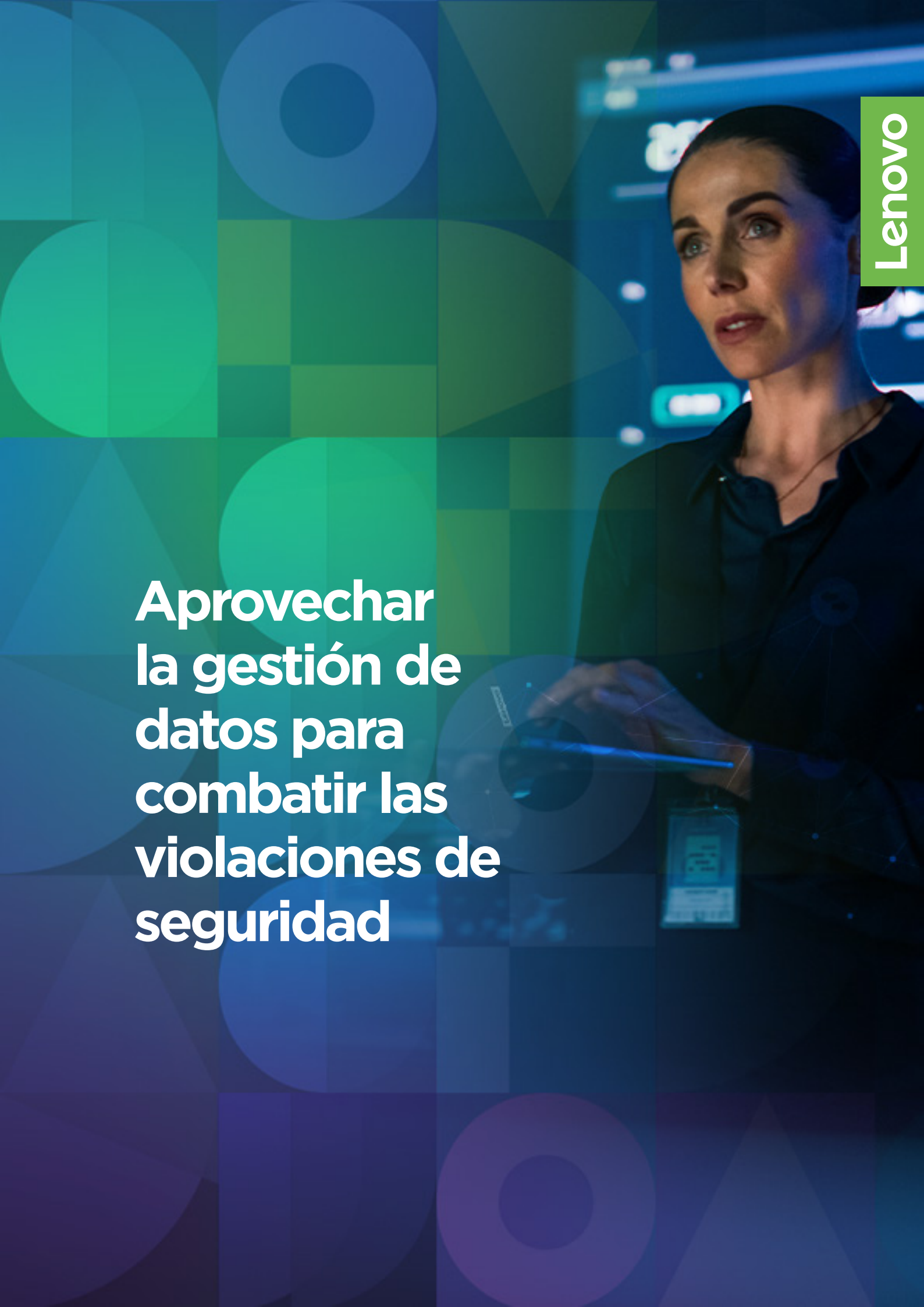
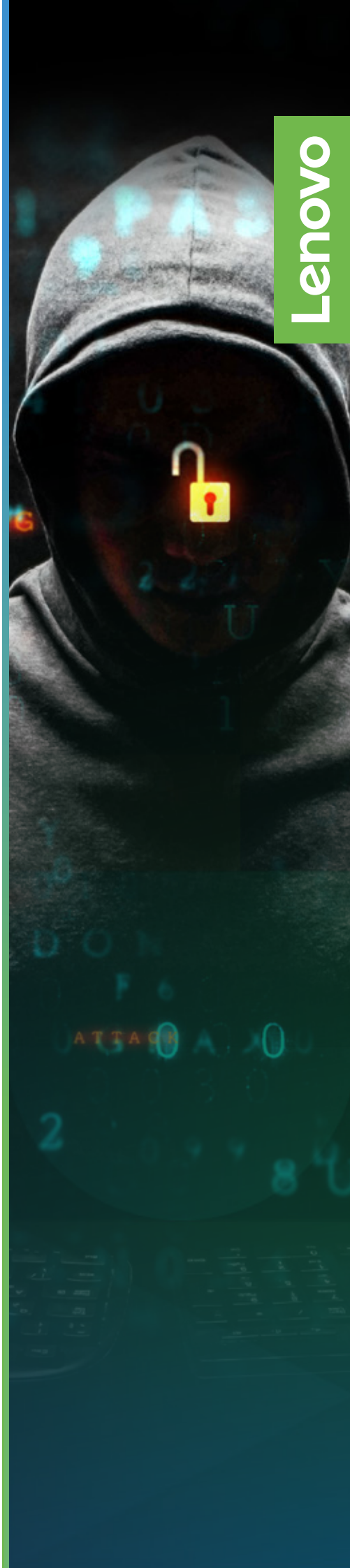


