RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PS-R01**

"I’m Still Standing," Says Each Cyber-Resilient Device

Abhilasha Bhargav-Spantzel

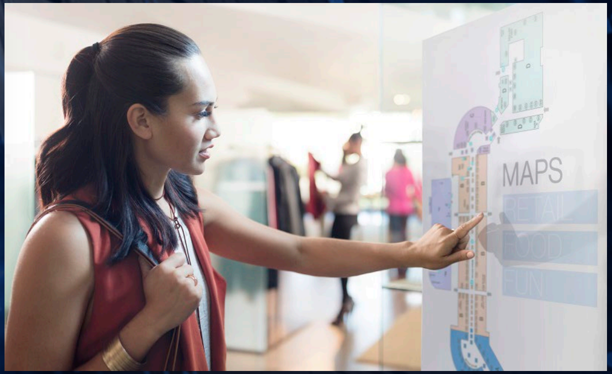
Principal Engineer
Intel Corporation

Nivedita Aggarwal

Firmware Engineer
Intel Corporation

the pc is the human touchpoint

Powering every person's greatest contribution to the data-centric enterprise



How is the security landscape shifting?

90% of INCIDENTS

Result from exploits in software[1]

Every 4.2 seconds

New malware in the first quarter of 2017[2]

Cost of a breach

Digital records stolen, brand damage, etc.

62% IT budget on Security

And 41% on risk analysis[4]

Attacks on the rise

General Data Protection Regulation

PCI Security Standards Council™

FISMA COMPLIANCE

NIST

increasing regulation

worldwide security spending[4]

2017: ~$102 Billion

2018: ~$114 Billion

2019: ~$124

15% CAGR

Increased spending

[1] McAfee Labs Threat Report, June 2018

[2] GData, Malware Trends 2017, 2017

[3] Gartner Press Release, August 15, 2018

[4] 2019 CIO Tech Poll, IDG/CIO

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

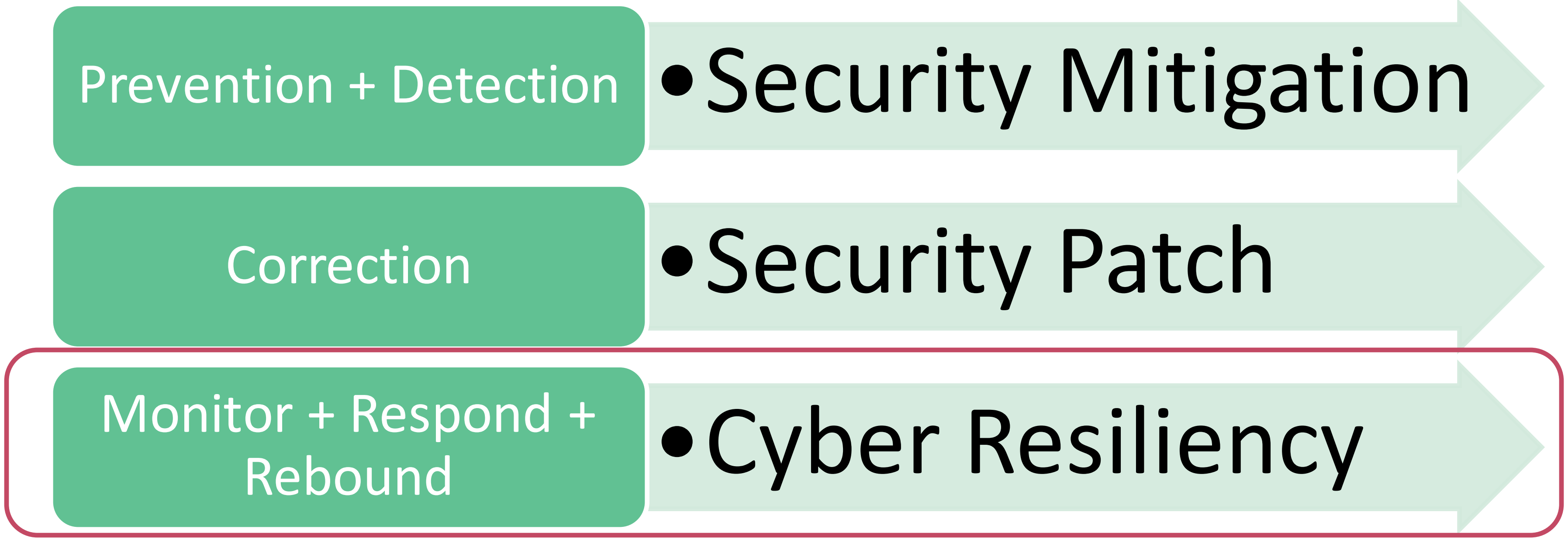
Agenda

- Cyber Resiliency Overview
- Problem Statement
- Enterprise Requirements
- Strategy and Challenges
- Resiliency Principles
- Deep dive of solution architecture for firmware resiliency
- Industry standards

When you go back you should be able to identify the need for resiliency and understand the current industry work

What is Cyber Resilience?

- NIST[1] defines Cyber Resilience as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources



Prevention + Detection
- Security Mitigation

Correction
- Security Patch

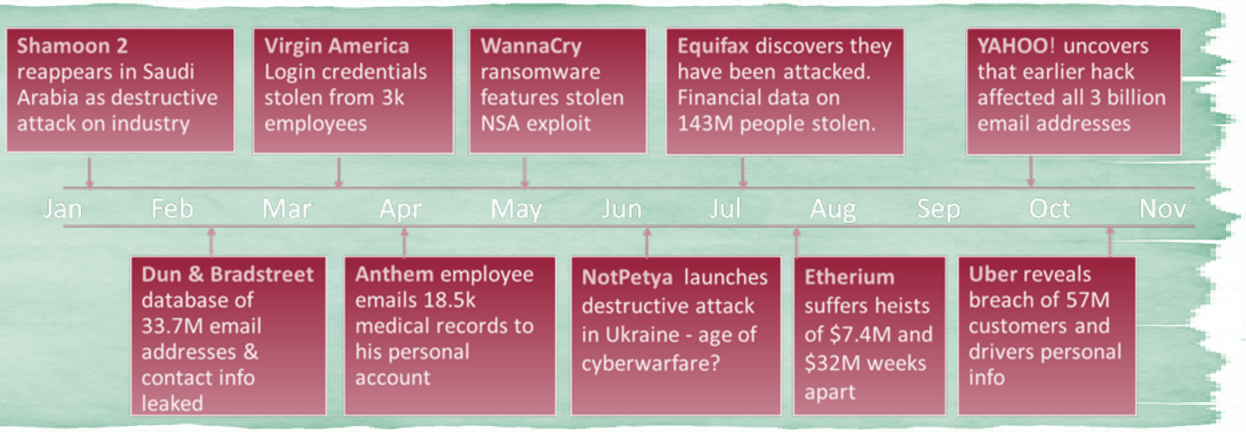
Monitor + Respond + Rebound
- Cyber Resiliency

