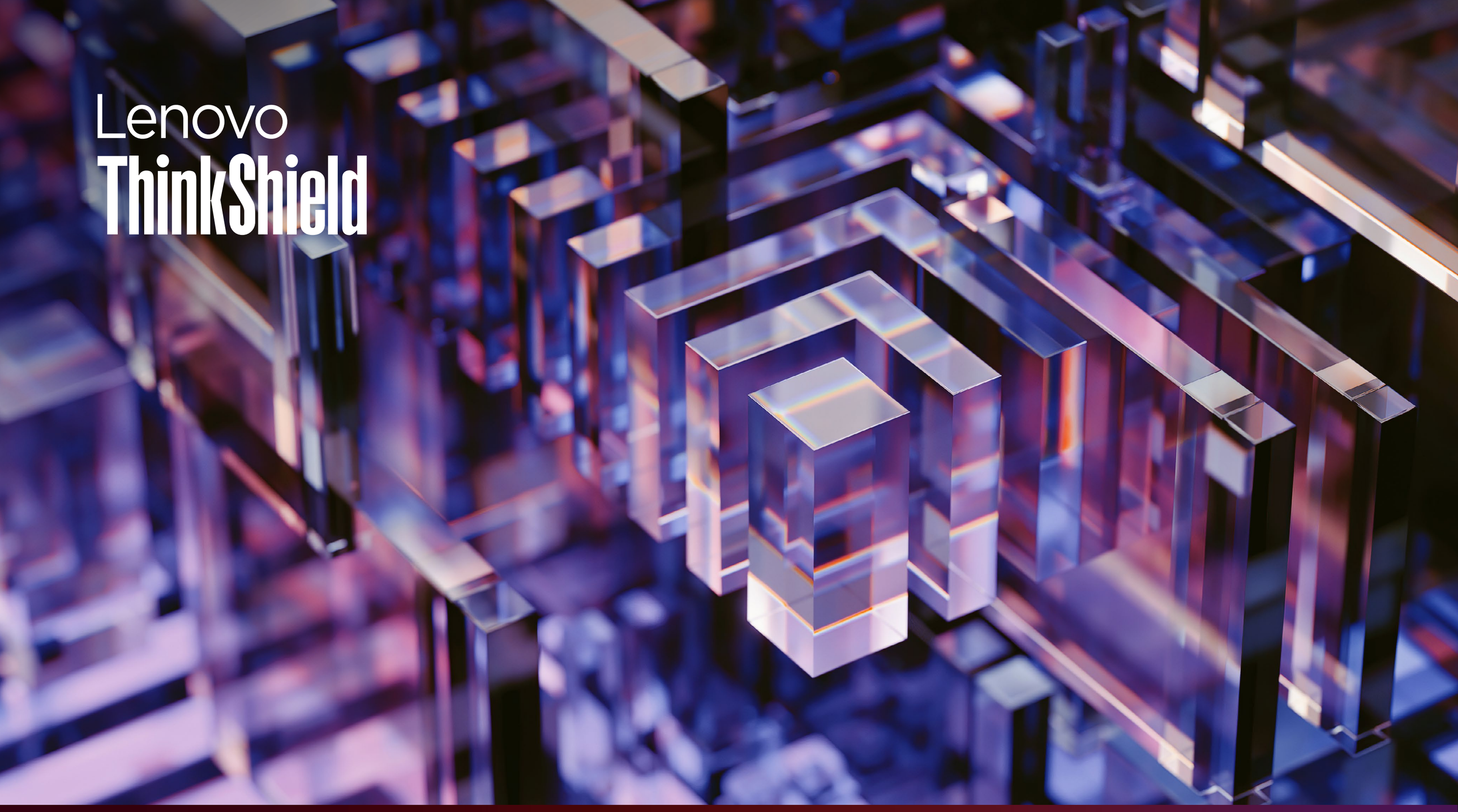


Lenovo | intel vPRO

Esse é o poder da Lenovo com Intel Inside®
Intel vPro® Platform

Proteção avançada em ação

Como implementar segurança empresarial em escala com soluções abrangentes, modernas e resilientes que protegem a produtividade na era da IA.

