Ficha Tecnica de Servicio
Security Services

Resumen Ejecutivo

El servicio Security de Maxtel ofrece a las organizaciones una proteccion integral disenada para resguardar infraestructura, datos y operaciones en un entorno digital cada vez mas complejo. Combinamos tecnologias de vanguardia, monitoreo continuo y practicas avanzadas de ciberseguridad para asegurar que cada capa de su entorno tecnologico este protegida frente a amenazas internas y externas. Nuestro enfoque se basa en una arquitectura de seguridad unificada, donde prevencion, deteccion y respuesta trabajan de manera coordinada. Esto permite a las empresas minimizar riesgos, fortalecer resiliencia operativa y cumplir con normativas locales e internacionales sin anadir carga operativa a sus equipos internos. America del Norte, Centro y Sudamerica (excepto Brasil, Nicaragua, Cuba y Haiti), utilizando nuestros data centers de:

Caracteristicas Clave

- Seguridad perimetral avanzada: Firewalls de proxima generacion (NGFW), filtrado inteligente, control granular de trafico y proteccion contra amenazas.

- Proteccion de red y segmentacion: Aislamiento por VLAN/VRF, politicas Zero Trust, inspeccion profunda de paquetes y deteccion de comportamientos anomalos.

- Gestion de identidades y accesos (IAM): Permite integracion con SSO, MFA, LDAP, OIDC y politicas de control de acceso basadas en roles (RBAC).

- Seguridad para aplicaciones y APIs: Mitigacion de ataques OWASP, proteccion WAF, rate limiting y validacion de trafico critico.

- Proteccion de datos: Cifrado en transito y en reposo, clasificacion de datos, auditorias de acceso y prevencion de fugas (DLP).

- Seguridad para entornos hibridos y multi-nube: Politicas consistentes en nubes publicas, privadas, contenedores y entornos de Colocation.

- Respuesta ante incidentes: Analisis de causa raiz, contencion y recuperacion asistida.

- Monitoreo y alertas 24/7: Deteccion continua mediante SIEM/SOAR, correlacion de eventos y alertamiento inteligente.

Beneficios para su Empresa

- Mayor resiliencia operativa, reduciendo el riesgo de interrupciones por ataques o brechas.

- Visibilidad total de amenazas, accesos y comportamiento anomalo dentro de su infraestructura.

- Menor complejidad interna, con seguridad administrada por expertos.

- Proteccion adaptable, soportando entornos tradicionales, cloud-native, contenedores y microservicios.

- Cumplimiento asegurado, con politicas consistentes y documentacion actualizada.

- Reduccion de costos, evitando inversiones en multiples herramientas, equipos o personal especializado.

- Capacidad de respuesta inmediata, mitigando incidentes antes de que generen impacto.

Datacenter