e-Governance Conference, Tallinn, Estonia

Security Challenges and Opportunities –
For today & tomorrow

Yasser Rasheed,

Global Director, Enterprise Endpoint Products

intel®

World-changing Technology

Our Purpose

We create world-changing technology
that enriches the lives of every person on Earth

How is the Security Landscape Shifting?

Attacks on the Rise

$10.5 trillion projected annual cybercrime cost to the world by 2025[2]

62% of IT execs are increasing security solutions budgets[3]

75% of companies attacked by Ransomware ran up to date endpoint protection software[4]

Increasing Regulation

- GDPR
- HIPAA
- PCI
- NIST

Increased Spending Year on Year

Worldwide Security Spending[1]

2017: ~$94Billion

2019: ~$120 Billion

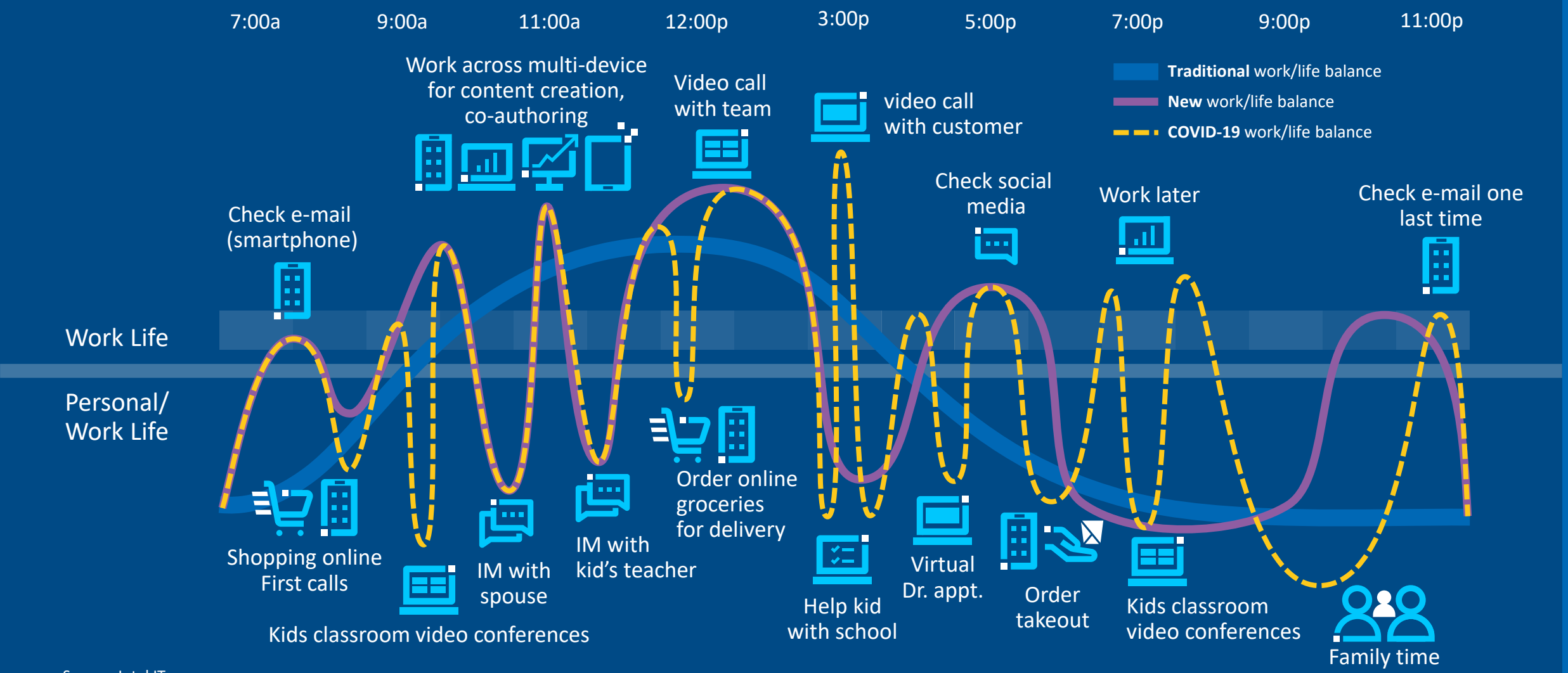
2020: ~$132 Billion

2021: ~$143.5 Billion forecast

1. IDC's Worldwide Security Spending Guide , V1 2021, February 2021
2. Cybersecurity Ventures, Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (link)
3. IDG, GlobeNewswire, 2019 CIO Tech Poll, June 2019 (link)
4. Sophos (link)