O novo imperativo de segurança: profundidade e inteligência

Proteger endpoints já não é suficiente. Somente uma segurança em camadas ao longo de todo o ciclo de vida do dispositivo, com arquitetura Zero Trust para enfrentar as ameaças modernas de IA, pode manter as empresas seguras sem comprometer a produtividade.

Principais resultados: o que as empresas precisam na era da IA

Detecção e resposta a ameaças mais rápidas. Redução da superfície de ataque com a aplicação dos princípios de Zero Trust. Maior produtividade por meio da resiliência dos negócios e da minimização do tempo de inatividade.

À medida que as empresas se transformam com a IA, os ganhos de desempenho e produtividade serão enormes. Mas somente se a empresa puder garantir a segurança total do ciclo de vida. Isso significa aplicar os princípios de Zero Trust para validar continuamente usuários, dispositivos e firmware ao longo de todo o ciclo de vida. Muitas empresas, por exemplo, estão migrando para o hardware líder de mercado da Lenovo ? ThinkPad, ThinkStation, ThinkCentre e AI PCs equipados com Intel® ? que são seguros desde a concepção com Lenovo, ThinkShield e a plataforma Lenovo Intel vPro®.

Uma abordagem segura desde a concepção é fundamental diante de ameaças mais sofisticadas impulsionadas por IA, que exploram lacunas de proteção nas empresas. Os invasores usam IA para phishing, geração de malware e reconhecimento ? elevando o custo mundial estimado do cibercrime para US$ 15,63 trilhões até 2029.1 O gasto previsto com cibersegurança somente em 2026 já chega a US$ 418 bilhões, um aumento de 12% em relação ao ano anterior.2

Proteções de ponta a ponta são essenciais

Para combater ameaças que evoluem rapidamente e ultrapassam fronteiras, cada etapa do ciclo de vida do dispositivo deve ser segura, com os princípios de Zero Trust incorporados em toda a jornada. Qualquer lacuna deve ser eliminada no design do dispositivo, na segurança em nível de plataforma, na fabricação e cadeia de suprimentos, no uso do dispositivo, na resposta a incidentes, na segurança de endpoints e no descomissionamento final.

Zero Trust

Zero Trust é uma abordagem de cibersegurança baseada em ?nunca confiar, sempre verificar?. Em vez de presumir que algo dentro de uma rede é seguro, o Zero Trust:

? Trata todos os usuários, dispositivos e aplicativos como não confiáveis por padrão.

? Exige verificação contínua de identidade e autenticação forte.

? Limita o acesso estritamente ao que é necessário (privilégio mínimo).

? Monitora e inspeciona todo o tráfego, independentemente da localização.

? Pressupõe que violações podem e irão acontecer e cria controles para minimizar o impacto.

Porém, com muita frequência, as empresas dependem de soluções antivírus (AV) tradicionais ou deixam lacunas em áreas críticas, como firmware ou cadeia de suprimentos. Mesmo no setor financeiro mundial, altamente regulamentado ? e altamente visado! ? 81% ainda dependem da proteção antivírus tradicional. E as duas principais opções de segurança de endpoint utilizadas globalmente são softwares tradicionais de antivírus/antimalware e soluções baseadas em nuvem.3

As abordagens tradicionais resultam em:

Falta de preparação para ameaças de IA
90% das organizações não estão ?muito confiantes? de que conseguem enfrentar os riscos de cibercriminosos que utilizam IA.4

Lacunas expostas
61% das organizações relataram uma violação de dados de terceiros nos últimos 12 meses.5

Subutilização da proteção por IA
77% das organizações preferem modelos de aprendizado baseados em comportamento para identificar atividades suspeitas, mas a adoção continua baixa.6

Neste whitepaper, exploraremos a proteção avançada em ação, mostrando como as soluções Lenovo ThinkShield, otimizadas para plataformas Intel®, fornecem as quatro camadas de segurança que precisam ser implementadas para proteger as empresas de hoje.

