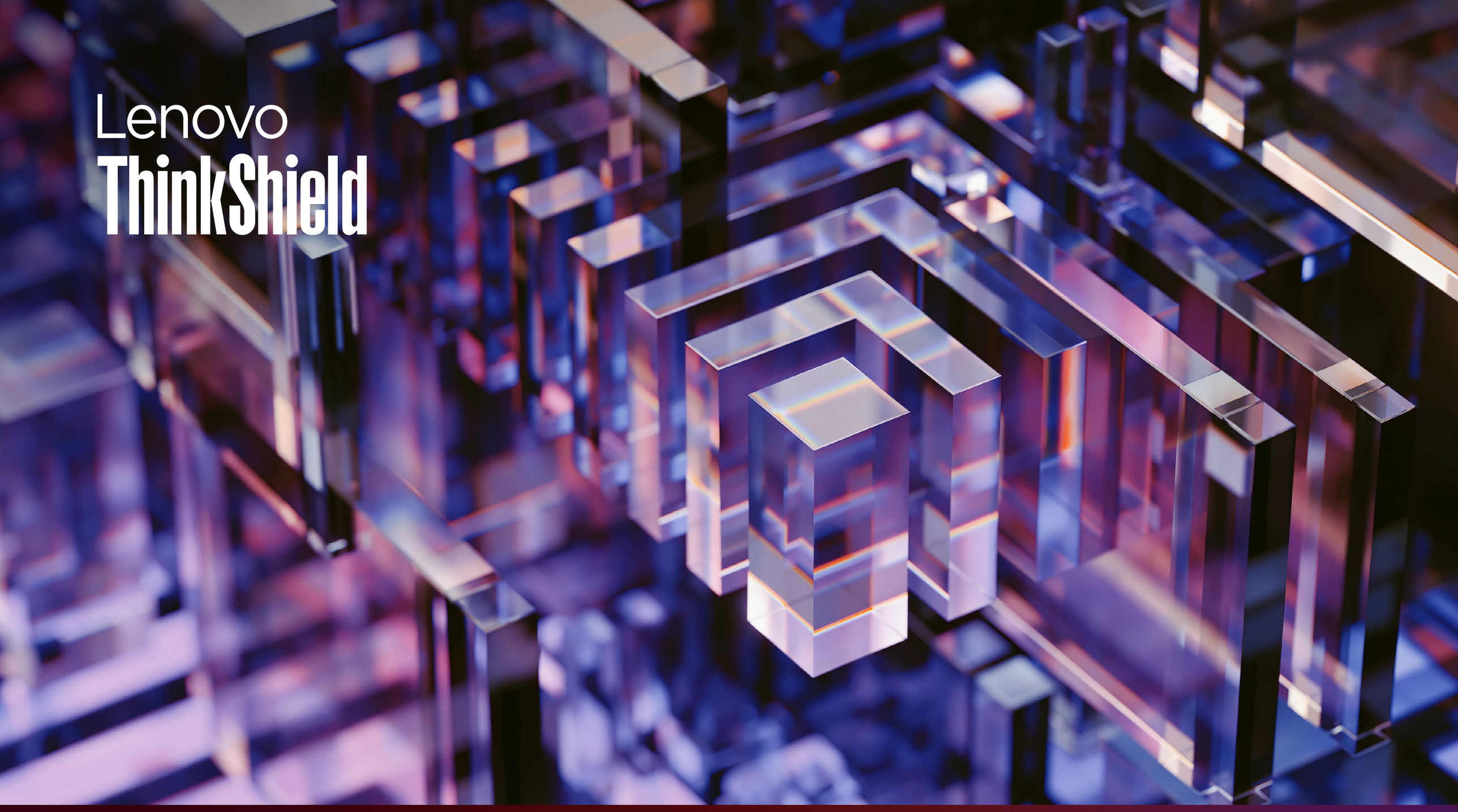


Lenovo | intel vPRO

Ese es el poder de Lenovo con Intel Inside®
Intel vPro® Platform

Protección avanzada en acción

Cómo implementar seguridad empresarial a escala con soluciones integrales, modernas y resilientes que protegen la productividad en la era de la IA.