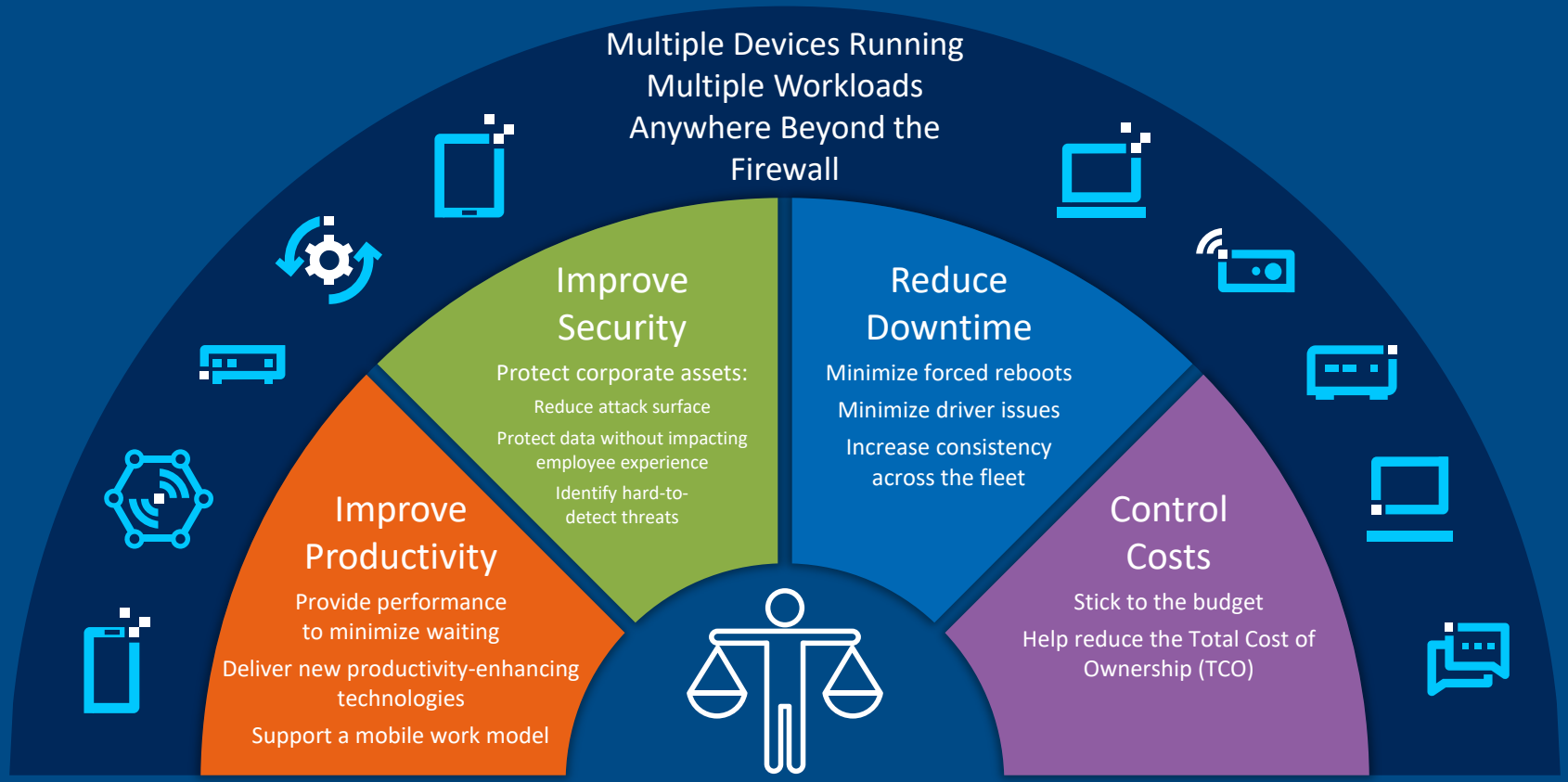
No product or component can be absolutely secure