?A IA mudou as regras do jogo. Quando os invasores atacam sua cadeia de suprimentos e seu firmware com a mesma intensidade com que atacam seus aplicativos e endpoints, não é possível simplesmente adicionar segurança e esperar o melhor. São necessárias plataformas seguras desde a concepção ? do silício à nuvem ? com a IA trabalhando a seu favor, validando continuamente cada dispositivo, cada identidade e cada conexão ao longo de todo o ciclo de vida.?

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

 © 2026 Lenovo. Todos os direitos reservados.

A resposta é proteção avançada para todos.

Principais resultados:

Segurança abrangente contra ataques em todos os níveis, incluindo ransomware, roubo de dados e ameaças maliciosas.

Proteção moderna com dispositivos que incorporam IA, análise baseada em comportamento e recursos de BIOS com autorrecuperação para proteger os dados.

Proteção resiliente com interrupções minimizadas por meio do diagnóstico e da correção de problemas de integridade dos dispositivos, proporcionando operações mais produtivas.

A proteção de cibersegurança não funciona em partes. Ela precisa estar em todos os lugares ? desde o design do produto até o desenvolvimento de soluções e serviços de segurança, estendendo-se por todo o ciclo de vida do produto. E o software de segurança precisa continuar evoluindo para permanecer eficaz contra ameaças cibernéticas cada vez mais sofisticadas. É necessário adotar uma abordagem mais ampla e profunda, que vá além dos endpoints, combinando dispositivos e softwares líderes do setor.

Hardware seguro desde a concepção na plataforma Intel vPro®

Lenovo ThinkPad, ThinkStation, ThinkCentre e AI PCs na plataforma Intel vPro®, com soluções Lenovo ThinkShield, oferecem suporte a uma arquitetura de segurança Zero Trust em camadas, que começa no hardware e se estende pelo firmware, sistema operacional, aplicativos e serviços em nuvem. Essa combinação reduz a superfície de ataque, fortalece os dispositivos contra ameaças avançadas e oferece à TI visibilidade e controle contínuos sobre toda a frota.



Lenovo ThinkPad X9 Copilot+ PC com plataforma Intel vPro® e processador Intel® Core? Ultra 7

Esse é o poder da Lenovo com Intel Inside®



Lenovo ThinkStation P7 com Intel vPro® Platform e processador Intel® Xeon®

Esse é o poder da Lenovo com Intel Inside®



ThinkCentre X AIO Aura Edition Copilot+ PC com plataforma Intel vPro® e processador Intel® Core? Ultra 5

