**Security & Reliability**

* Intel® AES New InstructionsYes
* Secure KeyYes
* Intel® Software Guard Extensions (Intel® SGX)Yes with Intel® ME
* Intel® Memory Protection Extensions (Intel® MPX)Yes
* Intel® OS GuardYes
* Intel® Trusted Execution Technology ‡No
* Execute Disable Bit ‡Yes
* Intel® Boot GuardYes

Intel® AES New Instructions (Intel® AES-NI) are a set of instructions that enable fast and secure data encryption and decryption. AES-NI are valuable for a wide range of cryptographic applications, for example: applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption.

Intel® Secure Key consists of a digital random number generator that creates truly random numbers to strengthen encryption algorithms.

Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications’ sensitive routines and data. Intel® SGX provides developers a way to partition their code and data into CPU hardened trusted execution environments (TEE’s).

Intel® Memory Protection Extensions (Intel® MPX) provides a set of hardware features that can be used by software in conjunction with compiler changes to check that memory references intended at compile time do not become unsafe at runtime due to buffer overflow or underflow.

Intel® Trusted Execution Technology for safer computing is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. It enables an environment where applications can run within their own space, protected from all other software on the system.

Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious-code attacks and prevent harmful software from executing and propagating on the server or network.

Intel® Device Protection Technology with Boot Guard helps protect the system’s pre-OS environment from viruses and malicious software attacks.