Spamina

1.- Parla Secure Cloud Email: (Email seguro para empresas)

Email corporativo, mensajería instantánea y entorno de colaboración seguro, a través de cualquier dispositivo y desde cualquier lugar.

Las comunicaciones digitales de las empresas están expuestas a ataques cada día más innovadores, sofisticados y difíciles de detectar. Lo que implica que los responsables de TI, busquen soluciones que ofrezcan un entorno seguro de colaboración que mantenga la información protegida de los ciberataques.

Parla es una solución de correo electrónico corporativo con una capa de seguridad integrada. Los usuarios pueden acceder a sus correos en cualquier momento, bien sea desde el ordenador o desde la nueva App de Spamina.

Disponible para pequeñas y medianas empresas, así como para grandes corporaciones y organismos, Parla ofrece a sus usuarios:

- Correo electrónico con sistema de seguridad integrado hasta 30GB.
- Mensajería Instantánea corporativa cifrada.
- Agendas, contactos, tareas y compartición de ficheros.
- Integración con Outlook.
- Sincronización con todos los dispositivos móviles.
- Capa de seguridad y filtrado integrado.
- Multidominio.
- Gestión de dispositivos móviles: Mobile Device Management (MDM).
- Cloud Email Encryption como solución de cifrado y Cloud Email Archiving para el archivado de correo y así garantizar la privacidad y disponibilidad del email.

Los usuarios de Parla podrán suscribir un servicio adicional de protección avanzada para prevenir y bloquear el email de amenazas avanzadas persistentes (APTs) como el ransomware y cryptolocker.

Este servicio, Advanced Threat Protection de Spamina, incorpora servicio Premium Antivirus y tecnología Sandboxing de análisis de ficheros y urls/links maliciosos.

2.- ParlaMI Enterprise Instant Messasing: (Mensajería instantánea segura para empresas)

Mensajería instantánea para empresas: Conversaciones protegidas y seguras en cualquier momento y desde cualquier dispositivo.

ParlaMI es el servicio de mensajería instantánea corporativa desarrollado por SPAMINA. ParlaMI ha sido desarrollado con tecnología de cifrado punto a punto, además de sistemas de filtrado antispam, antimalware y de prevención de fuga de datos, para asegurar la protección y confidencialidad de las conversaciones.

ParlaMI permite mantener conversaciones en tiempo real, bien sea a nivel individual o en grupos. Los usuarios pueden crear grupos y proteger el acceso a los grupos mediante contraseña además de hacer un seguimiento del estado de la conversación con la notificación y la identificación del estado del envío de los mensajes instantáneos.

Esta solución de mensajería instantánea para empresas, dispone de la opción de IM Archiving que permite el almacenar las conversaciones pudiendo realizar búsquedas y recuperar los mensajes en tiempo real desde la propia app y compartirlos bien sea a través de la propia mensajería o por email.

Las búsquedas de las conversaciones pueden realizarse por:

- Contenido
- Contacto
- Nombre de grupo o sala
- Rango de fecha

ParlaMI se encuentra totalmente integrado dentro de Outlook. El plugin de Outlook, permite a los usuarios utilizar y gestionar el correo electrónico y la mensajería instantánea corporativa segura desde la misma pantalla del ordenador, así como compartir archivos directamente desde la interfaz de Outlook.

ParlaMI está también disponible desde la versión webmail de Parla, y en versión App para dispositivos móviles Android e iOs. La funcionalidad de mensajes push, permite recibir alertas para un mejor seguimiento de las conversaciones en el chat corporativo independientemente del dispositivo que el usuario esté utilizando en ese momento.

3.- Cloud Email Firewall: (Protección antimalware y filtrado del correo)

Filtrado de correo entrante y saliente para mantener la información libre de malware, phishing, virus y spam.

El 78% de los usuarios de email considera preocupante que sus datos puedan no estar seguros y un 69% ha sufrido problemas con la protección del correo en algún momento del pasado.

Cloud Email Firewall incorpora innovadoras tecnologías propietarias de filtrado de email para la protección frente amenazas de última generación, como Simile Fingerprint Filter®. Esta técnica detecta el spam saliente, diferenciando y separando el email corporativo legítimo, de los envíos de correo masivos automatizados. Además, Cloud Email Firewall integra tecnologías de detección patentadas para analizar billones de correos electrónicos cada día que permiten identificar los patrones de spam y ciberamenazas en tiempo real y bloquear su entrada con una efectividad del 99,9%.

Utilizando los servicios de filtrado de correo de Spamina, las empresas reciben el email limpio mientras el correo no deseado se mantiene en nuestros CPDs hasta 28 días.

Además cada usuario tendrá su propia consola de gestión para administrar sus listas blancas y listas negras, directamente desde la interface de su correo electrónico.

Los usuarios de Cloud Email Firewall podrán suscribir un servicio adicional de protección avanzada para prevenir y bloquear el email de amenazas avanzadas persistentes (APTs) como el ransomware y cryptolocker. Este servicio, Advanced Threat Protection de Spamina, incorpora servicio Premium Antivirus y tecnología Sandboxing de análisis de ficheros y urls/links maliciosos.

Sin costes de migración, implementación inmediata, sin tener que volver a preocuparse por las actualizaciones o la escalabilidad de sus negocio.

4.- Advanced Threat Protection: (Máxima protección frente a APTs)

Nueva tecnología sandboxing y servicio premium antivirus para proteger su correo de amenazas persistentes avanzadas (Ransomware, Cryptolocker,…)

La mayoría de las organizaciones confían en técnicas de prevención de intrusiones como firewall y antivirus. Sin embargo, estas herramientas son insuficientes, los robos y pérdida de datos muestran la necesidad de mejorar la detección en tiempo real con soluciones de protección avanzada (ATP) contra cyberataques difíciles de detectar como Ransomware/Cryptoware.

