Proteja y potencie su empresa con Alcatel-Lucent Enterprise

Abordar la creciente complejidad de las amenazas cibernéticas y los requisitos normativos en constante evolución.

Folleto

Alcatel·Lucent
Enterprise

Introducción

A medida que las organizaciones se enfrentan a grandes cambios en sus negocios, la seguridad es uno de los aspectos clave que cambian drásticamente. El auge de las tecnologías de IA ha trastornado los modelos de seguridad tradicionales, lo que obliga a replantearse las prácticas arraigadas.

En respuesta a ello, nuestro equipo de expertos en ciberseguridad en soluciones de red, comunicaciones y nube ha unido fuerzas para compartir información clave sobre los nuevos riesgos a los que se enfrentan las empresas y cómo añadir capas de protección vitales para mantenerse a la vanguardia.

El cambiante panorama de la ciberseguridad

El entorno de la ciberseguridad se define por la rápida evolución de la tecnología, las amenazas más sofisticadas y los cambios de normativas. Los expertos del sector destacan tres tendencias principales que configuran actualmente la ciberseguridad empresarial:

1. El papel de doble filo de la inteligencia artificial
2. El continuo aumento de los ataques de ransomware y a la cadena de suministro
3. La necesidad de una sólida gestión de identidades en arquitecturas de confianza cero

El papel de doble filo de la inteligencia artificial

La IA como arma para los delincuentes

El uso malintencionado de la inteligencia artificial se ha convertido en una de las amenazas más importantes para la seguridad de las empresas. Los ciberdelincuentes aprovechan la IA para automatizar el reconocimiento, elaborar campañas de suplantación de identidad hiperpersonalizadas y desarrollar malware adaptable capaz de eludir los sistemas de detección tradicionales.

Las herramientas basadas en IA analizan los datos disponibles públicamente para perfilar objetivos, generar audio y vídeo ultrafalsos y convincentes y explotar puntos de vulnerabilidad con una precisión quirúrgica. Un ejemplo destacado son los correos electrónicos de suplantación de identidad generados por IA que imitan estilos de comunicación legítimos, aumentando las tasas de éxito en un 40 % en comparación con los métodos tradicionales. Estos ataques se amplifican aun más por la mercantilización de las herramientas de IA, que reduce la barrera de entrada para los delincuentes menos capacitados.

La tecnología deepfake representa una aplicación especialmente insidiosa de la IA, que permite a los actores de amenazas hacerse pasar por directivos o compañeros fiables en videollamadas en tiempo real para autorizar transacciones fraudulentas o revelar información confidencial. En un caso documentado, un vídeo ultrafalso de un director financiero dando instrucciones para una transferencia bancaria provocó una pérdida de 25 millones de dólares a una multinacional. Estos incidentes subrayan la necesidad de protocolos de autenticación avanzados y de formación de los empleados para reconocer los medios sintéticos.

La IA como mecanismo de defensa

Paradójicamente, la IA también constituye la espina dorsal de las defensas de ciberseguridad modernas. Los algoritmos de aprendizaje automático analizan enormes conjuntos de datos para detectar anomalías, predecir vectores de ataque y automatizar la respuesta a incidentes. Por ejemplo, los sistemas de seguridad mejorados con IA pueden identificar vulnerabilidades de día cero reconociendo patrones de comportamiento sutiles en el tráfico de red, reduciendo los tiempos medios de detección de semanas a horas. Gartner afirma que las organizaciones que invierten en plataformas de inteligencia sobre amenazas basadas en IA experimentan un 30 % menos de vulneraciones eficaces en comparación con las que confían en sistemas heredados[1]. Los sistemas basados en inteligencia artificial son especialmente eficaces para identificar amenazas internas, ya que supervisan el comportamiento de los usuarios y señalan patrones de acceso inusuales, lo que resulta cada vez más importante en los entornos de trabajo remotos e híbridos actuales.

