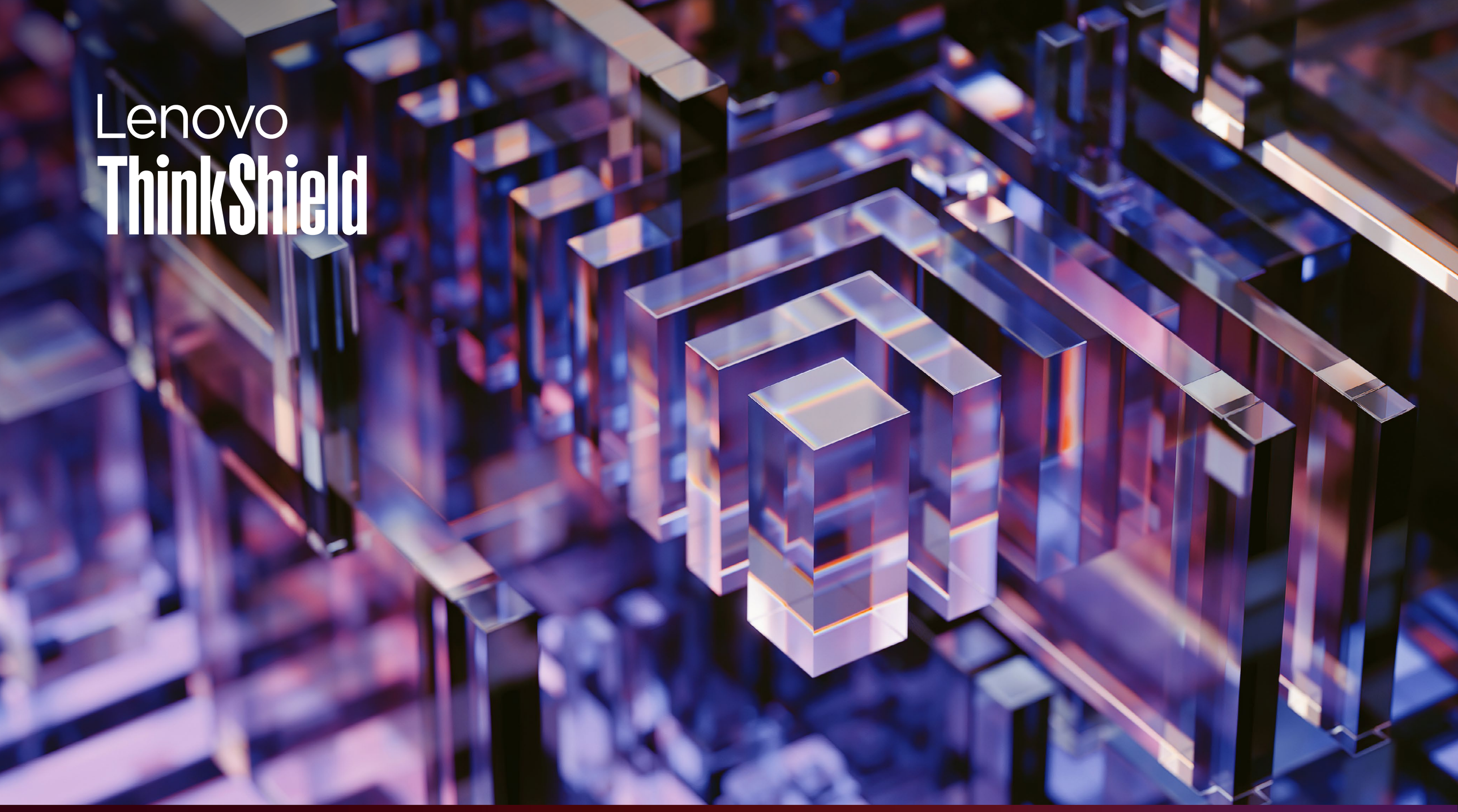


Lenovo

That's the power of Lenovo with Intel Inside®

intel vPRO

Intel vPro® Platform

Advanced protection in action

How to deploy enterprise security at scale with comprehensive, modern and resilient solutions that protect productivity in the AI age.

