Confía en tu seguridad. Confía en tu gente. Con Lenovo.

Cómo brindar protección a tu fuerza de trabajo en un entorno de seguridad cibernética en evolución

Smarter technology for all

Lenovo

El movimiento irrevocable hacia el trabajo híbrido ha creado un entorno de seguridad cibernética desafiante.

Hoy en día, la mayoría de los trabajadores necesitan estar equipados para el trabajo híbrido. Como resultado, la protección contra amenazas debe extenderse a múltiples nubes y diferentes plataformas.

Esto crea un entorno digital complejo que puede convertirse en un puerto oculto de amenazas desconocidas. Aplicar las políticas de seguridad en todos los dispositivos y diferentes capas digitales resulta ser una tarea realmente abrumadora. Sin duda, estas tareas conllevan noches de insomnio para quienes se encargan de brindar protección.

La ecuación hardware y nube seguros es una asociación única: Lenovo se ha unido a Microsoft en una asociación única, una en la que el hardware con tecnología ThinkShield se suma a los servicios de seguridad en la nube de Microsoft.

Seguridad por diseño con Lenovo ThinkShield

En Lenovo entendemos la necesidad urgente de proporcionar una protección integral. Estamos impulsando nuestro enfoque de seguridad ThinkShield para aumentar la seguridad de nuestra cartera de dispositivos por diseño mientras tenemos en cuenta la protección de las mejores prácticas.

Esto abarca desde la protección de las cadenas de suministro hasta el desarrollo de nuevos productos Lenovo que son seguros y están diseñados por los fabricantes de los PC comerciales más fiables del mundo.

Nuestra exclusiva cartera ThinkShield de hardware, servicios, software y procesos ofrece protección y llega a todos los niveles de la empresa. Nuestras asociaciones con proveedores de seguridad líderes en la industria permiten defensas radicales que encapsulan, retienen e impulsan una estrategia Zero Trust impulsada por las soluciones de seguridad de Microsoft.

Zero Trust. El futuro de la ciberprotección. Una nueva dirección.

El enfoque Zero Trust se desvía bastante de la seguridad de red tradicional en la que hay un «perímetro corporativo» o dispositivos conectados a través de una VPN, lo cual es la norma general hoy en día.

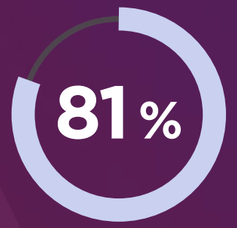
Los principios rectores de Zero Trust son: «No confíes nunca. Verifica siempre».

En el mundo actual de trabajo híbrido no debemos confiar en los dispositivos de forma predeterminada, ni siquiera si están conectados a una red «autorizada».

Zero Trust asume que un atacante está dentro de la red. La confianza se establece en función del **contexto**, como la **identidad y la ubicación del usuario, el estado de seguridad del dispositivo** y la **aplicación o el servicio que se solicita**. Hay controles de política en cada paso.

Esto garantiza que solo **las personas adecuadas con los recursos apropiados en dispositivos seguros puedan acceder a tus datos**.

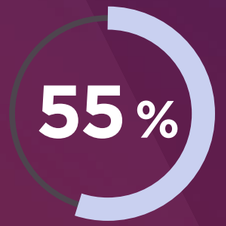
Nunca había sido tan urgente contar con una estrategia Zero Trust:



El 81 % de las empresas han iniciado el cambio hacia el trabajo híbrido[1]

El riesgo por infracción de datos se ha reducido en un 50 %[3]

Hubo un aumento del **1070 %** en ransomware entre julio de 2020 y junio de 2021[4]



El 55 % de las organizaciones afirman que han detectado un ataque de suplantación de identidad en los últimos 18 meses[2]

Las llamadas realizadas al equipo de IT y a los analistas del servicio de asistencia se ha reducido en un 50 %[3]

El tiempo de gestión debido a la mejora de los procesos de seguridad ha disminuido en un 50 %[3]

La cartera de productos de Lenovo ThinkShield y las soluciones de seguridad de Microsoft han sido diseñadas específicamente y con un propósito para ayudarte a implementar una **estrategia Zero Trust integral** y proteger tu negocio en todos los niveles.

