B.S.S.

BUSINESS SMART SOLUTIONS

SMART PROTECTION

Dirección: Pasaje N44B E10-26 y Av. 6 de diciembre
PBX: +593 (2) 382 7390 /
WhatsApp: 096 972 9361
ventas@competencia.com.ec
serviciotecnico@competencia.com.ec

LA COMPETENCIA S.A.
SOLUCIONES TECNOLÓGICAS DESDE 1963

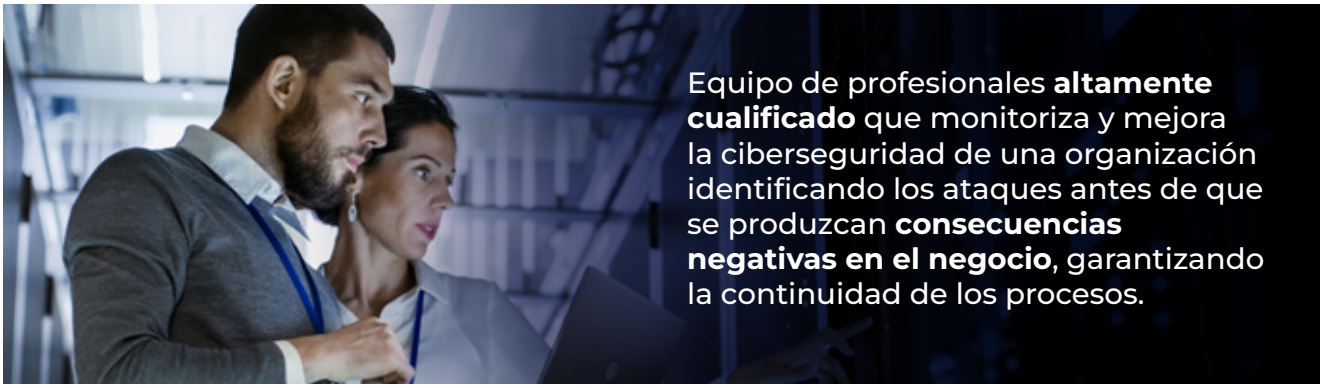
El mundo está cambiando y nosotros con él.

DESCRIPCIÓN DE LA SOLUCIÓN

SmartProtection es un servicio que permite protegerse de los ataques informáticos (Cyberataques) y asegurar la información, así como la continuidad del negocio.

El servicio está ajustado a la necesidad y tamaño de la empresa para lo cual, nuestro equipo de consultores realizará, en conjunto y de manera colaborativa con el cliente, una evaluación inicial de la situación actual, consensuarán una solución, planificación de la implementación, puesta en marcha y definición del cronograma de acompañamiento continuo.

La ciberseguridad comprende todas las medidas preventivas para detectar y evitar ataques y vulnerabilidades que ponen en juego la integridad y confidencialidad de los sistemas informáticos y sus datos. Estas acciones se encargan de proteger y asegurar al máximo la privacidad de la información.
El resultado, una solución a la medida del cliente flexible y escalable.



CARACTERÍSTICAS

- Plan mensual o anual dependiendo del tamaño de la compañía
- Alternativas de protección informática flexible, tanto para oficina principal con trabajadores centralizados, así como para entornos híbridos, remotos o móviles.
- Puede o no incluir equipamiento dependiendo de la realidad y necesidad del cliente.
- Cyberseguridad simple de implementar y fácil de administrar.
- Libre de preocupaciones tanto para los usuarios dentro como fuera de la red
- Políticas de seguridad consistentes tanto para usuarios internos como remotos
- Mejor rendimiento y satisfacción garantizada
- Permite lanzar rápidamente una respuesta coordinada al detectar una amenaza en todo el ecosistema de infraestructura de la organización en el momento en que se detecta un riesgo. Esto rompe la secuencia de ataque antes de que se puedan alcanzar los objetivos, ya que se hace uso de machine learning (ML) y artificial intelligence (AI).

