Lenovo
ThinkShield

Advancing enterprise security grounded in Zero Trust Architecture

Lenovo | intel

Executive summary

The security perimeter is no longer a single location. It is a dynamic set of signals spanning device health, firmware integrity, user behaviour, access patterns, and application context. Enterprise security has reached an inflection point. The shift to hybrid work, the decentralization of infrastructure, and the rapid growth of sophisticated threat vectors have rendered traditional perimeter-based models ineffective. Cyber-attacks no longer start at the application layer; they can now originate and exploit vulnerabilities through firmware, identity infrastructure, or deep within the manufacturing supply chain. Enterprise security must evolve to effectively mitigate these dynamic risks.

This whitepaper explores how organizations can meet this challenge by embedding Zero Trust into the fabric of enterprise computing. It introduces a modern architecture where trust is a consistent throughline—validated from the moment a device is prepared for enterprise deployment, before the OS even loads, and sustained throughout its lifecycle. In this model, hardware integrity is assured early, and access is governed by real-time posture rather than static credentials.

At the center of this transformation is Lenovo ThinkShield portfolio, designed to deliver comprehensive, modern, and resilient security that persists throughout the end-to-end device lifecycle. In collaboration with Intel, Lenovo extends this protection down to the silicon layer, further anchoring trust from supply chain transparency through runtime enforcement.

This paper explores how to operationalize Zero Trust, by showing how telemetry from firmware, BIOS, and device health integrates directly with identity systems to enable dynamic, context-aware decisions. It demonstrates how Lenovo and Intel security technologies make it possible to detect, isolate, and recover from security incidents with minimal human intervention. Additionally, it provides a structured execution roadmap that IT Decision Makers (ITDMs) can follow to ensure Zero Trust is embedded across the technology stack.

For organizations navigating increasing compliance pressure, endpoint expansion, and a threat landscape increasingly defined by stealth and speed, this white paper reinforces why Zero Trust is both a business and IT imperative and how Lenovo and Intel can enable this transition with a Comprehensive, Modern, and Resilient approach.

Rethinking security in a hybrid, threat-driven enterprise landscape

The architecture of enterprise IT has changed faster than what most security strategies have been able to keep up with. What was once a tightly managed network perimeter, protected by firewalls and static rules, has now been replaced by a boundaryless environment—distributed across home offices, cloud services, unmanaged endpoints, and global supply chains. Remote work and hybrid infrastructure have expanded attack and vulnerability surfaces. In parallel, enterprise operations are increasingly run on a mix of public cloud, SaaS, and on-prem environments, often with different security baselines which exposes how legacy security models were never designed for this level of dynamic complexity.

In many cases, adversaries have evolved and adapted faster than enterprise security. No longer confined to operating system-level exploits or phishing campaigns, attackers now deliberately target firmware, BIOS layers, identity providers, and device supply chains. Firmware-level attacks can persist undetected for months, operating beneath the OS and bypassing traditional endpoint detection tools entirely. Identity infrastructure has become a central point of failure, with attackers exploiting token theft, MFA fatigue, and misconfigured federation. As organizations procure devices from global suppliers, the risk of compromised components entering the enterprise has also become a legitimate concern.

Today, traditional perimeter-centric approaches often fall short. They rely on static definitions of trust—often limited to a successful login or VPN connection—and assume that once inside, users and devices remain trustworthy. But digital identity is now fluid, devices are mobile, and applications run across multiple clouds. In this model, trust and security must be managed continuously. The security perimeter is no longer a single location. It is a dynamic set of signals spanning device health, firmware integrity, user behavior, access patterns, and application context. Without the ability to assess and act on these signals in real time, enterprises are left with a patchwork of controls that don't scale, aren't interoperable, and don't protect against modern threats.

To mitigate these challenges, enterprises are moving toward Zero Trust Architecture. Neither a product, nor a single solution, Zero Trust Architecture is a strategic framework grounded in three key principles: assume breach, verify explicitly, and enforce least privilege. Rather than trusting anything by default—whether a device, identity, or network segment—Zero Trust requires continuous validation. A device must prove that it is in a known-good state before it can connect. A user must authenticate with strong, contextual signals that go beyond credentials. As a result, access decisions are based on real-time posture—not static role assignments or network location.

