to the system
- AES Encryption Provides Significantly Better Protection Against Cold Boot Attacks allowing the user to keep their PC in a standby state



2017 IEEE International Symposium on High Performance Computer Architecture

Cold Boot Attacks are Still Hot:
Security Analysis of Memory Scramblers in Modern Processors

Salessawi Ferede Yitbarek, salessaf@umich.edu
Misiker Tadesse Aga, misiker@umich.edu
Reetuparna Das, reetudas@umich.edu
Todd Austin, austin@umich.edu

University of Michigan, Ann Arbor

***Abstract*—Previous work has demonstrated that systems with unencrypted DRAM interfaces are susceptible to cold boot attacks – where the DRAM in a system is frozen to give it sufficient retention time and is then re-read after reboot, or is transferred to an attacker's machine for extracting sensitive data. This method has been shown to be an effective attack vector for extracting disk encryption keys out of locked devices. However, most modern systems incorporate some form of data scrambling into their DRAM interfaces making cold boot attacks challenging. While first added as a measure to improve signal integrity and reduce power supply noise, these scramblers today serve the added purpose of obscuring the DRAM**

destroy the data. However, in 2008, a team of researchers demonstrated that disk encryption keys could be recovered from DDR and DDR2 DRAMs by transferring memory modules from a locked machine into an attacker's machines [3]. Since charge decay in capacitors slows down significantly at lower temperatures, they cooled the DRAMs using off-the-shelf compressed air spray cans before transferring them to another machine. This technique came to be known as a *cold boot attack*. After this demonstration, other follow-on works have explored the feasibility of cold boot attacks

"Our results demonstrate that current memory scramblers cannot provide meaningful protection against cold boot attacks… On the other hand, replacing memory scramblers with cryptographically strong cipher engines (e.g., ChaCha, AES) can provide significantly better protection against cold boot attacks, since any cold boot attack would require bruteforce decryption of the strong cipher."

https://www.eecs.umich.edu/eecs/about/articles/2017/HPCA17-coldboot.pdf

* Tested by AMD engineering lab on AMD reference system with production parts. Performance impacts could vary on other platforms.