Retos normativos y éticos

La naturaleza dual de la IA ha dado lugar a respuestas normativas estrictas. La Ley de IA de la UE, promulgada en febrero de 2025, prohíbe las aplicaciones de IA de alto riesgo en ámbitos como la vigilancia biométrica y exige transparencia en la toma de decisiones algorítmicas. Ahora, las empresas deben realizar auditorías externas de los sistemas de IA, documentar la procedencia de los datos y garantizar un uso ético, una tarea compleja dada la opacidad de muchos modelos de aprendizaje automático. Las organizaciones están estableciendo comités de ética de IA interfuncionales para navegar por este panorama y asociarse con las entidades reguladoras para dar forma a futuros marcos.

Aumento de los ataques de ransomware y a la cadena de suministro

Los proveedores críticos, en el punto de mira

Los ataques de ransomware han pasado de campañas oportunistas a operaciones estratégicas dirigidas a distribuidores y proveedores de servicios críticos. Los ataques de 2024 a CDK Global y Change Healthcare fueron una demostración de cómo la puesta en peligro de un único proveedor puede paralizar sectores enteros, costando miles de millones en interrupciones operativas y trabajos de recuperación. Hoy, los delincuentes se centran cada vez más en los proveedores de software como servicio (SaaS) y en las empresas de infraestructura en la nube, aprovechando su papel centralizado en los ecosistemas empresariales. Por ejemplo, un ataque de ransomware a un importante proveedor de almacenamiento en la nube podría bloquear los datos de miles de empresas simultáneamente, magnificando la capacidad de extorsión.

La proliferación de sistemas interconectados y la insuficiente gestión del riesgo en la cadena de suministro facilitan estos ataques. Muchas empresas carecen de visibilidad de las posturas de seguridad de sus proveedores, lo que las hace vulnerables a fallos en cascada. Gartner informa que el 60 por ciento de las organizaciones se enfrentarán a una importante vulneración de la cadena de suministro antes de 2026, impulsada por vulnerabilidades de terceros en canales de DevOps y flotas de dispositivos IoT[1].

Ecosistemas de ransomware como servicio (RaaS)

El auge de las plataformas de ransomware como servicio ha democratizado el acceso a herramientas de ataque avanzadas, permitiendo incluso a delincuentes de poca monta lanzar campañas sofisticadas. Los operadores de RaaS proporcionan malware personalizable, portales de pago y apoyo a la negociación a cambio de una parte de los rescates, normalmente entre el 20 y el 30 por ciento. Este modelo ha provocado un aumento del 150 % en los incidentes de ransomware desde 2023, con un promedio de demandas de rescate que supera los 5 millones de dólares por incidente.

El ransomware moderno emplea técnicas de ofuscación basadas en la inteligencia artificial, como el código polimórfico y el cifrado diferido para eludir la detección. Los delincuentes también extraen datos antes de implementar el cifrado, amenazando con filtrar información confidencial a menos que se les pague: una táctica conocida como doble extorsión. Las empresas están contrarrestando estas amenazas con copias de seguridad físicamente aisladas, soluciones de almacenamiento descentralizadas y sistemas de verificación de la integridad basados en cadenas de bloques.

Las organizaciones necesitarán una tecnología segura en todos los ámbitos para prevenir, contener y limitar el impacto de los ataques de ransomware y a la cadena de suministro.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Gestión de identidades y el imperativo de la confianza cero

La crisis de identidad de las máquinas

A medida que las empresas adoptan IA generativa, IoT y arquitecturas nativas en la nube, las identidades de las máquinas (credenciales para dispositivos, API y cargas de trabajo automatizadas) han superado a las identidades humanas en volumen y riesgo. En 2025, Gartner identificó las identidades de máquinas no gestionadas como uno de los principales vectores de ataque como uno de los principales vectores de ataque, con claves API y cuentas de servicio comprometidas que permitirán el 45 % de vulneraciones en la nube[1]. Para hacer frente a esto, las empresas están desplegando cada vez más herramientas de gestión de certificados que automatizan una rotación de credenciales más frecuente, reforzando sus políticas de mínimos privilegios para detectar comportamientos anómalos de las máquinas en tiempo real.

Arquitecturas de confianza cero en la práctica

Los marcos de confianza cero, que asumen que ninguna entidad humana o de máquina es intrínsecamente digna de confianza, han pasado de ser objetivos a los que se aspira a convertirse en necesidades operativas. La implementación se centra en la autenticación continua, la microsegmentación y las comunicaciones cifradas. Por ejemplo, una red de confianza cero podría exigir la verificación biométrica para el acceso a datos sensibles, aislar los entornos de desarrollo de los sistemas de producción y cifrar todo el tráfico este-oeste dentro de los centros de datos.