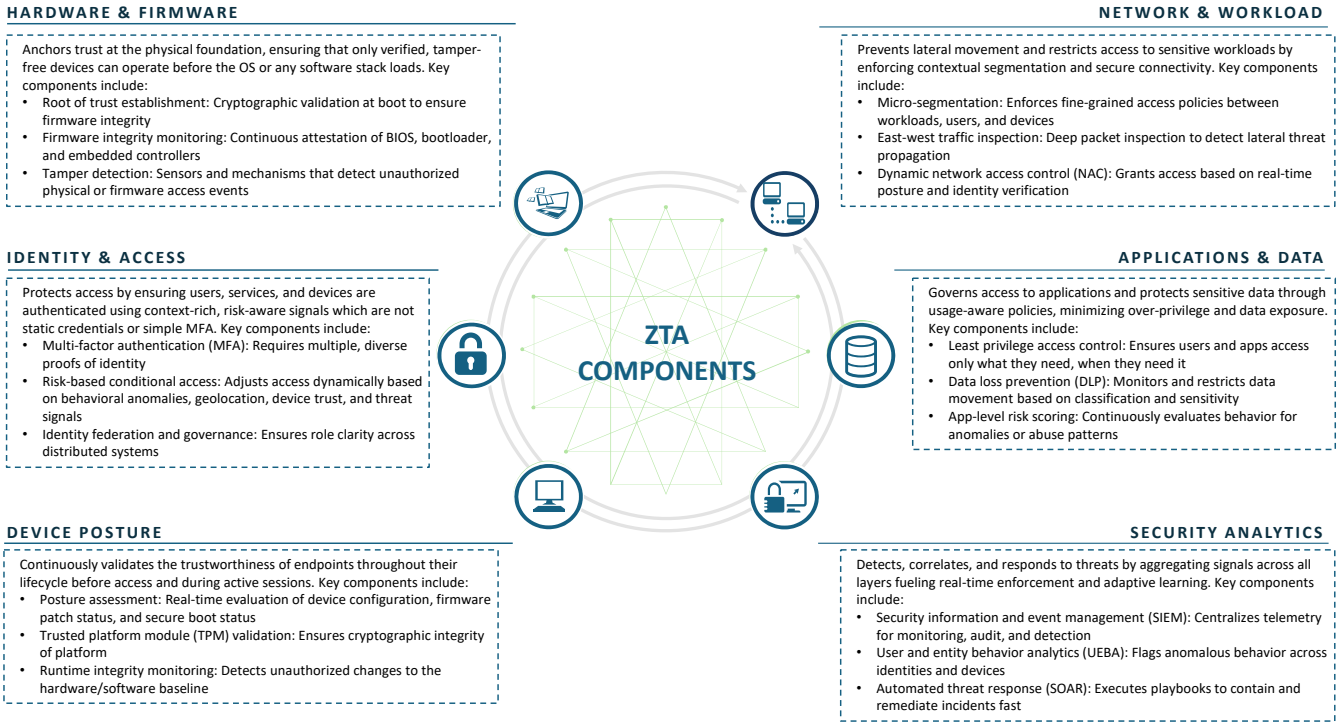


Figure 1: ZTA components in detail

Implementing this approach requires rethinking where trust starts. For Lenovo and Intel, trust begins in the supply chain, where tamper-resistant processes during manufacturing and optional in-transit safeguards (offered as part of the ThinkShield Build Assure solution) ensure components remain authentic and uncompromised before reaching the enterprise. This trust is then reinforced through hardware protections below the OS. Features such as Lenovo's self-healing BIOS, physical tamper detection, and Intel® Hardware Shield establish a verified root of trust before the operating system loads. Devices continue to report posture throughout their lifecycle, ensuring security does not stop at deployment but persists over time.

In this model, supply chain security serves as the first line of defense, while below-the-OS protections provide continuous assurance throughout the product lifecycle. Together, they feed into higher-level policy engines, risk models, and enforcement tools, creating a layered Zero Trust foundation.

Importantly, this direction is being codified into policy and regulation. Compliance frameworks now demand Zero Trust by design. NIST 800-193 guidelines mandate firmware resiliency, including protection, detection, and recovery mechanisms. CISA's Zero Trust Maturity Model outlines milestones for adaptive identity, device trust, and network segmentation.