Esse é o poder da Lenovo com Intel Inside®

Proteção contínua em todo o ciclo de vida do dispositivo

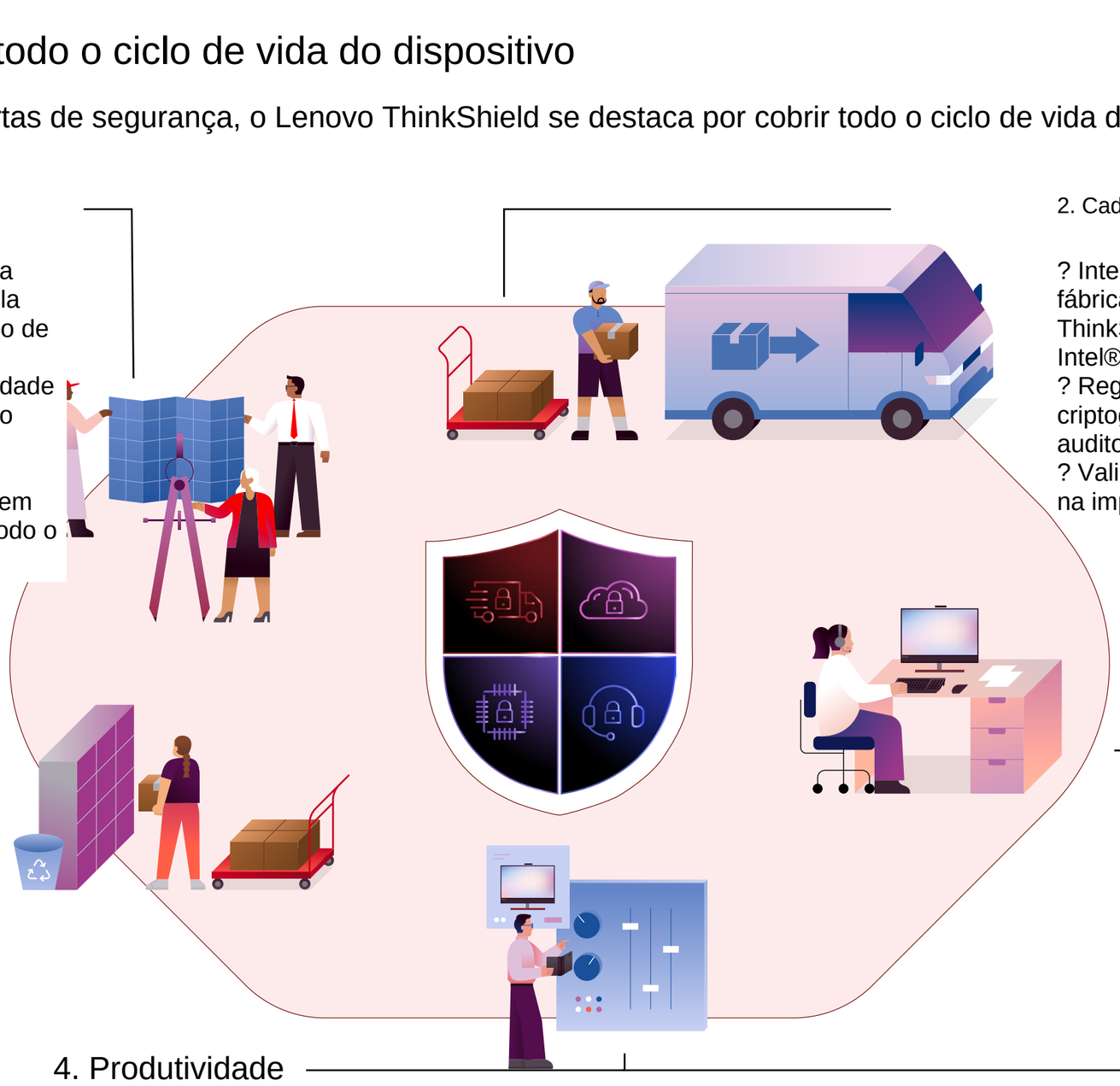
Diferentemente de outras ofertas de segurança, o Lenovo ThinkShield se destaca por cobrir todo o ciclo de vida do dispositivo.

1. Design e fabricação

? A segurança é incorporada desde a concepção do produto, passando pela fabricação e pelas operações do ciclo de vida. Os dispositivos contam com comprovação criptográfica da integridade da fabricação, registros de fabricação verificáveis e rastreabilidade de componentes.
? Uma base de confiança ancorada em hardware viabiliza o Zero Trust em todo o ciclo de vida do dispositivo.

2. Cadeia de suprimentos

? Integridade verificável do dispositivo, da fábrica à frota, viabilizada pelo ThinkShield Build Assure, powered by Intel® Transparent Supply Chain.
? Registros de fabricação assinados criptograficamente e prontos para auditoria.
? Validação automatizada do dispositivo na implantação.



3. Provisionamento

? Linha de base confiável desde a primeira inicialização, com imagens de BIOS, firmware e sistema operacional pré-validadas.

4. Produtividade

? Proteção autônoma baseada em IA em toda a superfície de ataque.
? Proteção contínua e em camadas, do firmware à nuvem.
? Integridade persistente do dispositivo com proteção de autorrecuperação.
? Visibilidade em tempo real da integridade do dispositivo e da postura de segurança.
? Resposta automatizada a ameaças para reduzir o tempo de permanência e o impacto.

? Cadeia de confiança mantida durante o uso ativo.
? Aplicação centralizada de políticas e controle de toda a frota para corrigir vulnerabilidades em escala.

5. Fim da vida útil

(descomissionamento seguro)

? Apagamento certificado de dados para eliminar riscos residuais.
? Sanitização de dados controlada e em conformidade.
? Desativação simplificada e segura em escala, incluindo gerenciamento centralizado de apagamento de dados, destinação de ativos e relatórios de conformidade.

© 2026 Lenovo. Todos os direitos reservados.