El nuevo imperativo de seguridad: profundidad e inteligencia

Proteger los endpoints ya no es suficiente. Solo una seguridad en capas a lo largo de todo el ciclo de vida del dispositivo, con una arquitectura Zero Trust para contrarrestar las amenazas modernas de IA, puede mantener seguras a las empresas sin comprometer la productividad.

Resultados clave: lo que las empresas necesitan en la era de la IA

Detección y respuesta ante amenazas más rápidas. Reducción de la superficie de ataque mediante la aplicación de principios Zero Trust. Mayor productividad gracias a la resiliencia empresarial y a la minimización del tiempo de inactividad.

A medida que las empresas se transforman con IA, las mejoras de rendimiento y productividad serán enormes. Pero solo si la empresa puede garantizar la seguridad total del ciclo de vida. Esto implica aplicar los principios de Zero Trust para validar continuamente usuarios, dispositivos y firmware a lo largo del ciclo de vida. Muchas empresas, por ejemplo, están migrando al hardware líder de Lenovo ?ThinkPad, ThinkStation, ThinkCentre y AI PCs con tecnología Intel®?, seguro desde el diseño con Lenovo, ThinkShield y la plataforma Lenovo Intel vPro®.

Un enfoque seguro desde el diseño es clave frente a amenazas cada vez más sofisticadas impulsadas por IA que atacan brechas de protección en las empresas. Los atacantes utilizan IA para phishing, generación de malware y reconocimiento, elevando el costo mundial estimado del ciberdelito a US$ 15,63 billones para 2029.1 El gasto previsto en ciberseguridad solo en 2026 asciende a US$ 418 mil millones, un aumento interanual del 12%.2

Las salvaguardas de extremo a extremo son fundamentales

Para hacer frente a amenazas que evolucionan rápidamente y trascienden fronteras, cada parte del ciclo de vida del dispositivo debe ser segura, con los principios de Zero Trust integrados en todo el proceso. Cualquier brecha debe cerrarse en el diseño del dispositivo, la seguridad a nivel de plataforma, la fabricación y la cadena de suministro, el uso del dispositivo, la respuesta a incidentes, la seguridad de endpoints y el retiro final.

Zero Trust

Zero Trust es un enfoque de ciberseguridad basado en ?nunca confiar, siempre verificar?. En lugar de asumir que algo dentro de una red es seguro, Zero Trust:

? Trata a cada usuario, dispositivo y aplicación como no confiables de forma predeterminada.

? Requiere verificación continua de identidad y autenticación sólida.

? Limita el acceso estrictamente a lo necesario (mínimo privilegio).

? Supervisa e inspecciona todo el tráfico, independientemente de la ubicación.

? Asume que las brechas pueden ocurrir y ocurrirán, y diseña controles para minimizar el impacto.

Sin embargo, con demasiada frecuencia las empresas dependen de soluciones antivirus (AV) tradicionales o dejan brechas en áreas críticas como el firmware o la cadena de suministro. Incluso en el sector financiero mundial, altamente regulado ?y altamente atacado?, el 81% todavía depende de la protección AV tradicional. Y las dos principales opciones de seguridad de endpoints utilizadas a nivel mundial son el software antivirus/antimalware tradicional y las soluciones basadas en la nube.3

Los enfoques tradicionales generan:

Falta de preparación ante amenazas de IA
El 90% de las organizaciones no está ?muy seguro? de poder abordar los riesgos de ciberdelincuentes que utilizan IA.4

Brechas expuestas
El 61% de las organizaciones informó una filtración de datos de terceros en los últimos 12 meses.5

Subutilización de la protección con IA
El 77% de las organizaciones prefiere modelos de aprendizaje basados en comportamiento para identificar actividades sospechosas, pero la adopción sigue siendo baja.6

En este whitepaper, exploraremos la protección avanzada en acción y mostraremos cómo las soluciones Lenovo ThinkShield, optimizadas para plataformas Intel®, proporcionan las cuatro capas de seguridad que deben implementarse para proteger a las empresas actuales.

?La IA ha cambiado las reglas del juego. Cuando los atacantes apuntan a su cadena de suministro y firmware con la misma intensidad que a sus aplicaciones y endpoints, no se puede simplemente añadir seguridad y esperar lo mejor. Se necesitan plataformas seguras desde el diseño ?del silicio a la nube? con la IA trabajando a su favor, validando continuamente cada dispositivo, cada identidad y cada conexión durante todo el ciclo de vida.?