El Instituto Nacional de Normas y Tecnología El NIST informó, en una evaluación de eficacia, que las arquitecturas[2] de confianza cero reducen el impacto de las vulneraciones en un 70 % de media. El éxito radica en la integración de los principios de confianza cero con la infraestructura existente, un reto para las empresas con sistemas heredados. Los enfoques híbridos están ganando terreno, como los perímetros definidos por software para activos locales y las soluciones de confianza cero nativas en la nube.

Factores humanos y amenazas internas

Según el Foro Económico Mundial, el 95 % de los incidentes de ciberseguridad se deben a errores humanos. Los ataques de suplantación de identidad que aprovechan el contenido generado por IA sortean los filtros de correo electrónico con una eficacia de más del 30 % en comparación con los métodos tradicionales, mientras que los empleados que exponen involuntariamente credenciales en herramientas colaborativas representan el 25 % de las infracciones. Las amenazas internas se ven exacerbadas por los errores de configuración del acceso manual a la red y el trabajo a distancia, donde los dispositivos personales y las redes no seguras crean puntos de entrada para los delincuentes.

Se ha convertido en algo fundamental ayudar a los usuarios a protegerse mejor al tiempo que se alivia la carga de unas políticas de seguridad cada vez más restrictivas. Para los administradores de redes y aplicaciones, la automatización de las operaciones y la asistencia activa mediante IA deben proporcionar las herramientas necesarias para protegerse de las consecuencias de posibles errores de configuración.

El enfoque de ALE para proteger las comunicaciones y los productos de red

El enfoque de Alcatel-Lucent Enterprise respecto de la seguridad garantiza que las interacciones digitales sean efectivas y cumplan las normas estándar de la industria. La tecnología digital está muy extendida, con la creciente adopción de dispositivos de IA e IoT que recopilan datos para respaldar las alertas en tiempo real y la planificación futura. Proteger y reforzar las redes y comunicaciones que impulsan las empresas de hoy en día es vital para evitar interrupciones del servicio. Las soluciones ALE para comunicaciones empresariales e infraestructura de red implementan la ciberseguridad de extremo a extremo porque es la única forma de garantizar la aplicación íntegra de la seguridad. Este enfoque de la ciberseguridad ayuda a empresas e instituciones públicas a:

- Prevenir los ciberataques implementando la ciberseguridad en cada aspecto del diseño del producto para reducir la superficie de ataque
- Protegerse contra los ciberataques aplicando las últimas normas de seguridad y las mejores prácticas en todos los componentes de la solución para aumentar la resistencia
- Reaccionar ante los ciberataques posibilitando medidas rápidas y adecuadas para limitar el impacto y mejorar la resistencia, en caso de que se produzca un ataque

Como fabricante de productos basados en hardware y software, el enfoque de ciberseguridad de ALE se centra en las áreas descritas a continuación para abordar los potenciales puntos de vulnerabilidad en el panorama de las ciberamenazas.

1. Segura por diseño

Históricamente, los diseños de soluciones principalmente se guiaban por la necesidad de nuevas funciones, y la seguridad era una cuestión esencial, pero secundaria. Con la evolución del panorama, las prioridades tradicionales del diseño se han invertido. Los requisitos de ciberseguridad deben impulsar ahora los diseños de las soluciones. Las soluciones de hardware y software seguras por diseño tienen en cuenta la seguridad en cada paso de la definición, el desarrollo y la entrega del producto. Todo el hardware y los sistemas operativos están reforzados, la protección contra la denegación de servicio (DoS) está integrada, y las soluciones aplican las mejores prácticas de ciberseguridad más importantes para el sector.