[1] National Institute of Standards and Technology: https://csrc.nist.gov/

Problem Statement

In 2012[1] Shamoon malware wiped out the hard drives of 35,000 Aramco computers. A three quarters of their Servers went unusable and several 10000s of their employees unable to login to their system and resume work for several months.

Just in the first quarter of 2017, new malware emerged every 4.2 seconds[2] Critical infrastructure e.g. hospitals were forced to stop production. This trend continues till date.



Shamoon 2 reappears in Saudi Arabia as destructive attack on industry

Virgin America Login credentials stolen from 3k employees

WannaCry ransomware features stolen NSA exploit

Equifax discovers they have been attacked. Financial data on 143M people stolen.

YAHOO! uncovers that earlier hack affected all 3 billion email addresses

Dun & Bradstreet database of 33.7M email addresses & contact info leaked

Anthem employee emails 18.5k medical records to his personal account

NotPetya launches destructive attack in Ukraine - age of cyberwarfare?

Etherium suffers heists of $7.4M and $32M weeks apart

Uber reveals breach of 57M customers and drivers personal info

What we would like to do :

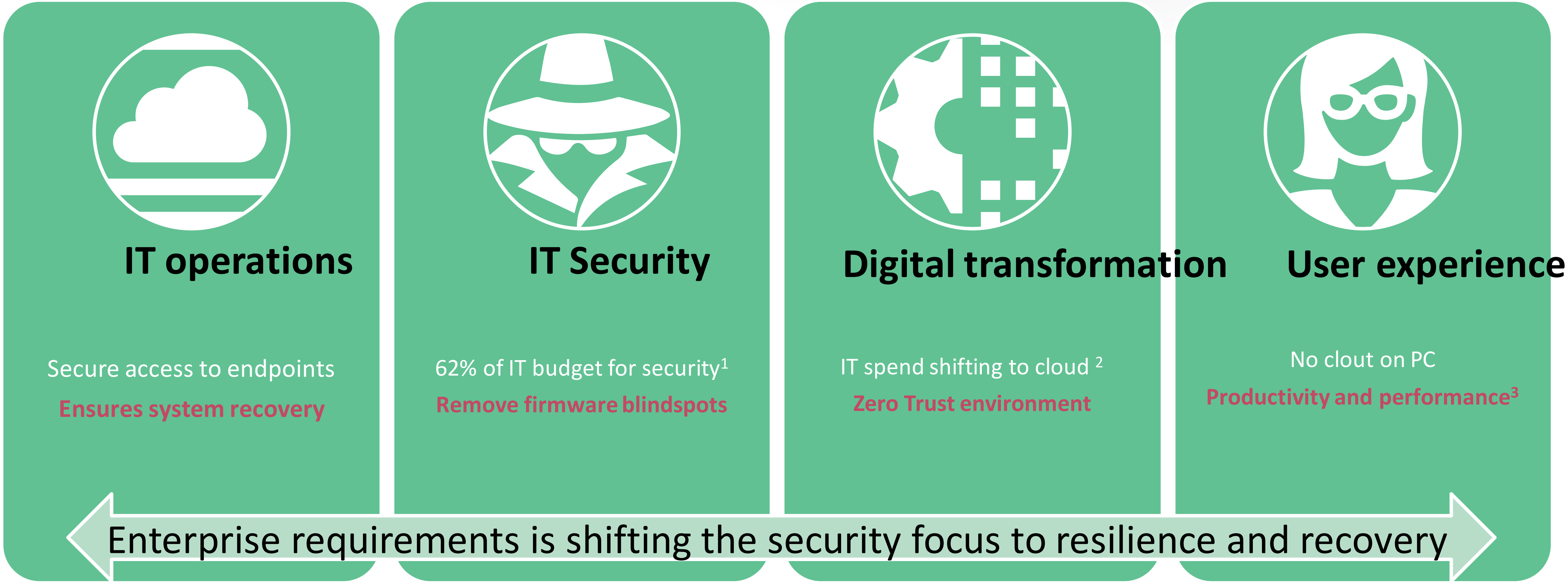
1. Get back to work immediately after a corruption, failure or an attack
2. Ensure our devices are ready and responsive when we need them
3. Have the ability to automatically install of urgent security updates

[1] https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

[2] GData, Malware Trends 2017

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

Enterprise requirements



IT operations

Secure access to endpoints

Ensures system recovery

IT Security

62% of IT budget for security[1]

Remove firmware blindspots

Digital transformation

IT spend shifting to cloud [2]

Zero Trust environment

User experience

No clout on PC

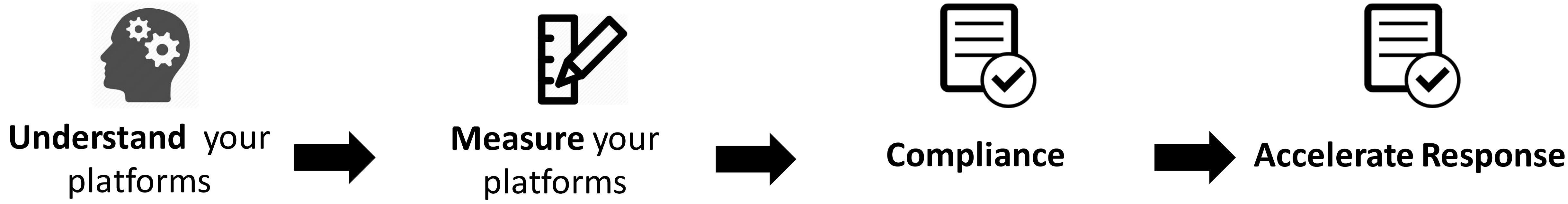
Productivity and performance[3]

