citione
Mail Protect

www.xcitione.com

PROTECCIÓN DEFINITIVA CONTRA EL CORREO NO DESEADO

FICHA TÉCNICA

BIENVENIDO A XCITIONE MAIL PROTECT

En Xcitione Mail Protect, entendemos la importancia de mantener tu bandeja de entrada libre de amenazas. Nuestra solución avanzada antispam en la nube está diseñada para ofrecer una protección imponente y efectiva contra el correo no deseado, garantizando la seguridad y eficiencia de tu comunicación empresarial.

MÚLTIPLES COMPATIBILIDADES

Xcitione Mail Protect es compatible con servidores de correos como Microsoft 365, Google Workspace, Zimbra, Carbonio, Cpanel, MS Exchange y otros servidores que admiten protocolos estándares de correo como SMTP, IMAP y POP3. Esto asegura que Xcitione Mail Protect pueda integrarse fácilmente en la mayoría de las infraestructuras de correo electrónico, proporcionando una capa adicional de seguridad y protección contra amenazas de spam y phishing.

Google Workspace

zimbra® A SYNACOR PRODUCT

cPanel

CONFIGURACIÓN EXCLUSIVA EN EL DNS

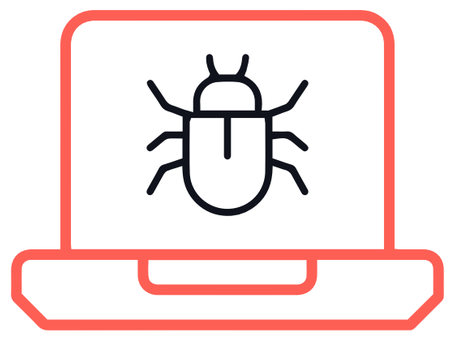
PROTECCIÓN MULTICAPA EN NUBE

ANÁLISIS Y FILTRADO ANTISPAM

- **Integración con SpamAssassin para detectar spam.**
- **Uso de listas negras (RBLs) para bloquear dominios y direcciones IP maliciosas.**
- **Filtrado de spam basado en heurísticas y reglas de puntuación.**
- **Capacidad para aprender (Bayesiano) y mejorar la detección de spam con el tiempo.**
- **Verificación de Reverse DNS (rDNS) para detectar correos sospechosos.**
- **Soporte para Greylisting para retrasar correos sospechosos y reducir spam.**
- **Integración con listas blancas/negras locales y personalizadas.**

PROTECCIÓN ANTIVIRUS Y ESCANEO DE ARCHIVOS ADJUNTOS

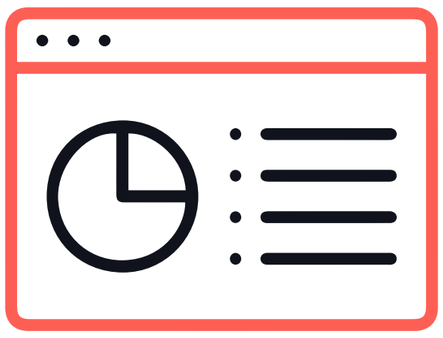
- **Soporte para múltiples motores antivirus (ClamAV, Sophos, McAfee, Avira, F-Secure, entre otros).**
- **Escaneo de archivos adjuntos comprimidos (ZIP, RAR, 7z, TAR, etc.).**
- **Bloqueo de archivos sospechosos o ejecutables peligrosos (EXE, BAT, VBS, SCR).**
- **Análisis heurístico para detección de amenazas ocultas en archivos adjuntos.**
- **Eliminación automática de correos con malware detectado.**



PROTECCIÓN CONTRA PHISHING Y SPOOFING

- **Análisis de enlaces en correos electrónicos para detectar URLs maliciosas.**
- **Comparación de enlaces con bases de datos de sitios de phishing conocidos.**
- **Protección contra spoofing con verificación de SPF, DKIM y DMARC.**
- **Filtrado de correos con encabezados falsificados o remitentes suplantados.**
- **Bloqueo de correos con técnicas de Brand Impersonation Attack.**

FILTRADO BASADO EN REGLAS DE SEGURIDAD

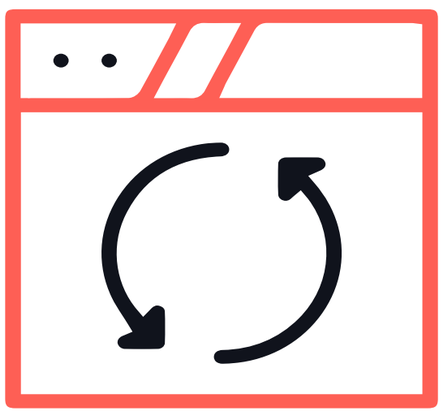


- **Bloqueo de palabras clave y frases sospechosas en correos electrónicos.**
- **Reglas avanzadas para filtrar correos entrantes y salientes.**
- **Definición de políticas de retención y cuarentena para correos sospechosos.**
- **Filtrado de mensajes por idioma o contenido específico.**

