HOW DOES ONE INNOCENT EMPLOYEE MISTAKE BRING DOWN A WHOLE COMPANY?

ThinkShield

Sometimes employees make mistakes—losing devices, clicking on things they shouldn't, or even disabling protections that get in their way. Lenovo ThinkShield helps to prevent and contain human error before it turns into a devastating breach—without getting in the way of productivity.

For IT admins seeking more visibility into endpoints, as well as solutions that are less cumbersome for end-users, ThinkShield's portfolio includes:

- Persistent endpoint visibility by Absolute
- Business data protection with BitLocker[3] data and device encryption
- Advanced boot and run time protection with Windows Defender System Guard[4]
- Intel® Authenticate Solution
- Lenovo Wi-Fi Security

LEADING BIOS SECURITY

With Intel® Hardware Shield

With the power of the Intel® vPro™ platform, Lenovo ThinkShield provides BIOS that can self-heal in the event of corruption by human error or attack. And unlike other PC manufacturers, we did not build in a backdoor, so BIOS can be administered securely. If you're skeptical, you can arrange a look through the 2,000,000+ lines of code in our secure BIOS Reading Room.[5] We'll even let you create a unique signature for the BIOS you reviewed.

In 2015, one click from an employee at Anthem **EXPOSED THE PERSONAL DATA OF 78 MILLION PEOPLE**, costing the company an estimated

$100+ million.[1]

48%

of breaches originate from **HUMAN ERROR.**[2]

ThinkShield is Lenovo's portfolio of secure Think devices, software, and services—fully customizable to keep your business ahead of dangerous breaches. Get the most comprehensive protection with a modern Windows 10 Pro device powered by the Intel® vPro™ platform.

intel vPro™ Platform

Windows 10

Windows 10 Pro means business.

Learn more at **www.lenovo.com/ThinkShield**.

1 Fortune: "Anthem's Historic 2015 Health Record Breach Was Likely Ordered by a Foreign Government." http://fortune.com/2017/01/09/anthem-cyber-attack-foreign-government/
2 Kaspersky: "Small Business IT Security Practical Guide." https://go.kaspersky.com/rs/802-IJN-240/images/Small_Business_Practical_Guide.pdf?alild=466030355
3 Requires TPM 1.2 or greater for TPM-based key protection
4 Windows Defender System Guard's boot time integrity protection requires the use of UEFI 2.3.1 or greater with Secure Boot. The optional remote integrity validation capability using the Windows Defender System Guard cloud service requires TPM 1.2 or greater and a management system that supports remote attestation capabilities (e.g.: Intune and System Center Configuration Manager).
5 BIOS Reading Room service is available for additional charge

Smarter technology for all

Lenovo