Regulatory measures such as US Executive Order 13694 on supply chain risk transparency and EO 14144 on continuous diagnostics and mitigation further reinforce these expectations. Enterprises operating without these controls are not only exposed—they are no longer compliant with the latest regulatory demands.

Lenovo's strategic approach to enterprise-grade security

Lenovo's security model is grounded in engineering innovation. Every Think-branded device is designed around the principle of securing the endpoint lifecycle from the ground up—before the OS loads, before users log in, and before any policy is enforced. This 'secure-by-design' approach drives the three foundational commitments Lenovo makes through its ThinkShield portfolio: Comprehensive, Modern, and Resilient protection for enterprise customers.

Comprehensive security means end-to-end protection that keeps employees productive and IT in control. Enterprises benefit from proactive health monitoring that minimizes downtime, robust identity protection with strong authentication for every user, encryption and access controls that safeguard business data, and centralized visibility into hardware, software, and device health. Lost or stolen devices can be remotely tracked and secured, ensuring sensitive data is protected across the entire device lifecycle.

Lenovo delivers this protection through ThinkShield. Security begins with supply chain transparency by embedding tamper-evidence, traceable components, and controlled firmware insertion. It extends below the OS with BIOS-level integrity checks, digitally signed firmware, and resilience against tampering. Organizations can extend this protection with optional endpoint telemetry services that stream BIOS, firmware, and hardware configuration data into SIEM platforms via integration hooks, helping enterprises maintain compliance with frameworks such as NIST 800-53 and 800-193.

Protection continues through OS-to-cloud integrations with Microsoft Intune, Azure AD, and partner security platforms that enforce posture-aware access policies. Finally, Lenovo provides enterprise-grade support, ensuring devices remain secure and productive throughout their lifecycle from deployment to secure retirement.

Modern protection helps enterprises stay ahead of emerging threats with AI-driven defenses that operate in real time. Organizations can instantly block ransomware and malware with AI-powered threat detection that identifies and stops attacks before they spread. Employees can safely use public and private LLMs with optional partner-provided guardrails, available through ThinkShield, which help protect sensitive data and enforce responsible use of generative AI.

Phishing attempts and malicious links are prevented through on-device and cloud-based AI solutions that customers can opt into, to isolate threats and keep users safe. Deep system monitoring ensures ongoing visibility into device posture so security teams can respond quickly to potential risks.

Lenovo delivers this modern protection through ThinkShield. Devices continuously report BIOS version, firmware patch state, TPM health, and boot history, with telemetry sharing enabled by customer choice and integrated with Microsoft Intune, Azure AD, or partner identity providers for conditional access enforcement. ThinkShield Endpoint Visibility enables seamless integration with leading EDR and cloud-native security tools. Unlike traditional security layers that activate only after a device is turned on, Lenovo embeds below-the-OS validation to block execution of compromised or out-of-policy firmware long before operating system controls can be bypassed.

Resilient protection ensures business continuity even in the face of attacks or disruptions. Enterprises gain assurance against supply chain risks with hardware authenticity that is verified from the factory floor through end-user provisioning. IT teams benefit from streamlined operations with automated BIOS, firmware, and driver updates that reduce manual effort and minimize downtime.

Devices are built to self-heal, restoring critical system functions after compromise to keep employees productive. Firmware integrity is continuously validated, preventing foundational device compromise and ensuring long-term trust in every endpoint. These capabilities directly support the uptime, integrity, and security needs of industries such as Manufacturing, Healthcare, and Education.

Lenovo delivers this resilience through ThinkShield. ThinkPad devices powered by Intel Core Ultra processors include self-healing BIOS modules that detect tampering and automatically reflash from a protected partition, ensuring continuity even after attempted compromise. Firmware rollback protections prevent downgrade attacks, while intrusion detection sensors flag unauthorized access attempts.

Devices can be locked or remotely wiped if thresholds are triggered, providing enterprises with fleet-wide control and containment. These security capabilities are available as optional offerings within the ThinkShield portfolio, allowing customers to deploy and enable the features that best support their security outcomes.