2. Seguridad con acceso a la red de confianza cero

Las estrategias de seguridad que ofrecen confianza en función de la ubicación del usuario dentro del cortafuegos de la empresa, las credenciales que introduce o la aplicación o el dispositivo que utiliza ya no son adecuadas, ni siquiera cuando se combinan varios mecanismos de seguridad. En la actualidad, ningún usuario, dispositivo o aplicación debe tener confianza implícita El modelo de seguridad con acceso a la red de confianza cero (ZTNA) ayuda a las organizaciones a contrarrestar eficazmente las amenazas en constante evolución. El modelo ZTNA no confía en ningún usuario, dispositivo o aplicación, independientemente de su ubicación. ALE refuerza el modelo ZTNA permitiendo la aplicación de políticas basadas en funciones, el control (Administrador de autenticación de políticas unificadas integrado - UPAM) de acceso en función de la ubicación y la segmentación dinámica entre usuarios, dispositivos y aplicaciones (por defecto con Shortest Path Bridging-SPB, User Network Profiles-UNP), ya sean gestionados o no.

3. Macro y microsegmentación

La macrosegmentación y la microsegmentación permiten un enfoque granular y altamente controlado de la ciberseguridad para todos los usuarios, dispositivos y aplicaciones que acceden a la red. La macrosegmentación segrega a los usuarios, dispositivos y aplicaciones según su dominio funcional para que no puedan comunicarse con los elementos de otros macrosegmentos. Por ejemplo, las aplicaciones de comunicaciones unificadas y colaboración de un macrosegmento no pueden comunicarse con tecnologías de seguridad, como cámaras de CCTV y sistemas de cierre de puertas, de otro macrosegmento, ni con los sensores y controles de iluminación, calefacción y aire acondicionado de un tercer macrosegmento.

La microsegmentación define el modo en que usuarios, dispositivos y aplicaciones de un macrosegmento pueden interactuar entre sí, y suele regirse por políticas de seguridad específicas. Por ejemplo, no debe permitirse que una cámara de vigilancia interactúe con una cerradura de puerta, aunque se encuentren en el mismo macrosegmento relacionado con la seguridad.

4. Cifrado de extremo a extremo

En las organizaciones modernas, los empleados, clientes, partners y proveedores pueden estar en cualquier parte del mundo. Y las soluciones que utilizan para comunicarse y colaborar pueden estar instaladas en el edificio desde el que trabajan, al otro lado de la ciudad o en un centro de datos al otro lado del mundo. En todos los casos, las personas deben poder intercambiar información de forma segura y confidencial mediante voz, vídeo y texto. Para garantizar que solo los participantes en la conversación puedan acceder a la información que se intercambia, cada conversación debe estar totalmente cifrada de origen a destino. Eso significa que todos los elementos de hardware y software que intervienen en las comunicaciones de extremo a extremo deben llevar incorporados de forma nativa mecanismos de cifrado aprobados por los organismos de seguridad.

5. Certificaciones de seguridad y privacidad y cumplimiento de normativas

Hace unos años, las certificaciones y acreditaciones de seguridad más estrictas sólo se exigían para productos de seguridad, como cortafuegos, o para industrias, como la defensa. Hoy en día, las normas específicas de seguridad deben aplicarse a todos los productos tecnológicos en todos los sectores. Es fundamental verificar que las certificaciones y acreditaciones reconocidas respaldan las solicitudes de ciberseguridad.

He aquí algunos ejemplos del cumplimiento normativo que debe buscarse:

- Normas mundiales en materia de seguridad y privacidad, como ISO 27001
- Normas de seguridad y privacidad específicas del sector, como la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA) en EE. UU. y Hébergeurs de Données de Santé HDS, relativa al alojamiento de datos sanitarios en Francia
- Normativas regionales de seguridad y privacidad, como el Reglamento general de protección de datos (RGPD) y la Directiva NIS 2 de la Unión Europea

6. Pruebas de seguridad continuas y especializadas

Al igual que las normas de seguridad, los procesos especializados de pruebas de seguridad que antes se reservaban a los productos de seguridad son ahora obligatorios en las soluciones de comunicaciones unificadas y colaboración. Las pruebas de penetración son un buen ejemplo. Estas pruebas simulan ciberataques para revelar vulnerabilidades de seguridad, de modo que puedan abordarse de forma proactiva antes de que surjan problemas. Para anticiparse a las ciberamenazas en un panorama en constante evolución, deben realizarse continuamente pruebas de penetración basadas únicamente en los requisitos de ciberseguridad. Los proveedores de tecnología dedicados a ayudar a sus clientes a mantener la máxima ciberseguridad deben proporcionar los recursos, herramientas y conocimientos necesarios para realizar pruebas de penetración continuas.