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

 © 2026 Lenovo. Todos los derechos reservados.

La respuesta es protección avanzada para todos.

Resultados clave:

Seguridad integral contra ataques en todos los niveles, incluidos ransomware, robo de datos y amenazas maliciosas.

Protección moderna con dispositivos que incorporan IA, análisis basado en comportamiento y capacidades de BIOS con autorrecuperación para proteger los datos.

Protección resiliente con interrupciones minimizadas mediante el diagnóstico y la corrección de problemas de estado de los dispositivos para operaciones más productivas.

La protección de ciberseguridad no funciona por partes. Debe estar en todas partes: desde el diseño del producto hasta el desarrollo de soluciones y servicios de seguridad, extendiéndose a todo el ciclo de vida del producto. Y el software de seguridad debe seguir evolucionando para mantener su eficacia frente a amenazas cibernéticas cada vez más sofisticadas. Se trata de adoptar un enfoque más amplio y profundo que vaya más allá de los endpoints, combinando dispositivos y software líderes del sector.

Hardware seguro desde el diseño en la plataforma Intel vPro®

Lenovo ThinkPad, ThinkStation, ThinkCentre y AI PCs en la plataforma Intel vPro®, con soluciones Lenovo ThinkShield, admiten una arquitectura de seguridad Zero Trust en capas que comienza en el hardware y se extiende al firmware, sistema operativo, aplicaciones y servicios en la nube. Esta combinación reduce la superficie de ataque, refuerza los dispositivos frente a amenazas avanzadas y brinda a TI visibilidad y control continuos en toda la flota.



Lenovo ThinkPad X9 Copilot+ PC con plataforma Intel vPro® y procesador Intel® Core? Ultra 7

Ese es el poder de Lenovo con Intel Inside®



Lenovo ThinkStation P7 con Intel vPro® Platform y procesador Intel® Xeon®

Ese es el poder de Lenovo con Intel Inside®



ThinkCentre X AIO Aura Edition Copilot+ PC con plataforma Intel vPro® y procesador Intel® Core? Ultra 5