La solución ATP de Spamina es una capa adicional de protección ante amenazas, que incorpora 2 tecnologías:

Análisis Sandboxing de Ficheros & URLs y links maliciosos

La solución ATP de Spamina está desarrollada sobre la segunda generación de tecnología sandboxing, que aprovecha las facilidades ofrecidas por el Complete run-time Environment Instrumentation (CEI, Instrumentación detallada del entorno de ejecución) para realizar verificaciones exhaustivas de todos los objetos sometidos a análisis y sus partes.

Análisis e identificación de ficheros y documentos adjuntos maliciosos:

Las soluciones ATP de Spamina, chequean los documentos y ficheros adjuntos dentro de un entorno virtualizado, antes de ser entregado y ejecutado en el endpoint del receptor del mensaje. La principal ventaja es un email libre de contenido malicioso.

Análisis de URL y links maliciosos:

La tecnología sandboxing de URL, permite identificar ataques dirigidos hacia navegadores vulnerables y links maliciosos. Al mismo tiempo que se realiza el escaneo de la url sospechosa, si el usuario pincha en el link, Spamina devuelve una imagen del contenido de la url en tiempo real, garantizando que cada vez que accede a ese link, ha sido verificado y el usuario puede acceder al contenido sin riesgo.

Advanced Premium Antivirus (APAV)
APAV es un sistema basado en firmas de definiciones de malware locales y con motores heurísticos, caracterizados por:

Basado en la detección de firmas
Detección de todos los ejemplos de malware conocidos
Rápida actualización de amenazas
Análisis de comportamiento
Reputación de aplicaciones

5.- Cloud Email Archiving: (Archivado y recuperación del email)

Mantenga sus correos corporativos archivados, inalterados y siempre disponibles para cumplimiento de normativas, regulaciones y auditorías tanto internas como externas.

El archivado y retención del correo electrónico debe cumplir con una serie de requisitos clave, incluyendo la disposición legal, cumplimiento normativo y la garantía de tener siempre los emails originales de la organización, manteniendo la confidencialidad y que la información esté accesible en todo momento.

Un servicio de archivado de correo electrónico debe cumplir todos estos requisitos y, además, facilitar que los departamentos de TI puedan reducir tanto costes como complejidad en la gestión de grandes volúmenes de datos, tanto en los sistemas administrados como en los sistemas que están fuera del control directo del TI.

Cloud Email Archiving guarda y mantiene los correos originales de la empresa hasta 10 años, para su búsqueda y recuperación de correo inmediata ante requerimientos legales y consultas. Los usuarios y administradores tienen acceso directo a la búsqueda de una forma sencilla e intuitiva,

desde su panel de control, y ahora también desde la nueva App de Spamina disponible para iOS y Android.

Spamina cuida la experiencia del usuario en el uso, ofreciendo la opción de acceder a los servicios de Cloud Email Archiving a través del propio interface de Outlok (plugin disponible para las versiones 2007, 2010, 2013 y 2016) o bien a través de la nueva App disponible tanto para iOS como Android. Los usuarios pueden realizar búsquedas, recuperar los emails y conversaciones de mensajería instantánea por distintos criterios como la fecha, contenido del email o nombre de la persona que realiza o recibe el correo.

6.- Cloud Email Encryption & DLP: (Cifrado del email y prevención de fuga de datos)

Evite la fuga de datos y garantice la privacidad de los correos corporativos.

La solución de cifrado de Spamina, permite a las empresas garantizar la confidencialidad de la información que contienen los emails. Los emails pueden ser cifrados individualmente en el momento del envío, o automáticamente a través de definición de políticas.

Cloud Email Encryption & DLP (CEE) está diseñado para que cualquier usuario pueda enviar un correo cifrado desde cualquier dispositivo. El Add-in para Outlook está disponible para usuarios de las versiones 2007 a 2016. Además la nueva App de Spamina incorpora la funcionalidad de cifrado, así los clientes de CEE podrán enviar y recibir respuesta a los correos cifrados desde la aplicación de una forma sencilla, garantizando siempre la privacidad de la información.

A nivel administrador, Cloud Email Encryption está disponible en la consola de gestión de Spamina, integrado con el resto de soluciones. Los administradores podrán definir políticas, controlar el uso del cifrado y generar dashboards de actividad.

7.- Cloud Web Security: (Filtrado de tráfico Web)

Cloud Web Security es un servicio de filtrado de tráfico Web que opera como un Proxy de gestión de tráfico bloqueando entrada de malware. Este servicio dotará a su empresa de una conexión a Internet segura y protegida, libre de todo tipo de malware y amenazas, al mismo tiempo asegurará que la navegación web sea adecuada y se ajuste a sus políticas de uso aceptable.

Las amenazas entrantes a través de las páginas web no son la única preocupación para las empresas: con millones de usuarios web que aportan activamente contenidos a estas webs a través de ”tweets”, blogs, correo web y páginas de redes sociales, las compañías se encuentran ante la necesidad de controlar, ahora más que nunca, el tráfico Web tanto entrante como saliente. La mayor parte de las empresas dan una especial importancia a sus datos relativos a la propiedad intelectual y financieros así como aquellos de carácter sensible que podrían ser susceptibles de sufrir una filtración a través de la web. En definitiva se requiere la tranquilidad de que el uso de Internet es seguro, protegido, productivo y adecuado.