Enterprise requirements is shifting the security focus to resilience and recovery

[1] CIO, "2019 CIO Tech Poll: Economic Outlook Research," June 2019
[2] Gartner, "Market Insight: Cloud Shift — 2018 to 2022." Sep 2018
[3] IDC "The Future of Productivity: How Today's Next-Gen PCs Empower Workers and Why Performance Still Matters." Tom Mainelli, April 2019

Firmware Resiliency Strategy and Challenges

Strategy :



Understand your platforms → **Measure** your platforms → **Compliance** → **Accelerate Response**

Challenges :

Limited Telemetry information

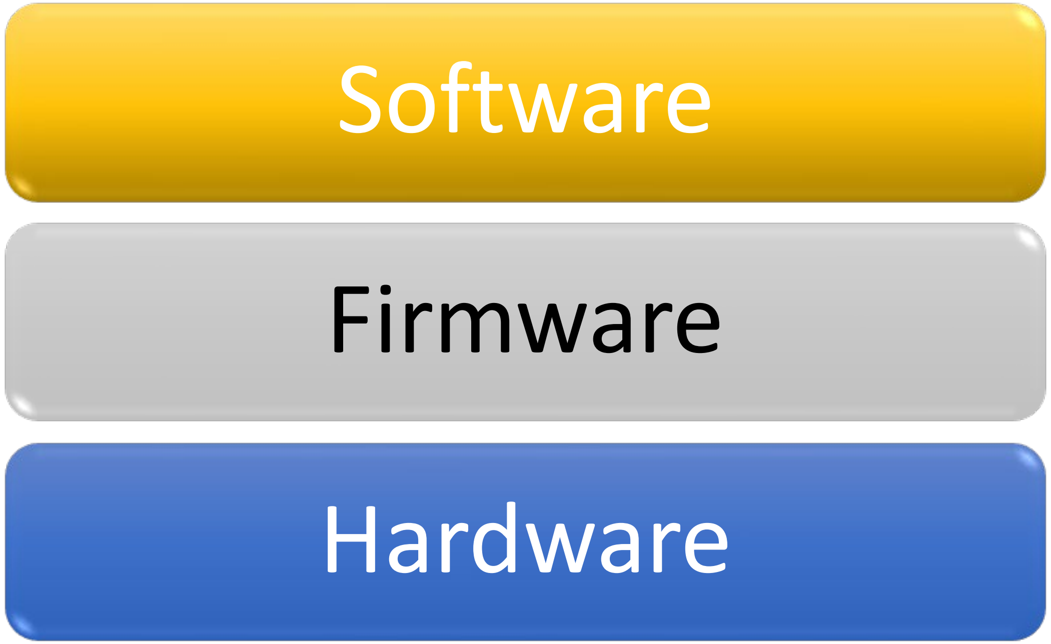
Lack of readiness of local and remote attestation

Limited compliant devices in ecosystem

Finite Hardware resources

Ecosystem and infrastructure readiness to deploy updates easily

Hardware based security foundation



Software

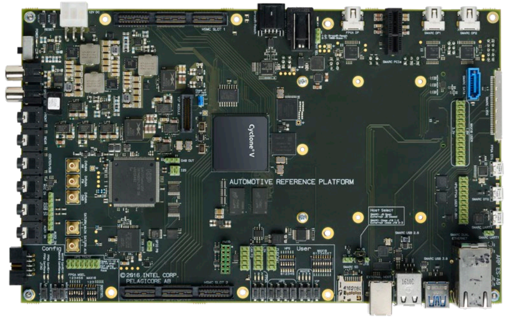
Creative and open by design
A more visible surface for tampering