Ultimately, ThinkShield is Lenovo's enterprise commitment to embed security into the DNA of every endpoint, aligned to the rapidly evolving needs of ITDMs. This Comprehensive, Modern, and Resilient approach helps enterprises better navigate growing regulatory, operational, and cyber pressures. In a world where breaches are constant and device sprawl is accelerating, Lenovo builds trust at the silicon layer with Intel, defends posture through the cloud, and embeds tamper-resistant components and security features to meet modern enterprise demands.

Building platform trust the Lenovo x Intel security stack

Establishing platform trust begins before the OS is even aware the system has powered on. Lenovo and Intel have co-engineered a trusted foundation that validates firmware, authenticates hardware, and verifies platform integrity through a set of layered, hardware-bound protections. This security leadership makes Zero Trust enforcement reliable at scale.

Each Lenovo Think device powered by Intel includes a suite of below-the-OS protections enabled by Intel vPro® platforms. These protections include Intel BIOS Guard, which prevents unauthorized changes to BIOS code; Intel Boot Guard, which verifies cryptographic signatures before boot; and Advanced Threat Detection, which uses silicon telemetry to detect ransomware and memory injection patterns.

Lenovo extends these protections with its proprietary BIOS resilience architecture, which includes a dedicated recovery partition, cryptographically validated rollback, and BIOS lockout in the event of tamper or downgrade attempts. This ecosystem of features establishes a robust root-of-trust for enterprise endpoints.

Starting with the supply chain, Lenovo's Supply Chain Security organization, in partnership with the Lenovo CSO Organization, ensures that all Intel platform components used in enterprise systems are sourced through traceable, authorized channels. Firmware insertion is tightly controlled and audited to prevent unauthorized images or microcode updates during factory provisioning. This component-level verification enables customers to meet compliance requirements such as FIPS 140-3, EO 13694 traceability, and CISA's supply chain risk guidelines.

At runtime, ThinkShield telemetry combines Lenovo's device-level health data with Intel's silicon-level monitoring. This real-time telemetry informs posture evaluation tools that IT teams use to enforce adaptive access control. For example, IT teams can immediately restrict access to cloud resources if a device reports a failed secure boot, expired firmware signature, or unexpected change in hardware configuration, which then triggers user reauthentication or device quarantine. These signals can be consumed by various XDR and SIEM platforms through pre-built integrations.

The joint Lenovo and Intel stack also delivers audit readiness. Hardware event logs, signed firmware manifests, and boot history are available for inspection, supporting forensic investigations and compliance reporting. ThinkShield audit tooling simplifies these operations for enterprise security teams, reducing manual validation and improving response readiness across distributed device fleets.

By anchoring Zero Trust enforcement at the silicon and firmware layers, Lenovo and Intel provide platform-level confidence—ensuring that device trust is earned, validated, and visible.

	Comprehensive	Modern	Resilient
Key Outcomes	Protect the full device lifecycle with proactive health monitoring, strong identity and authentication, encryption and backup safeguards, and centralized IT visibility and control.	Defend against advanced threats with AI-powered detection, safe and responsible LLM use, phishing and malware prevention, and real-time insight into device posture and events.	Reduce security risks by streamlining tasks related to software, BIOS, and driver updates across fleet. Device integrity from manufacturing to end-user provisioning.
ThinkShield Offerings	Threat Protection, Identity Security, Password-less Authentication with MFA, ThinkShield Data Defense, Cloud Backup, ThinkShield Data Erasure, Lenovo Device Orchestration, ThinkShield Hardware Defense.	ThinkShield XDR, AI LLM Guardrails, Threat Isolation, ThinkShield Firmware Assurance.	Lenovo Patch, ThinkShield Build Assure.
Intel Offerings	vPro, Hardware Shield, Intel Threat Detection Technology (TDT)	TDT AI analytics, AMT visibility, Device Health Attestation	Transparent Supply Chain, Secure Boot

Figure 2: Analyzing the tech stack across Lenovo & Intel

Translating zero trust principles into today's ITDM needs

Lenovo and Intel enable organizations to implement Zero Trust end-to-end, beginning with hardware trust, extending through optional telemetry, and culminating in policy-based real-time enforcement that is responsive to change and resistant to evasion.

