Cyber Resiliency in Platforms and Systems

NIST SP 800-193, Platform Resiliency Guidelines

Andrew Regenscheid

Computer Security Division, NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

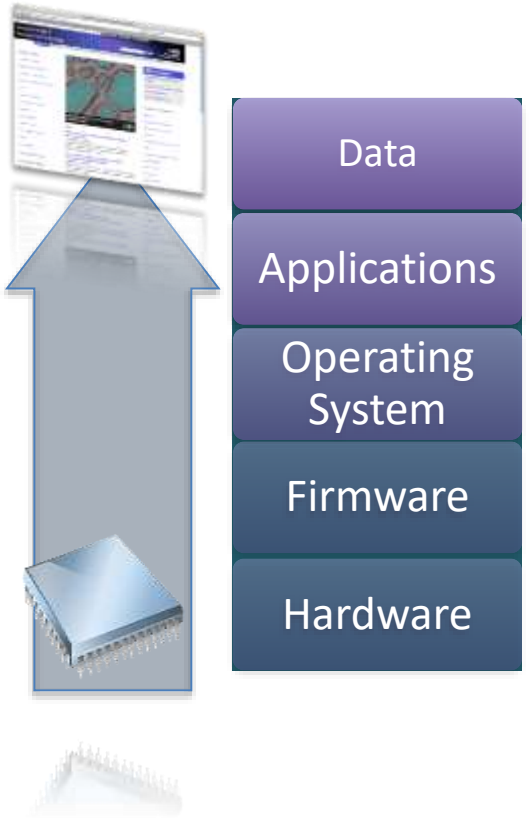
Rising Threat of Destructive Malware

- **Increases in global destructive malware attacks**
  - "Shamoon" attack against Saudi Aramco - 2012
  - Attack against South Korean banks and broadcasting companies - 2013
  - Sony Picture Entertainment Attack - 2014
  - Attack against Saudi Arabia's critical infrastructure - 2016
- **Malware complexity and destructive impact is increasing**
  - PDOS – Permanent Denial of Service
  - Attacks on the platform serious enough that the platform can not be recovered or requires a return to the factory to be restored
  - Increasingly sophisticated methods to destroy data
- **Leading to longer times to restore the enterprise after an attack**
  - In some cases, recovery is measured in weeks, not hours or days

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

Providing a Foundation for Recovery

- **Ensure platform firmware is resilient to attacks**
  - Firmware and configuration data are security-critical components
  - Must remain available and trustworthy in face of attacks
    - ***Protect*** firmware and critical data from unauthorized changes
    - ***Detect*** and ***Recover*** from problems
- **Provide secure and scalable means to recover OS, applications, and user/enterprise data**
  - These mechanisms must themselves be resilient to tampering/corruption by destructive malware
  - Built upon trust in the platform firmware recovery support

