WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER
WHITEPAPER

intexus
CREANDO UN MUNDO CONFIABLE

Cómo proteger **la información en la era digital**

www.
intexus
.la

Tabla de **contenidos**

Introducción

Vivimos en una era donde la información se ha convertido en uno de los activos más valiosos para las organizaciones. Sin embargo, ese valor también se transforma en uno de los blancos más atractivos para los cibercriminales.

Durante 2023, los ciberataques aumentaron un 38% a nivel global, según Check Point Research, y América Latina fue una de las regiones más afectadas, especialmente en sectores como finanzas, salud y educación. En paralelo, el Forrester Research estima que más del 80% de las brechas de seguridad comienzan por accesos no autorizados o mal gestionados.

La evolución de las amenazas ha dejado claro que los modelos tradicionales de seguridad **ya no son suficientes.** Hoy, las organizaciones enfrentan **desafíos complejos** como la protección de datos sensibles, el uso seguro de aplicaciones en la nube, el trabajo remoto, la movilidad del personal y la gestión de múltiples dispositivos.

En este contexto, garantizar la **protección de datos y el acceso seguro a sistemas** y aplicaciones no es solo una necesidad técnica, sino una prioridad estratégica.

Para responder a este entorno cambiante, surgen soluciones complementarias como **DLP (Data Loss Prevention) y ZTNA (Zero Trust Network Access).** Mientras DLP se enfoca en prevenir la fuga o uso indebido de información crítica, ZTNA redefine la forma en que se conceden accesos, bajo el principio de "nunca confiar, siempre verificar".

Además, herramientas como **CASB (Cloud Access Security Broker)** juegan un papel clave al permitir una visibilidad y control completos sobre el uso de aplicaciones en la nube, ayudando a las organizaciones a cumplir con normativas y minimizar riesgos.

Este whitepaper explora cómo estas tecnologías convergen para construir un entorno más seguro, eficiente y flexible, diseñado para ayudar a las organizaciones a enfrentar con confianza los desafíos de la era digital.

Tendencias en ciberseguridad

En los últimos años, la ciberseguridad ha dejado de ser un área técnica aislada para convertirse en una prioridad estratégica para las organizaciones. En un mundo donde los datos viajan constantemente entre usuarios, dispositivos, nubes y aplicaciones, la protección de la información ya no puede depender de perímetros fijos.

Según el informe Global Cybersecurity Outlook 2024 del Foro Económico Mundial, el 91% de las organizaciones a nivel mundial considera que un ciberataque significativo podría producirse en los próximos dos años. En América Latina, el número de incidentes aumentó un 30% en 2023, con sectores como banca, salud y gobierno entre los más afectados, así lo señala la firma Kaspersky.

En este escenario, emergen tres grandes tendencias tecnológicas que están transformando la forma en que las empresas enfrentan el riesgo digital: **DLP, SSE y ZTNA.**

1 DLP (Data Loss Prevention):
proteger los datos donde sea que estén

Las soluciones de DLP permiten a las organizaciones identificar, monitorear y proteger datos sensibles en movimiento, en uso y en reposo. Esto es clave en un entorno donde el trabajo remoto, el BYOD (Bring Your Own Device) y el uso masivo de la nube aumentan las superficies de ataque.

Ejemplo: Una entidad bancaria en Costa Rica utiliza DLP para prevenir la fuga de información financiera a través de correos no autorizados y dispositivos USB, reduciendo en un 70% los incidentes internos en solo 6 meses.

2 SSE (Security Service Edge):
seguridad en la nube, desde la nube

SSE integra varias funciones de seguridad en un solo servicio basado en la nube, incluyendo Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) y ZTNA. Esto permite proteger el acceso a aplicaciones desde cualquier ubicación, con visibilidad y control en tiempo real.

Dato clave: Gartner predice que para 2025, el 80% de las empresas adoptará alguna forma de SSE para reducir la complejidad y aumentar la eficiencia en sus estrategias de seguridad.

intexus

3 ZTNA (Zero Trust Network Access): acceso sin confianza implícita

ZTNA es una evolución del modelo tradicional de VPN. En lugar de otorgar acceso total a una red, ZTNA aplica el principio de **"nunca confiar, siempre verificar"**, autenticando continuamente a los usuarios y evaluando el contexto (ubicación, dispositivo, comportamiento).

Ejemplo: Una empresa de retail en México implementa ZTNA para su fuerza de ventas móvil, reduciendo un 60% los accesos no autorizados en sus aplicaciones internas y aumentando la velocidad de conexión segura.

La combinación de **DLP, SSE y ZTNA** permite a las organizaciones construir una arquitectura de seguridad más moderna, flexible y orientada a los datos. Estas tecnologías, cuando se implementan de forma integrada, ayudan a reducir riesgos, cumplir regulaciones y garantizar una experiencia segura para usuarios y clientes.

La transformación digital exige una ciberseguridad igual de transformadora. Las organizaciones que adopten estas tendencias estarán mejor preparadas para enfrentar los desafíos actuales y futuros.

intexus

NGSWG: La evolución del filtro web en la nueva era de la ciberseguridad

Las amenazas evolucionan constantemente y los usuarios acceden a información desde múltiples ubicaciones, dispositivos y redes, los filtros web tradicionales ya no son suficientes. Aquí es donde entra en juego el Next-Generation Secure Web Gateway (NGSWG): una solución avanzada que redefine la protección del tráfico web, integrándose con tecnologías clave como DLP, ZTNA y SSE para construir una arquitectura de seguridad moderna y proactiva.