The new security imperative: depth and intelligence

Protecting endpoints is no longer enough. Only security layered across the entire device lifecycle, with Zero Trust architecture to counter modern AI threats, can keep businesses safe without compromising productivity.

Key outcomes: what enterprises need in the AI era

Faster threat detection and response.

Reduced attack surface by enforcing Zero Trust principles.

Stronger productivity through business resilience and minimized downtime.

As businesses transform with AI, the performance and productivity gains will be huge. But only if the enterprise can be sure of total lifecycle security. That means enforcing Zero Trust principles to continuously validate users, devices and firmware across the lifecycle. Many businesses, for example, are upgrading to Lenovo's market-leading hardware—ThinkPad, ThinkStation, ThinkCentre and AI PCs powered by Intel®—that are secure by design with Lenovo, ThinkShield and the Lenovo Intel vPro® platform.

A secure-by-design approach is key in the face of more sophisticated AI-driven threats that target protection gaps across enterprises. Attackers are using AI for phishing, malware generation and reconnaissance—pushing the expected worldwide cost of cybercrime to $15.63 trillion by 2029.[1] The anticipated spend on cybersecurity in 2026 alone is now $418 billion, a 12% year-on-year increase.[2]

End-to-end safeguards are critical

To counter such fast-evolving, boundary-breaking threats, every part of the device lifecycle must be secure with Zero Trust principles embedded throughout. Any cracks must be filled across device design, platform-level security, manufacturing and supply chain, device usage, incident response, endpoint security and final decommissioning.

Zero Trust

Zero Trust is a "never trust, always verify" cybersecurity approach. Instead of assuming anything inside a network is safe, Zero Trust:

- Treats every user, device and application as untrusted by default.
- Requires continuous identity verification and strong authentication.
- Limits access strictly to what is needed (least privilege).
- Monitors and inspects all traffic, regardless of location.
- Assumes breaches can and will happen, and designs controls to minimize impact.

But far too often, enterprises rely on traditional antivirus (AV) solutions or leave gaps in critical areas like firmware or supply chain. Even in the highly regulated—and highly targeted!—financial industry worldwide, 81% still rely on traditional AV protection. And the top two endpoint security options in use globally are traditional antivirus/antimalware software and cloud-based solutions.[3]

Traditional approaches lead to:

Lack of preparation for AI threats

90% of organizations aren't 'very confident' they can address the risks from cybercriminals using AI.[4]

Gaps exposed

61% of organizations reported a third-party data breach in the past 12 months.[5]

Underutilization of AI protection

77% of organizations favor behavior-based learning models for identifying suspicious activities, but adoption remains low.[6]

In this whitepaper, we'll explore advanced protection in action, showing how Lenovo ThinkShield solutions, optimized for Intel® platforms, provide the four layers of security that must be implemented to safeguard today's enterprises.

"AI has changed the game. When attackers target your supply chain and firmware as aggressively as your apps and endpoints, you can't bolt security on and hope for the best. You need platforms that are secure by design—from silicon to cloud—with AI working for you, continuously validating every device, every identity and every connection across the entire lifecycle."

Nima Baiati, VP and GM
Lenovo Software & Security Solutions.

The answer is advanced protection for all.

Key outcomes:

Comprehensive security against attacks at every level, including ransomware, data theft and malicious threats.

Modern safeguarding with AI-embedded devices, behavior-based analysis and self-healing BIOS capabilities to protect data.

Resilient protection with minimized disruption through diagnosing and remediating device health issues for more productive operations.

Cybersecurity protection doesn't work in parts. It must be everywhere—from the product design to the security solution and service development, extending across the entire product lifecycle. And security software needs to continue evolving to stay effective against increasingly sophisticated cyber threats. It's a question of taking a wider, deeper approach that goes beyond endpoints by marrying industry-leading devices and software.

Secure-by-design hardware on the Intel vPro® platform

Lenovo ThinkPad, ThinkStation, ThinkCentre and AI PCs on the Intel vPro® platform with Lenovo ThinkShield solutions support a layered Zero Trust security architecture that starts in hardware and extends through firmware, OS, applications and cloud services. It's a combination that reduces attack surface, hardens devices against advanced threats, and gives IT continuous visibility and control across the fleet.