Ese es el poder de Lenovo con Intel Inside®

Protección continua durante todo el ciclo de vida del dispositivo

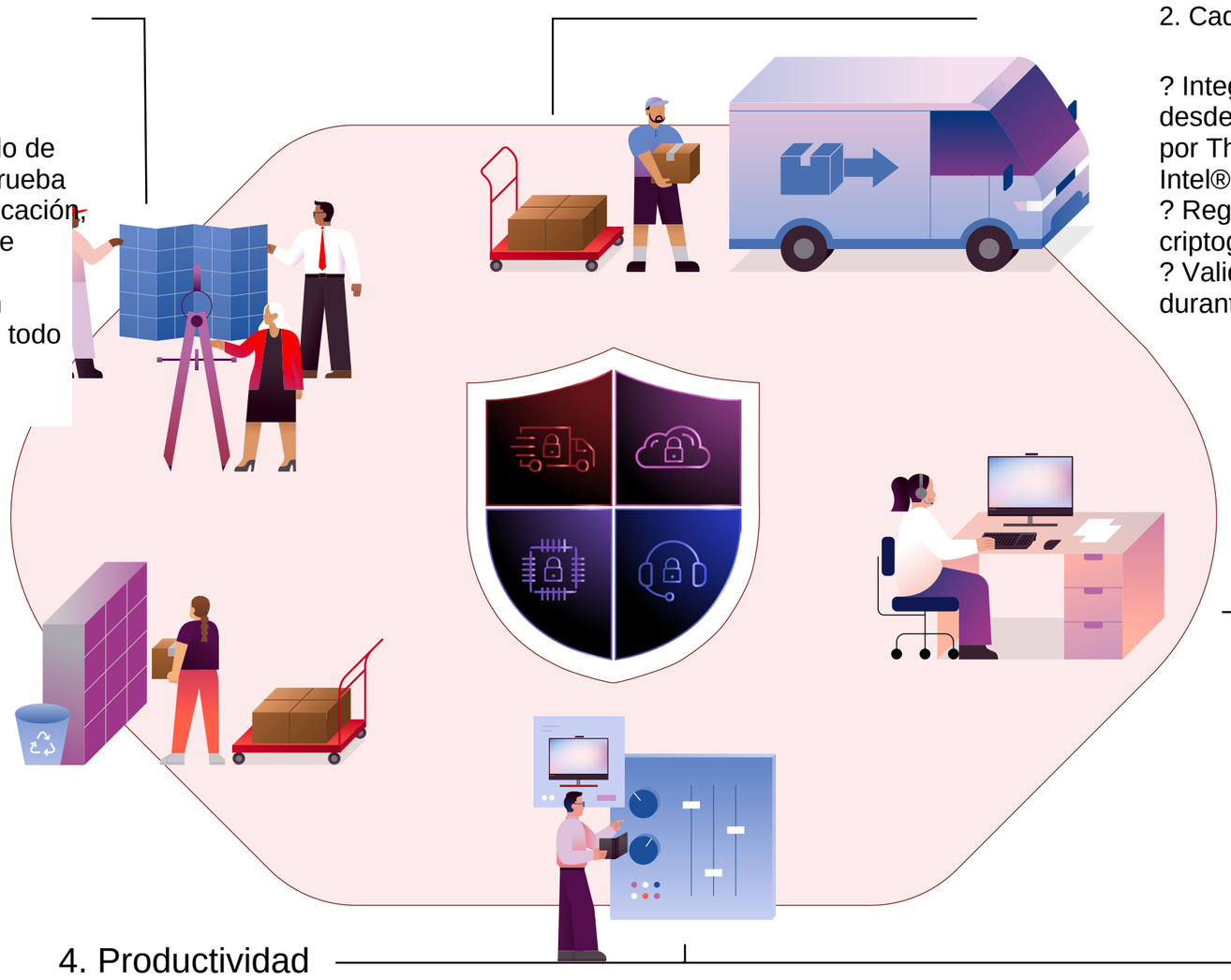
A diferencia de otras ofertas de seguridad, Lenovo ThinkShield se distingue por cubrir todo el ciclo de vida del dispositivo.

1. Diseño y fabricación

? La seguridad se integra desde la concepción del producto hasta la fabricación y las operaciones del ciclo de vida. Los dispositivos cuentan con prueba criptográfica de la integridad de fabricación, registros verificables y trazabilidad de componentes.
? Una base de confianza anclada en hardware habilita Zero Trust durante todo el ciclo de vida del dispositivo.

2. Cadena de suministro

? Integridad verificable del dispositivo desde la fábrica hasta la flota, habilitada por ThinkShield Build Assure, powered by Intel® Transparent Supply Chain.
? Registros de fabricación firmados criptográficamente y listos para auditoría.
? Validación automatizada del dispositivo durante la implementación.



3. Aprovisionamiento

? Línea base confiable desde el primer arranque, con imágenes de BIOS, firmware y sistema operativo previamente validadas.

4. Productividad

? Protección autónoma impulsada por IA en toda la superficie de ataque.
? Protección continua y en capas, del firmware a la nube.
? Integridad persistente del dispositivo con protección de autorrecuperación.
? Visibilidad en tiempo real del estado del dispositivo y la postura de seguridad.
? Respuesta automatizada ante amenazas para reducir el tiempo de permanencia y el impacto.

? Cadena de confianza mantenida durante el uso activo.
? Aplicación centralizada de políticas y control de toda la flota para corregir vulnerabilidades a escala.

5. Fin de vida

(retiro seguro)

? Borrado certificado de datos para eliminar riesgos residuales.
? Sanitización de datos controlada y conforme.
? Retiro simplificado y seguro a escala, incluida la gestión centralizada del borrado de datos, disposición de activos e informes de cumplimiento.

© 2026 Lenovo. Todos los derechos reservados.

Todos los dispositivos seguros desde el inicio



Resultados clave:

Integridad del dispositivo verificada desde la fábrica hasta la implementación.

Riesgo minimizado de componentes manipulados o falsificados y de modificaciones no autorizadas.

Aprobación de cumplimiento y auditoría más rápida.

Base de confianza anclada en hardware para respaldar el aprovisionamiento Zero Trust y la validación del ciclo de vida.

