ThinkShield

MISSED PATCHES LEAD TO BIG BREACHES

Amidst a never-ending stream of new vulnerabilities and subsequent patches, it's easy to see why most IT departments are playing catch up instead of staying ahead. ThinkShield features a customizable selection of automated solutions for finding and delivering critical patches efficiently so that IT can remain agile in other areas.

Win 10 Pro & Intel® Active Management Technology

Both platforms provide automated features for keeping critical OS, hardware, and firmware always up to date.

Absolute

Offers a fully automated system that monitors endpoints on- and off-network. Persistence technology ensures the patching agent activates when the device comes back on-network.

Lenovo Patch for SCCM

A plug-in for SCCM that broadens the kinds of updates it can deliver, allowing critical patches to be instantly delivered organization-wide.

Update Retriever & Thin Installer

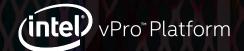
Brings automation and intelligence to retrieving and installing OS & device-specific patches—simplifying the patching of diverse hardware environments.

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.

of breached businesses say their hack was due to a known, unpatched vulnerability.1

EQUIFAX HACK

customers had their data exposed because a known vulnerability was not patched.²





Windows 10 Pro means business.

Learn more at www.lenovo.com/ThinkShield

Ponemon Institute State of Vulnerability Response https://www.servicenow.com/content/dam/servicenow-a Wired: The Equifas Breach Was Entirely Preventable https://www.wired.com/story/equifax-breach-no-excuse/ enow-assets/public/en-us/doc-type/resource