Technology | United States

Zero Trust: Validating the integrity of employee devices

Meta

Global tech giant Meta is working with Lenovo and Intel to validate the provenance, security, and authenticity of employee devices and also reduce the provisioning burden for Meta's IT teams. The core of this zero-trust approach is provided by Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain.

1 Customer background

Who is Meta?

Meta's mission is to build the future of human connection and the technology that makes it possible. When Facebook launched in 2004, it changed the way people connect. Today, Meta's products, including Facebook, Messenger, Instagram, Threads, and WhatsApp, empower more than three billion people around the world to connect, find communities, and grow businesses. Now, Meta is moving beyond 2D screens towards immersive experiences such as augmented, virtual, and mixed reality to help build the next evolution in social technology.

Meta

2 The challenge

Meta's Challenge

Billions of people around the world use Meta technologies to connect with their friends, families, and communities.

As part of its ongoing efforts to safeguard its technology environment from threats, the company sought to validate the integrity of Lenovo devices as part of Meta's enterprise fleet. This initiative was a critical part of Meta's broader commitment to innovation, security, and compliance in a rapidly evolving digital landscape.

2 The challenge

Meta has unique security challenges to ensure its production and development environments can only be accepted from genuine employee issued corporate devices.

“We operate a zero-trust architecture,” begins Venkatesh Gopal, Security Engineer at Meta. “We use lots of different authentication and authorization workflows for employee devices to maintain strict access controls.”

2 The challenge

As cyberattacks and supply chain risks increase, Meta needed a solution to ensure the integrity of the components powering its IT systems. Specific pain points included:

Trust and Transparency Issues: Difficulty verifying the authenticity and integrity of hardware components, increasing the risk of malicious actors tampering with or compromising computing devices.

Supply Chain Visibility Gaps: Limited visibility into the source of critical hardware components, which posed security and compliance risks.

Compliance with Industry Standards: The need to meet stringent industry standards for hardware supply chain security, especially in light of global data privacy and security regulations.

2 The challenge

For years, Meta had been using certificate-based authentication to identify employee devices before granting access to its network. Previously, the company issued disk certificates for its corporate fleet, but these were not backed by secure hardware chips and therefore potentially at risk of data exfiltration.

“Certificates were purely on the disk, which raised concerns about credential exfiltration and certificate key exfiltration,” says Venkatesh Gopal. “We’re always looking to increase the maturity of our verification workflows to improve overall security and reliability. So, we were eager to back up the certificates with hardware-based security measures such as Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain.”

> “Zero Trust is based on the principle **‘never trust, always verify.’** But how do we verify that the endpoint requesting access to our network is actually an employee laptop? How do we make sure that it’s not some other bogus device? That’s where **supply chain assurance** comes in.”

Ruben Recabarren Velarde

Security Engineer, Meta

3 The solution

Solution

Meta has teamed up with Lenovo and Intel to ensure the trust and transparency of its employee devices based on Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain.

Device Transparency: The sourcing and provenance of employee devices in the supply chain is the key foundation to establishing a Trusted Device. Lenovo ThinkShield Supply Chain Assurance provides Meta visibility into critical components that go into each employee device. In the Lenovo factories, devices built with Lenovo ThinkShield Supply Chain Assurance will capture the platform data file along with the component data file. The data is then signed and certified by Intel, generating an x509 platform certificate to ensure the device arrives in the same configuration and has not been tampered with.

Device Trust: Assurances of a device's origin help to establish the foundation for a trusted supply chain. Attesting to the device as being authentic has been one of the fundamental goals of trusted supply chain assurance. In order to perform this attestation, the device requires an immutable Root of Trust to provide that assurance.

3 The solution

Zero Trust, Zero Touch

Meta was looking for a solution based on Zero Trust to attest to the authenticity of its employee devices. The criteria for establishing this trust were based on the principle of “Zero Touch” where the device that is being enrolled onto a corporate network is provided with a certificate.

