[DATA SHEET]

Puesto de Usuario Seguro

Secure Browsing

Las oportunidades que nos brinda Internet para facilitar muchas de las actividades empresariales y contribuir al desarrollo personal y profesional de usuarios y organizaciones son indiscutibles, pero también conlleva riesgos ineludibles. Internet es cada vez un entorno más complejo y peligroso y requiere de un uso responsable tomando las medidas necesarias para que el consumo que hagamos no redunde en un perjuicio personal ni empresarial.

A través del servicio de ***Puesto de Usuario Seguro*** o ***Navegación Segura***, podrá asegurar la navegación de aquellos *usuarios claves* para la organización. Realizarán un uso de internet seguro y sin sobresaltos, desde cualquier red y lugar, sabiendo que la información sensible contenida en sus dispositivos está protegida.

Asegura la navegación de los usuarios clave de la organización, estén donde estén.

Nuestro servicio de navegación segura permitirá que los dispositivos de la organización puedan acceder a internet sin sobresaltos y de forma asegurada, despreocupándonos de si el método de acceso a internet (red wifi aeropuerto, hotel, etc ...) que están utilizando es el adecuado, y si es realmente un riesgo para nuestra organización.

El servicio cuenta con el respaldo y toda la potencia de las tecnologías Palo Alto Networks para asegurar un alto nivel de protección en las comunicaciones desde y hacia internet.

Este servicio **convertirá la seguridad** de todos tus accesos a internet **en una *commodity*** de forma que tanto desde los puestos de trabajo corporativos (oficinas) como los puestos de trabajo remotos (domicilios), o los puestos de trabajo itinerantes (ejecutivos, comerciales, etc ...) puedan estar seguros de que estén donde estén su relación con internet estará siempre asegurada.

Objetivos del Puesto de Usuario Seguro

Los principales objetivos que se persiguen a través del servicio "*Secure Browsing*" son los siguientes:

- **Asegurar** la navegación por internet
- **Proteger** los accesos a internet de las amenazas que circulan
- **Mitigar** los riesgos asociados a la necesidad del uso de servicios en internet
- **Reforzar** la seguridad en el teletrabajo
- **Reforzar** la seguridad en perfiles itinerantes

En qué consiste el servicio

Para dar inicio al servicio, nuestro equipo de expertos coordinará con el cliente el despliegue de los agentes necesarios en los dispositivos contratados.
Para ello, trasladaremos a la organización un procedimiento detallado para la instalación de los agentes que protegerán las comunicaciones con internet, quién deberá aplicar este procedimiento en todos los dispositivos que haya contratado.

A partir de ese momento, los dispositivos sobre los que se haya desplegado el servicio estarán conectados permanentemente a nuestros servidores que protegerán toda la comunicación que los dispositivos realicen desde y hacia internet.

Detalle de la protección

El servicio proporcionará protección en toda aquella comunicación que salga o entre al dispositivo desde y hacia internet. El tipo de protección con la que contará variará dependiendo del modelo de servicio elegido. A continuación se detallan los tipos de protección ofrecidos y los diferentes modelos de servicios.

A continuación detallamos los distintos niveles de protección ofrecidos a través del servicio de Puesto de Usuario Seguro:

- ✓ **PREVENCIÓN CONTRA AMENAZAS:** a traves del control del tráfico de los dispositivos, detectaremos y bloquearemos cualquier amenaza antes de que esta pueda llegar a generarte un problema en tu dispositivo y en la información que guardas en el.

- ✓ **DETECCIÓN Y BLOQUEO DE INTRUSIONES:** se bloquearán todos los ficheros que a través de diferentes medios (correos electrónicos, descargas redes sociales, descargas de sitios compartidos, sitios web comprometidos, etc...) puedan instalarse en nuestro dispositivo para en base a diferentes técnicas generarnos problemas como el cifrado de nuestro dispositivo, el robo de información, la extensión a nuestra red corporativa ...