Lenovo ThinkPad X9 Copilot+ PC with Intel vPro® platform and Intel® Core™ Ultra 7 processor

That's the power of Lenovo with Intel Inside®

Lenovo ThinkStation P7 with Intel vPro® Platform and Intel® Xeon® processor

That's the power of Lenovo with Intel Inside®

ThinkCentre X AIO Aura Edition Copilot+ PC with Intel vPro® platform and Intel® Core™ Ultra 5 processor

That's the power of Lenovo with Intel Inside®

Continuous protection across the device lifecycle

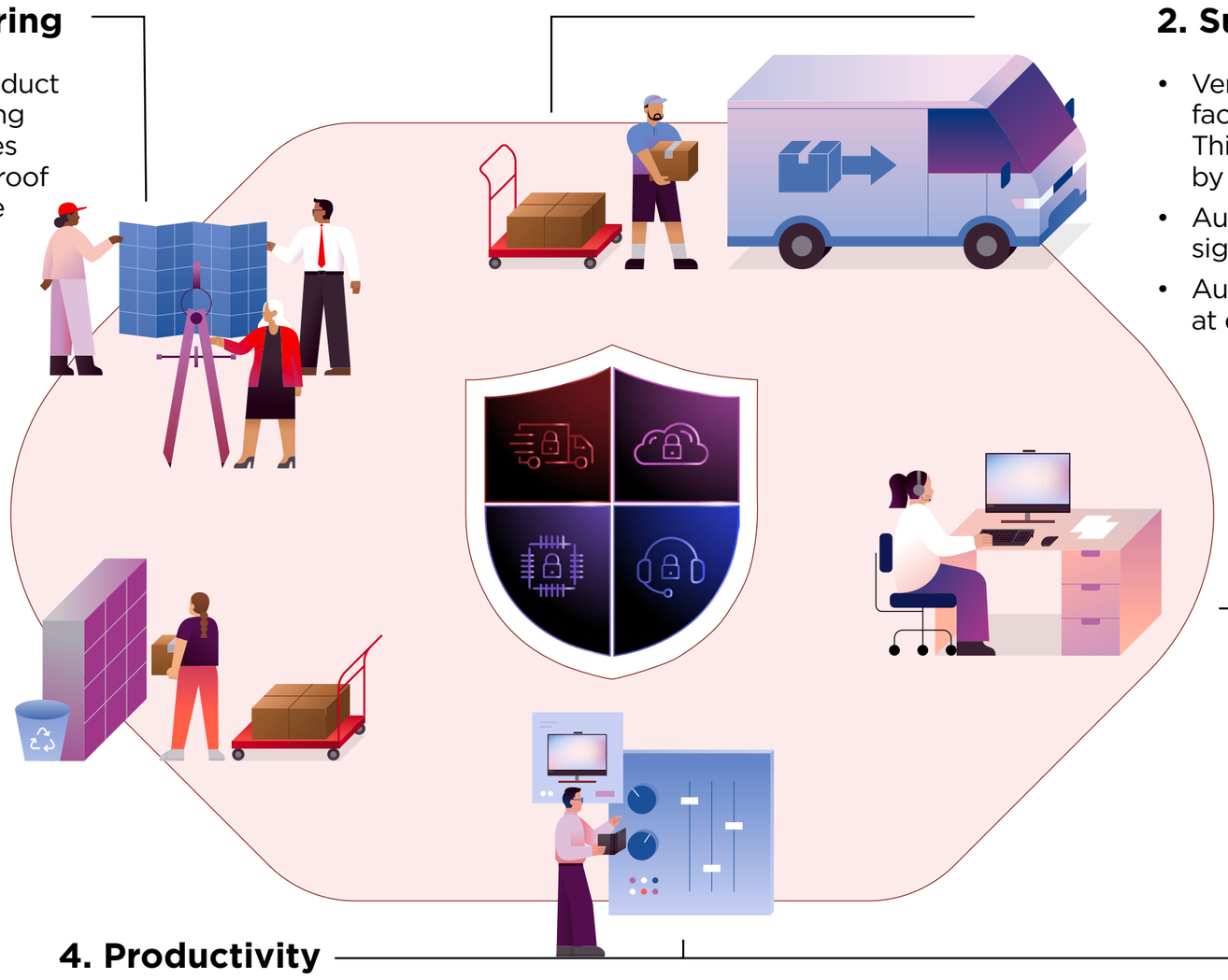
Unlike other security offerings, Lenovo ThinkShield is unique in its coverage of the entire device lifecycle.