Every Lenovo endpoint in a Zero Trust architecture acts as both a sensor and a policy enforcement point. At boot, the system's BIOS and firmware are validated against signed baselines using Intel Boot Guard and Lenovo Secure BIOS. Any deviation triggers a local quarantine action and can be escalated to cloud policy engines.

The risk score informs policy decisions in real time. Access to protected resources can be gated or modified based on the trust level reported by the device. For example, a Lenovo ThinkPad attempting to connect to a financial trading application may be allowed only if its firmware is current, its TPM state is valid, and its BIOS matches the signed baseline. Otherwise, access is denied or redirected to remediation. These workflows are automated through integration with modern identity platforms like Azure AD Conditional Access or Okta, enabling dynamic trust decisions based on hardware-rooted signals.

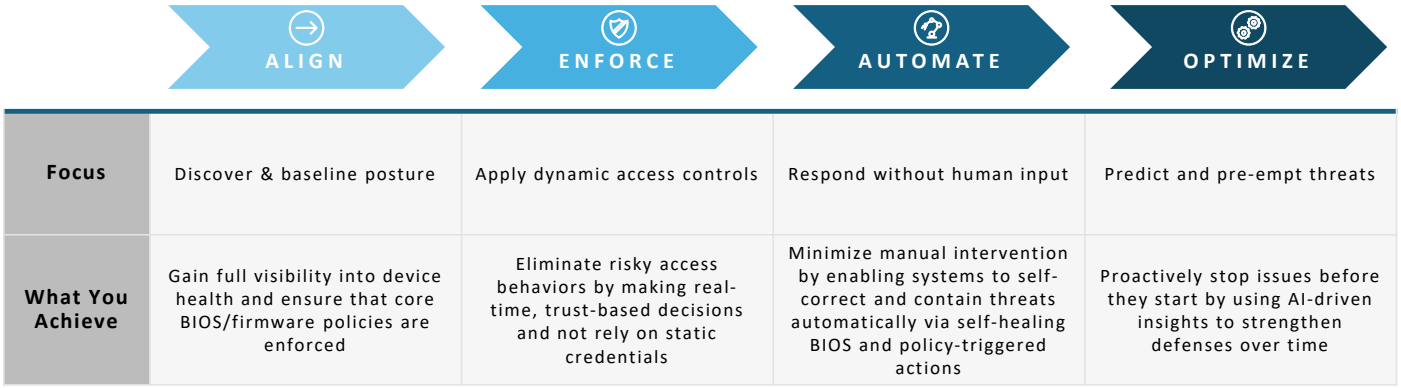
In-session validation is equally critical. Lenovo and Intel platforms support telemetry revalidation at runtime, allowing posture changes—such as firmware tampering or physical intrusion events—to trigger access revocation mid-session. This is essential in protecting high-value assets from session hijack, lateral movements, and insider threats.

A complete Zero Trust reference architecture using Lenovo and Intel includes secure boot, BIOS attestation, TPM-based identity anchoring, optional runtime telemetry streaming, cloud-native policy enforcement, and automated remediation workflows. These components align to NIST 800-207 guidelines and are actively being deployed in regulated industries requiring continuous control assurance.

By grounding Zero Trust in hardware-first telemetry and real-time enforcement capabilities, Lenovo and Intel allow organizations to operationalize Zero Trust with precision—not just at the point of login, but throughout the full session lifecycle.

Execution playbook for IT decision makers

Adopting Zero Trust at scale is not a matter of simply selecting the right tools—it requires orchestration across devices, identity, policy, and operations. ITDMs face the dual challenge of modernizing their security posture while maintaining compliance, uptime, and user experience. Lenovo and Intel provide an industry leading technical foundation that is Comprehensive, Modern, and Resilient in how it meets modern enterprise demands. However, it is incumbent on ITDMs to operationalize this Zero Trust Architecture system, using a proven adoption roadmap.