Todos os dispositivos seguros desde o início



Principais resultados:

Integridade do dispositivo verificada da fábrica à implantação.

Risco minimizado de componentes adulterados ou falsificados e de modificações não autorizadas.

Aprovação de conformidade e auditoria mais rápida.

Base de confiança ancorada em hardware para oferecer suporte ao provisionamento Zero Trust e à validação do ciclo de vida.

Para a maioria das organizações, o risco começa muito antes de um dispositivo se conectar à rede. À medida que os componentes passam por diferentes mãos ? fábricas, centros logísticos, distribuidores e revendedores ? surgem pontos cegos em que adulterações, peças falsificadas ou firmware malicioso podem comprometer a segurança.

Confiar simplesmente no equipamento já não é uma opção. Ferramentas de endpoint, sistema operacional e nuvem não conseguem corrigir uma base comprometida. A própria cadeia de suprimentos deve ser protegida, verificada e continuamente auditável, do chão de fábrica à primeira inicialização.

45%

das organizações enfrentaram interrupções nos negócios relacionadas a terceiros nos dois anos anteriores ? mostrando que o risco da cadeia de suprimentos é uma questão real de resiliência.7

Soluções que funcionam, dos líderes do setor

A parceria entre Lenovo e Intel® fortalece a segurança da cadeia de suprimentos ao combinar soluções Lenovo ThinkShield com tecnologias Intel®. Oferecemos confiança em nível de silício, validação da integridade do dispositivo e garantia verificável da cadeia de custódia, da fabricação à primeira inicialização.

ThinkShield Build Assure powered by Intel® Transparent Supply Chain

? Integridade verificada do dispositivo da fábrica à primeira inicialização, com ferramentas automatizadas de verificação e registros assinados e auditáveis que confirmam a autenticidade do dispositivo e a integridade dos componentes, da fabricação ao provisionamento do usuário final.

? Fornecedores confiáveis e cadeia de custódia documentada reduzem o risco de componentes comprometidos entrarem na frota.

? Implantação segura e pronta para inicialização em escala permite que a TI envie dispositivos diretamente aos funcionários com uma linha de base confiável e validada.

? Postura de conformidade e risco mais robusta combina atestado de integridade, rastreabilidade de componentes e detecção de adulteração, ajudando a atender às expectativas regulatórias e reduzindo a superfície geral de ataque associada à entrega de hardware.

Controles confiáveis e baseados em padrões para a cadeia de suprimentos

? Garanta a procedência desde a origem dos componentes até a distribuição, alinhada às orientações do NIST e DFARS sobre detecção de falsificações e risco da cadeia de suprimentos, utilizando padrões do Trusted Computing Group para entrega de hardware.

Raiz de confiança de hardware, do silício ao sistema operacional

? Valide o firmware, autentique o hardware e aplique inicialização segura com Intel® Trusted Device Setup e a abordagem de segurança desde a concepção da Lenovo, garantindo que apenas imagens de firmware assinadas e aprovadas possam ser executadas e estabelecendo a base para políticas de acesso Zero Trust e atestado em nível de dispositivo.

Preparado para o ciclo de vida de equipes distribuídas

? Habilite envio direto seguro e provisionamento remoto para que a TI possa comprovar que um dispositivo é genuíno, não foi adulterado e está em conformidade com as políticas antes de entregá-lo a um funcionário.

Validando a integridade dos dispositivos dos funcionários da Meta

A Meta implementa o Lenovo ThinkShield Build Assure, powered by Intel® Transparent Supply Chain, para validar a procedência, a segurança e a autenticidade dos dispositivos dos funcionários, reduzindo ao mesmo tempo a carga de provisionamento das equipes de TI da Meta.

Read case study

Segurança incorporada, integridade em todos os níveis

Menor superfície de ataque abaixo do sistema operacional.



Principais resultados:

Melhoria de 13 a 48 vezes na mitigação de violações.8

Detecção mais rápida de ataques furtivos.

Reduced downtime after compromise.

Menor tempo de inatividade após comprometimento.