A Day in The Life



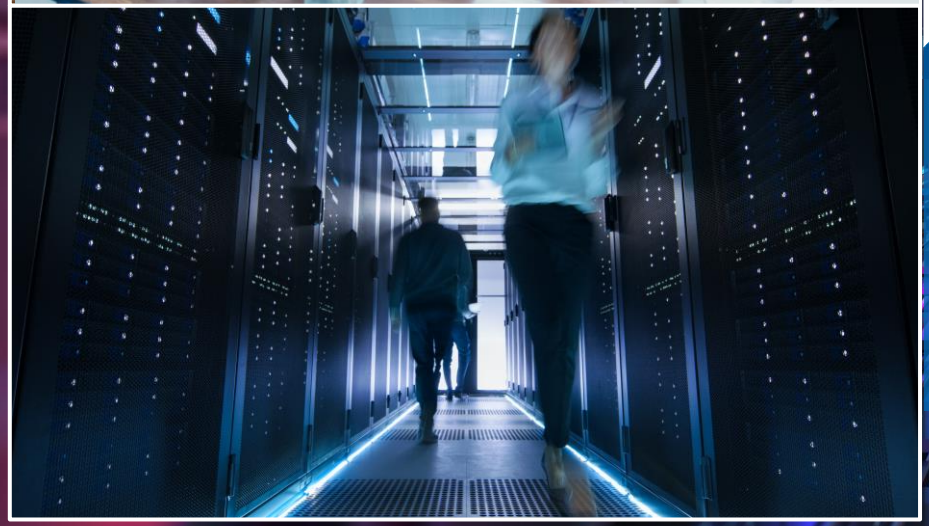
Source: Intel IT

The IT Challenge: Balancing Top Priorities



Security engineered from the ground up can help IT be more strategic, take the pressure off the CISO, become more resilient and support the business

Intel’s End-to-End Security Perspective



We orient our platforms to put security features inside to alleviate a lot of the pressures that the government CISOs are facing.

SECURITY HISTORY

Security Starts with Intel

For years, Intel has inspired organizations to raise the bar in the way they think about keeping products secure. Intel hardware security has played a pivotal role in building trust for these innovations. Security is in our DNA: yesterday, today and tomorrow.

"We are on record as saying that VT is the most significant change to PC architecture this decade"
Martin Reynolds, Gartner Senior Analyst