	ALIGN	ENFORCE	AUTOMATE	OPTIMIZE
Focus	Discover & baseline posture	Apply dynamic access controls	Respond without human input	Predict and pre-empt threats
What You Achieve	Gain full visibility into device health and ensure that core BIOS/firmware policies are enforced	Eliminate risky access behaviors by making real-time, trust-based decisions and not rely on static credentials	Minimize manual intervention by enabling systems to self-correct and contain threats automatically via self-healing BIOS and policy-triggered actions	Proactively stop issues before they start by using AI-driven insights to strengthen defenses over time

Figure 3: Adoption Roadmap for ZTA

ALIGNMENT: This phase focuses on visibility and control over the devices that touch sensitive systems. IT teams should start by inventorying device posture, BIOS and firmware state, and TPM readiness across the device fleet. Lenovo Think-branded devices, paired with Intel silicon and ThinkShield telemetry services, enable posture discovery at scale—surfacing below-the-OS integrity metrics and identifying devices that fall outside of enterprise policy. Organizations can begin enforcing baseline controls like BIOS password management, secure boot enablement, and device-level attestation using native Lenovo tools and Microsoft Endpoint Manager.

ENFORCEMENT: This phase applies Zero Trust principles to real-world workflows. Lenovo devices feed real-time telemetry—covering boot integrity, firmware versioning, and chassis tamper events—into cloud-native access control engines. At this stage, ITDMs should shift from static policies to dynamic, posture-aware enforcement. Access to sensitive applications should be contingent on device trustworthiness, with integration into identity providers like Azure AD or Okta for conditional access. Policies can be configured to quarantine endpoints with known risks, enforce remediation before login, or route high-risk sessions into monitored environments.

AUTOMATION: As telemetry maturity increases, organizations can start automating Zero Trust principles. Lenovo and Intel platforms provide inputs for policy engines to make adaptive, high-frequency decisions. Threat response becomes event-driven and automated—as self-healing BIOS capabilities initiate automatic rollback after unauthorized changes, while posture deviations detected mid-session trigger token revocation or credential refresh. SIEM and SOAR platforms ingest ThinkShield telemetry to coordinate broader incident response, reducing manual triage and increasing MTTR performance. This phase depends on tight integration between device telemetry, identity control, and enforcement logic.

OPTIMIZATION: Enterprises can begin using hardware-rooted telemetry not just for control—but for prediction. AI-enhanced monitoring systems use historical BIOS and device state data to identify anomalies and flag early-stage compromise patterns. Policy engines are refined with machine learning models that incorporate user context, device lineage, and known threat behaviors. Lenovo continues to evolve ThinkShield capabilities in this area, integrating predictive analytics and modern, AI-assisted diagnostics into its endpoint management tools to help organizations proactively anticipate rather than react.

A few key organizational considerations will enable successful deployment of this model:

- Governance structures must reflect the distributed nature of control in Zero Trust environments.
- Security teams must collaborate with infrastructure, compliance, and identity stakeholders to define enforcement points and escalation paths.
- Role clarity is essential—endpoint security owners, identity architects, and platform teams must operate with shared telemetry sources and unified access models.
- ThinkShield framework supports this alignment through shared telemetry, cross-platform tooling, and supply chain visibility that meets both CISO and CIO priorities.

Conclusion

Zero Trust is no longer optional—it is the new standard for enterprise security. Lenovo and Intel deliver the Comprehensive, Modern, and Resilient foundation to make it real. With ThinkShield and Intel vPro®, organizations can secure every device from factory to frontline and enforce Zero Trust by design.

ThinkShield extends protection across the full spectrum of enterprise risk, starting with supply chain security, continuing below the OS, and reaching through OS-to-cloud integrations, all supported by enterprise-grade services that help customers meet growing security needs.

Strategically, Lenovo and Intel provide IT decision makers with a stack that makes Zero Trust integral to the entire enterprise technology foundation. From silicon-level verification to firmware controls, telemetry pipelines, and cloud enforcement, Lenovo's and Intel's security products, features, and solutions gives enterprises the tools to build a Zero Trust model that is technically credible, operationally scalable, and regulation-ready.

Modern enterprise security can no longer be a reactive defense. It must be built through systems that continuously measure trust, enforce policy, and adapt to change—at hardware level speeds. With the Lenovo and Intel platform, Zero Trust becomes a new baseline that supports ITDMs in meeting modern enterprise demands.

The time to act is now.

Lenovo and Intel are ready to help you build Zero Trust from the ground up—and execute with confidence.

Lenovo | intel®