Firmware

Talks to software, but hides things
Makes tampering more difficult

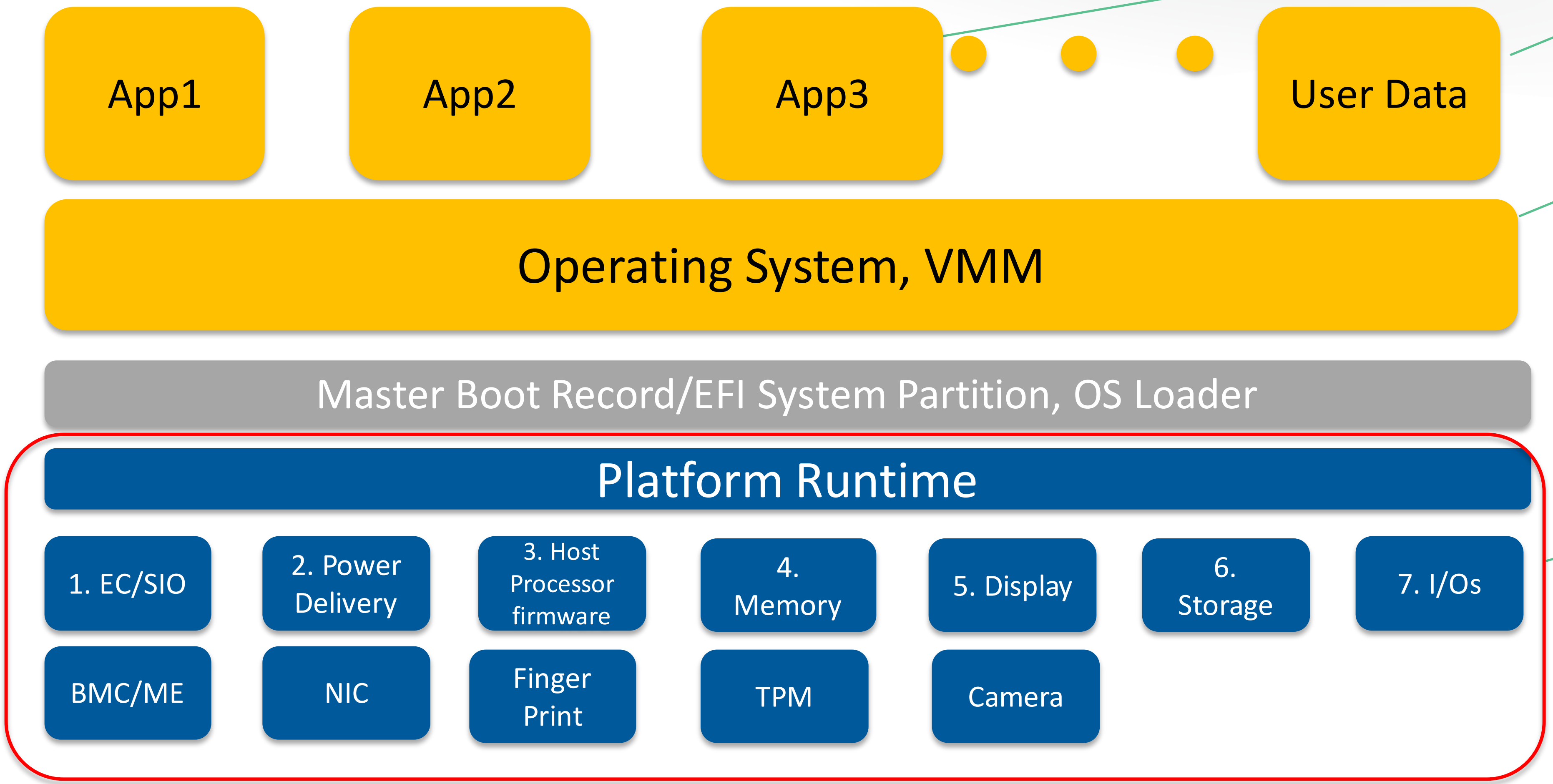
Hardware

Vaulted by design
Farther from sight and reach



Hardware and firmware resilience help build a secure foundation

Computer System Hierarchy



App1

App2

App3

User Data

Operating System, VMM

Master Boot Record/EFI System Partition, OS Loader

Platform Runtime

1. EC/SIO

2. Power Delivery

3. Host Processor firmware

4. Memory

5. Display

6. Storage

7. I/Os

BMC/ME

NIC

Finger Print

TPM

Camera

Reinstall on corruption

Reinstall on corruption

Requires special Recovery

EC – Embedded Controller
SIO – Serial I/O
BMC – Bus Management controller
TPM – Trusted Platform Module
ME – Manageability Engine
NIC – Network Interface Card

We focus our discussion on Firmware Resiliency

Key Principles of Firmware Resiliency (NIST SP800-193)

Protection

Ensure device remains in a state of integrity and is protected from corruption or attack

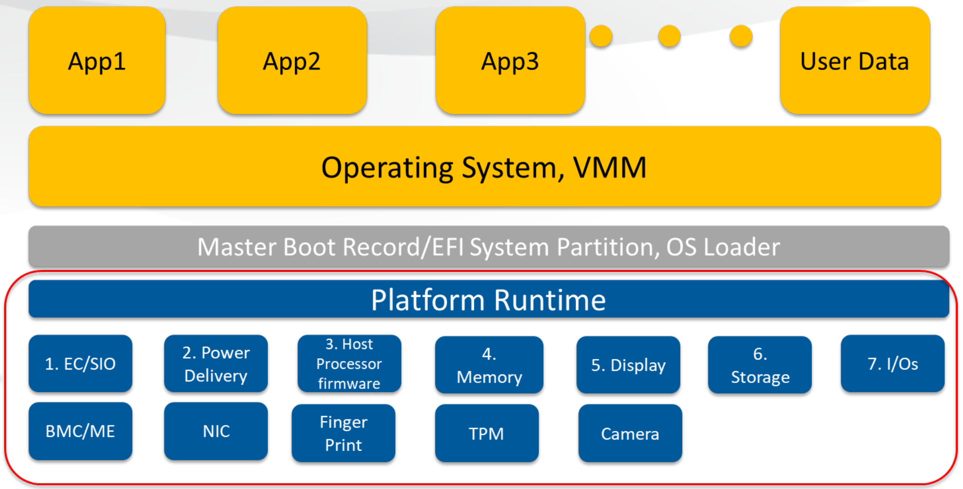
Detection

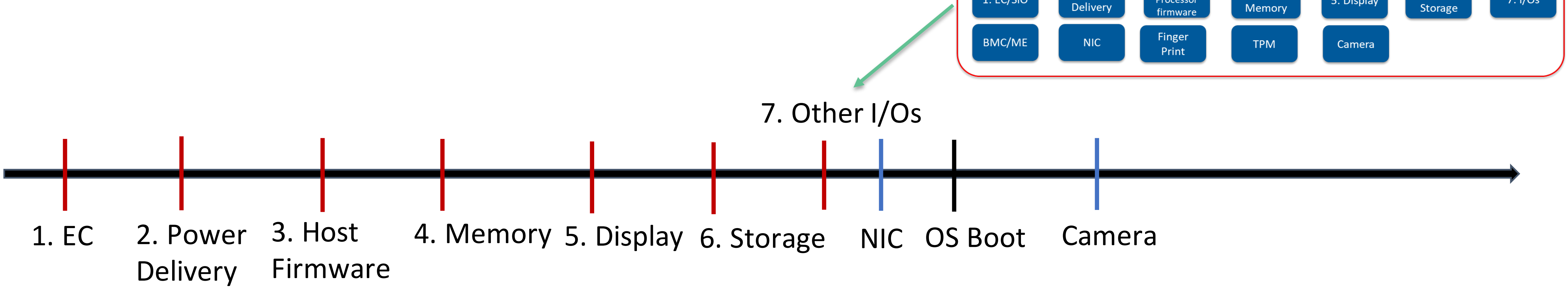
Detecting when device has been corrupted or attacked or otherwise changed from an authorized state

Recovery

Restore the device to a state of integrity in the event of attack, or when forced to recover

The mysterious few seconds during PC boot..