MADE FOR PROFESSIONALS TOP TO BOTTOM

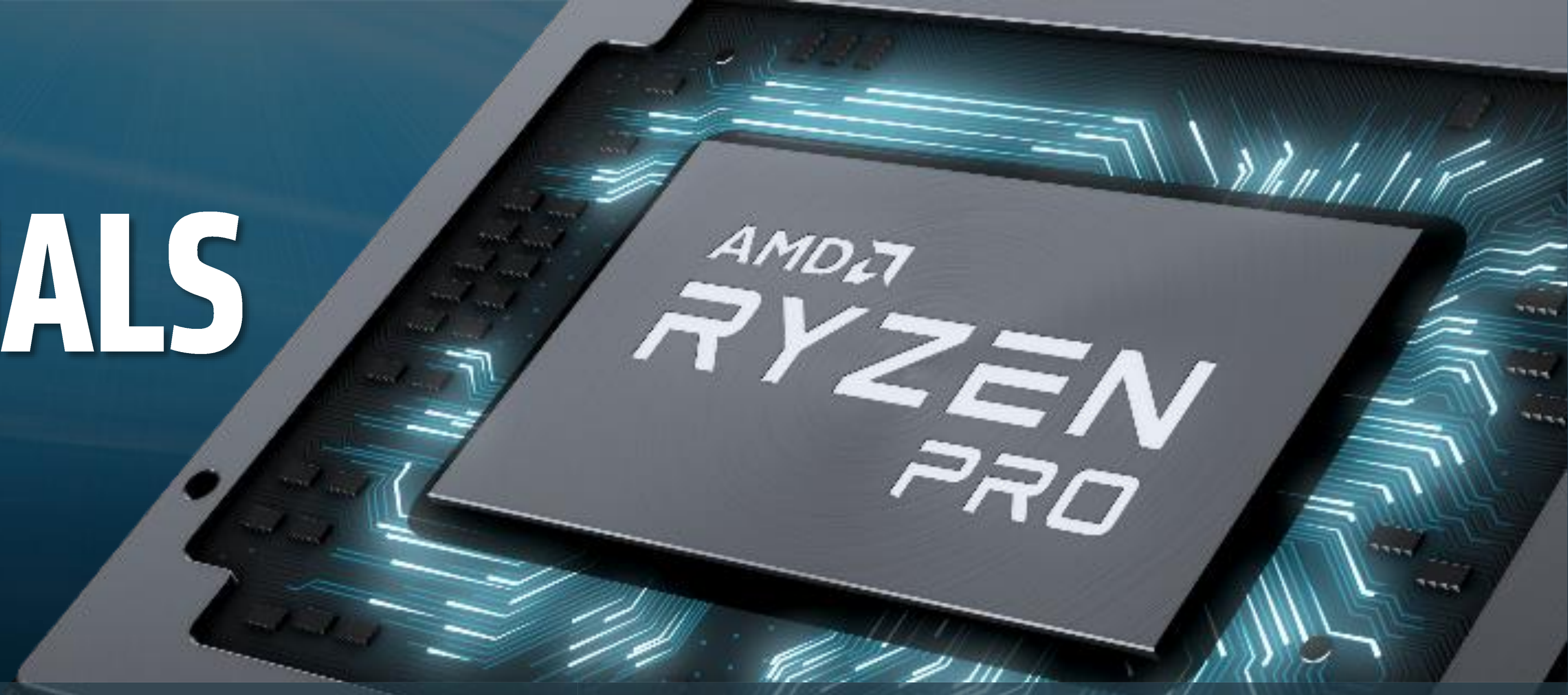


IMAGE STABILITY

18 months of planned software stability brings peace of mind

PROCESSOR AVAILABILITY

24 months of planned availability for a stable enterprise

COMMERCIAL-GRADE QUALITY

Commercial-grade QA process

Our best silicon for long-term reliability and performance

ENTERPRISE-CLASS MANAGEABILITY

Open standard DASH manageability standard

CPU agnostic, no vendor lock-ins

Introducing KVM feature

COMMERCIAL LIMITED WARRANTY

36-Month Limited Warranty to System Manufacturer vs. 12 months for consumer parts

Security, Manageability, And Support Across All AMD PRO Processors

AMD PRO vs Intel vPRO

DASH Manageability open-standards and industry-backed solution comparable to Intel vPRO on all AMD PRO processors. Now includes AMD KVM for BIOS

Security Features on all AMD PRO processors

Commercial Grade Support on all AMD PRO processors

https://developer.amd.com/tools-for-dmtf-dash/
https://www.youtube.com/watch?v=6m6_2K45Y7k
https://www.youtube.com/watch?v=39XAMP73MiQ
https://developer.amd.com/tools-for-dmtf-dash/

