TECHNICAL REFERENCE

2017 Intel® vPro™ Platform Specification: DESKTOP

Fully-Realized Platform Inclusive of Requirements and Recommendations

PROCESSORS & CHIPSETS

7th Gen Intel® Core™ i5 and i7 vPro™ Processors

7700 7700T | 7600 7600T | 7500 7500T

Intel® Peripheral Control Hub

Q270

PLATFORM SECURITY FEATURES

- Intel® Software Guard Extensions (Intel® SGX)
- Intel® Identity Protection Technology with public key infrastructure (Intel® IPT-PKI)
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Virtualization Technology for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x)
- USB Provisioning Disabled in BIOS

INTEL® THUNDERBOLT™ 3 TECHNOLOGY

40 Gbps I/O USB-Type C

INTEL® SIPP

Intel® Stable Image Platform Program

TRUSTED PLATFORM MODULE (TPM)

Cryptographic processor

INTEL® DATA GUARD

Hardware-hardened file protection

INTEL® OPTANE™ MEMORY

HDD acceleration

INTEL® MANAGEMENT ENGINE WITH 6MB CORPORATE FIRMWARE IMAGE

Intel® ME Software Kit

INTEL® ACTIVE MANAGEMENT TECHNOLOGY (INTEL® AMT) 11.6

INTEL® AMT FEATURES

- In/Out of Band Remote Control w/KVM
- Hardware Assets
- Power Control
- Boot to BIOS
- IDE Redirection
- USB Redirection
- Event Manager
- Serial over LAN
- Alarm Clock
- Network Settings
- Audit Log
- Access Control List
- Environment Detection
- Access Monitor
- Time Sync
- System Defense
- Agent Presence
- Discovery
- Certificate Mgnt

INTEL® AUTHENTICATE SOLUTION

Hardware-hardened multi-factor authentication

INTEL® SSD PRO 6000P SERIES

Intel® Remote Secure Erase

INTEL® AMT INTERFACES

- Intel® Ethernet Controller: I219LM
- Intel® Wireless AC (Wi-Fi and Bluetooth* wireless technology) with Intel® PROSet Wireless Software

INTEL® SETUP AND CONFIGURATION SOFTWARE (INTEL® SCS)

DISCOVER | ACTIVATE | CONFIGURE

INTEL® MANAGEABILITY COMMANDER

Stand-alone or pluggable console

CONTROL