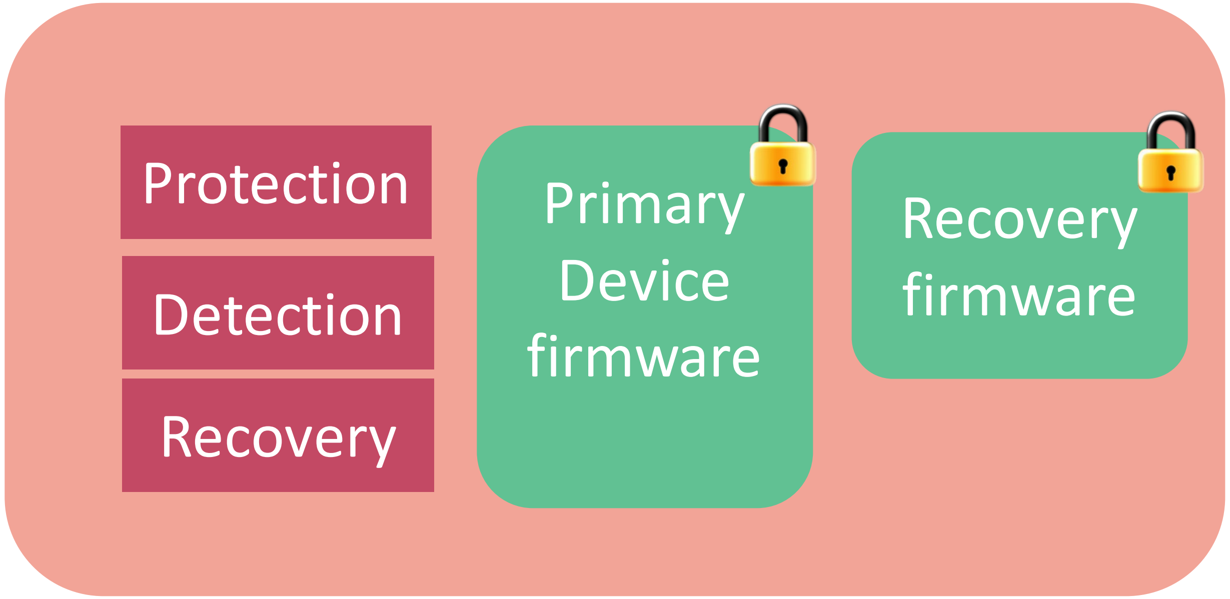


Note: Boot flow is for example only, IA architecture based

EC – Embedded Controller
NIC – Network Interface Card

Goal: Recover Boot Critical Devices first
Hand-off all other Recovery to OS based mechanisms

Key Ingredients in Device Firmware Resiliency



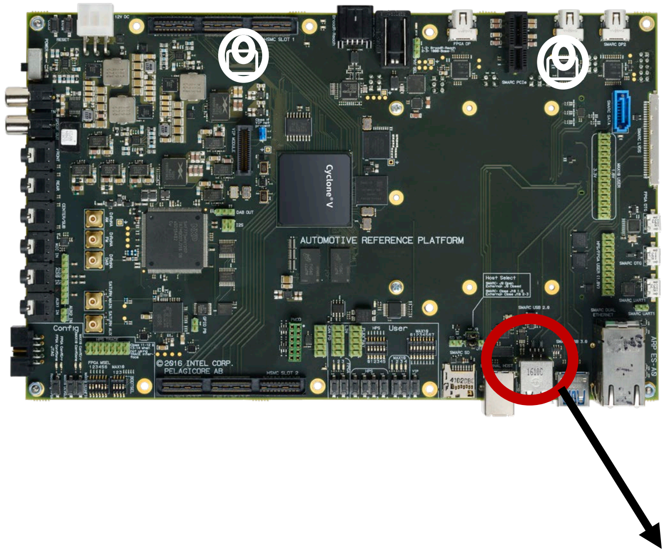
Protection

Detection

Recovery

Primary Device firmware

Recovery firmware



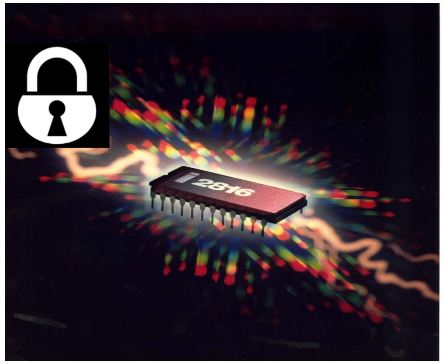
Host Processor firmware

Disclaimer: No product or component can be absolutely secure.

Active Players and Resources together build the Device Resiliency

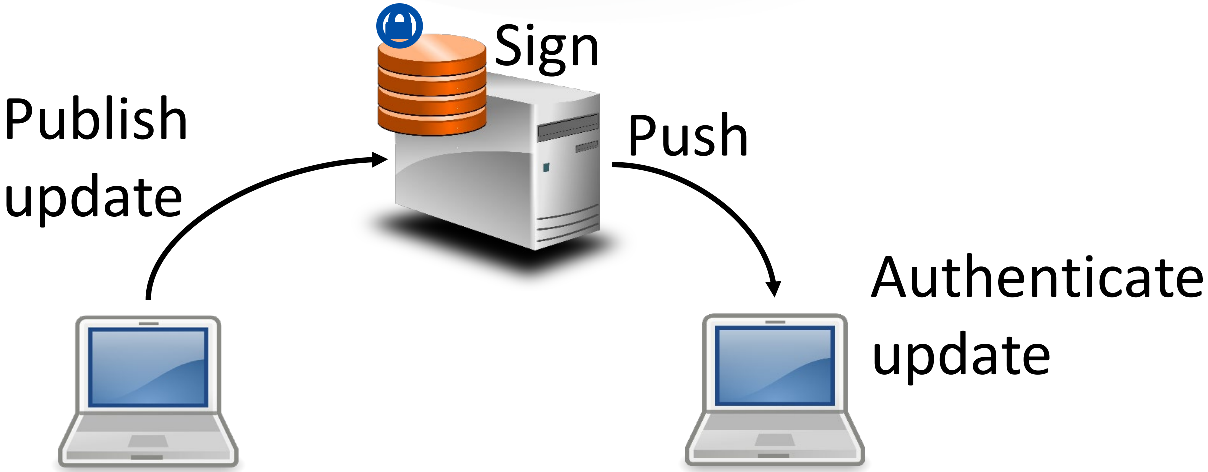
Protecting Device firmware

1. Read/Write Protection



- Physical Write Protect mechanisms
- Access controls defined at storage controller level

