



INMUNOS 1.0



UN SISTEMA OPERATIVO SEGURO

InmunOS consiste en un entorno extremadamente seguro donde poder ejecutar todo tipo de aplicaciones de un modo confiable, resultado de la experiencia acumulada a lo largo de más de diez años en la realización de Test de Intrusión. Tras años de investigación sobre aplicaciones de sistemas de seguridad avanzados conocidos -Seguridad Multinivel, Control de Accesos Basado en Roles, Protección de Memoria, etc.- se llegó a la conclusión que si se deseaba robustez en la solución, ésta debía implementarse al nivel más profundo que permite el software: el núcleo del sistema operativo. De esa manera, y como respuesta a la necesidad de diseñar el producto "desde los cimientos", se estudiaron las posibilidades que ofrecía la tecnología más avanzada en cada uno de los campos que componen la solución y se adoptaron las mejores teniendo en cuenta los siguientes factores: nivel de seguridad, madurez, escalabilidad y sencillez. De ésta forma, InmunOS incorpora la mejor combinación posible de tecnologías.

UNA NECESIDAD NO CUBIERTA

Desde ahora, empresas y usuarios no tendrán que preocuparse por los problemas típicos que afectan al mundo actual de las Tecnologías de la Información:

- Infecciones de sistemas con código malicioso -virus, gusanos, malware, etc.-
- Pérdida de datos -por robo del ordenador o soporte digital-
- Pérdida de datos por fallos mecánicos o electrónicos -fallos de discos duros, placas base o periféricos-
- Pérdida de datos debido a desastres naturales -incendio, accidentes, etc.-
- Sabotajes deliberados
- Robo de información de acceso a sistemas de banca electrónica -phishing, pharming, troyanos

GRUPO TECHCAVA, S.L.

Avda. Diagonal 468 - 8ªA
08006
Barcelona
Spain

Correo: inmunos@inmunos.com





BENEFICIOS CLAVE

- NAVEGACIÓN SEGURA
- SISTEMA DE BANCA ONLINE IMPERMEABLE (EN MODO NATIVO)
- PROTECCIÓN ANTE CÓDIGO MALICIOSO, KEYLOGGERS... P2P E IM SEGURO
- SISTEMA DE COMUNICACIÓN SEGURO
- DLP (EN MODO NATIVO)
- MÁXIMO RENDIMIENTO SIEMPRE, EL SISTEMA NO SE DEGRADA
- ZTA—ZERO TECHNICAL ASSISTANCE—(EN MODO NATIVO)

UNA SOLUCIÓN, DOS SABORES

InmunOS puede ejecutarse de dos maneras: en modo nativo y desde un sistema de virtualización. Para ejecutarlo en modo nativo, el ordenador debe arrancar desde un CD, USB u otro dispositivo que contenga una imagen de InmunOS. Si se desea ejecutar InmunOS desde otro sistema operativo, se utiliza un software de virtualización. Para ello, se han desarrollado toda una serie de asistentes de instalación del entorno de virtualización - VMWare - que son completamente transparentes para el usuario.

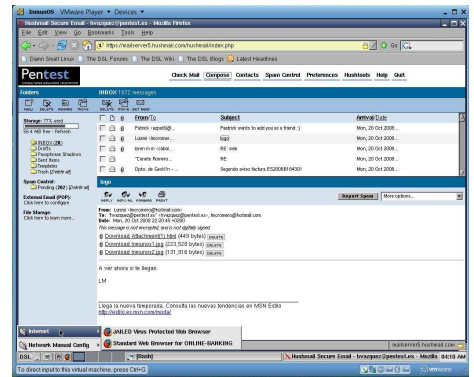
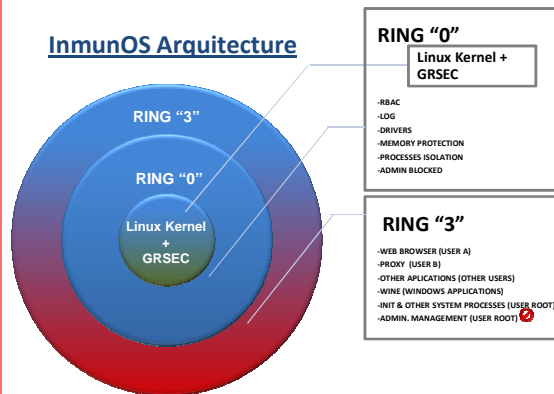


Fig. 1. Vista de InmunOS corriendo sobre VMWare

La decisión de ejecutar InmunOS en modo nativo o bajo un entorno de virtualización, depende principalmente de las necesidades del usuario o la empresa. En modo nativo, InmunOS alcanza un grado de seguridad similar al de un sistema de información militar.



En modo virtualizado, InmunOS mejora sustancialmente la seguridad del ordenador sobre aspectos concretos, como el acceso seguro a Internet: navegación, chat, P2P, etc. sin necesidad de cambiar su sistema.

UNA ARQUITECTURA ÚNICA

El Kernel de InmunOS es el encargado de aplicar las políticas de control basadas en roles, velar porque no se ejecute código malicioso en zonas de memoria no permitidas y proteger la integridad del sistema de ficheros.

El resto de aplicaciones se ejecutan en un nivel superior, encapsuladas mediante políticas RBAC, por lo que la dificultad de explotar una vulnerabilidad se une al impacto nulo que tendría en el sistema, habida cuenta de que el sistema se ejecuta en memoria y se restablece en cada reinicio del mismo.