- ✓ **ANTI MALWARE NAVEGACIÓN:** nos protegerá de todo el tráfico que realicemos en internet y que pueda estar comprometido o contaminado con virus, malware o cualquier otro artefacto malicioso. Todo ello aplicado a múltiples protocolo de internet que usemos (HTTP, FTP, SMTP, IMAP, SMB ...)

- ✓ **FILTRADO DE URLS:** prevenimos el acceso a sitios de intenet potencialmente maliciosos. Podrán detectarse y bloquearse accesos a sitios con el siguiente contenido: paneles de control de malware, sitios de phising, DNS dinámicos, anonimizadores, extremismo, incumplimiento de copyright. Este tipo de sitios son grandes fuentes de peligros potenciales para nuestro dispositivo, la información que alberga y toda nuestra organización.

- ✓ **PROTECCIÓN VULNERABILIDADES:** protección frente a “buffer overflow”, “illegal code execution” y otro tipo de intentos de explotación de vulnerabilidades tanto de nuestros sistemas clientes, como móviles, portátiles/PC sobremesa) como de los servicios o servidores a los que nos conectemos en nuestra navegación (servicios de correo, paginas web, redes sociales, portales de gestión del banco, seguros, etc ....).

- ✓ **CONTROL APLICACIONES MALICIOSAS:** el tráfico de internet que generan las aplicación que utilicemos será analizado y protegido de acciones sospechas o ilegítimas.

- ✓ **ANTI APTS:** las APT (amenazas avanzadas persistentes) representan un nivel de amenaza en el que el objetivo es blanco único y el posible ataque es preparado escrupulosamente y con una gran capacidad de recursos materiales y temporales. Con esta protección evitaremos

- ✓ **PROTECCIÓN ZERO DAYS:** búsqueda y detección de vulnerabilidades desconocidas en múltiples fabricantes y productos. Capacidad de detección y protección de zero days (vulnerabilidades que aún no tienen parche o solución por parte del fabricante) de los productos utilizados en nuestro diario uso de internet.

- ✓ **CONTROL DNS MALICIOSOS:** es práctica habitual de los ciber-delincuentes el uso de DNS (servicios de internet que traducen los nombres de las páginas web en direcciones IPs que tienen los servidores que albergan esas páginas) maliciosos para realizar suplantaciones de páginas web. Con esta modalidad del servicio, estaremos protegidos del uso de este tipo de DNS.

- ✓ **SANDBOXING:** en caso de que en alguno de los ficheros analizados en las diferentes protecciones en su verificación no se haya podido conocer su legitimidad, este será enviado a una “sandbox” donde se ejecutará y analizará si las acciones que realiza tienen intenciones maliciosas o no y etiquetará ese fichero con el nivel de riesgo concluido para tomar una decisión, todo ello en tiempo real, sobre si debe o no llegar y/o ejecutarse en nuestro dispositivo.

PROFESSIONAL

PROTECCIÓN BÁSICA DE LA NAVEGACIÓN DEL PUESTO DE USUARIO:

Prevención contra amenazas
Detección y bloqueo de intrusiones
Anti malware navegación
Control aplicaciones maliciosas
Filtrado de URLs
Protección vulnerabilidades
Anti APTs
Protección zero days

PREMIUM

AÑADE UN NIVEL SUPERIOR DE PROTECCIÓN, INCLUYENDO:

Control DNS maliciosos
Sandboxing navegación

"Llévate el firewall contigo. Asegura tu navegación, estés dónde estés.

its by Ibermática

Sobre ITS by Ibermática

Somos la compañía de ciberseguridad de próxima generación que está transformando la seguridad en un servicio, ayudando a empresas y organizaciones a prevenir las infracciones de ciberseguridad, permitiendo mantener así la confianza.

Nuestra profunda experiencia en ciberseguridad, nuestro compromiso con la innovación y nuestra plataforma unificada de seguridad de nueva generación (CiD360) permiten la prevención de violaciones, ataques e intrusiones mediante el uso de técnicas de inteligencia y contrainteligencia al combinar la seguridad de red, nube y punto final.