[1] Microsoft Zero Trust Adoption Report, 2021
[2] IBM Cost of a Data Breach Report 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, December 2021. Study by Forrester Consulting, commissioned by Microsoft.
[4] 1H Global Threat Landscape Report from FortiGuard Labs

La arquitectura Zero Trust se define de esta manera.

El concepto Zero Trust se extiende a muchas partes de IT, pero la protección comienza con los dispositivos modernos de Windows 11, las identidades de los usuarios y la supervisión de dispositivos terminales.

Mejora y asegura la experiencia del trabajo híbrido de tus empleados con dispositivos Lenovo Windows 11 Pro

Windows 11 Pro, el Windows más seguro hasta el momento, te ayuda a **optimizar la gestión** de tu lugar de trabajo híbrido mientras **proteges los datos y el acceso** desde cualquier lugar.

Diseñado para dispositivos modernos optimizados para la seguridad, te brinda las últimas ventajas en cuanto a **protección basada en hardware**, estrechamente integrada con el software. Windows 11 Pro está diseñado específicamente para el **trabajo híbrido seguro** con una **base de seguridad más alta que Windows 10**. Esto incluye nuevos requisitos de protección, integrados y habilitados de forma predeterminada.

ThinkPad X1 Carbon

Mejora la seguridad de tu dispositivo Lenovo Windows 11 Pro ThinkShield con gestión en la nube

Proteger las identidades y los dispositivos terminales es el primer paso fundamental para establecer una estrategia Zero Trust. Las identidades y los dispositivos son las dos áreas principales atacadas por ladrones de credenciales de identidad, correos electrónicos de suplantación de identidad, ransomware, otros tipos de malware y amenazas avanzadas.

Combina los dispositivos Windows 11 de Lenovo con las soluciones de seguridad en la nube de Microsoft para implementar una estrategia Zero Trust.

Gestión de identidades

- Habilita la autenticación multifactor (MFA), que puede detener el 99,9 % de los ataques de identidad.
- Ofrece un motor de política «inteligente» de acceso condicional que te permite establecer reglas específicas para el «inicio de sesión» de los usuarios. En combinación con MFA, permite un equilibrio sólido entre la seguridad y la productividad de los usuarios.

Gestión de terminales

- Asegúrate de que las aplicaciones cumplan con los protocolos de seguridad de tu empresa mediante Mobile Access Management (MAM).
- Asegúrate de que los dispositivos cumplan con los protocolos de seguridad de tu empresa mediante Mobile Device Management (MDM), ya sea en los propios dispositivos de la empresa o mediante BYOD.

Controla, protege y gestiona con las ventajas de las soluciones de seguridad en la nube

Gestión de identidades con Azure Active Directory

- Azure Active Directory es un servicio de gestión de accesos e identidades basado en la nube simple y eficiente que proporciona autenticación multifactor y acceso condicional.
- Combina servicios de directorio básicos, gestión de accesos a aplicaciones y protección de identidades en una única solución.
- Ayuda a tus empleados a acceder de forma segura a recursos externos, como Microsoft 365, Azure Portal y miles de otras aplicaciones SaaS.
- Protege los recursos internos, como una intranet y aplicaciones en la nube desarrolladas por tu organización.

Microsoft Defender for Endpoint

Esta solución de seguridad para terminales basada en la nube líder en el sector se caracteriza por lo siguiente:

- Ayuda a proteger contra ransomware, malware sin archivos y otros ataques sofisticados en Windows, Mac OS, Linux, Android e iOS.
- Detecta amenazas ocultas, ya que supervisa continuamente y en tiempo real el comportamiento del código y las técnicas del atacante, lo que da paso a una detección y respuesta rápidas.
- Respuesta y reparación automática de incidentes 24/7, lo cual ayuda a los equipos de seguridad a pasar inmediatamente de las alertas a la reparación impulsada por IA.
- Servicio gestionado de búsqueda de amenazas de la mano de expertos de Microsoft «bajo demanda».

