Built-In, More Secure Foundation

Advanced security built on the Intel vPro® platform

intel®

Key messages

- Every Intel product is architected with security in mind
- The Intel vPro® platform provides enhanced hardware-level security
- Intel vPro® security meets key IT priorities: protect, detect and recover

Customer benefits

Protect data

- Better security capabilities built directly into the silicon
- 100+ new system integrations per year from top manufacturers
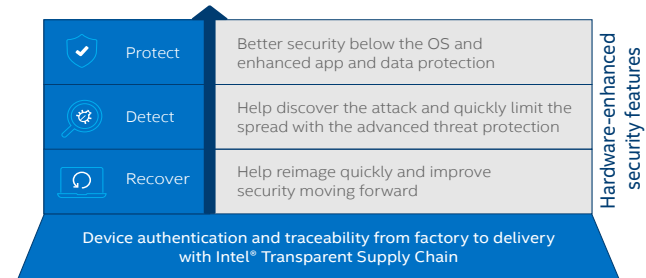- Improve data protection with discrete Trusted Platform Module cryptography

Recover a device using remote management (Intel® AMT)

- Secure device waking and access to restore, upgrade and protect
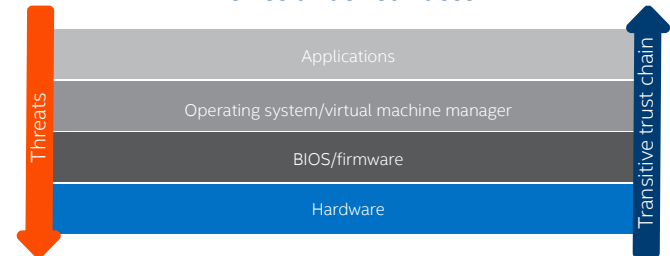- Quickly and remotely recover data and devices

Detect and prevent threats

- Improve threat detection via memory scanning with virtually no additional impact on user experience or system performance
- Built-in firmware attack protection
- Better PC component tracing with Intel® Transparent Supply Chain
- Ensure that operating systems are running on legitimate hardware

A built-in more secure foundation

		Hardware-enhanced security features
✓ Protect	Better security below the OS and enhanced app and data protection	
⊘ Detect	Help discover the attack and quickly limit the spread with the advanced threat protection	
↻ Recover	Help reimage quickly and improve security moving forward	

Device authentication and traceability from factory to delivery with Intel® Transparent Supply Chain

Device attack surfaces

Threats

Applications
Operating system/virtual machine manager
BIOS/firmware
Hardware

Transitive trust chain

Security must be rooted in hardware to offer a better end-to-end defense

Built-In, More Secure Foundation

Advanced security built on the Intel vPro® platform

intel®

Proactive PC protection with the Intel vPro® platform with Intel® Hardware Shield

HOW IS THE SECURITY LANDSCAPE SHIFTING?

ATTACKS ON THE RISE	INCREASING REGULATION	INCREASED SPENDING
90% of INCIDENTS Result from exploits in software[1]	General Data Protection Regulation	WORLDWIDE SECURITY SPENDING[3]
EVERY 4.2 SECONDS New malware in the first quarter of 2017[2]	PCI Security Standards Council	2017: ~$102 BILLION **2018: ~$114 BILLION**
COST OF A BREACH Digital records stolen, brand damage, etc	FISMA COMPLIANCE	**2019: ~$124 BILLION**
62% IT EXECS INCREASING BUDGET ON SECURITY[4]	NIST	**15% CAGR**

Intel® Hardware Shield Below the OS security: BIOS & Boot flow protection

Intel® Hardware Shield

Helps prevent malicious software injection by locking down memory and critical system resources

Helps dynamically ensure OS and virtual environment are running directly on Intel® Hardware

OS visibility into how BIOS is using hardware protection

intel vPro® PLATFORM

The Intel vPro platform provides a hardware foundation for an end-to-end security strategy

Intel Silicon-Enabled Security

Intel® Hardware Security

For more information please contact your Intel Sales Representative

Technology Essentials Notices & Disclaimers

Built-In More Secure Foundation

[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 2019

Notices & Disclaimers

No computer system, product or component can provide absolute security under all conditions.
Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services and/or an Internet connection.
Results may vary depending upon configuration.
Consult your PC manufacturer for more details.

© 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.