1. Design and manufacturing

- Security is embedded from product inception through manufacturing and lifecycle operations. Devices are backed by cryptographic proof of build integrity, with verifiable manufacturing records and component traceability.
- Hardware-rooted trust foundation enables Zero Trust across the device lifecycle.

2. Supply chain

- Verifiable device integrity from factory to fleet enabled by ThinkShield Build Assure, powered by Intel® Transparent Supply Chain.
- Audit-ready, cryptographically signed build records.
- Automated device validation at deployment.



3. Provisioning

- Trusted baseline from first boot onward, with pre-validated BIOS, firmware and OS images.

4. Productivity

- AI-powered, autonomous protection across the attack surface.
- Continuous, layered protection from firmware to cloud.
- Persistent device integrity with self-healing protection.
- Real-time visibility into device health and security posture.
- Automated threat response to reduce dwell time and impact.
- Maintained chain of trust during active use.
- Centralized policy enforcement and fleet-wide control to remediate vulnerabilities at scale.

5. End-of-life

(secure decommissioning)

- Certified data erasure to eliminate residual risk.
- Controlled and compliant data sanitization.
- Simplified and secure retirement at scale, including centralized management of data erasure, asset disposition and compliance reporting.

Lifecycle protection: Supply chain

Every device secure from the start

Key outcomes:

Verified device integrity from factory to deployment.

Minimized risk of tampered, counterfeit components and unauthorized modification.

Faster compliance and audit sign-off.

Hardware-rooted foundation of trust to support Zero Trust provisioning and lifecycle validation.

For most organizations, risk starts long before a device ever connects to the network. With components changing hands—across factories, logistics hubs, distributors and resellers—blind spots are created where tampering, counterfeit parts or malicious firmware can breach security.

Trusting the box is no longer an option. Endpoint, OS and cloud tools can't fix a poisoned foundation. The supply chain itself must be secured, verified and continuously auditable from factory floor to first boot.

45%

of organizations experienced third party-related business interruptions in the previous two years—showing that supply chain risk is a real resilience issue.[7]

Solutions that work, from the industry leaders

The partnership between Lenovo and Intel® strengthens supply chain security by combining Lenovo ThinkShield solutions with Intel® technologies. We provide silicon-level trust, device integrity validation and verifiable chain-of-custody assurance from manufacture to first boot.

ThinkShield Build Assure powered by Intel® Transparent Supply Chain

- **Verified device integrity** from factory to first boot with automated verification tools and signed, auditable records that confirm device authenticity and component integrity from manufacturing through to end-user provisioning.
- **Trusted suppliers and documented chain of custody** reduce the risk of compromised components entering the fleet.
- **Secure, boot-ready deployment at scale** allows IT to ship devices directly to employees with a trusted, validated baseline.
- **Stronger compliance and risk posture** combines integrity attestation, component traceability and tamper detection, helping meet regulatory expectations and reducing the overall attack surface associated with hardware delivery.

Trusted, standards-based supply chain controls

- **Ensure provenance from component sourcing through distribution** with alignment to NIST and DFARS guidance on counterfeit detection and supply chain risk, using Trusted Computing Group standards hardware delivery.

Hardware root of trust from silicon to OS

- **Validate firmware, authenticate hardware and enforce secure boot** with Intel® Trusted Device Setup and Lenovo's security-by-design approach that ensure only signed, approved firmware images can run, laying the foundation for Zero Trust access policies and device-level attestation.

Lifecycle-ready for distributed workforces

- **Enable secure dropship and remote provisioning** so IT can prove a device is genuine, untampered and policy-compliant before handing it to an employee.