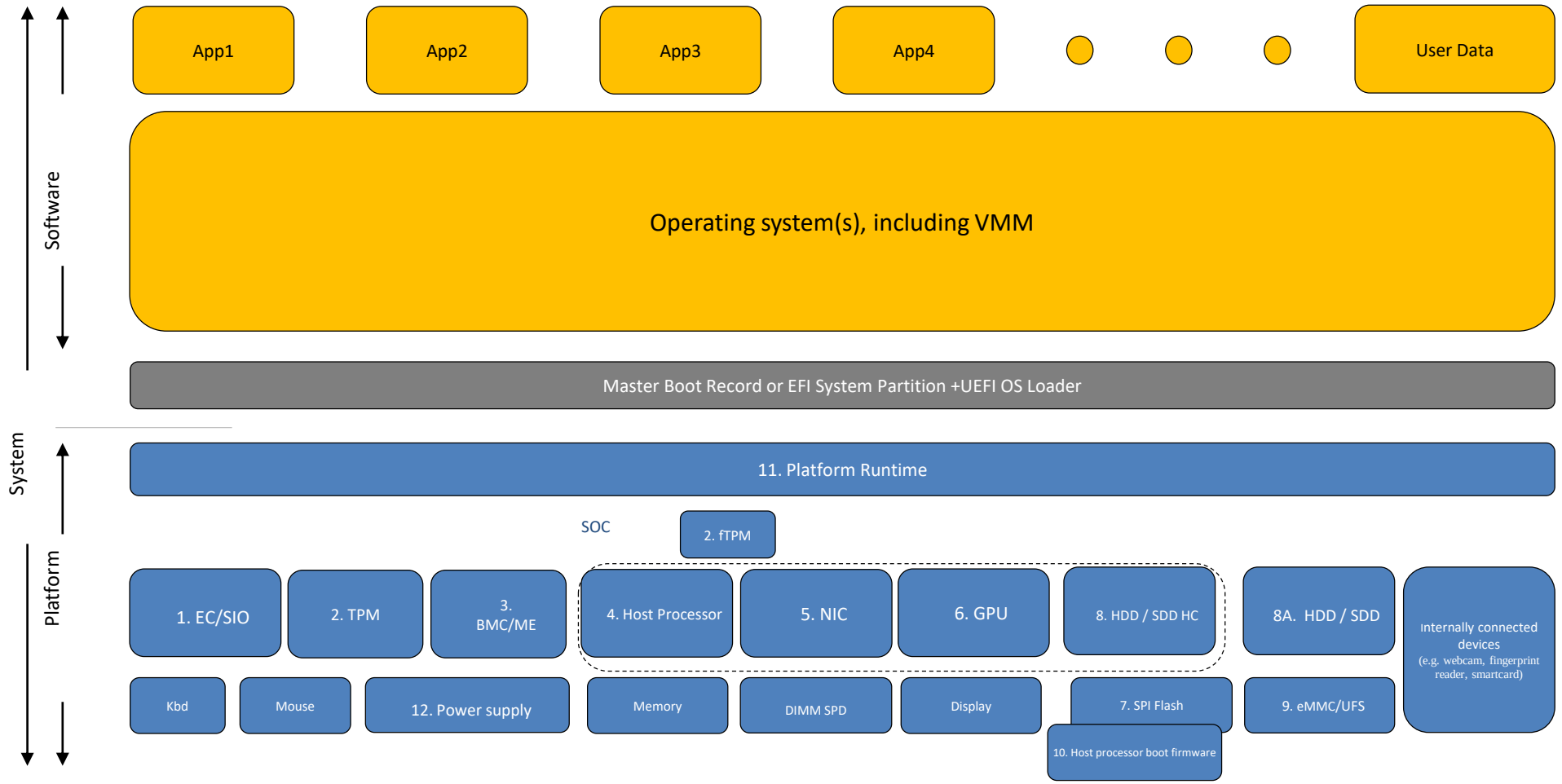


NIST National Institute of Standards and Technology U.S. Department of Commerce

Platform Resiliency

NIST SP 800-193, Platform Firmware Resiliency Guidelines

Architecture

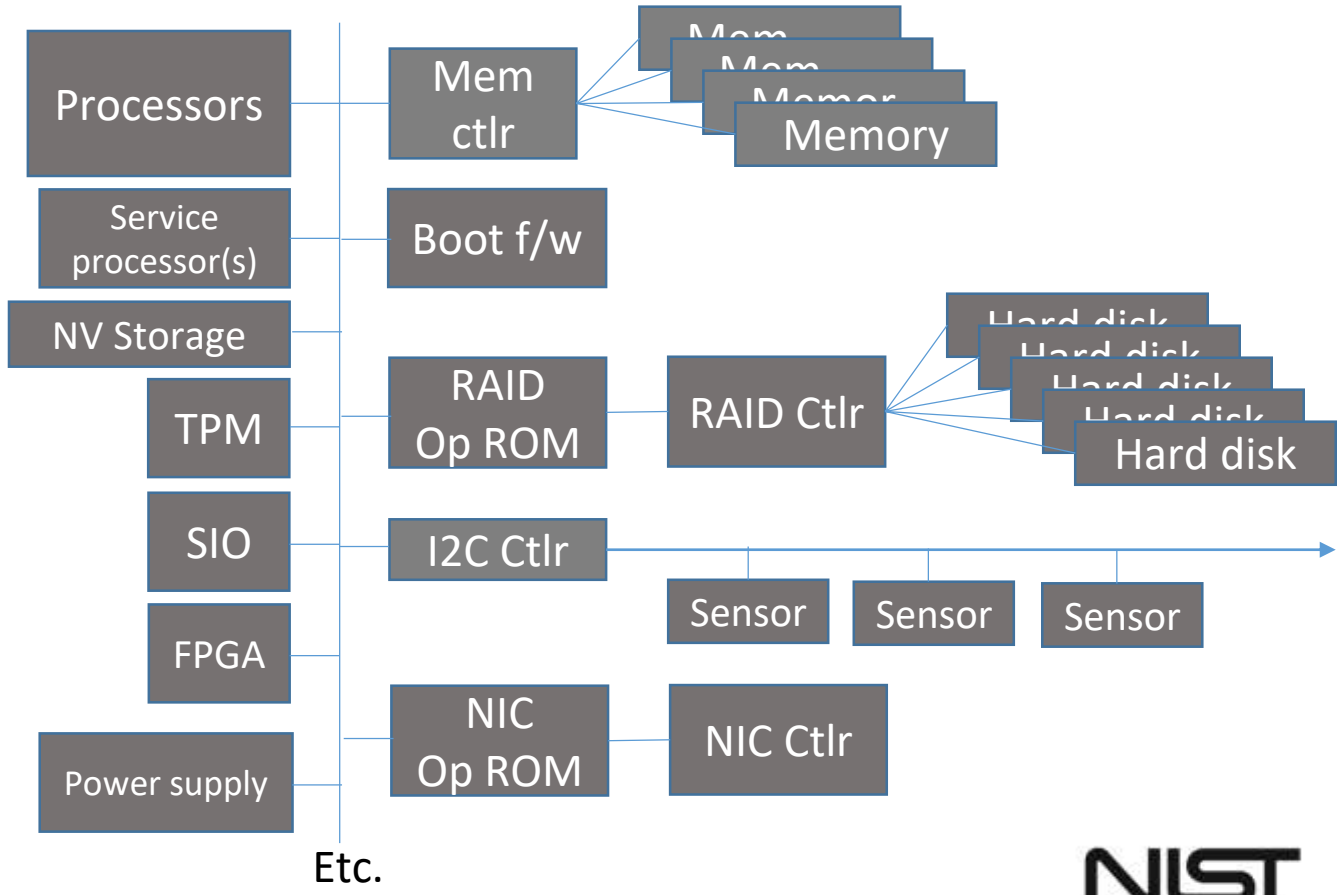


