



Intel® Tiber™ Transparent Supply Chain

End-to-End Visibility and Transparency for Your Technology Supply Chain

Intel® Tiber™ Transparent Supply Chain is designed to provide provenance data and traceability of hardware components, firmware, and systems

With the expansion of data centers, intelligent edge devices, and cloud computing, ensuring trust in the supply chain has become more important than ever. To mitigate these risks, [60% of supply chain management](#) leaders plan to prioritize cybersecurity risks in business decisions by 2025.¹

That's where Intel Tiber Transparent Supply Chain comes in, designed to enhance security from component sourcing to distributing the final product.

Device Security from the Factory Floor Through End of Life

Intel Tiber Transparent Supply Chain provides businesses with powerful tools to verify the authenticity and integrity of their hardware, ensuring system security from production through lifecycle. Starting in the manufacturing process, this service helps safeguard system components by detecting changes and preventing potential breaches, enabling companies to conduct business confidently.

Product Benefits

Provenance: A digitally signed statement of conformance for every platform attests to the authenticity of the platform as built during manufacturing.

Traceability: Platform certificates linked to the discrete Trusted Platform Module (TPM) provide system-level traceability.

Assurance: The Auto Verify utility compares the "snapshot" of the direct platform data taken during manufacturing with a "snapshot" of the platform components taken at the first boot to help detect tampering.

Accountability: Component-level traceability via Direct Platform Data File covers [Manufacturing Level 9 \(L9\)](#) integrated components including processor, storage, memory, and add-in cards.

Detect Potential Threats Before They Affect Your Network

Detecting changes and verifying system configuration helps mitigate the risk of counterfeit components and malicious hardware, tampering during transit, and even espionage or sabotage, adding a layer of protection to both the device and the company's network.

Intel Tiber Transparent Supply Chain allows you to detect and prevent unwanted system changes, verify platform certificate validity, and monitor firmware versions below the OS. This helps mitigate risks related to counterfeit components, tampering, supply chain transparency, and insider threats while helping ensure regulatory compliance.

Lenovo ThinkShield Build Assure

Lenovo ThinkShield Build Assure is built on Intel Tiber Transparent Supply Chain. Lenovo's collaboration with Intel extends from motherboard production through the factory floor to customer platforms, enabling customers to verify the authenticity of components, installed firmware, and system configuration.

When customers receive a device from Lenovo, Intel Tiber Transparent Supply Chain tools establish device integrity by matching what they received with the original order description. This automated process is designed to verify key components have not been tampered with during transit or deployment to end-users.

"ThinkShield Build Assure is the latest advancement in our collaboration with Intel to offer customers more options to meet rapidly evolving security goals as workforces continue to disperse and AI-enabled devices become common within the enterprise."

Nima Baiati, Executive Director & General Manager, Commercial Cybersecurity Solutions, Lenovo.

Manage Employee Devices and Reduce the Risk of Tampering

Administer and enhance security of your employees' devices with Intel Tiber Transparent Supply Chain tools. Improve device management by verifying and updating the current machine state and storing new system images signed by Intel. This helps reduce IT help desk calls and risk exposure.

Strengthen device tamper resistance and verify machine state integrity through attestation to help reduce risk exposure to vulnerabilities below the OS and prevent non-compliant systems from accessing your network.

Verify the Authenticity of Your Infrastructure

Owning the entire stack—including the network and infrastructure used to deliver services—offers the opportunity to provide unique solutions and gives control over the end-to-end experience and functionality. It also means you must demonstrate the integrity and security of your infrastructure to potential customers.

Intel Tiber Transparent Supply Chain is designed to provide verified evidence of hardware integrity to relying parties, verify the authenticity of infrastructure components, offer visibility into firmware updates and vulnerability patches below the OS, and strengthen compliance with security controls.

Support for Intel® Assured Supply Chain

The [Intel® Assured Supply Chain \(ASC\) program](#) is designed to provide additional transparency and assurance in the silicon manufacturing process. This specialized client system-on-chip (SoC) solution, initially offered on specific Intel® Core™ Ultra (Series 2) mobile and desktop SKUs, provides a digitally attestable chain of custody of each chip's progress through the chip manufacturing process, leveraging a dedicated chip manufacturing pathway through specific Intel manufacturing locations.

Intel Tiber Transparent Supply Chain helps customers take advantage of this transparent process by incorporating manufacturing data provided by Intel Assured Supply Chain into its overall platform measurement.

Learn more

For more information, please visit intel.com/tsc



[1- Gartner Says Cybersecurity Risk Set to Be a Primary Buying Consideration for Chief Supply Chain Officers](#)

Notices and disclaimers

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel® technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary.

© 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.