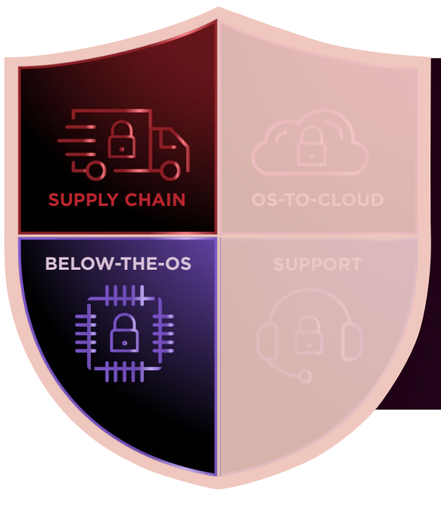
Validating the integrity of employee devices for Meta

Meta deploys Lenovo ThinkShield Build Assure, powered by Intel® Transparent Supply Chain to validate the provenance, security and authenticity of employee devices, while reducing the provisioning burden on Meta's IT teams.

Read case study

Lifecycle protection: Below-the-OS

Security built in, integrity at every level



Key outcomes:

13–48x improved breach mitigation.[8]

Reduced downtime after compromise.

Faster detection of stealthy attacks.

Smaller attack surface at below-the-OS.

Most endpoint security solutions stop at the OS. ThinkShield extends protection below it, where firmware has become a prime target for persistent, stealthy attacks. When compromised, firmware can bypass boot protections, disable security tools, and remain undetected for long periods.

Despite this risk, many organizations still rely on one-time checks instead of continuous monitoring. A Zero Trust approach addresses this gap by continuously verifying firmware integrity and using real-time telemetry as a trusted foundation for access and security decisions.

76%

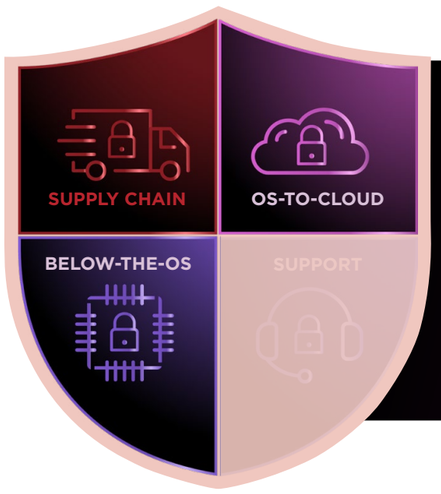
of IT security decision-makers in the finance industry have gaps in their awareness concerning their organization's firmware blind spot.[9]

Lenovo ThinkShield extends protection to below-the-OS

Business challenge:	Business impact:	Outcomes with Lenovo ThinkShield Solutions:
Unable to verify firmware integrity across the fleet	• Incomplete Zero Trust posture • Exposure to advanced threats • Operational risk	• **Strengthen resilience, maintain continuity, unify risk visibility** with ThinkShield lifecycle security and centralized telemetry.
Untrusted firmware updates across fleet	• Persistent compromise • Data loss risk • Operational disruption	• **Prevent unauthorized execution, reduce downtime, ensure trust** with Lenovo Secure boot, hardware-rooted trust of Lenovo ThinkShield, Intel vPro® platform. • **Verify updates, improve auditability** with ThinkShield Firmware Assurance.
Firmware blind spot	• Long dwell time • Hidden compromise • Weak Zero Trust enforcement	• **Reduce downtime, and close visibility gaps** with ThinkShield Firmware Assurance (continuous UEFI telemetry). • **Detect hidden firmware threats** with ThinkShield Firmware Defense, powered by Eclypsium.
Firmware attacks bypass security tools	• Persistent attacker control • Business disruption risk • Security stack failure	• **Maintain continuity, enforce trusted execution, stop stealth persistence** with hardware-rooted trust from Lenovo secure-by-design devices and Intel vPro®. • **Expose attacks outside OS visibility** with ThinkShield Firmware Defense, powered by Eclypsium.
Physical tampering goes undetected below existing monitoring layer	• Backdoors introduced • Compliance exposure • Increased breach risk	• **Contain threats fast, reduce downtime, prove device integrity** with Think UEFI tamper detection and ThinkShield Firmware Assurance.
Rogue hardware / "shadow hardware" risk	• Expanded attack surface • Data exfiltration risk • Untrusted devices in fleet	• **Reduce attack surface, enforce hardware trust, maintain control** with ThinkShield Hardware Defense, powered by Sepio. • **Validate device integrity at scale** with ThinkShield Security Chip and ThinkShield Firmware Assurance.
Unauthorized firmware and BIOS changes outside IT visibility	• Rootkits and persistent malware • Audit failures • Integrity breakdown	• **Accelerate audits, detect drift, maintain compliance posture** with ThinkShield Firmware Assurance.
Devices off-network or powered down cannot be managed or secured by traditional tools	• Loss of device visibility and control • Inability to enforce policies or remediate threats • Increased risk of data loss, compliance gaps, and unrecoverable devices	• **Maintain control, recover devices and enforce policies anywhere** with ThinkShield TraceLock, powered by Absolute Security, for firmware-anchored persistence.