Microsoft Endpoint Manager

Reúne la gestión y la seguridad de los dispositivos terminales en una plataforma de gestión unificada:

- Protege, implementa y gestiona todos los usuarios, aplicaciones y dispositivos terminales sin interrumpir los procesos de trabajo existentes.
- Ayuda a brindar un lugar de trabajo moderno y una gestión moderna para proteger los datos tanto en la nube como en las instalaciones.
- Combina servicios que quizás ya conozcas y que ya estés utilizando, incluidos Microsoft Intune, Configuration Manager, Desktop Analytics, coadministración y Windows Autopilot.

Dispositivo correcto, lugar adecuado, momento apropiado con la solución de implementación Lenovo Zero Touch

La tecnología segura y moderna es clave para garantizar el éxito de cualquier negocio. Pero el enfoque manual tradicional para la implementación es complejo, requiere mucho tiempo y es propenso a errores.

Ahora existe un modo más sencillo para que tus empleados híbridos y remotos arranquen a toda velocidad: **la implementación Lenovo Zero Touch con Autopilot**.

Impulsará el trabajo híbrido, aumentará la productividad y liberará a tus equipos de IT para que se centren en la innovación que impulsa el negocio.

Con **Windows Autopilot**, los departamentos de IT ya no tendrán que volver a crear un perfil o configurar nuevos dispositivos manualmente. Todo se hace de forma remota. Los dispositivos Lenovo Windows 11 incluyen Autopilot preconfigurado. Los administradores de IT pueden personalizar el usuario y aplicar configuraciones desde cualquier ubicación.

- **Listo desde el primer momento:** el usuario enciende el dispositivo Lenovo y, con unos simples clics, está listo para trabajar.
- **Administración de perfiles sencilla:** crea, administra y asigna hasta 350 perfiles diferentes para determinar la configuración de un usuario y su experiencia con el PC.
- **Transición a la nube sin esfuerzo:** es posible unir dispositivos automáticamente a Azure Active Directory e inscribirlos en la gestión de dispositivos móviles.
- **Aprovisionamiento sin problemas:** configuración personalizada y simplificada.
- **Seguimiento del progreso:** con el uso de Autopilot, los usuarios pueden realizar un seguimiento del progreso de la configuración del dispositivo.
- **Registro de productos:** dispositivos registrados automáticamente en el servicio Autopilot Cloud Deployment.

Adopta un enfoque Better Together

Seguridad al instante

- **Protege lo fundamental** con seguridad asistida por silicio TPM 2.0 y protección de datos e identidad.
- Inicio de sesión más sencillo y seguro con métodos de **autenticación sin contraseña** como Windows Hello para empresas.
- Ayuda a bloquear el software malicioso con **la protección integrada ya habilitada**.
- Para ayudarte a mantener tu **seguridad desde el principio**, Windows 11 evita que el malware se cargue cuando arrancas el dispositivo.
- Protección de datos y redes respaldada por raíz de **confianza basada en hardware** que ayuda a mantener y verificar la integridad del dispositivo.

Protégete contra las amenazas en evolución

- Protege las credenciales con **protección mejorada contra la suplantación de identidad** en Microsoft Defender Smartscreen.
- Inicia sesión sin usar las manos con **detección de presencia**: se inicia cuando te acercas y se bloquea cuando te vas.
- Protege tus datos más confidenciales con **PC de núcleo seguro de Lenovo**.
- Obtén protección de credenciales basada en hardware con **Microsoft Pluton**.
- Aprovecha la **detección inteligente de amenazas y las respuestas rápidas** informadas por 43 billones de señales de seguridad analizadas diariamente.
- El cifrado BitLocker ayuda a proteger la **información de tu empresa**, incluso en dispositivos perdidos o robados.
- Siéntete más **protegido con fuentes no fiables**: abre archivos y sitios web en un contenedor aislado con Microsoft Defender Application Guard.