7. Soberanía de los datos

La soberanía de los datos se ha convertido en una preocupación importante para la mayoría de las empresas que deben proteger su propiedad intelectual, preservar la confianza de los clientes y garantizar una ventaja competitiva. Con la adopción de nuevas tecnologías como la nube y, más recientemente, la IA, la apertura de los sistemas de comunicaciones de las organizaciones al mundo exterior nunca ha sido tan importante, y la seguridad del acceso a la red es igual de crítica. Algunas empresas optarán por una solución de nube pública que satisfaga sus necesidades y limite la superficie de ataque interna de su sistema de información. Otras optarán por un enfoque más tradicional, con aplicaciones de comunicaciones unificadas alojadas en su red privada, ya sea en las instalaciones o en una nube privada específica. Sea cual sea la elección del cliente, ALE puede ofrecer sus productos y servicios en todos los contextos de implementación para garantizar la soberanía sobre los datos críticos.

8. Automatización de la seguridad y las operaciones inteligentes

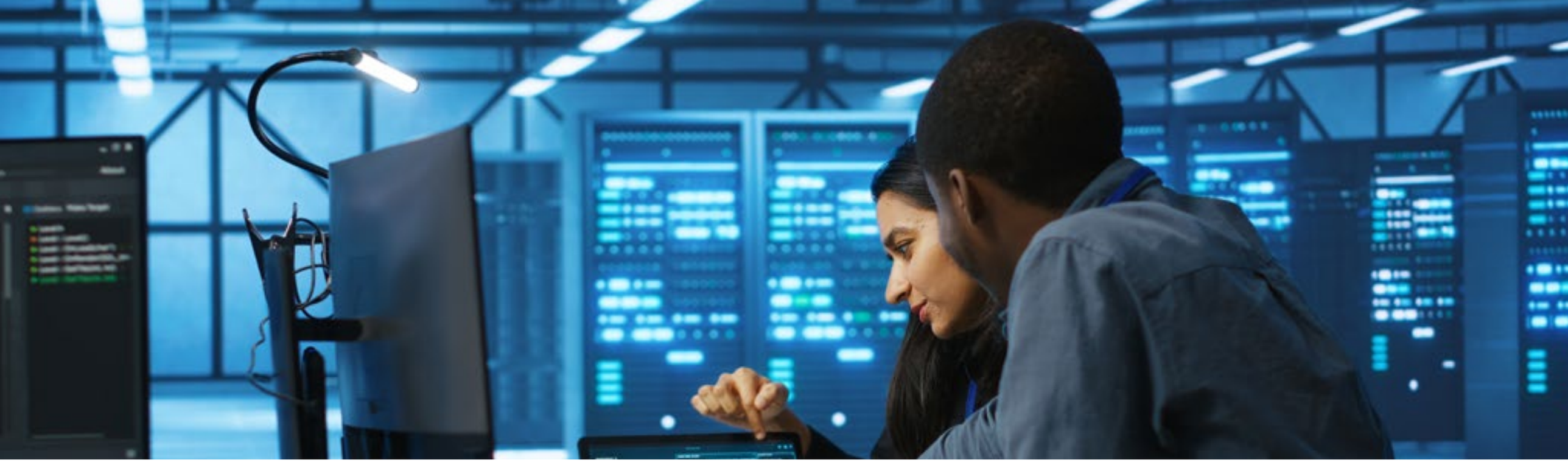
El paquete OmniVista y Network Advisor de ALE introducen una seguridad operativa avanzada mediante la supervisión en tiempo real, las auditorías de configuración y la automatización de la respuesta a las amenazas. Con la AIOps integrada, las anomalías de la red se detectan de forma proactiva y se facilitan correcciones guiadas, que a menudo requieren un solo clic para resolver los problemas de calidad de la experiencia (QoE) o de conformidad normativa. Esto reduce los errores humanos, acelera la respuesta ante incidentes y garantiza el cumplimiento de las políticas en entornos complejos.