Lifecycle protection: OS-to-cloud

Smarter protection with AI and Extended Detection and Response (XDR)



Key outcomes:

Consistent Zero Trust enforcement across hybrid workforces.

85% predictive accuracy for common endpoint and IT failures.[10]

Protected data, even during breaches.

Ransomware, phishing and account takeover are business-stopping events that now move at machine speed across devices, identities and cloud apps. Point security solutions can spot fragments of a sophisticated attack, but they can't see, prevent or remediate the full story from endpoints to SaaS.

At the same time, stretched security teams face rising alert volumes and long dwell times. Breaches can take weeks or even months to identify and contain, exposing enterprise data to further attacks and putting the business at risk of compliance failures.

37% increase

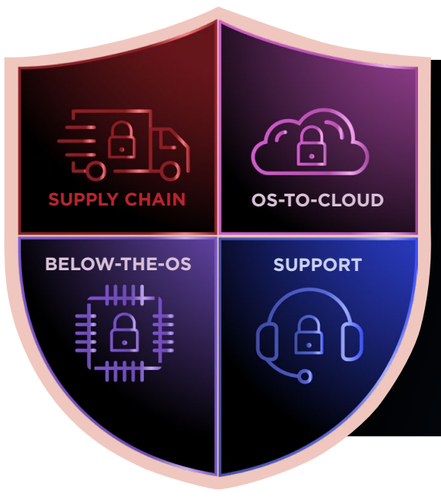
in global ransomware attacks in 2025 compared to 2024.[11]

Lenovo ThinkShield delivers unified, lifecycle protection, from endpoint to cloud, to reduce downtime, accelerate audits and maintain business continuity.

Business challenge:	Business impact:	Outcomes with Lenovo ThinkShield Solutions:
No unified lifecycle protection from endpoint to cloud	• Gaps between detection, response and remediation • Slower recovery and inconsistent controls • Risk to business continuity	• **Maintain continuity, unify protection and simplify operations** with a comprehensive ThinkShield platform, including ThinkShield XDR, powered by SentinelOne, Lenovo Device Orchestration, Absolute Security, and integrated security stack across the device lifecycle.
Fragmented tools cannot detect and respond across the full attack lifecycle	• Missed attack signals • Long dwell time • Increased breach impact	• **Reduce downtime and contain attacks faster** with ThinkShield XDR for AI-driven detection and automated response.
Ransomware and advanced malware evade legacy security tools	• Systems encrypted • Operations disrupted • High recovery cost and business impact	• **Maintain operations and minimize disruption** with ThinkShield XDR for behavioral detection and autonomous ransomware blocking.
Unpatched devices and inconsistent configurations across the fleet	• Large attack surface • Compliance gaps • High operational overhead	• **Reduce attack surface and automate compliance** with Lenovo Device Orchestration for centralized updates and policy-based remediation.
Security controls fail or are disabled without visibility (no persistence)	• Loss of protection coverage • Devices operating outside IT control • Increased compliance risk	• **Maintain protection and ensure continuous compliance** with Absolute Security for firmware-anchored persistence and self-healing controls.
Sensitive data exposed during endpoint compromise or ransomware events	• Data loss or exfiltration • Regulatory penalties • Business disruption	• **Protect data and reduce breach impact** with ThinkShield Data Defense, powered by Cigent, for MFA-gated access, encryption and secure vaults.
User-driven threats (phishing, unsafe browsing) introduce attacks into environment	• Compromised identities and devices • Increased incident volume • Entry point for ransomware	• **Prevent infection and reduce entry points** with Threat Isolation, powered by BufferZone, for browser and document isolation.