CADEIA DE SUPRIMENTOS

76%

A maioria das soluções de segurança de endpoint termina no sistema operacional. O ThinkShield estende a proteção para abaixo dele, onde o firmware se tornou um alvo importante de ataques persistentes e furtivos. Quando comprometido, o firmware pode contornar proteções de inicialização, desabilitar ferramentas de segurança e permanecer sem detecção por longos períodos.

Proteção do ciclo de vida: abaixo do sistema operacional

Desafio de negócio:	Impacto no negócio:	Resultados com as soluções Lenovo ThinkShield:
		Lenovo ThinkShield estende a proteção para abaixo do sistema operacional
		Impossibilidade de verificar a integridade do firmware em toda a frota ? Postura Zero Trust incompleta ? Exposição a ameaças avançadas ? Risco operacional
? Fortaleça a resiliência, mantenha a continuidade e unifique a visibilidade de riscos com a segurança de ciclo de vida ThinkShield e telemetria centralizada.		Atualizações de firmware não confiáveis em toda a frota ? Comprometimento persistente ? Risco de perda de dados ? Interrupção operacional ? Impeça a execução não autorizada, reduza o tempo de inatividade e garanta confiança com Lenovo Secure boot, confiança ancorada em hardware do Lenovo ThinkShield e plataforma Intel vPro®.
? Verifique atualizações e melhore a capacidade de auditoria com ThinkShield Firmware Assurance.		Ponto cego de firmware ? Longo tempo de permanência ? Comprometimento oculto ? Aplicação fraca de Zero Trust ? Reduza o tempo de inatividade e elimine lacunas de visibilidade com ThinkShield Firmware Assurance (telemetria UEFI contínua).
? Detecte ameaças ocultas de firmware com ThinkShield Firmware Defense, powered by Eclypsium.		Ataques ao firmware contornam as ferramentas de segurança ? Controle persistente do invasor ? Risco de interrupção dos negócios ? Falha da pilha de segurança ? Mantenha a continuidade, aplique execução confiável e interrompa a persistência furtiva com confiança ancorada em hardware dos dispositivos Lenovo seguros desde a concepção e Intel vPro®.
? Exponha ataques fora da visibilidade do sistema operacional com ThinkShield Firmware Defense, powered by Eclypsium.	Adulterações físicas não são detectadas abaixo da camada de monitoramento existente	? Backdoors introduzidos ? Exposição de conformidade ? Maior risco de violação
? Contenha ameaças rapidamente, reduza o tempo de inatividade e comprove a integridade do dispositivo com detecção de adulteração Think UEFI e ThinkShield Firmware Assurance.		Risco de hardware não autorizado / ?shadow hardware? ? Superfície de ataque ampliada ? Risco de exfiltração de dados ? Dispositivos não confiáveis na frota ? Reduza a superfície de ataque, aplique confiança de hardware e mantenha o controle com ThinkShield Hardware Defense, powered by Sepio.
? Valide a integridade dos dispositivos em escala com ThinkShield Security Chip e ThinkShield Firmware Assurance.	Alterações não autorizadas de firmware e BIOS fora da visibilidade da TI	? Rootkits e malware persistente ? Falhas de auditoria ? Perda de integridade
? Acelere auditorias, detecte desvios e mantenha a postura de conformidade com ThinkShield Firmware Assurance.	Dispositivos fora da rede ou desligados não podem ser gerenciados ou protegidos por ferramentas tradicionais	? Perda de visibilidade e controle do dispositivo ? Incapacidade de aplicar políticas ou corrigir ameaças ? Maior risco de perda de dados, lacunas de conformidade e dispositivos irrecuperáveis

dos tomadores de decisão de segurança de TI do setor financeiro têm lacunas de conhecimento sobre o ponto cego de firmware de suas organizações.9

Lenovo | intel vPRO

Proteção mais inteligente com IA e Extended Detection and Response (XDR)



Principais resultados:

Aplicação consistente de Zero Trust em forças de trabalho híbridas.

85% de precisão preditiva para falhas comuns de endpoint e TI.10

Dados protegidos, mesmo durante violações.

Ransomware, phishing e tomada de contas são eventos capazes de paralisar os negócios e agora se propagam em velocidade de máquina por dispositivos, identidades e aplicativos em nuvem. Soluções pontuais de segurança podem identificar fragmentos de um ataque sofisticado, mas não conseguem visualizar, prevenir ou corrigir toda a cadeia, dos endpoints ao SaaS.