2. Update Protection



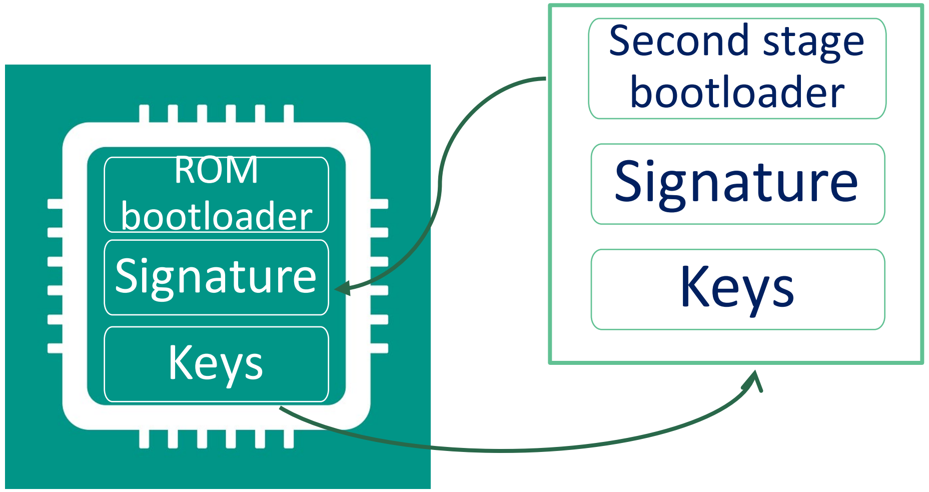
HW/SW vendor

- Signed updates hosted in Secure Server
- Local device authentication through key store in protected region

Disclaimer: No product or component can be absolutely secure.

Both Read\Write and Update Protection are necessary for Device firmware Protection

Detecting anomalies ahead



ROM bootloader

Signature

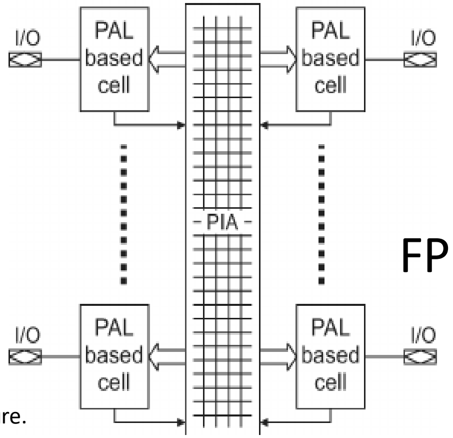
Keys

Second stage bootloader

Signature

Keys

1. Hardware rooted authentication mechanisms



FPGA/CPLD Bus monitoring

2. Hardware based Detection

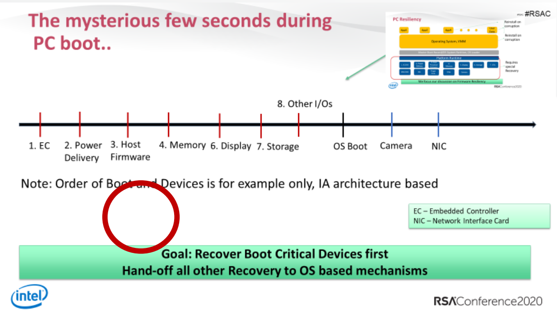
3. Watchdog Timer monitoring

- Trusted runtime monitoring
- Device and system level monitoring

FPGA – Field Programmable Gate Array
PAL – Programmable Array Logic
CPLD – Complex Programmable Logic Device

Disclaimer: No product or component can be absolutely secure.

Detection in System Boot flow context



The mysterious few seconds during PC boot..

8. Other I/Os

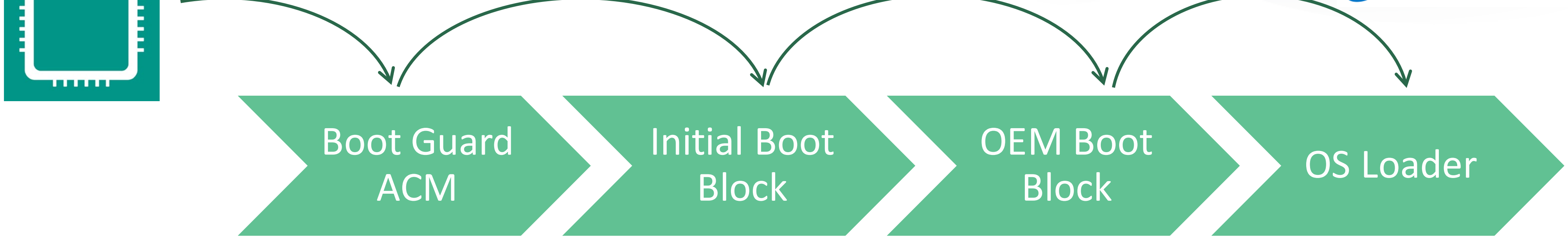
1. EC · 2. Power Delivery · 3. Host Firmware · 4. Memory · 6. Display · 7. Storage · OS Boot · Camera · NIC