Aprovechar la gestión de datos para combatir las violaciones de seguridad

Las amenazas a la ciberseguridad aumentan a diario, lo que genera problemas operativos, financieros, normativos y de marca incalculables para las organizaciones. El ransomware, el malware, el robo de identidad y otros desafíos de seguridad deben identificarse, prevenirse y remediarse antes de que se produzcan daños importantes y se comprometan los datos críticos.

Este artículo analiza por qué y cómo se debe construir una estructura defensiva basada en la gestión de datos para bloquear las amenazas cibernéticas y proteger a las empresas de la pérdida de datos.

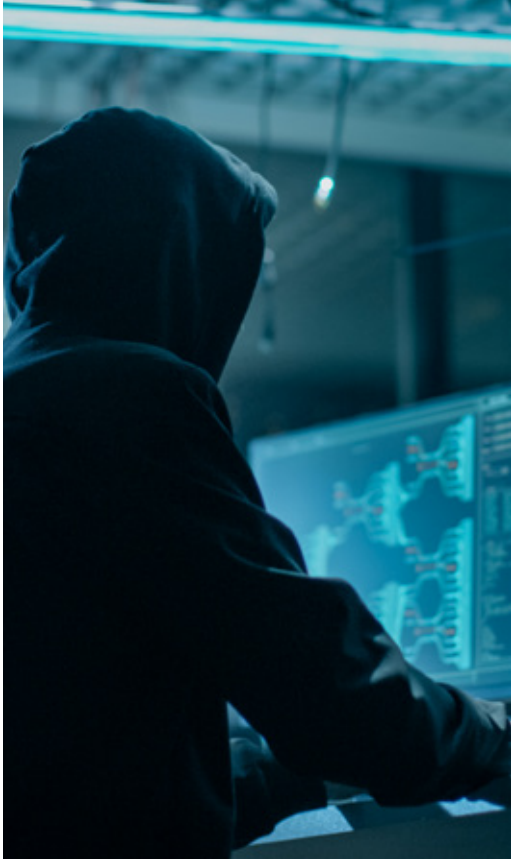


Cada minuto de cada hora de cada día, las organizaciones están sujetas a ataques cibernéticos. De hecho, los hackers atacan en algún lugar del mundo cada 39 segundos. 1La amenaza de ataques cibernéticos, como el ransomware, los ataques de día cero y el malware móvil, crece a un ritmo alarmante a medida que los ciberdelincuentes se vuelven más persistentes e ingeniosos, utilizando los recursos colectivos de otros atacantes y algoritmos de aprendizaje automático.

