1 Hannah Mitchell, “Data breaches have lasting effects on hospitals, report suggests,” Becker’s Health IT, beckershospitalreview.com, February 2021

2 “Five questions to evaluate and improve your firmware security posture,” Eclypsium Assessing Enterprise Firmware Security Risk blog, eclypsium.com, January 2020

3 The Ponemon Institute, Cost of a Data Breach Report 2020, sponsored and published by IBM Security, capita.com


Software-level security
Deep integration and alignment with the silicon and firmware protect the vulnerable software layer from viruses and malware.

Silicon-level security
CPU security features ensure root-of-trust boot-up to keep malicious code out of the BIOS. The Intel® Evo™ vPro® platform is built for what IT needs and users want.

Healthcare has the highest industry average cost per data breach at $7.13 million.3

More than 90% of healthcare organizations suffered at least one cybersecurity breach in the previous three years, according to the U.S. Healthcare Cybersecurity Market 2020 report.1

Lock devices with layered security and protect patient privacy

Integrated, unified security supports the workforce of the future. You need a comprehensive solution that defends devices below, in, and above the operating system.

Silicon-level security

CPU security features ensure root-of-trust boot-up to keep malicious code out of the BIOS. The Intel® Evo™ vPro® platform is built for what IT needs and users want.

Firmware- and OEM-level security
Block malicious attacks with features that detect threats, prevent intrusion, and even autonomously repair devices.

Firmware attacks have increased since 2016.2

750%

Firmware attacks increased by 750% in 2020 compared to 2019.2

Software-level security

Harden against known vulnerabilities and prevent attacks.

Shadow stack technology
SentinelOne AI-powered endpoint protection

Absolute endpoint management

Firmware and OEM-level security

Integrated, unified security supports the workforce of the future. You need a comprehensive solution that defends devices below, in, and above the operating system.

Firmware attacks have increased since 2016.2

Microsoft Secured-core PC integration

Intel® Transparent Supply Chain

Intel® AI threat detection

Intel® Active Management Technology

Microsoft Secured-core PC

Intel® Hardware Shield on the Intel vPro® platform

Device as a Service (DaaS)

Deploy devices that are always up to date and protected by the latest security features. Choose Lenovo DaaS for modular, scalable, end-to-end lifecycle support.

40% of ITDMs in large organizations are extremely interested in moving to a DaaS model.4

End-to-end management and support

Faster device refresh

Best-in-class hardware

Flexible package design and financing

Microsoft Secured-core PC integration

Intel® Transparent Supply Chain

Intel® AI threat detection

Intel® Active Management Technology

Microsoft Secured-core PC

Intel® Hardware Shield on the Intel vPro® platform