This is where Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain comes in, providing a “Zero Touch technology” solution based upon the Trusted Platform Module (TPM) and the platform certificates. Platform certificates are generated based upon the unique, immutable identity of the TPM, which is cryptographically bound to the device’s platform certificate.

The Results

To date, Meta has enabled TPM on several thousand Lenovo laptops, representing about 15% of its corporate fleet.

“Cryptographic attestation and platform certificates give us the metadata required to validate the hardware Root of Trust of those employee laptops,” says Ruben Recabarren Velarde, Security Engineer at Meta. “We validate all this metadata to make sure that any network access request originates from a certified Meta-owned device.”

- ✓ **Tamper-proof, hardware-based Root of Trust**
- ✓ **Immutable cryptographic authentication**
- ✓ **Trusted, transparent supply chain**

Venkatesh Gopal adds: “Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain brings us to a very advanced level of security. It allays our concerns around data exfiltration and negates a wide range of attacks that our security teams are typically worried about. The transparent supply chain significantly boosts our trust in the authenticity and integrity of our hardware.”

Faster, smoother verification

Today, employees with TPM-enabled laptops integrated with Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain can access internal applications, services, and websites without having to go through the usual multi-factor authentication workflows. All that Meta needs to verify is the device's platform certificate, which significantly speeds up provisioning.

"We have an SLA that new hires at Meta can set up their device and start working in just 15 minutes," says Ruben Recabarren Velarde. "With Lenovo ThinkShield Supply Chain Assurance, we expect to be able to shorten time-to-productivity."

Venkatesh Gopal notes: "By removing manual authentication and authorization workflows, TPM eliminates the risk of human error. This not only enables a very advanced level of security, but also makes for a smoother, easier experience for the end user."

> “Simplification is the key here. By rolling out Lenovo ThinkShield Supply Chain Assurance to more employee devices and moving away from traditional authentication and authorization workflows, we will **simplify and improve the efficiency of the entire process**.”

Ruben Recabarren Velarde

Security Engineer, Meta

Securing the supply chain against attack

Supply chain attacks can take many forms, but the most prevalent supply chain attack is to intercept and inject malware into the BIOS or firmware. Changes to the BIOS or firmware will leave a change that can be detected since the original BIOS and firmware information was captured by the Lenovo ThinkShield Supply Chain Assurance manufacturing process. BIOS and firmware changes that are designed to clone the original device will also be detected, since the TPM identity is tied to the platform certificate generated for each individual device.

Continued collaboration

For Meta, this collaboration with Lenovo and Intel marks the start of an exciting new chapter.

“Our ultimate goal is to make TPM verification the default for all employee devices,” says Venkatesh Gopal. “Right now, we’re only using TPM to validate the device’s identity, but platform certificates are very powerful and there’s potential to do much more, such as validating modifications to the hardware or firmware. For example, we could use the platform certificates to check that any modification to a device’s hard drive had been authorized by the user’s management and security teams.”

Why Lenovo and Intel?

As an early adopter of TPM technology, Meta looked to industry leaders Lenovo and Intel for advice, technical expertise, and implementation support.

“My main takeaway from this collaboration is how willing the Lenovo and Intel teams have been to help us make our vision a reality,” says Ruben Recabarren Velarde. “They have been so open and receptive to our feedback; it’s a true collaboration. I believe that this can only mean more and better success in the future.”

Learn more about Lenovo ThinkShield Supply Chain Assurance powered by Intel® Tiber™ Transparent Supply Chain

Lenovo ThinkShield Supply Chain Assurance powered by 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. To learn more about Lenovo ThinkShield, visit lenovo.com/thinkshield

Learn how by Intel® Tiber™ Transparent Supply Chain helps safeguard system components by detecting changes and preventing potential breaches, enabling companies to conduct business confidently. Learn more at intel.com/tsc