Note: Order of Boot and Devices is for example only, IA architecture based

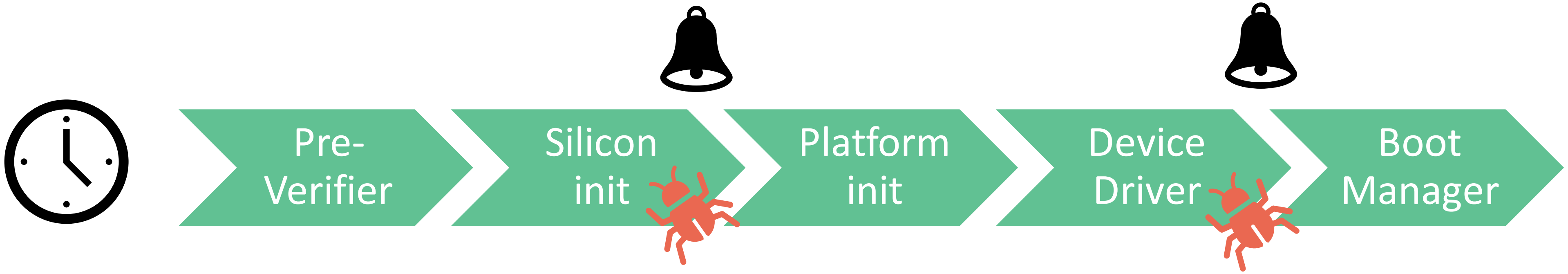
EC – Embedded Controller
NIC – Network Interface Card

Goal: Recover Boot Critical Devices first
Hand-off all other Recovery to OS based mechanisms

RSAConference2020



Detection at Boot time – UEFI Secure Boot



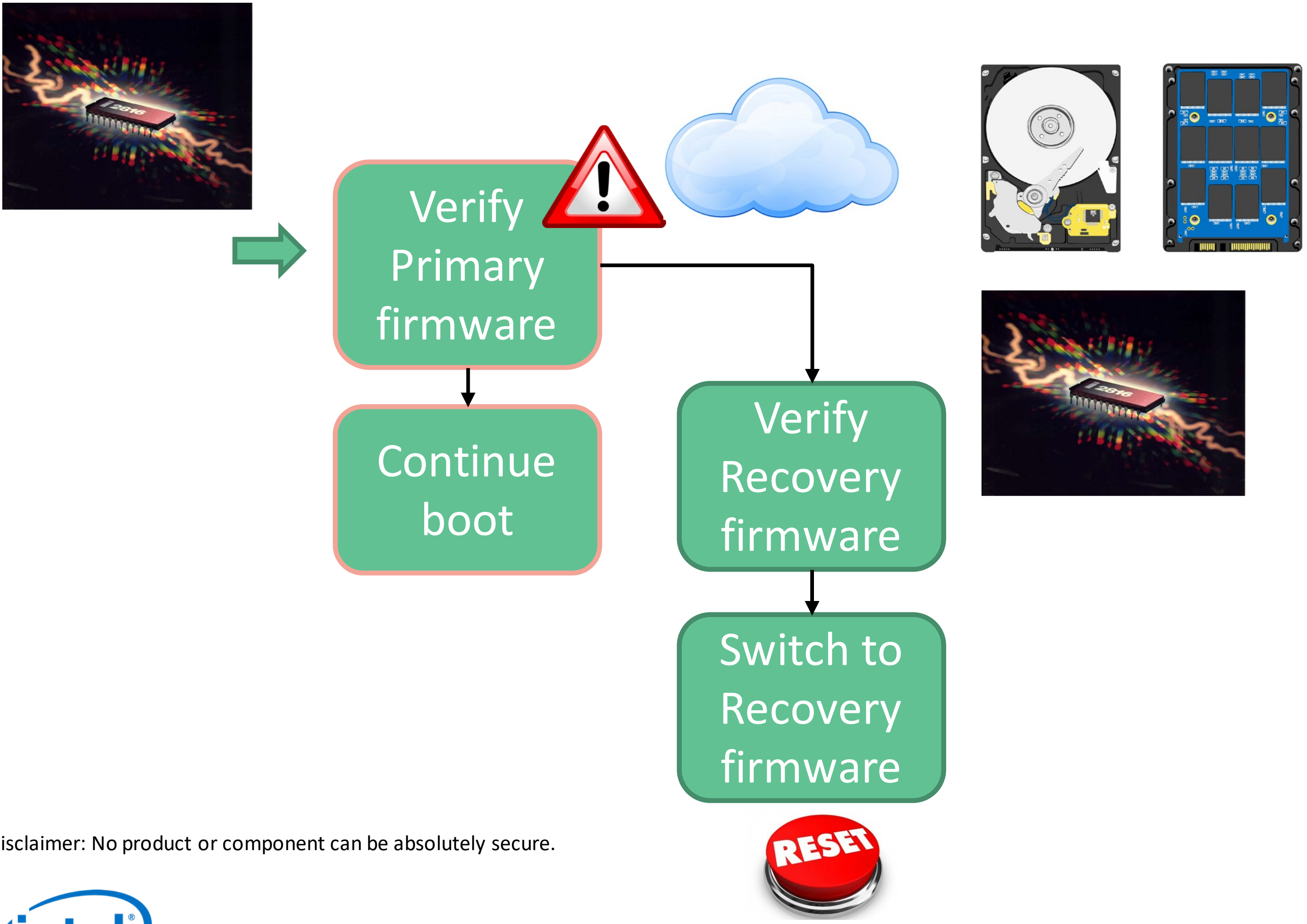
Detection at runtime

Disclaimer: No product or component can be absolutely secure.

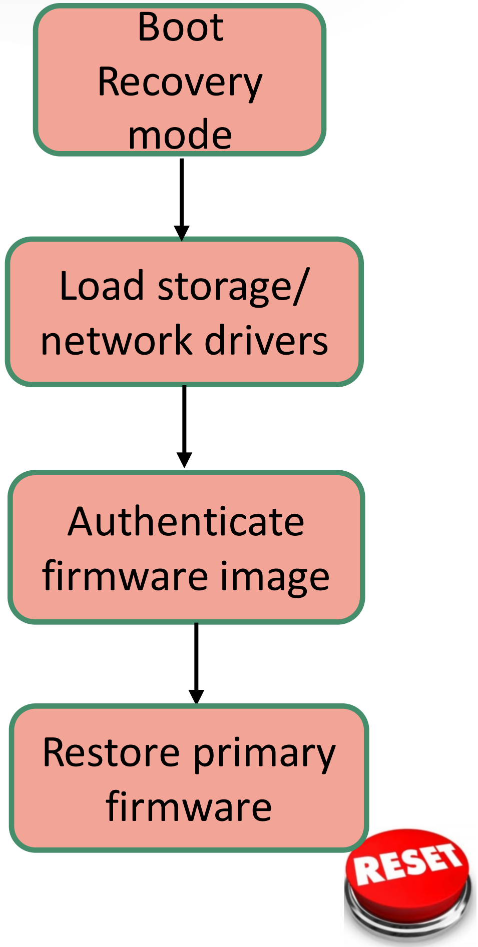
Both Boot time and Runtime Detection are essential for Resiliency

How to Recover

Stage 1: Primary Boot flow



Stage 2: Recovery flow



Disclaimer: No product or component can be absolutely secure.