Hardware-based root of trust

1992
Intel drives the formation of the Desktop Management Task Force, the first open system for PC security management

2004
Intel® Virtualization Technology (Intel® VT)

2006
Intel Virtualization Technology for Directed I/O

2007
Intel® Trusted Execution Technology (Intel® TXT)

Secure enclaves in hardware to help protect application code and data

Bakes cryptographic keys into the silicon at manufacture

Pervasive, accelerated encryption in areas where it was previously not possible

2015
Intel® Software Guard Extensions (Intel® SGX)

2013
Intel® Platform Trust Technology (Intel® PTT) Integrated HW TPM2.0

2009
Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

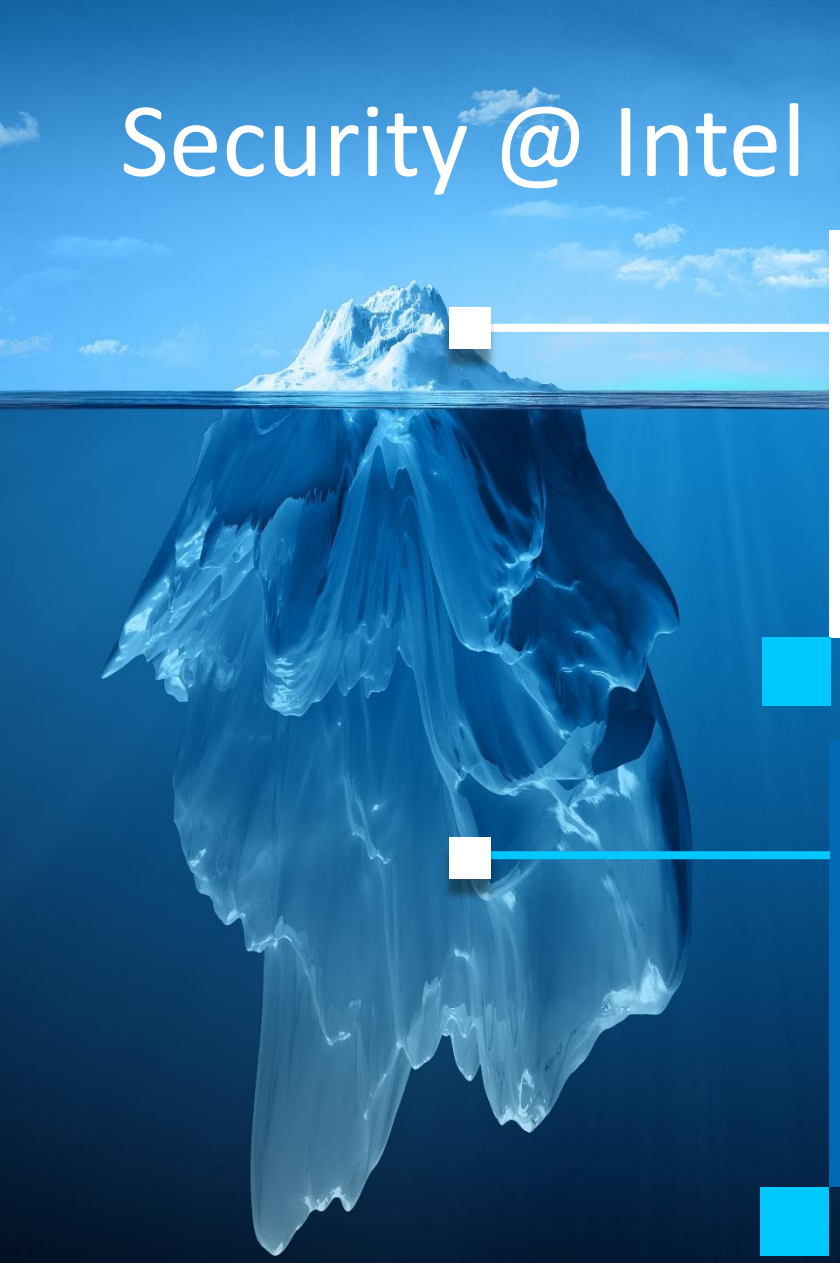
Intel® Hardware Shield addresses security needs on an increasingly remote workforce

Intel engineers invented ground-breaking technology to help shut down an entire class of attacks that long evaded software only solution

2019
Intel Hardware Shield adds TXT-based trustworthy attestation to Intel® Runtime BIOS Resilience (Intel® IRBR) via Intel® System Security Report (Intel® ISSR)

2021
Intel® Control-flow Enforcement Technology (Intel® CET) now available as part of Intel Hardware Shield, on 11th Gen Intel® Core™ vPro® mobile processors

Security @ Intel



Advanced Security Features

Innovative processor and device capabilities rooted in hardware to help provide maximum protection for customer data

Examples

Servers

Clients

IOT

Compute Lifecycle Assurance

Foundational security assurance & features built into every Intel product, maintained and managed across the entire lifecycle

- BUILD
- TRANSFER
- OPERATE
- RETIRE

Compute Lifecycle Assurance

Assuring platform integrity throughout the compute lifecycle

BUILD

Design, Source, Manufacture

TRANSFER

Distribute, Integrate

OPERATE

Provision, Manage, Update, Track

RETIRE

Wipe, EOL, Log, Second Life

Prevent

Resolve

Innovate

Lead

Intel® Hardware Shield

Built-in security to help protect your mission

intel vPRO PLATFORM
BUILT FOR BUSINESS

Protected with Intel® Hardware Shield

Advanced Threat Protection

Hardware-powered, AI-enabled threat detection without a performance hit

Application & Data Protection

Achieved through virtualization-based security

Below-the-OS Security

Lock down memory in the BIOS against firmware attacks and enforce secure boot at the hardware level

- APPS
- OS
- VM
- HYPERVISOR
- BIOS/FIRMWARE
- CPU

No product or component can be absolutely secure.

A Strategy Built for Modern Endpoint Security

A simple, effective security strategy to help CISOs modernize government IT

Buy the right devices

Keep the devices updated and patched

Layer in additional services for greater protection

intel vPRO PLATFORM
BUILT FOR BUSINESS

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.


intel