Para la mayoría de las organizaciones, el riesgo comienza mucho antes de que un dispositivo se conecte a la red. A medida que los componentes pasan por distintas manos ?fábricas, centros logísticos, distribuidores y revendedores? se crean puntos ciegos donde la manipulación, las piezas falsificadas o el firmware malicioso pueden vulnerar la seguridad.

Confiar simplemente en el equipo ya no es una opción. Las herramientas de endpoint, sistema operativo y nube no pueden corregir una base comprometida. La propia cadena de suministro debe estar protegida, verificada y ser continuamente auditable, desde la fábrica hasta el primer arranque.

45%

de las organizaciones experimentaron interrupciones del negocio relacionadas con terceros en los dos años anteriores, lo que demuestra que el riesgo de la cadena de suministro es un verdadero problema de resiliencia.7

Soluciones que funcionan, de los líderes del sector

La alianza entre Lenovo e Intel® fortalece la seguridad de la cadena de suministro al combinar soluciones Lenovo ThinkShield con tecnologías Intel®. Proporcionamos confianza a nivel de silicio, validación de la integridad del dispositivo y garantía verificable de la cadena de custodia, desde la fabricación hasta el primer arranque.

ThinkShield Build Assure powered by Intel® Transparent Supply Chain

? Integridad verificada del dispositivo desde la fábrica hasta el primer arranque mediante herramientas automatizadas de verificación y registros firmados y auditables que confirman la autenticidad del dispositivo y la integridad de los componentes desde la fabricación hasta el aprovisionamiento del usuario final.

? Proveedores confiables y cadena de custodia documentada reducen el riesgo de que componentes comprometidos ingresen en la flota.

? Implementación segura y lista para arrancar a escala permite a TI enviar dispositivos directamente a los empleados con una línea base confiable y validada.

? Una postura de cumplimiento y riesgo más sólida combina certificación de integridad, trazabilidad de componentes y detección de manipulaciones, ayudando a cumplir las expectativas regulatorias y reduciendo la superficie general de ataque asociada con la entrega de hardware.

Controles confiables y basados en estándares para la cadena de suministro

? Garantice la procedencia desde el origen de los componentes hasta la distribución, en línea con las directrices de NIST y DFARS sobre detección de falsificaciones y riesgo de la cadena de suministro, utilizando estándares de Trusted Computing Group para la entrega de hardware.

Raíz de confianza de hardware, del silicio al sistema operativo

? Valide el firmware, autentique el hardware y aplique arranque seguro con Intel® Trusted Device Setup y el enfoque de seguridad desde el diseño de Lenovo, garantizando que solo puedan ejecutarse imágenes de firmware firmadas y aprobadas y estableciendo la base para políticas de acceso Zero Trust y certificación a nivel de dispositivo.

Preparado para el ciclo de vida de fuerzas de trabajo distribuidas

? Habilite envío directo seguro y aprovisionamiento remoto para que TI pueda demostrar que un dispositivo es genuino, no ha sido manipulado y cumple las políticas antes de entregarlo a un empleado.

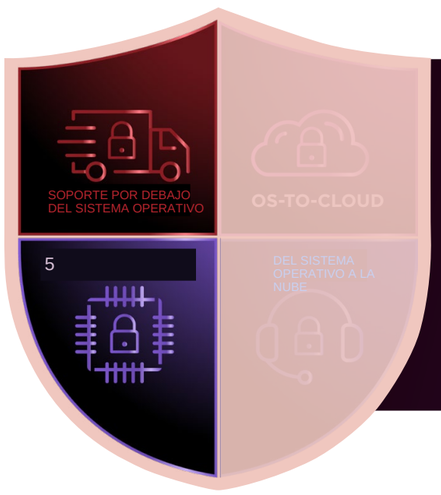
Validación de la integridad de los dispositivos de empleados de Meta

Meta implementa Lenovo ThinkShield Build Assure, powered by Intel® Transparent Supply Chain, para validar la procedencia, seguridad y autenticidad de los dispositivos de sus empleados, al tiempo que reduce la carga de aprovisionamiento de los equipos de TI de Meta.

Read case study

Seguridad integrada, integridad en todos los niveles

Menor superficie de ataque por debajo del sistema operativo.