Ao mesmo tempo, equipes de segurança sobrecarregadas enfrentam volumes crescentes de alertas e longos tempos de permanência. Violações podem levar semanas ou até meses para serem identificadas e contidas, expondo os dados corporativos a novos ataques e colocando a empresa em risco de falhas de conformidade.

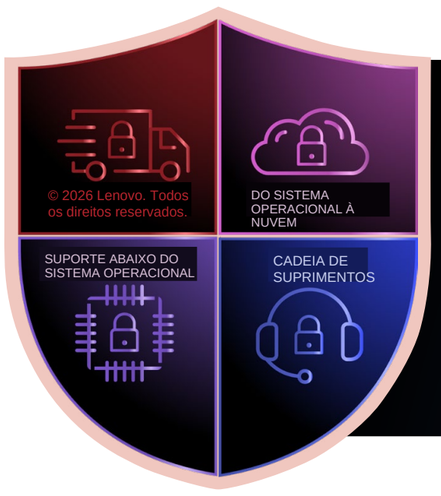
Aumento de 37%
nos ataques globais de ransomware em 2025 em comparação com 2024.11

Lenovo ThinkShield oferece proteção unificada ao longo do ciclo de vida, do endpoint à nuvem, para reduzir o tempo de inatividade, acelerar auditorias e manter a continuidade dos negócios.

Desafio de negócio:	Impacto no negócio:	Resultados com as soluções Lenovo ThinkShield:
Ausência de proteção unificada do ciclo de vida, do endpoint à nuvem ? Lacunas entre detecção, resposta e correção ? Recuperação mais lenta e controles inconsistentes ? Risco à continuidade dos negócios		? Mantenha a continuidade, unifique a proteção e simplifique as operações com uma plataforma ThinkShield abrangente, incluindo ThinkShield XDR, powered by SentinelOne, Lenovo Device Orchestration, Absolute Security e uma pilha de segurança integrada em todo o ciclo de vida do dispositivo.
Ferramentas fragmentadas não conseguem detectar e responder em todo o ciclo de vida do ataque ? Sinais de ataque não detectados ? Longo tempo de permanência ? Maior impacto da violação		? Reduza o tempo de inatividade e contenha ataques mais rapidamente com ThinkShield XDR para detecção orientada por IA e resposta automatizada.
Ransomware e malware avançado contornam ferramentas de segurança legadas ? Sistemas criptografados ? Operações interrompidas ? Alto custo de recuperação e impacto nos negócios		? Mantenha as operações e minimize interrupções com ThinkShield XDR para detecção comportamental e bloqueio autônomo de ransomware.
Dispositivos sem patches e configurações inconsistentes em toda a frota ? Grande superfície de ataque ? Lacunas de conformidade ? Alta sobrecarga operacional		? Reduza a superfície de ataque e automatize a conformidade com Lenovo Device Orchestration para atualizações centralizadas e correção baseada em políticas.
Controles de segurança falham ou são desabilitados sem visibilidade (sem persistência) ? Perda de cobertura de proteção ? Dispositivos operando fora do controle da TI ? Maior risco de conformidade		? Mantenha a proteção e garanta conformidade contínua com Absolute Security para persistência ancorada em firmware e controles com autorrecuperação.
Dados confidenciais expostos durante comprometimento de endpoint ou eventos de ransomware ? Perda ou exfiltração de dados ? Penalidades regulatórias ? Interrupção dos negócios		? Proteja os dados e reduza o impacto de violações com ThinkShield Data Defense, powered by Cigent, para acesso protegido por MFA, criptografia e cofres seguros.
Ameaças causadas por usuários (phishing, navegação insegura) introduzem ataques no ambiente	? Identidades e dispositivos comprometidos ? Maior volume de incidentes ? Ponto de entrada para ransomware	? Evite infecções e reduza os pontos de entrada com Threat Isolation, powered by BufferZone, para isolamento de navegador e documentos.

© 2026 Lenovo. All rights reserved.