Lifecycle protection: Support

Continuous support. Always on



Key outcomes:

24x7 security coverage.

80% of low-level incidents resolved without analyst intervention.[12]

Secure and compliant device retirement.

Security at scale with 180+ markets covered by regulation-aligned services.[13]

IT teams are under constant pressure: more tools, more alerts, more regulations. And not enough staff to manage them, let alone support employees. So how can they give enough focus to security?

It's no surprise that 83% of executives cite skill gaps as a barrier to sustaining a secure posture.[14] When incidents hit, internal teams can be overwhelmed by investigation, response and recovery tasks. To stay resilient, enterprises need a trusted partner who can provide 24x7 coverage, outcome-driven services and secure end-to-end lifecycle management. A partner who delivers from deployment to productivity to responsible end-of-life reuse or recycling.

52%

of IT leaders don't feel fully confident in addressing the risks emerging from AI adoption.[15]

Lenovo ThinkShield Global Support

Lenovo ThinkShield offers 24x7 global support in 180 markets and the simplicity of a single-vendor contact in the event of a security breach or need.

Our experts help IT quickly diagnose issues, coordinate vendor responses and keep users productive, wherever they're based.

Managed Protection & Response (MDR) services for 24x7 protection

- Non-stop threat monitoring and incident response from Lenovo and our global SOC.
- Analysts investigate alerts, hunt for threats and executive containment actions.

Additional support

Lenovo Security Services for AI-enhanced support

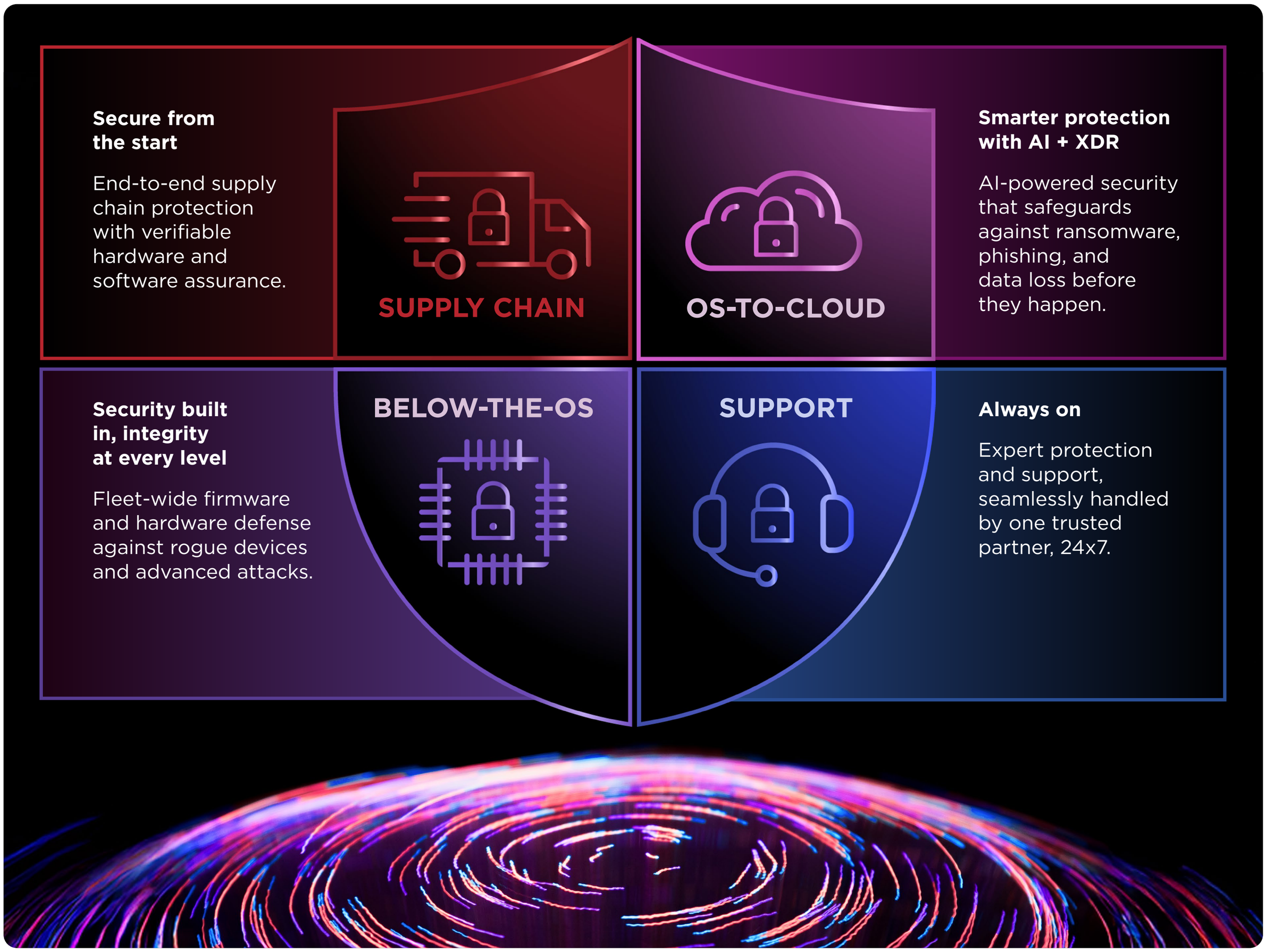
- Advisory, Implementation and Configuration services.
- Ongoing Managed Services for operationalizing Zero Trust using the ThinkShield stack.