¿Qué es un NGSWG y por qué es esencial?

El NGSWG es mucho más que un filtro de navegación. Se trata de una pasarela inteligente que inspecciona, analiza y controla todo el tráfico web, incluso aquel cifrado mediante HTTPS, para detectar amenazas, prevenir fugas de datos y aplicar políticas de acceso dinámicas.

Según el informe Cybersecurity Forecast 2024 de Gartner, el 75% del tráfico web empresarial ya está cifrado, lo que representa un reto importante para los sistemas de seguridad tradicionales. Los NGSWG permiten inspeccionar ese tráfico cifrado sin comprometer el rendimiento ni la privacidad, una capacidad crítica en la actualidad.

Cómo funciona y qué lo hace diferente:

A diferencia de los firewalls convencionales, el NGSWG:

- Analiza el contenido en tiempo real (Deep Packet Inspection)DPI
- Identifica y bloquea sitios maliciosos, phishing y descargas sospechosas.
- Clasifica aplicaciones según su nivel de riesgo con sistemas de puntaje.
- Aplica políticas por rol, dispositivo o ubicación.
- Se integra con herramientas como DLP, ZTNA y CASB para ofrecer una protección completa.

Un ejemplo claro es el de una institución financiera que implementó un NGSWG y redujo en un 60% los intentos de acceso a sitios maliciosos y en un 40% las filtraciones accidentales de datos confidenciales en el primer trimestre, según un caso documentado por Check Point Research.

Integracion con tecnologías enmarcadas dentro de SSE -y DLP: una sinergia poderosa

El verdadero poder del NGSWG se potencia al integrarse con otras tecnologías clave:

DLP (Data Loss Prevention): evita que datos sensibles (como números de tarjetas, documentos personales o credenciales) salgan de la red, incluso en plataformas web aparentemente seguras.

ZTNA (Zero Trust Network Access): asegura que cada acceso web se base en la verificación continua del usuario, su dispositivo y su contexto.

SSE (Security Service Edge): NGSWG es un componente esencial dentro de SSE, junto a CASB y ZTNA, para una protección unificada del entorno cloud y los accesos remotos.

intexus

Beneficios de implementar NGSWG en las organizaciones

» Navegación segura y controlada
» Bloqueo proactivo de amenazas web y malware
» Visibilidad total sobre el tráfico web, incluidos sitios cifrados
» Reducción del riesgo de fuga de datos al integrase con DLP
» Accesos más seguros con políticas de Zero Trust (ZTNA)
» Mejor control sobre el uso de aplicaciones en la nube (CASB)
» Análisis basado en inteligencia artificial para tomar decisiones más precisas.

Según Forrester, las empresas que adoptan una arquitectura basada en NGSWG e integraciones SSE experimentan una reducción del 45% en incidentes de seguridad relacionados con navegación web en su primer año de implementación.

Conclusiones

La ciberseguridad moderna exige mucho más que herramientas aisladas. En un entorno donde los ataques son cada vez más sofisticados y los usuarios operan desde múltiples dispositivos y ubicaciones, las organizaciones deben adoptar una arquitectura integral, adaptable y centrada en los datos.

El uso conjunto de soluciones como NGSWG, DLP, ZTNA y SSE permite a las empresas no solo prevenir amenazas y accesos no autorizados, sino también proteger sus datos más sensibles, garantizar el cumplimiento normativo y ofrecer una mejor experiencia al usuario.

Implementar una estrategia de ciberseguridad basada en estas tecnologías ofrece múltiples ventajas concretas:

Implementar una estrategia de ciberseguridad basada en estas tecnologías ofrece múltiples ventajas concretas:

Mayor protección de datos sensibles: DLP permite detectar y prevenir fugas de información en tiempo real.

Navegación segura: NGSWG filtra el tráfico web, incluso cifrado, y bloquea amenazas antes de que afecten la red.

Accesos controlados y personalizados: ZTNA garantiza que solo usuarios verificados accedan a los recursos necesarios, sin confianza implícita.

Seguridad en la nube: La integración con SSE permite proteger el acceso a aplicaciones cloud y reducir la exposición al Shadow IT.

Reducción de incidentes: Las organizaciones que adoptan estas tecnologías reducen en hasta **50% los incidentes de seguridad relacionados con acceso y navegación**, según lo señala Gartner, Forrester.

Cumplimiento normativo más eficiente: Estas soluciones ayudan a cumplir regulaciones como GDPR, ISO 27001, HIPAA, PCI DSS, entre otras.

intexus

Próximos pasos para su organización

1. **Evaluar su postura actual de ciberseguridad:** ¿Cuenta con visibilidad sobre el tráfico web, las aplicaciones en la nube y la gestión de accesos?

2. **Identificar los activos más críticos:** Determine qué datos y sistemas requieren mayor protección.

3. **Adoptar un enfoque Zero Trust:** Implemente políticas que no asuman confianza, sino que validen cada acceso.

4. **Modernizar su infraestructura de seguridad:** Considere integrar NGSWG, DLP, ZTNA y SSE en una sola estrategia.

5. **Aliarse con expertos en seguridad:** Trabajar con un socio como Intexus, que brinda soluciones avanzadas y acompañamiento personalizado, puede acelerar la implementación y maximizar el impacto.

intexus

Invertir hoy en las herramientas adecuadas es la mejor manera de proteger el valor, la reputación y la continuidad del negocio en el futuro.

¿Listo para llevar la protección de datos de su organización al siguiente nivel?

Contacto

soluciones@intexus.la

www.intexus.la

@Intexus