Suporte contínuo. Sempre ativo



Principais resultados:

Cobertura de segurança 24x7.

80% dos incidentes de baixo nível resolvidos sem intervenção de analistas.12

Desativação de dispositivos segura e em conformidade.

Segurança em escala, com mais de 180 mercados cobertos por serviços alinhados às regulamentações.13

As equipes de TI estão sob pressão constante: mais ferramentas, mais alertas, mais regulamentações. E não há profissionais suficientes para gerenciar tudo isso, muito menos para dar suporte aos funcionários. Então, como dedicar atenção suficiente à segurança?

Não surpreende que 83% dos executivos apontem lacunas de competências como uma barreira para manter uma postura segura.14 Quando ocorrem incidentes, as equipes internas podem ficar sobrecarregadas com tarefas de investigação, resposta e recuperação. Para permanecer resilientes, as empresas precisam de um parceiro confiável que ofereça cobertura 24x7, serviços orientados a resultados e gerenciamento seguro de ponta a ponta do ciclo de vida. Um parceiro que atue desde a implantação e produtividade até a reutilização ou reciclagem responsável no fim da vida útil.

52%

dos líderes de TI não se sentem totalmente confiantes para enfrentar os riscos decorrentes da adoção de IA.15

Lenovo ThinkShield Global Support

Lenovo ThinkShield oferece suporte global 24x7 em 180 mercados e a simplicidade de um único ponto de contato com o fornecedor em caso de violação de segurança ou necessidade.

Nossos especialistas ajudam a TI a diagnosticar problemas rapidamente, coordenar respostas de fornecedores e manter os usuários produtivos, onde quer que estejam.

Serviços Managed Protection & Response (MDR) para proteção 24x7

? Monitoramento ininterrupto de ameaças e resposta a incidentes pela Lenovo e por nosso SOC global.

? Analistas investigam alertas, buscam ameaças e executam ações de contenção.

Suporte adicional

Lenovo Security Services para suporte aprimorado por IA

? Serviços de consultoria, implementação e configuração.

? Managed Services contínuos para operacionalizar Zero Trust usando a plataforma ThinkShield.

Lenovo Asset Recovery Services (ARS) para gerenciamento seguro do fim da vida útil de TI

? Estende a proteção à etapa final do ciclo de vida do dispositivo.

? Sanitização certificada de dados, certificados de conformidade, coleta coordenada e relatórios ambientais.

© 2026 Lenovo. All rights reserved.

Proteção avançada para todos.

Juntos, Lenovo ThinkShield e Intel® fornecem as quatro camadas de segurança necessárias para proteger as empresas na era da IA.



? ROI de 353% com a plataforma SentinelOne Singularity XDR.16

? Implementação simples com suporte especializado em todas as etapas.

? Independente de marca: ThinkShield protege os dispositivos de toda a sua frota, independentemente do OEM.

? Design de arquitetura flexível com planos adaptados a orçamentos, frotas e necessidades de negócio.

? Consultoria para identificar lacunas e recomendar soluções que as eliminem.

Parceiros líderes do setor do ThinkShield

Intel®

Sentinel One
Absolute Security
BufferZone®
Sepio
Cigent
Eclypsium
Ivanti
Veeam
8

Acronis
Carbonite
FileWave
CyberArk
Secret Double Octopus
Dynamo AI
Blanco
Churchill & Harriman

© 2026 Lenovo. Todos os direitos reservados.

© 2026 Lenovo. All rights reserved.



Lenovo | intel vPRO

Esse é o poder da Lenovo com Intel Inside®
Intel vPro® Platform

Pronto para uma proteção avançada?

Proteja a produtividade na era da IA com soluções de segurança empresarial alinhadas aos princípios de Zero Trust da Lenovo e Intel®.

Comece hoje mesmo com Lenovo ThinkShield

1. Statista, Custo estimado do cibercrime em todo o mundo 2018?2029.
2. Omidia, Cybersecurity Ecosystem Outline 2026, £311 bilhões convertidos para US$ para fins de consistência (taxa de câmbio 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, dados internos de desempenho do SOC, 2024.
13. Lenovo, mapeamento de conformidade e regulamentação, 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 os direitos reservados.