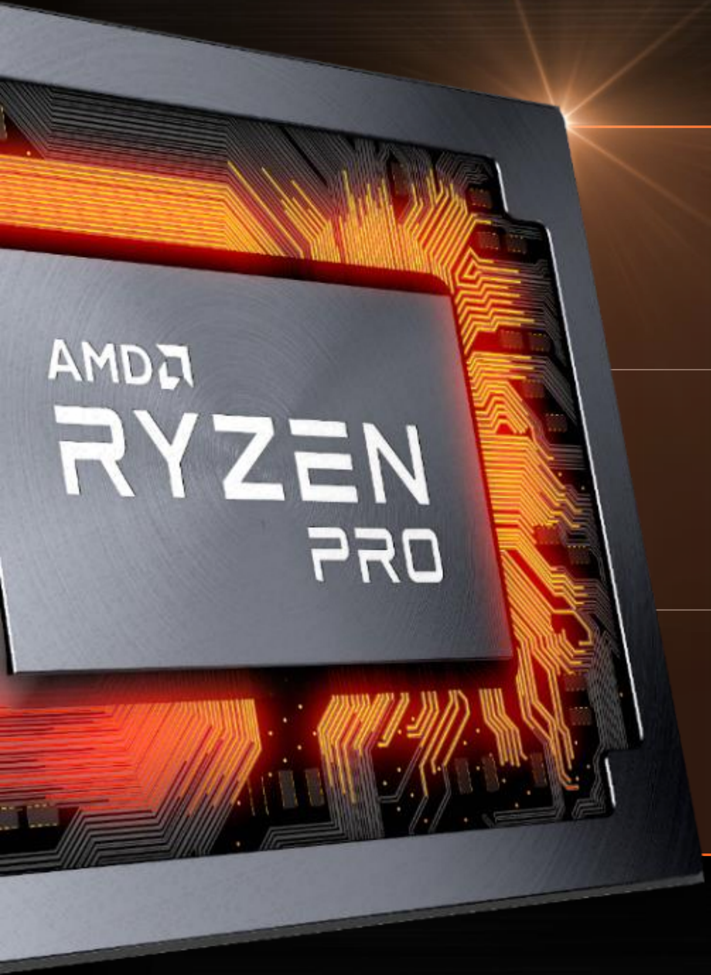
MANAGEABILTY FEATURE	AMD PRO	INTEL vPro (i7 & i5 only)
Asset Inventory – HW/SW	✓	✓
Remote Power Control (DASH Power Control)	✓	✓
Boot Control	✓	✓
Platform Alerts	✓	✓
Secure Transport (HTTPS) & WS-Management (SOAP-based)	✓	✓
Standardized Discovery	✓	✓
User Administration	✓	✓
Web GUI/Embedded web server	✓	✓
IPv6 (out-of-band)	✓	✓
Active Directory w/ Kerberos	✓	✓
Network Quarantine	✓	✓
802.1X (EAPoL) Authentication for Out-Of-Band (OOB) Management	✓	✓
Wireless In-Band Management (Requires Wi-Fi capability in the platform)	✓	✓
Zero-touch provisioning	✓	✓
Text Console Redirection	✓ (telnet/SSHv2)	✓ (SoL)
Opaque Management Data Mailbox (3rd party non-volatile datastore)	✓	✓
BIOS Management	✓	✓ (1:1 only)
USB/Media Redirection	✓	✓
OEM-Branded Customizable Web GUI	✓	✓
PLDM/MCTP Interfaces for Health monitoring (fan speed, temp, etc.)	✓	✓
Co-existence of OOB Management and Network Proxy functions	✓	✓
OS Status	✓	✓
"Graceful"/"Soft" Shutdown	✓	✓
Management Firmware Update (Remotely)	✓	✓
KVM Redirection	✓ (HP EliteDesk)	✓
KVM (BIOS)	✓ AMD KVM	✓

SECURITY FEATURE	AMD PRO	INTEL vPro (i7 & i5 only)
Dedicated Security Co-processor	✓ On-chip	✓ Off-chip - In chipset
System Memory Encryption	✓	✓ Application recompile
Boot Control	✓	✓

COMMERCIAL FEATURE	AMD PRO	INTEL vPro (i7 & i5 only)
Stable image and Longevity	✓ 18 – 24 Months	✓ 15 months
Commercial quality	✓	✓

Source: https://en.wikipedia.org/wiki/Intel_Management_Engine
Source : https://www.intel.com/content/www/us/en/computer-upgrades/pc-upgrades/sipp-intel-stable-image-platform-program.html

WHY AMD NOW?



1 ROADMAP EXECUTION – AMD Ryzen™ PRO is the most competitive technology ever for AMD, built from all-new ‘Zen’ Architecture, which delivered an industry record of 50%+ performance improvement in one generation. AMD is now passing the competition on process technology.

2 SUPPLY EXECUTION – AMD has executed on our roadmap and has full global supply availability on Ryzen™, able to ship TODAY

3 SECURITY – AMD Ryzen™ ship with a unique security architecture that enables advanced HW based security and is NOT vulnerable to new security threats our competition is faced with

This has resulted in a 200%+ increase in AMD’s stock in 2018, and their best financial performance in 7+ years.