Para el 2020, el costo promedio de una violación de datos corporativos superará los 150 millones de dólares. 2Sin mencionar los impactos económicos, operativos y de reputación igualmente importantes de las violaciones de cumplimiento causadas por aspectos como el riesgo de la información de identificación personal.

La protección de datos, identidades y otros activos digitales requiere una combinación de técnicas de gestión de datos innovadoras, inteligentes y automatizadas. Las organizaciones también deben insistir en un almacenamiento e infraestructura de computación resilientes y "seguros de fábrica". Este documento analiza lo que las organizaciones pueden y deben hacer para mitigar las amenazas de ciberseguridad y por qué la gestión de datos es un elemento fundamental para enfrentar el malware, las amenazas persistentes avanzadas, el ransomware y otros formatos de ataque. También ofrece algunas sugerencias concretas para asociarse con un aliado de tecnología confiable y comprobado para soluciones de gestión de datos.

1 "15 Alarming Cyber Security Facts and Stats", Cybint Solutions, 23 de septiembre del 2019.
2 "Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024", Juniper Research, 27 de agosto del 2019.



Lo que las empresas deben hacer hoy

Las empresas se han vuelto más ingeniosas en su lucha contra las amenazas de seguridad, que comprometen cientos de miles de millones de dólares al año en todo, desde suscripciones de monitoreo de amenazas y servicios de reparación de violaciones de datos hasta firewalls de última generación y servidores resistentes al malware. Sin embargo, los ataques continúan proliferando, lo que aumenta la presión sobre las organizaciones para reforzar sus esfuerzos de protección de datos desde el núcleo, pasando por el borde, hasta la nube.

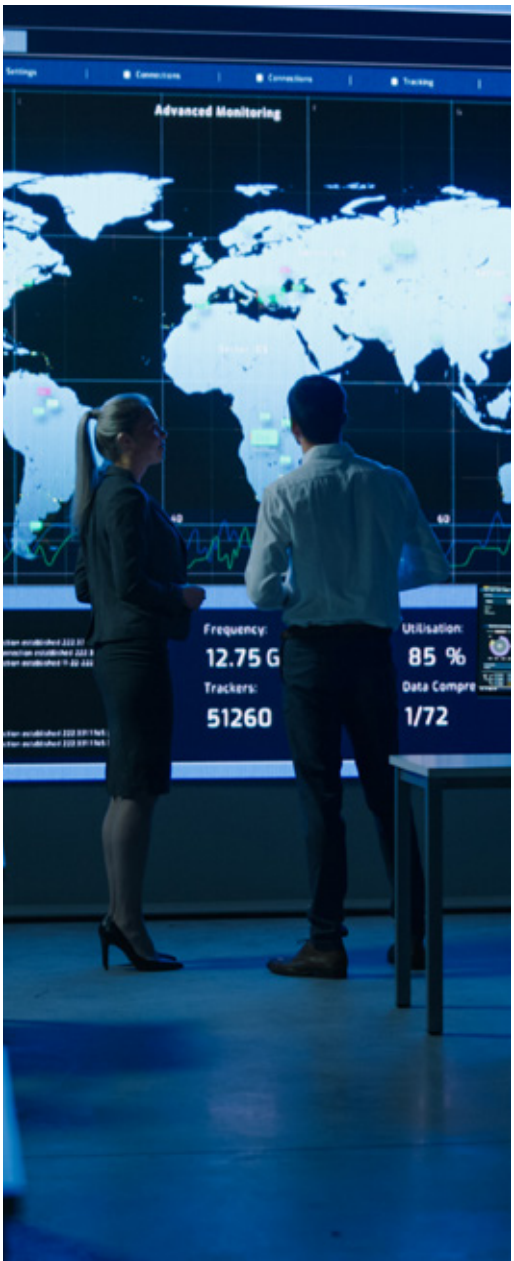
Cuando "hacer lo que siempre se ha hecho" ya no funciona, es hora de usar nuevas ideas, nuevas estrategias y nuevas herramientas.