Gestión moderna de la seguridad

- **Mantén actualizadas las funciones de seguridad** con Windows Update para empresas.
- Habilita la adopción de marcos de **seguridad Zero-Trust**.
- **Garantiza el cumplimiento de las políticas para los empleados in situ y remotos** con Microsoft Endpoint Manager.
- Implementa dispositivos **preconfigurados con políticas de seguridad** corporativas utilizando Windows Autopilot y la implementación Zero Touch.
- Obtén seguridad y visibilidad habilitando el **inicio de sesión único seguro** en todas tus aplicaciones con Azure Active Directory.
- **El diseño basado en la nube facilita la extensibilidad** con Microsoft 365, Microsoft Defender for Cloud y Microsoft Defender for Endpoint.
- Ayuda a **evitar códigos maliciosos** y a protegerte frente a malware y otros softwares no fiables con Windows Defender Application Control.

Lenovo, tu partner de confianza para implementar la estrategia Zero Trust y el trabajo híbrido

¿Por qué elegir Lenovo?

Experiencia, conocimiento, capacidad de solidez empresarial y un equipo exclusivo de expertos que te brindarán soporte en tus adopciones en la nube, definición de políticas de seguridad e implementaciones. Como partner autorizado de las soluciones en la nube (CSP) de Microsoft, Lenovo ofrece la cartera completa de servicios en la nube de Microsoft, incluidos los servicios de Microsoft 365 y Azure.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner y Device Partner of the Year

Lenovo cumple con los estrictos requisitos de Microsoft para ser reconocido como Gold Partner, lo que confirma que Lenovo tiene la experiencia y las capacidades para brindarte soluciones seguras y de alto nivel para tu trabajo remoto.

Además de esto, Lenovo ha recibido el prestigioso premio Microsoft Device Partner of the Year. Este premio reconoce la excelencia en la fabricación, marketing o venta de dispositivos y soluciones de IT que defienden la tecnología basada en Microsoft.

El premio se ha concedido en base al historial de Lenovo en la prestación de soluciones y servicios integrados, de manera consistente, flexible y predecible, para satisfacer la demanda actual de transformación digital de sus clientes y preparar sus negocios para el futuro.

Nuestra estrategia en la nube: todo de un único proveedor

El objetivo de Lenovo es convertirse en una verdadera organización híbrida, capaz de implementar nubes locales, privadas y públicas, que satisfagan las necesidades de almacenamiento, software y soluciones de nuestros clientes. Esto se relaciona con nuestra capacidad de ofrecer hardware, servicios, software, Device-as-a-Service y soporte, todo ello de un solo proveedor.

Así es como hacemos que tu solución de estrategia Zero Trust funcione para tu negocio

Los servicios profesionales y administrados de Lenovo te llevan por el camino hacia una actualización fluida y sin problemas a las defensas Zero Trust.

- Desde el diseño de la solución hasta la incorporación y la migración final, Lenovo cubre todas tus necesidades.
- Si tienes una licencia de Microsoft 365, simplemente actualizamos los dispositivos con Windows 11 y Microsoft 365 e incluimos Azure Active Directory, Microsoft Defender y Endpoint Manager.
- Premier Support: línea directa exclusiva para el usuario, 24/7, los 365 días al año.
- Expertos dedicados: expertos locales preparados para acompañarte en tu cambio hacia un trabajo híbrido seguro.
- Seguridad de nivel empresarial: las mejores defensas de seguridad cibernética que hacen retroceder la marea creciente de malware y ataques dirigidos.

Smarter technology for all

Lenovo

Ponte hoy mismo en contacto con nosotros para descubrir cómo Lenovo puede ayudarte a desarrollar la estrategia de seguridad Zero Trust para tu organización.

Solicita una reunión

Microsoft 365