BENEFICIOS

- Baja inversión y trasladada al gasto de operación (OPEX) en lugar de inversión de activos (CAPEX) mejorando el flujo de efectivo orientando los recursos al objetivo central del negocio.
- Actualización tecnológica garantizada evitando la obsolescencia que pone en riesgo la seguridad informática de la empresa.
- Cero paralizaciones de las operaciones del negocio y protección contra secuestro de información (Ramsonware).
- La protección informática alineada con la nueva forma de trabajo: híbrido, remoto, móvil así como el acceso a centros de datos descentralizados y en nube.
- Protección de cualquier dispositivo independientemente del lugar en donde se encuentre (computador, Tablet, portátil, smartphone, IoT)

PREVENCIÓN

Estar preparados al tener una visibilidad absoluta de los dispositivos, las amenazas, las redes, las aplicaciones, los usuarios y los procesos para evitar posibles incidentes.

DETECCIÓN E IDENTIFICACIÓN

El monitoreo debe ser constante y diario. Tener programas especializados para la detección temprana puede hacer toda la diferencia antes de poner los activos de las organizaciones en riesgo.

ACCIÓN

Un ataque informático es similar a una enfermedad. Cuanto antes se reaccione, antes se podrá atender y así reducir o evitar el daño en un alto porcentaje.

VISIÓN ORGANIZATIVA Y DE NEGOCIO
El servicio no solo se centra en la monitorización y vigilancia, sino en la **mejora continua** y aplicación de las mejores prácticas.
Aumentando su nivel de madurez en ciberseguridad.

¿POR QUÉ SE DEBE IMPLEMENTAR ESTA SOLUCIÓN?

- Simple; para seguir haciendo negocios de manera segura y rentable
- El entorno de trabajo ha cambiado, los ataques informáticos se han incrementado independientemente del tamaño de empresa, los puntos vulnerables han aumentado, los usuarios están interactuando digitalmente de manera acelerada. Estas realidades hacen que las compañías se vean amenazadas y susceptibles a robo de información o paralización de operaciones.
- Acelera la transformación digital y empresarial apoyando el crecimiento global de su empresa manteniendo la seguridad en entornos y ecosistemas multi cloud.
- Enfoque de arquitectura abierta para asegurar la infraestructura tecnológica.

MAYOR PROTECCIÓN
Evita y combate ataques de amenazas como ransomware, virus, malware, spyware y programas no deseados.

RENDIMIENTO DE TODO TIPO DE DISPOSITIVOS
Evita y combate ataques de amenazas como ransomware, virus, malware, spyware y programas no deseados

NAVEGACIÓN SEGURA EN LA WEB
Evita peligros en línea con sus herramientas de seguridad en la web.

BARRERAS DE SEGURIDAD
Protege computadoras, teléfonos móviles y demás artículos tecnológicos resguardando a sus usuarios de los peligros de Internet.

COMO FUNCIONA COMO SE IMPLEMENTA:

Aplica las mejores prácticas para el aseguramiento y protección contra Cyberataques. En función de la realidad de la empresa se diseña una arquitectura que se ajuste a la misma soportados en líderes de la industria como Fortinet y CISCO.

Fortinet Security Fabric

Fortinet Security Fabric, construido sobre el sistema operativo de red FortiOS, permite que múltiples tecnologías de seguridad funcionen sin problemas de manera conjunta, en todos los entornos y respaldados por una única fuente de inteligencia de amenazas. Esto elimina las brechas de seguridad en la red y acelera Respuestas a ataques.

Los cinco pilares Smart Protection:

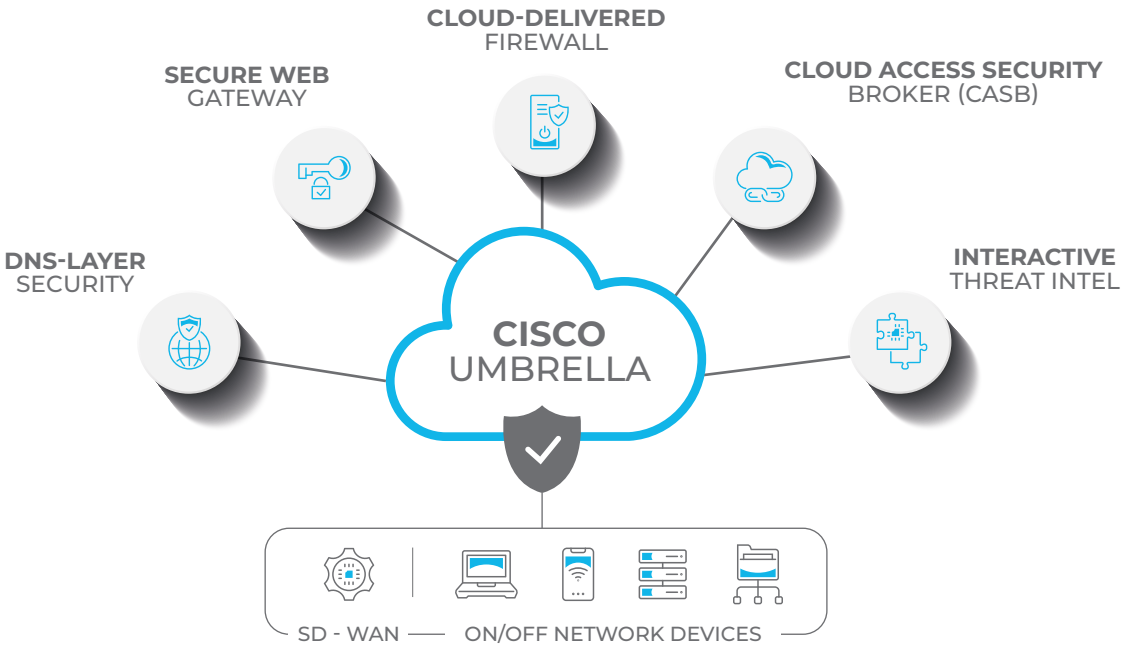
1. Security-driven networking. Los NGFW de FortiGate con sus secure web gateways (SWGs) administran los riesgos de seguridad y bloquean las amenazas, y Fortinet Secure SD-WAN (software-defined wide-area network) mejora y asegura la experiencia del usuario y aplicaciones.

2. Zero-trust network access. Icluye FortiNAC y FortiAuthenticator, identifican los dispositivos y usuarios en la red. Fortinet Fabric Security Agent proporciona seguimiento de usuarios y dispositivos dentro y fuera de la red corporativa.

3. Dynamic cloud security. FortiCASB cloud access security broker (CASB), and FortiCWP cloud workload protection (CWP) proporcionan seguridad en la nube, control de acceso y gestión de la configuración. FortiWeb, FortiMail y FortiCASB aseguran servicios web y de emaill en la nube como también aplicaciones Software-as-a-Service (SaaS).

4. AI-based security operations. La inteligencia de amenazas impulsada por AI ayuda a predecir y prevenir ataques y detectar amenazas desconocidas. SOAR permite una respuesta y contención de amenazas más rápidas.

5. Fabric Management Center. Permiten una gestión centralizada y gestion de la configuración en toda una arquitectura de seguridad de la organización. Estos también sienta las bases para las operaciones de seguridad automatizadas y la generación de informes.



¿TU ORGANIZACIÓN ESTÁ PREPARADA PARA LOS POSIBLES ATAQUES?

En La Competencia S.A. comprendemos la importancia de proteger tu empresa, tu información y a tus colaboradores. Por eso trabajamos con marcas de nivel mundial para darte la mejor seguridad y encontrar un plan de protección perfecto para tus necesidades.

B.S.S.

BUSINESS SMART SOLUTIONS

Dirección: Pasaje N44B E10-26 y Av. 6 de diciembre
PBX: +593 (2) 382 7390 /
WhatsApp: 096 972 9361
ventas@competencia.com.ec
serviciotecnico@competencia.com.ec

LA COMPETENCIA S.A.
SOLUCIONES TECNOLÓGICAS DESDE 1963

El mundo está cambiando y nosotros con él.