En el centro de una estructura de ciberseguridad y protección de datos sólida, eficiente y flexible se encuentra la gestión de datos. Hay muchos elementos de una arquitectura de gestión de datos que contribuyen a una postura de ciberseguridad inteligente, automatizada y responsiva. Por ejemplo, la copia de seguridad y el archivo son esenciales para la protección de datos y la restauración de datos rápida y confiable, mientras que las instantáneas (snapshots), la deduplicación y la compresión mejoran la optimización del almacenamiento. La gestión de datos también es fundamental para la continuidad del negocio, la visibilidad de los datos y la auditabilidad para fines de cumplimiento y gobernanza en caso de un ataque. Esto es particularmente cierto en una nube cada vez más híbrida y en un entorno de TI de múltiples nubes, donde los datos a menudo se migran desde las instalaciones a la nube y hacia/desde diferentes sistemas de almacenamiento.

La gestión de datos es una parte inestimable de la detección y mitigación de los ataques de ciberseguridad, y debe ser una parte integral de la infraestructura de TI, como el almacenamiento, para asegurar que la gestión se realice fácilmente, sin mucho monitoreo e intervención manual.

Un líder probado de la industria con experiencia demostrable en la gestión de datos es Lenovo, líder mundial en infraestructura, software y servicios de TI. La amplia línea de recursos de almacenamiento, cómputo, software y servicio/soporte de Lenovo ayuda a las organizaciones a crear una estructura de seguridad integral basada en la gestión de datos de última generación.

La estrategia de defensa de ciberseguridad de Lenovo se construye con base en varios principios fundamentales, incluida la primacía de la gestión de datos para detectar y prevenir automáticamente ataques potencialmente perjudiciales sin tener que depender de un ejército de analistas de seguridad. Las soluciones de almacenamiento y software de Lenovo también se construyen con base en la “seguridad por diseño”, en que los productos y servicios se crean desde cero con la seguridad en el centro, en lugar de incorporarla después de la implementación de la infraestructura y del surgimiento de amenazas.



Cómo la gestión de datos, la infraestructura y el software de Lenovo fortalecen sus defensas

Durante la última década y media, Lenovo ha construido una reputación de liderazgo en infraestructura de TI desde el terminal hasta el data center. Sus desktops, portátiles, servidores y almacenamiento son ampliamente reconocidos por sus requisitos empresariales, como el rendimiento, la escalabilidad, la resiliencia y la seguridad.

Las soluciones de almacenamiento y computación de Lenovo son partes fundamentales de la estructura de defensa de ciberseguridad de una organización. Sus series DM y DE de almacenamiento completamente flash y flash híbrido, combinadas con la línea de servidores ThinkSystem, ayudan a detectar y mitigar el impacto de las violaciones de seguridad en múltiples niveles, que incluyen:

- Autenticación multifactor
- Access points leves
- Monitoreo de cuentas y grupos privilegiados
- Segmentación de red
- Acceso basado en la función
- Cifrado de volumen
- Cifrado agregado
- Limpieza segura
- Cifrado de almacenamiento
- Arranque seguro del Onboard Key Manager

El hardware y el software de almacenamiento de Lenovo detectan y mitigan el impacto de las amenazas cibernéticas en múltiples niveles, que incluyen:

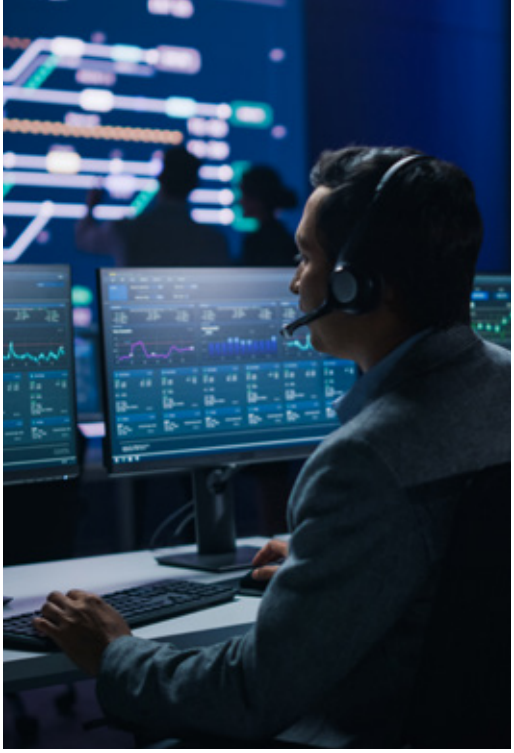
- Generación de instantáneas (snapshots) para garantizar que no se pierdan datos en las principales cargas de trabajo.
- Restauraciones de datos rápidas, simples y confiables.
- Replicación para mover los datos fuera del sitio para reiniciar cargas de trabajo en caso de violación de datos o interrupción del servicio.
- Arquitectura segura por diseño que comienza en el nivel de los componentes en la fábrica.

Las organizaciones están gastando grandes sumas de dinero en herramientas de copia de seguridad, servicios de detección de amenazas, protección contra malware y firewalls de última generación. Sin embargo, si, o cuando, estos pasos fallan, las organizaciones aún deben tener la capacidad de realizar una copia de seguridad completa, confiable y segura de los datos de producción, independientemente de su movimiento o ubicación. Además, los datos de las copias de seguridad deben validarse para garantizar que los administradores de TI y de almacenamiento no inicialicen datos malos.

Además, la seguridad de la infraestructura de almacenamiento de Lenovo se ve reforzada por las sólidas alianzas de la empresa con los principales proveedores de software de almacenamiento de copia de seguridad. Las alianzas de Lenovo ayudan a las organizaciones a resistir el impacto de las violaciones de datos con una implementación de cifrado simple pero potente para proporcionar recursos básicos de copia de seguridad, respaldos validados y pruebas sencillas de los procesos de restauración.

Los arrays de almacenamiento Lenovo DM aprovechan el software de gestión de almacenamiento líder del sector para combatir las amenazas por medio de un cifrado potente, instantáneas y tecnología SnapLock para crear datos no grabables ni borrables en los medios de almacenamiento para evitar que los archivos se modifiquen o se eliminen hasta una fecha de retención predeterminada o estándar.