Lenovo Asset Recovery Services (ARS) for secure IT end-of-life management

- Extends protection to final stage of device lifecycle.
- Certified data sanitization, compliance certificates, coordinated pickup and environmental reporting.

Advanced protection for all.

Together, Lenovo ThinkShield and Intel® provide the four layers of security needed to safeguard enterprises in the age of AI.



A comprehensive, modern, and resilient end-to-end security portfolio—spanning supply chain, below-the-OS and OS-to-cloud—delivered by a single, trusted partner and aligned to Zero Trust principles.

- **353% ROI** from SentinelOne Singularity XDR platform.[16]
- **Easy implementation** with expert support throughout.
- **Brand agnostic:** ThinkShield protects devices across your entire fleet, regardless of OEM.
- **Flexible architecture design** with plans tailored to budgets, fleets and business needs.
- **Advisory** to identify gaps and recommend solutions that plug them.

ThinkShield industry-leading partners

Intel®
SentinelOne
Absolute Security
BufferZone®
Sepio
Cigent
Eclypsium
Ivanti
Veeam
WinMagic
Acronis
Carbonite
FileWave
CyberArk
Secret Double Octopus
Dynamo AI
Blanco
Churchill & Harriman

That’s the power of Lenovo with Intel Inside®

Intel vPro® Platform

Ready for advanced protection?

Safeguard productivity in the AI age with enterprise security solutions aligned to Zero Trust principles from Lenovo and Intel®.

Get started today at Lenovo ThinkShield

1. Statista, Estimated cost of cybercrime worldwide 2018-2029.
2. Omidia, Cybersecurity Ecosystem Outline 2026, £311 billion converted to US$ for consistency (exchange rate 0.74).
3. IDC, Endpoint Security in the Age of AI, 2025.
4. Lenovo, Work Reborn: Reinforcing the Modern Workplace, 2025.
5. IDC, Endpoint Security in the Age of AI, 2025.
6. IDC, Endpoint Security in the Age of AI, 2025.
7. Gartner, Gartner Survey Finds 45% of Organizations Experienced Third Party-Related Business Interruptions During the Past Two Years, 2023.
8. Forrester Consulting, Total Economic Impact™, 2020.
9. Eclypsium, Firmware security in financial services supply chains, 2022.
10. Lenovo Device Intelligence+ internal results, 2024.
11. Comparitech, Worldwide ransomware roundup, 2026.
12. Lenovo, internal SOC performance data, 2024.
13. Lenovo, compliance and regulatory mapping, 2024.
14. Accenture, State of Cybersecurity Resilience, 2025.
15. Lenovo, Work Reborn: Reinforcing the modern workplace, 2025.
16. Forrester Consulting, Total Economic Impact™, 2020.