Microsoft Surface

Microsoft Surface Security

Chip to Cloud Modern Protection from Microsoft

Surface is secured chip-to-cloud

Secure from chip-level to cloud management
- Silicon, firmware, OS, and cloud service each play a role

Defense in depth

Layering of independent defensive sub-components

chip

- UEFI w/TPM 2.0
- SEMM
- Secure Boot
- BitLocker
- MDM UEFI Management
- Windows Hello

to cloud

- Advanced Windows Security Features
- Conditional Access
- Windows Update for Business
- Microsoft Defender ATP
- Intune Wipe and Retire

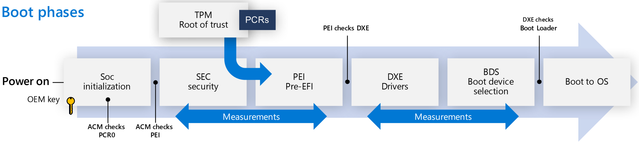
Securing boot

Security standard to boot only a trusted OS

Trust chain
- Root of Trust anchored in HW
- Each stage checks the next
- Boot Guard, Secure Boot

Security components
- SoC security processor—vendor and OEM keys
- TPM 2.0—security processor
  - Crypto engine
  - Keys
  - Measurements
  - VMK (BitLocker)

Boot phases

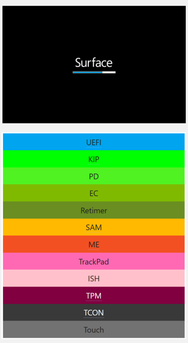


Surface firmware

Firmware are built by Surface
- Surface builds UEFI/controllers/sensors/SoC firmware
- Surface UEFI based from Windows' UEFI Project Mu open source
- Mitigation against supply chain attacks

A-B update mechanism
- Guard against corrupted updates

FW is kept current via Windows Update
- Windows signed drivers wrap Capsule Updates
- Surface signed capsule update
- UEFI applies FW update payload
- Color progress bar indicates which FW is updating



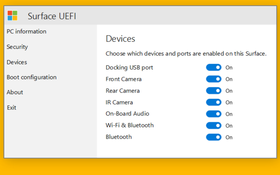
Surface Enterprise Management Mode

UEFI software tool for volume deployments

Secure and manage UEFI firmware configuration

Standalone tool or integration with SCCM

Manage individual components, boot order and advanced settings
- Disable and lock devices (no drilling!)
- Lock out UEFI front pages



DFCI/Cloud UEFI Management

Capabilities of SEMM through Intune/MDM

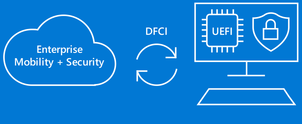
Cloud-scale remote firmware management with zero-touch device provisioning

Eliminates BIOS passwords, provides control of security settings including boot options and built-in peripherals

Lays the groundwork for advanced security scenarios in the future

BRK2362 – Ignite Online
Managing Surface UEFI BIOS settings with Microsoft Intune

Implemented first on Surface



For more information on Microsoft Surface, contact us today.