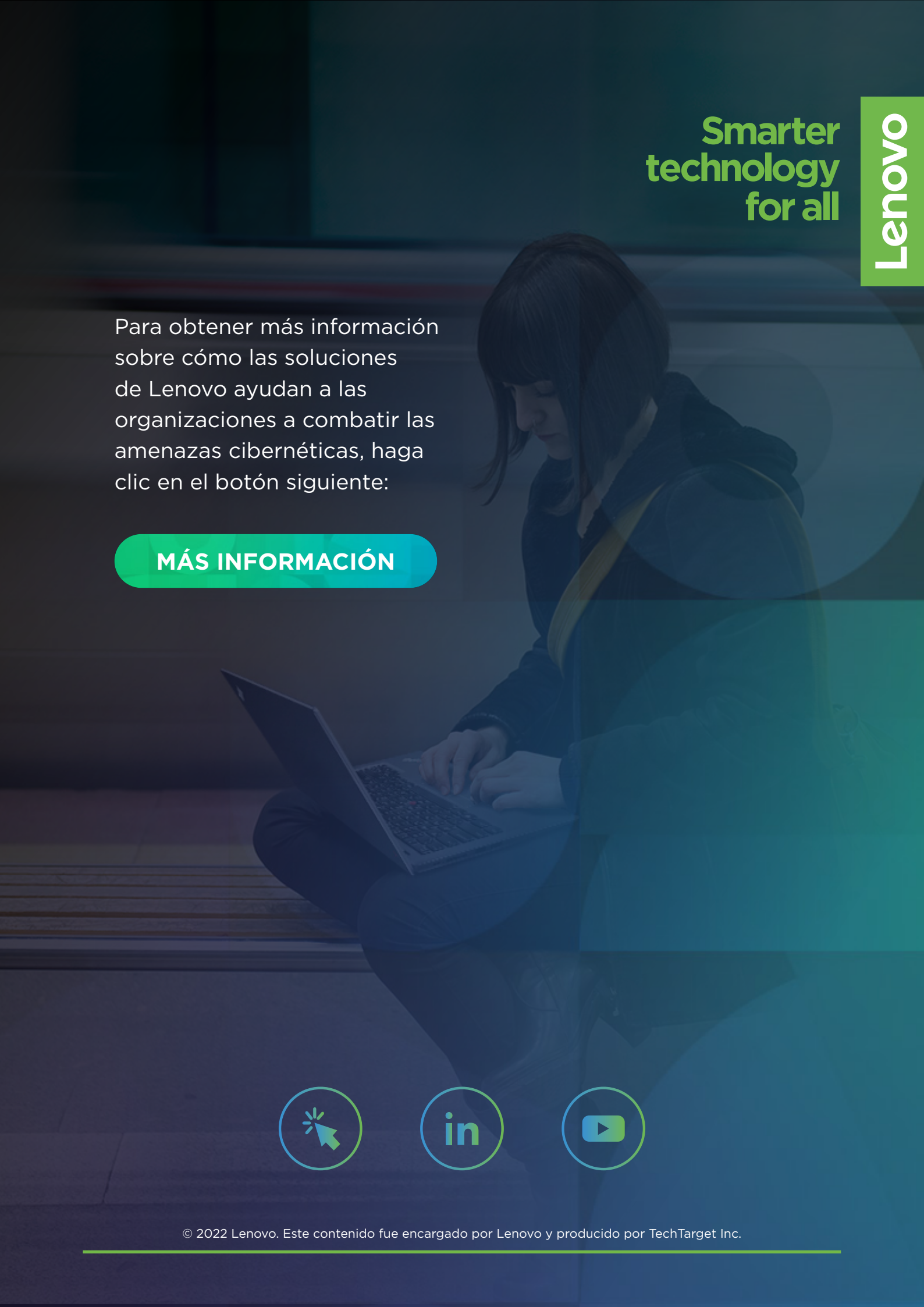
Estas y otras herramientas de seguridad están integradas en las soluciones de almacenamiento de Lenovo desde cero, lo que asegura que las organizaciones puedan aprovechar las ventajas de las defensas comprobadas de inmediato, sin tener que “agregar” herramientas de seguridad.



Conclusión

Los ataques cibernéticos van en aumento y ninguna organización es inmune a ellos. Las empresas de todos los tamaños, geografías y sectores deben abordar las causas fundamentales de los riesgos de ciberseguridad con un enfoque de múltiples capas. El elemento clave para proteger los datos críticos antes de que los hackers puedan penetrar en los sistemas y exfiltrar los datos es una estrategia de gestión de datos bien planificada y bien ejecutada para garantizar que los datos críticos estén siempre disponibles y puedan restaurarse fácilmente si los sistemas están comprometidos.

Las soluciones de infraestructura de almacenamiento de Lenovo han sido diseñadas desde cero para brindar resiliencia, escalabilidad y rendimiento, y para ayudar a las organizaciones a resistir los ataques cibernéticos y mitigar su impacto.



Smarter technology for all

Lenovo

Para obtener más información sobre cómo las soluciones de Lenovo ayudan a las organizaciones a combatir las amenazas cibernéticas, haga clic en el botón siguiente:

MÁS INFORMACIÓN