Resultados clave:

Mejora de 13 a 48 veces en la mitigación de brechas.8

Detección más rápida de ataques sigilosos.

Reduced downtime after compromise.

Menor tiempo de inactividad tras un compromiso.

CADENA DE SUMINISTRO

76%

La mayoría de las soluciones de seguridad de endpoints terminan en el sistema operativo. ThinkShield extiende la protección por debajo de este, donde el firmware se ha convertido en un objetivo principal de ataques persistentes y sigilosos. Cuando se compromete, el firmware puede eludir las protecciones de arranque, deshabilitar herramientas de seguridad y permanecer sin ser detectado durante largos períodos.

Protección del ciclo de vida: por debajo del sistema operativo

Lenovo ThinkShield extiende la protección por debajo del sistema operativo

Desafío de negocio:	Impacto en el negocio:	Resultados con las soluciones Lenovo ThinkShield:
		Imposibilidad de verificar la integridad del firmware en toda la flota ? Postura Zero Trust incompleta ? Exposición a amenazas avanzadas ? Riesgo operativo
? Refuerce la resiliencia, mantenga la continuidad y unifique la visibilidad de riesgos con la seguridad de ciclo de vida ThinkShield y telemetría centralizada.		Actualizaciones de firmware no confiables en toda la flota ? Compromiso persistente ? Riesgo de pérdida de datos ? Interrupción operativa ? Evite la ejecución no autorizada, reduzca el tiempo de inactividad y garantice la confianza con Lenovo Secure boot, confianza anclada en hardware de Lenovo ThinkShield y la plataforma Intel vPro®.
? Verifique las actualizaciones y mejore la capacidad de auditoría con ThinkShield Firmware Assurance.		Punto ciego de firmware ? Largo tiempo de permanencia ? Compromiso oculto ? Aplicación débil de Zero Trust ? Reduzca el tiempo de inactividad y cierre las brechas de visibilidad con ThinkShield Firmware Assurance (telemetría UEFI continua).
? Detecte amenazas ocultas de firmware con ThinkShield Firmware Defense, powered by Eclypsium.		Los ataques al firmware eluden las herramientas de seguridad ? Control persistente del atacante ? Riesgo de interrupción del negocio ? Falla de la pila de seguridad ? Mantenga la continuidad, aplique ejecución confiable y detenga la persistencia sigilosa con confianza anclada en hardware de dispositivos Lenovo seguros desde el diseño e Intel vPro®.
? Exponga ataques fuera de la visibilidad del sistema operativo con ThinkShield Firmware Defense, powered by Eclypsium.	La manipulación física no se detecta por debajo de la capa de monitoreo existente	? Introducción de puertas traseras ? Exposición de cumplimiento ? Mayor riesgo de brecha
? Contenga amenazas rápidamente, reduzca el tiempo de inactividad y demuestre la integridad del dispositivo con detección de manipulación Think UEFI y ThinkShield Firmware Assurance.		Riesgo de hardware no autorizado / ?shadow hardware? ? Superficie de ataque ampliada ? Riesgo de exfiltración de datos ? Dispositivos no confiables en la flota ? Reduzca la superficie de ataque, aplique confianza de hardware y mantenga el control con ThinkShield Hardware Defense, powered by Sepio.
? Valide la integridad de los dispositivos a escala con ThinkShield Security Chip y ThinkShield Firmware Assurance.	Cambios no autorizados de firmware y BIOS fuera de la visibilidad de TI	? Rootkits y malware persistente ? Fallas de auditoría ? Pérdida de integridad
? Acelere auditorías, detecte desviaciones y mantenga la postura de cumplimiento con ThinkShield Firmware Assurance.	Los dispositivos fuera de la red o apagados no pueden gestionarse ni protegerse con herramientas tradicionales	? Pérdida de visibilidad y control del dispositivo ? Incapacidad para aplicar políticas o corregir amenazas ? Mayor riesgo de pérdida de datos, brechas de cumplimiento y dispositivos irrecuperables

de los responsables de decisiones de seguridad de TI del sector financiero tienen brechas de conocimiento sobre el punto ciego de firmware de sus organizaciones.9

Protección más inteligente con IA y Extended Detection and Response (XDR)



Resultados clave:

Aplicación consistente de Zero Trust en fuerzas de trabajo híbridas.