9. Conectividad segura en cualquier lugar

ALE admite SD-WAN seguras para empresas distribuidas y trabajo remoto, combinando visibilidad de red, seguridad y optimización del rendimiento, ajustándose así a los modernos modelos de trabajo desde cualquier lugar. Con el cifrado MACsec, la integridad y confidencialidad de los datos se preservan en entornos WAN multisitio.

10. Una cadena de suministro de software fiable

ALE aplica medidas rigurosas para proteger su cadena de suministro de software, como las imágenes de firmware firmadas, los procesos de arranque seguros, los sistemas operativos reforzados y la validación independiente del código fuente. Estas prácticas limitan la exposición a las amenazas basadas en software y garantizan entornos de implementación fiables.



Por qué ALE es su proveedor fiable para proteger su infraestructura de red y su plataforma de comunicaciones empresariales

Aunque muchos proveedores de tecnología hacen hincapié en la ciberseguridad, no todos cuentan con los conocimientos exhaustivos necesarios para implantar la seguridad de extremo a extremo. Alcatel-Lucent Enterprise va más allá que otros proveedores a la hora de implantar todas las mejores prácticas necesarias para la ciberseguridad de extremo a extremo.

Nos comprometemos a:

- Seguir las mejores prácticas y recomendaciones del Instituto Nacional de Ciencia y Tecnología (NIST) a la hora de realizar evaluaciones de riesgos sobre nuevas funciones y de implantar funciones de ciberseguridad, como el cifrado nativo, en nuestros productos
- Aplicar las normas ISO 27001 a todas nuestras soluciones
- Admitir el modelo ZTNA, segmentación granular de la red y políticas de seguridad concretas para reducir el riesgo de actividades no autorizadas
- Ejecutar pruebas específicas de seguridad altamente especializadas, como pruebas de penetración, en todos nuestros productos
- Garantizar que nuestros productos obtienen las certificaciones clave del sector, como HDS, HIPAA, la Ley de Derechos Educativos y Privacidad Familia (FERPA) y FIPS 140-2 en relación con la administración pública y la defensa
- Tener en cuenta las certificaciones regionales para nuestros productos, como CSPN de ANSSI en Francia, ENS en España, C5 en Alemania y ANATEL en Brasil
- Cumplir las normativas regionales sobre seguridad y privacidad, como el RGPD, CRA y la Directiva NIS 2 de la Unión Europea

Como expertos reconocidos en ciberseguridad, contribuimos a las propuestas de directivas sobre ciberseguridad de la Unión Europea. También aprovechamos nuestra experiencia para ayudar a nuestros clientes a elegir e implantar con el TCO más bajo (30-50 % de descuento) la combinación adecuada de soluciones de redes y comunicaciones seguras para sus necesidades y formar a sus empleados en las mejores prácticas de ciberseguridad. Nuestro enfoque integral de la arquitectura Zero-Trust permite a nuestros clientes demostrar a sus aseguradoras que están adoptando un enfoque proactivo y, en general, se benefician de un descuento de hasta un 20-30 % en su seguro de ciberseguridad.

Conclusión

Las tendencias en ciberseguridad de 2026 exigen un cambio de paradigma en la estrategia empresarial. Las organizaciones deben conciliar el doble papel de la IA como amenaza y como defensor, invertir en cadenas de suministro resistentes para soportar las embestidas de ransomware y rediseñar los sistemas de gestión de identidades para lograr un mundo de confianza cero. El cumplimiento normativo, el uso ético de la IA y la colaboración entre sectores serán fundamentales para mitigar los riesgos. A medida que se amplían las superficies de ataque con la adopción de la computación perimetral y el IoT, las empresas que priorizan las defensas adaptables, la formación de los empleados y la caza proactiva de amenazas estarán mejor posicionadas para prosperar en este panorama volátil.

El camino a seguir requiere innovación tecnológica y el apoyo y la experiencia de un fabricante fiable como ALE.

Más información

Para obtener más información, entre en Soluciones de seguridad ALE. Si desea hablar con uno de nuestros expertos en seguridad, póngase en contacto con nosotros.

Alcatel·Lucent Enterprise