Industry Standards

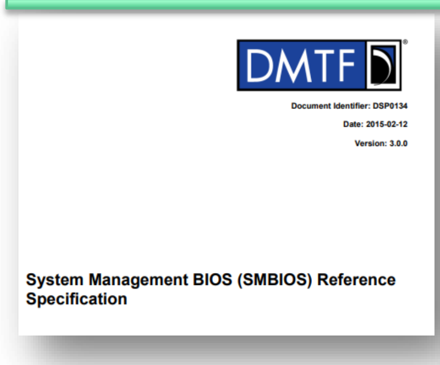
Understand your platforms → **Measure** your platforms → **Compliance** → **Accelerate Response**

- DMTF System Management BIOS (SMBIOS)

- NIST 800-155 “BIOS Integrity Measurement Guideline”

- NIST SP800-193 “Platform Firmware Resiliency Guidelines”

- NIST SP800-147 “BIOS Protection Guidelines”



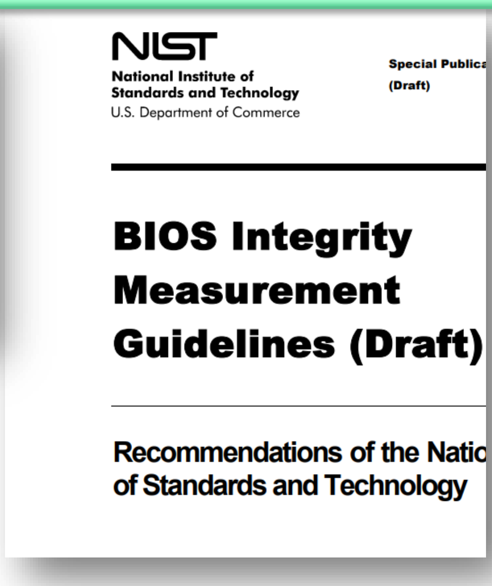
DMTF

Document Identifier: DSP0134

Date: 2015-02-12

Version: 3.0.0

System Management BIOS (SMBIOS) Reference Specification

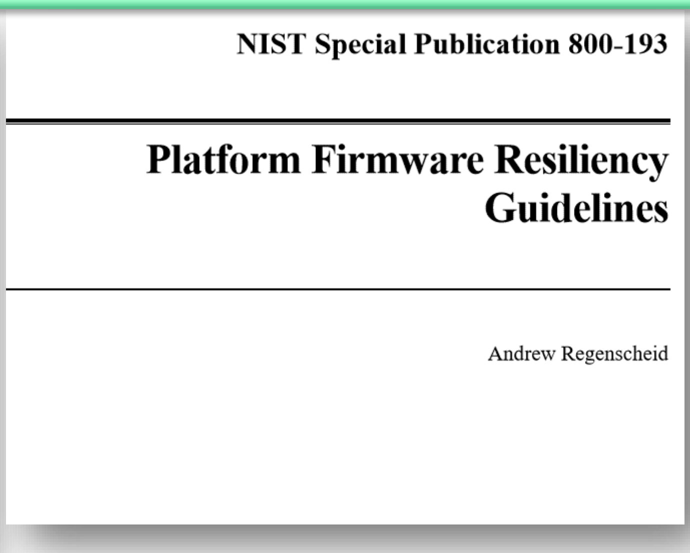


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publica
(Draft)

BIOS Integrity Measurement Guidelines (Draft)

Recommendations of the Natio
of Standards and Technology

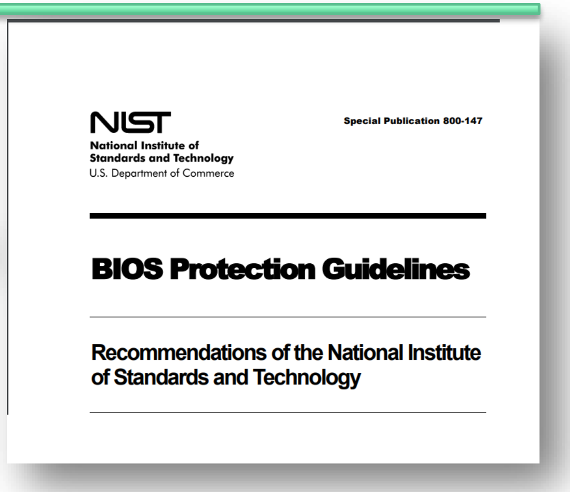


NIST Special Publication 800-193

Platform Firmware Resiliency Guidelines

Andrew Regenscheid

TRUSTED COMPUTING GROUP®



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-147

BIOS Protection Guidelines

Recommendations of the National Institute of Standards and Technology

Summary and Call to Action

- Device resiliency is important to prepare for future cyber attacks
- Understand which devices in your platform are resilient from failures and attacks and what are the gaps
- Take advantage of resilience features to create your own innovative cyber risk management solutions
- Stand out from the crowd by applying robust protect, detect and recover techniques to build a good Resiliency solution

References

- DMTF System Management BIOS : https://www.dmtf.org/standards/smbios
- NIST Specifications: https://www.nist.gov/

Legal Disclaimer

- Intel technologies may require enabled hardware, software or service activation.
- No product or component can be absolutely secure.
- Intel does not control or audit third -party data. You should consult other sources to evaluate accuracy.
- © Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.