
Lenovo
Modern IT
End-to-end security for a work from anywhere era. That's smarter.
From the factory floor straight to your employees' hands, Intel® **Trusted Device Setup**, Intel® **Transparent Supply Chain**, and **Conditional Access** keep devices and data safe and secure.
intel vPRO PLATFORM BUILT FOR BUSINESS
Smarter technology for all
Lenovo

New security solutions to meet new security problems

More companies than ever are embracing hybrid work environments. But as the technology to serve those working from anywhere grows more sophisticated, so do the techniques to exploit it. For PCs, an oft-overlooked vulnerability occurs in the supply chain. This window—after devices leave the manufacturer and before they reach the end-user creates an opening for malicious actors.

2x as many

cyber intrusions happened in the first quarter of this year compared to all of last year.[1]

3 in 4 CFOs

plan to shift some employees to remote work permanently.[2]

Without the right protection, criminals can seize this moment to remove or replace components—resulting in anything from malfunctioning devices to compromised systems through unauthorized operating system access. Lenovo ThinkShield keeps you protected in this evolving threat landscape, securing your critical data and business technologies with comprehensive, end-to-end protection. Now, three services keep your devices even safer:

Intel® Trusted Device Setup

For devices with the Intel® Core™ vPro® platform, **Trusted Device Setup** seals software at the point of manufacturing, protecting it until first boot and securing your tech from the get-go.

Intel® Transparent Supply Chain

Intel® **Transparent Supply Chain** brings Lenovo security into the transport and delivery cycle with a documented, auditable supply chain security program.

Conditional Access

Conditional Access is Microsoft technology that leverages **Transparent Supply Chain** and **Trusted Device Setup** services to automatically identify and prevent untrusted devices from accessing corporate resources.

Trusted Device Setup, **Transparent Supply Chain**, and **Conditional Access** protect devices and sensitive data...

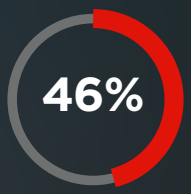
from the point of manufacture... **and during transport...** **until they're on-site with the end user**

Lenovo

Comprehensive protection with ThinkShield

Trusted Device Setup, **Transparent Supply Chain**, and **Conditional Access** form just three components of the end-to-end protection offered by Lenovo ThinkShield. This holistic approach to security has four primary focus areas:

- **Device Protection:** Includes Trusted Device Setup, Transparent Supply Chain, and Conditional Access
- **Built-in Platform Security:** Includes self-healing BIOS and Trusted Supplier Program
- **Security Management:** Includes integrated system management solutions for deploying, monitoring, and reporting for IT assets
- **Threat and Data Protection:** Includes endpoint protection with capabilities like ransomware rollback and integration with Microsoft Defender



of global businesses have encountered at least one cybersecurity scare since shifting to a remote working model in the first quarter of this year.[3]

Trusted Device Setup: The tip of the spear

Today, it's more common for employees to work from anywhere—which means that organizations increasingly run the risk of devices getting compromised between leaving the factory floor and reaching the end user.

With IT needing to configure devices and send them to employees, new vectors of attack (everything from physical theft to implanting malicious software) have opened, ultimately putting your company's data at risk.

Trusted Device Setup seals software preload at the point of manufacture, enabling companies to ship boot-ready devices directly to employees—completely secure and ready to use. Preload verification helps protect against ever-evolving security threats and minimizes the risk of tampering before devices are in end users' hands, while certificate-based comparison ensures the integrity of the OS.

year-over-year increase in supply chain attacks.[4]

Transparent Supply Chain: End-to-end device protection

Transparent Supply Chain expands the Lenovo security footprint to detect any hardware or firmware changes made between the factory and the customer. It secures devices from manufacturing, through transport and setup, until in use by your employees.

Documented, auditable supply chain security program

Allows you and Lenovo to trace all purchases at the component and system level

Web portal

Enables you to access the platform certificate and auto-verification, confirming the device is the same one shipped from the factory

Trusted supplier guarantee

All suppliers must adhere to Lenovo's strict manufacturing standards and pass regular compliance and security assessments

Statement of conformance

An added layer of security that guarantees the authenticity of the system

Unlock the benefits of the Intel® vPro® platform

While all Lenovo business PCs come equipped with 10th Gen Intel® processors, users can get additional benefits by upgrading to the 10th Gen Intel® vPro® platform:

- Enable Trusted Device Setup
- Secure the BIOS against malware attacks and get advanced threat protection features with Intel® Hardware Shield
- Empower IT to control BIOS, firmware, and driver versions and upgrades thanks to Intel® Stable Image Platform

intel vPRO PLATFORM BUILT FOR BUSINESS

Trusted Device Setup is only available on Lenovo Think devices on the 10th Gen and above Intel® vPro® platform.

Lenovo

Conditional Access: Prevent unauthorized devices from accessing sensitive data

Conditional Access is Microsoft technology that automatically identifies and prevents untrusted devices from accessing corporate resources. Feature benefits:

- Automates security verification
- Helps IT securely and effectively deploy devices
- Allows IT to create a Custom Compliance Policy
- Automatically flags non-compliant devices and notifies an admin

With Trusted Device Setup, Transparent Supply Chain, and Conditional Access, businesses can:

- Ensure device protection through transport and delivery
- Minimize the risk of tampering throughout the supply chain
- Reduce the chance of receiving counterfeit electronic parts
- Help keep data secure by identifying and isolating unauthorized devices

Smarter ensures security from manufacture to first boot.

Talk to your Lenovo representative to see how **Trusted Device Setup**, **Transparent Supply Chain**, **Conditional Access**, and **ThinkShield solutions** can protect your sensitive data.

ThinkShield

Smarter technology for all

Lenovo

1. EU Agency for Cybersecurity 2. Gartner 3. Barracuda 4. Symantec.