NIST National Institute of Standards and Technology U.S. Department of Commerce

Platform Firmware

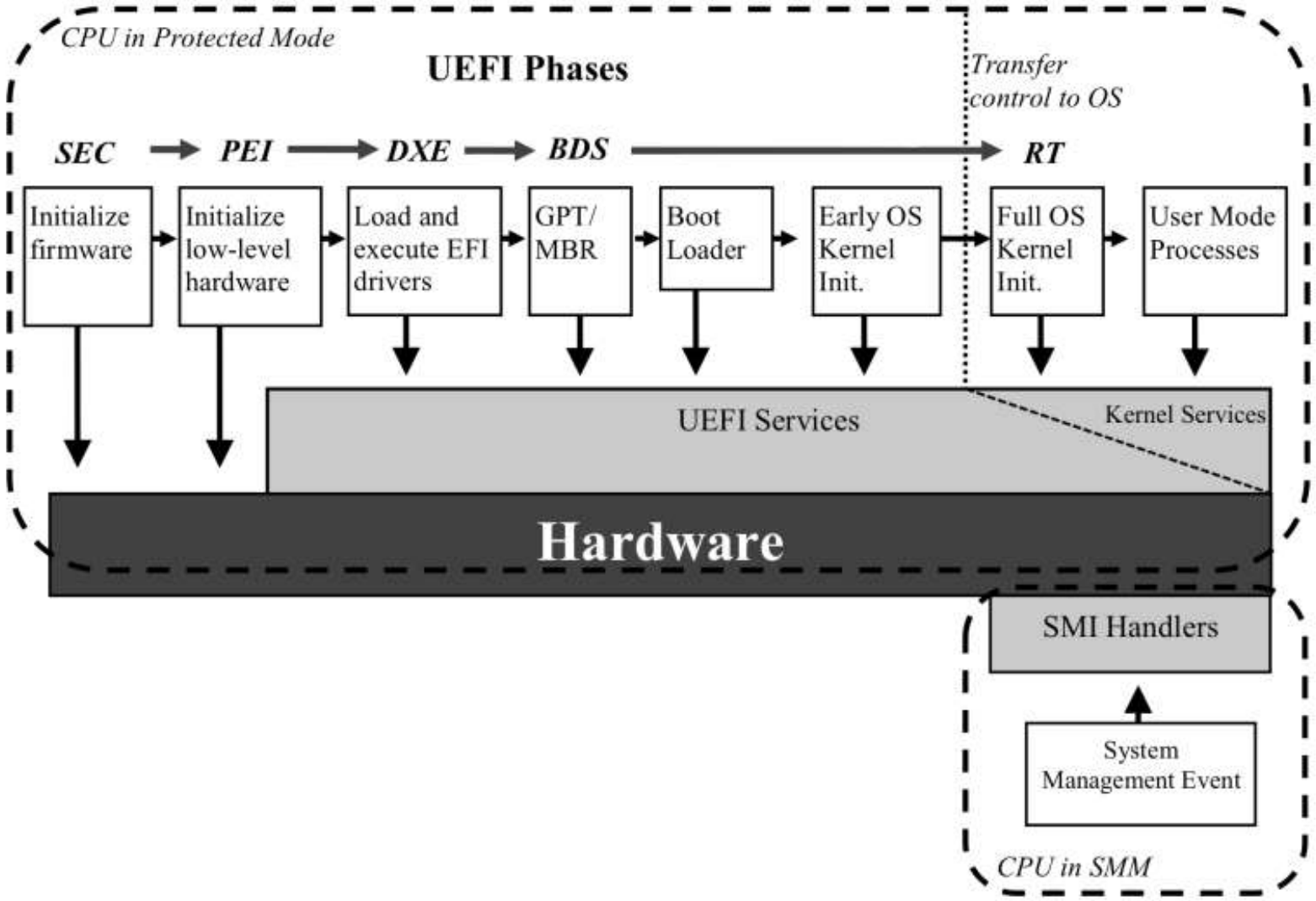
To be resilient against destructive attacks, firmware and critical data must:

- be ***protected***,
- corruption must be ***detected***, and,
- in the event of corruption, ***recovered*** to a functional state.



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

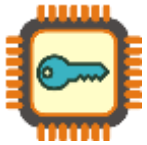
Boot Firmware- BIOS/UEFI



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

Previous Work: BIOS Protections

- **NIST SP 800-147, *BIOS Protection Guidelines***
  - Released: April 2011
  - Standardized in ISO/IEC 19678:2015
- ***Scope:***
  - Provides requirements and guidance to vendors for preventing the unauthorized modification of ***BIOS firmware*** on PC client systems


Authenticated updates


Flash protection


Non-bypassability

  - Provides system administrators guidance for managing the BIOS in an operational environment
- BIOS protections now a standard feature in PCs and servers

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

Platform Firmware Resiliency

- **Draft NIST SP 800-193, *Platform Firmware Resiliency Guidelines***
- ***Scope:***
  - ***Firmware*:** mutable firmware for host, devices, and non-host processors *internal* to a computer system
  - ***Critical Data*:** mutable data which persists across power cycles and must be in a valid state for booting/recovery to proceed
- Intended to address a variety of computer systems, including:
  - Clients
  - Servers
  - Network devices
- Concepts broadly applicable to other classes, e.g., IoT, mobile, etc.

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

Platform Security Principles

- **Protection**
  - *Firmware* updates are authenticated using digital signatures
  - *Critical data* only updated through authorized channels and checked for validity
  - Backed by a *Root of Trust for Update (RTU)*

- **Detection**
  - Verify integrity of *firmware* during boot
  - Validate *critical data* via inspection before use (where possible), or detect signs of boot failures (e.g., watch dog timers)
  - Backed by *Root of Trust for Detection (RTD)*

- **Recovery**
  - Capability to restore code/data when invoked through automated or manual means
  - Firmware recovery images verified through digital signatures (like an update)
  - Capability to backup known-good copies of critical data
  - Backed by *Root of Trust for Recovery (RTRec)*

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

Platform Resiliency - Next Steps

- Draft NIST SP 800-193 released May 2017
  - *Available at*: https://csrc.nist.gov
  - *Send to*: sp800-193comments@nist.gov
- Encourage adoption by USG and its suppliers
- Boot/Recovery-critical devices are initial priorities
  - Boot firmware
  - Other system/motherboard firmware
  - Service Processors/BMCs
  - Network Interface Cards
  - Storage Controllers
  - Storage Devices
  - TPMs

Draft NIST Special Publication 800-193

Platform Firmware Resiliency Guidelines

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

May 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

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

OS & Software Recovery

Upcoming in NIST SP 800-194, *Guidelines for Recoverable Systems*

OS, Software, and Data Recovery

- ***Goal:*** to securely and quickly recover systems after destructive attacks
  - Operating System
  - Enterprise configuration
  - Applications
  - User and enterprise data
- Addresses recovering software, settings, and data above the platform firmware layer
  - Works best when the hardware platform implements resiliency guidelines
  - Requires some additional hardware support to launch software recovery mechanisms when triggered
- Recovery mechanisms must be resilient to destructive attacks

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

Recoverable Systems

"… new capabilities that provide robust, easy-to-use and easy-to-manage recovery of the operating systems, applications, and user-data of computer platforms that have been damaged by malware or misconfiguration."