85% de precisión predictiva para fallas comunes de endpoints y TI.10

Datos protegidos, incluso durante brechas.

Ransomware, phishing y apropiación de cuentas son eventos capaces de detener el negocio y ahora se propagan a velocidad de máquina por dispositivos, identidades y aplicaciones en la nube. Las soluciones puntuales de seguridad pueden detectar fragmentos de un ataque sofisticado, pero no pueden ver, prevenir ni corregir toda la cadena, desde los endpoints hasta SaaS.

Al mismo tiempo, los equipos de seguridad sobrecargados enfrentan volúmenes crecientes de alertas y largos tiempos de permanencia. Las brechas pueden tardar semanas o incluso meses en identificarse y contenerse, exponiendo los datos empresariales a nuevos ataques y poniendo al negocio en riesgo de incumplimiento.

Aumento del 37%
en los ataques globales de ransomware en 2025 frente a 2024.11

Lenovo ThinkShield ofrece protección unificada durante todo el ciclo de vida, del endpoint a la nube, para reducir el tiempo de inactividad, acelerar auditorías y mantener la continuidad del negocio.

Desafío de negocio:	Impacto en el negocio:	Resultados con las soluciones Lenovo ThinkShield:
Sin protección unificada del ciclo de vida, del endpoint a la nube ? Brechas entre detección, respuesta y corrección ? Recuperación más lenta y controles inconsistentes ? Riesgo para la continuidad del negocio		? Mantenga la continuidad, unifique la protección y simplifique las operaciones con una plataforma ThinkShield integral, incluidos ThinkShield XDR, powered by SentinelOne, Lenovo Device Orchestration, Absolute Security y una pila de seguridad integrada durante todo el ciclo de vida del dispositivo.
Las herramientas fragmentadas no pueden detectar ni responder durante todo el ciclo de vida del ataque ? Señales de ataque no detectadas ? Largo tiempo de permanencia ? Mayor impacto de la brecha		? Reduzca el tiempo de inactividad y contenga ataques más rápido con ThinkShield XDR para detección impulsada por IA y respuesta automatizada.
Ransomware y malware avanzado eluden las herramientas de seguridad heredadas ? Sistemas cifrados ? Operaciones interrumpidas ? Alto costo de recuperación e impacto en el negocio		? Mantenga las operaciones y minimice las interrupciones con ThinkShield XDR para detección basada en comportamiento y bloqueo autónomo de ransomware.
Dispositivos sin parches y configuraciones inconsistentes en toda la flota ? Gran superficie de ataque ? Brechas de cumplimiento ? Alta carga operativa		? Reduzca la superficie de ataque y automatice el cumplimiento con Lenovo Device Orchestration para actualizaciones centralizadas y corrección basada en políticas.
Los controles de seguridad fallan o se deshabilitan sin visibilidad (sin persistencia) ? Pérdida de cobertura de protección ? Dispositivos operando fuera del control de TI ? Mayor riesgo de cumplimiento		? Mantenga la protección y garantice el cumplimiento continuo con Absolute Security para persistencia anclada en firmware y controles con autorrecuperación.
Datos confidenciales expuestos durante el compromiso de endpoints o eventos de ransomware ? Pérdida o exfiltración de datos ? Sanciones regulatorias ? Interrupción del negocio		? Proteja los datos y reduzca el impacto de las brechas con ThinkShield Data Defense, powered by Cigent, para acceso protegido por MFA, cifrado y bóvedas seguras.
Amenazas originadas por usuarios (phishing, navegación insegura) introducen ataques en el entorno	? Identidades y dispositivos comprometidos ? Mayor volumen de incidentes ? Punto de entrada para ransomware	? Prevenga infecciones y reduzca los puntos de entrada con Threat Isolation, powered by BufferZone, para aislamiento del navegador y documentos.

© 2026 Lenovo. All rights reserved.

Soporte continuo. Siempre activo



Resultados clave:

Cobertura de seguridad 24x7.

80% de los incidentes de bajo nivel resueltos sin intervención de analistas.12

Retiro seguro y conforme de dispositivos.