Recovery-Enabled Platform

+

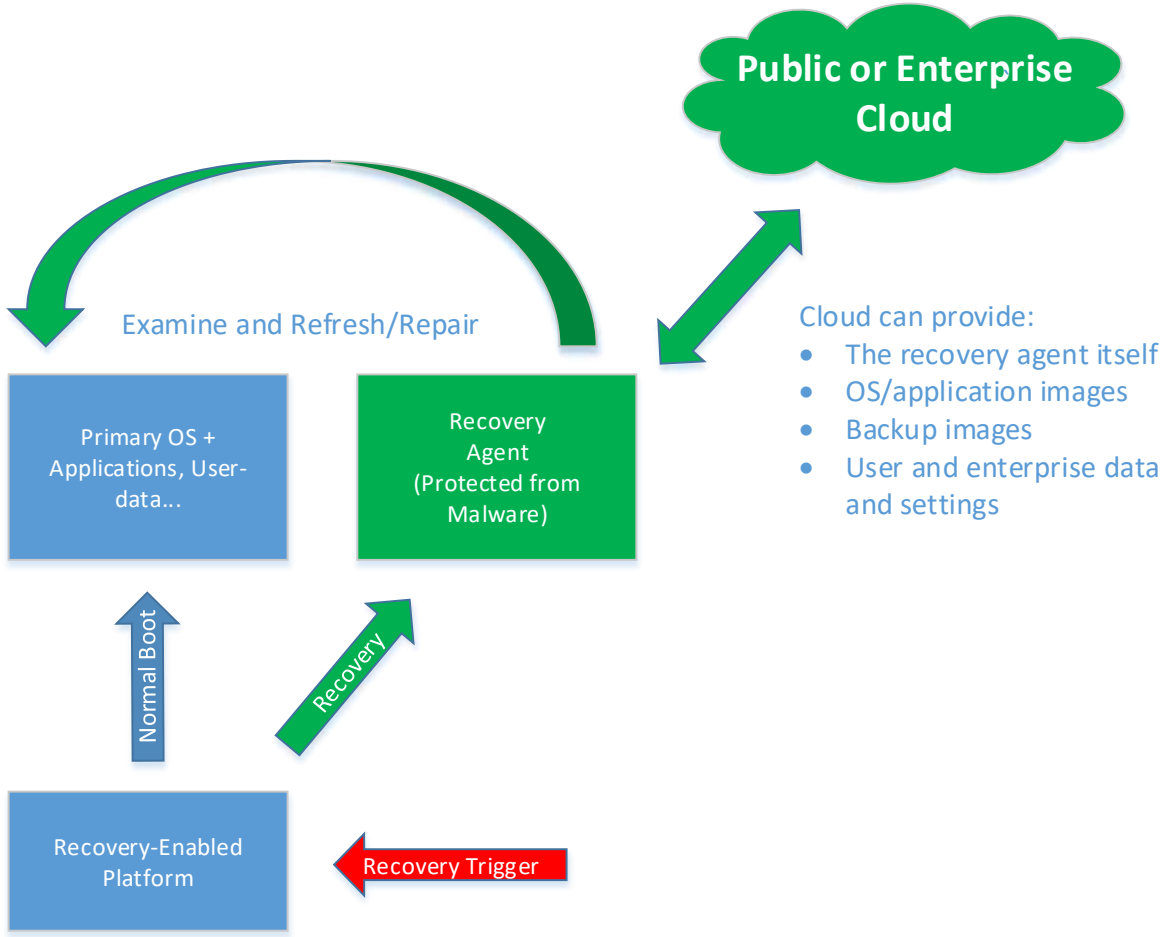
Recovery Agent

=

Recoverable System

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

Notional Recovery Architecture



- **Recovery Agents can perform a variety of servicing actions:**
  - Repair
  - Restore from backup
  - Fresh install + configure
- **The Recovery Agent is dormant until it is needed (via a *Recovery Trigger*)**
- **The Recovery Agent is protected from OS-level malware by the Recovery-Enabled Platform**
  - A malware-protected place on the platform
  - A public or private network service
- **Various triggers can initiate recovery**
  - User, administrator, or auto-triggered
- **The Recovery Agent does all necessary repairs and restarts the repaired OS**

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

Software Recovery - Next Steps

- Draft guidelines will be released in upcoming draft NIST SP 800-194, *Guidelines for Recoverable Systems*
- Outreach to standards organizations and industry groups
  - Trusted Computing Group, UEFI Forum
  - New features added to UEFI specifications to support recovery

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

Questions?

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov

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