Seguridad a escala, con más de 180 mercados cubiertos por servicios alineados con las regulaciones.13

Los equipos de TI están bajo presión constante: más herramientas, más alertas, más regulaciones. Y no hay suficiente personal para gestionarlo todo, mucho menos para brindar soporte a los empleados. Entonces, ¿cómo pueden dedicar suficiente atención a la seguridad?

No sorprende que el 83% de los ejecutivos cite las brechas de habilidades como una barrera para mantener una postura segura.14 Cuando ocurren incidentes, los equipos internos pueden verse desbordados por tareas de investigación, respuesta y recuperación. Para mantener la resiliencia, las empresas necesitan un socio confiable que pueda ofrecer cobertura 24x7, servicios orientados a resultados y gestión segura de extremo a extremo del ciclo de vida. Un socio que acompañe desde la implementación y la productividad hasta la reutilización o el reciclaje responsable al final de la vida útil.

52%

de los líderes de TI no se sienten totalmente seguros para abordar los riesgos derivados de la adopción de IA.15

Lenovo ThinkShield Global Support

Lenovo ThinkShield ofrece soporte global 24x7 en 180 mercados y la simplicidad de un único punto de contacto con el proveedor en caso de una brecha de seguridad o necesidad.

Nuestros expertos ayudan a TI a diagnosticar rápidamente los problemas, coordinar respuestas de proveedores y mantener productivos a los usuarios, estén donde estén.

Servicios Managed Protection & Response (MDR) para protección 24x7

? Monitoreo ininterrumpido de amenazas y respuesta a incidentes por parte de Lenovo y nuestro SOC global.

? Los analistas investigan alertas, buscan amenazas y ejecutan acciones de contención.

Soporte adicional

Lenovo Security Services para soporte mejorado con IA

? Servicios de consultoría, implementación y configuración.

? Managed Services continuos para operacionalizar Zero Trust utilizando la plataforma ThinkShield.

Lenovo Asset Recovery Services (ARS) para gestión segura del fin de vida de TI

? Extiende la protección a la etapa final del ciclo de vida del dispositivo.

? Sanitización certificada de datos, certificados de cumplimiento, recolección coordinada e informes ambientales.

© 2026 Lenovo. All rights reserved.

Protección avanzada para todos.

Juntos, Lenovo ThinkShield e Intel® proporcionan las cuatro capas de seguridad necesarias para proteger a las empresas en la era de la IA.



? ROI del 353% con la plataforma SentinelOne Singularity XDR.16

? Implementación sencilla con soporte experto en todo momento.

? Independiente de la marca: ThinkShield protege los dispositivos de toda su flota, independientemente del OEM.

? Diseño de arquitectura flexible con planes adaptados a presupuestos, flotas y necesidades del negocio.

? Consultoría para identificar brechas y recomendar soluciones que las eliminen.

Socios líderes del sector de ThinkShield

Intel®

SentinelOne

Absolute Security

BufferZone®

Sepio

Cigent

Eclypsium

Ivanti

Veeam

8

Acronis

Carbonite

FileWave

CyberArk

Secret Double Octopus

Dynamo AI

Blanco

Churchill & Harriman

© 2026 Lenovo. Todos los derechos reservados.

© 2026 Lenovo. All rights reserved.

WinMagic

Lenovo | intel vPRO



Lenovo | intel vPRO

Ese es el poder de Lenovo con Intel Inside®
Intel vPro® Platform

¿Listo para una protección avanzada?

Proteja la productividad en la era de la IA con soluciones de seguridad empresarial alineadas con los principios de Zero Trust de Lenovo e Intel®.

Comience hoy con Lenovo ThinkShield

1. Statista, Costo estimado del ciberdelito en todo el mundo 2018?2029.
2. Omidia, Cybersecurity Ecosystem Outline 2026, £311 mil millones convertidos a US$ para mantener la consistencia (tipo de cambio 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, datos internos de rendimiento del SOC, 2024.
13. Lenovo, mapeo de cumplimiento y regulación, 2024.
14. Accenture, State of Cybersecurity Resilience, 2025.
15. Lenovo, Work Reborn: Reinforcing the modern workplace, 2025.
16. Forrester Consulting, Total Economic Impact?, 2020.

© 2026 Lenovo. Todos los derechos reservados.