ADMINISTRACIÓN DE CUARENTENA Y REPORTES

- **Interfaz web fácil de usar para gestionar y liberar correos en cuarentena.**
- **Posibilidad de permitir o bloquear remitentes específicos con un clic.**
- **Programación de reportes automáticos de actividad y estadísticas de filtrado.**
- **Estadísticas detalladas sobre cantidad de spam, virus, phishing y correos legítimos.**
- **Registros detallados de cada correo analizado con estado de procesamiento.**

MONITOREO EN TIEMPO REAL Y AUDITORÍA



- **Visualización en tiempo real de los correos procesados.**
- **Logs completos de análisis de cada correo (cuerpo, encabezados, adjuntos).**
- **Auditoría y trazabilidad de correos con búsquedas avanzadas por remitente, asunto, contenido o IP.**
- **Alertas en tiempo real sobre intentos de ataque o actividad sospechosa.**

COMPATIBILIDAD Y FLEXIBILIDAD

- **Integración con servidores de correo como Postfix, Sendmail, Exim y Zimbra.**
- **Soporte para bases de datos MySQL/MariaDB para almacenamiento y administración.**
- **Soporte para múltiples usuarios y perfiles con diferentes niveles de acceso.**
- **Capacidad de personalizar reglas y configuraciones según necesidades específicas.**
- **Funciona en sistemas Linux (Debian, Ubuntu, CentOS, RedHat, etc.).**

FASES DE PROTECCIÓN

XCITIONE MAIL PROTECT

1

RECEPCIÓN SMTP

Primera línea de defensas: validación de conexión y reputación para bloquear spam masivos y bots antes de consumir recursos.

AUTENTICACIÓN

Autenticación de dominio con SPF, DKIM y DMARC para prevenir suplantación de identidad y fraudes de marca.

2

3

INSPECCIÓN PROFUNDA

Análisis profundo de contenido, enlaces y adjuntos para detectar phishing, BEC, malware y amenazas avanzadas.

RESPUESTA

Acciones automatizadas basadas en riesgo: cuarentena, etiquetado, reescritura de enlaces o bloqueo para neutralizar amenazas.

4

5

VISIBILIDAD Y MEJORA

Reportes detallados, análisis de tendencias e integración con EasyDmarc para mejorar continuamente la postura de seguridad.

BENEFICIOS PRINCIPALES

FILTRADO Y ANÁLISIS ANTISPAM

- ✓ **Integración con motores avanzados como SpamAssassin.**
- ✓ **Análisis heurístico y bayesiano para detección adaptativa.**
- ✓ **Verificación de Reverse DNS (rDNS) y uso de listas negras (RBLs).**
- ✓ **Filtrado por reglas, puntuación y comportamiento.**
- ✓ **Soporte de listas blancas y negras personalizadas.**
- ✓ **Compatibilidad con SMTP, POP3 e IMAP.**

AUTENTICACIÓN Y REPUTACIÓN DEL DOMINIO

- ✓ **Implementación de protocolos SPF, DKIM, DMARC, BIMI, MTA-STS y TLS-RPT.**
- ✓ **Monitoreo de reputación y exposición de IPs.**
- ✓ **Identificación de fuentes no autorizadas de envío.**
- ✓ **Simulación de impacto de políticas DMARC**
- ✓ **Reportes forenses y agregados automáticos.**

PROTECCIÓN ANTIVIRUS Y ESCANEO DE ADJUNTOS

- ✓ **Escaneo con múltiples motores antivirus (ClamAV, Sophos, Avira, McAfee, etc.).**
- ✓ **Análisis de archivos comprimidos (ZIP, RAR, TAR, 7z).**
- ✓ **Bloqueo de archivos ejecutables peligrosos (EXE, BAT, VBS).**
- ✓ **Detección heurística y eliminación automática de malware.**

DEFENSA CONTRA PHISHING Y SPOOFING

- ✓ **Verificación y cumplimiento de protocolos SPF, DKIM y DMARC.**
- ✓ **Análisis y validación de enlaces sospechosos en correos.**
- ✓ **Bloqueo de intentos de suplantación de remitente.**
- ✓ **Protección contra ataques de “Brand Impersonation”.**

CUARENTENA, REPORTES Y AUDITORÍA

- ✓ Consola web intuitiva para gestionar correos en cuarentena.
- ✓ Liberación manual o automática de correos legítimos.
- ✓ Trazabilidad completa de correos procesados.
- ✓ Alertas en tiempo real y registro de auditoría por usuario.
- ✓ Reportes programados con métricas detalladas de spam, virus y phishing.

GESTIÓN Y MONITOREO CENTRALIZADO

- ✓ Panel de control en la nube con acceso SSL seguro.
- ✓ Roles y permisos personalizados (administrador, usuario, lectura).
- ✓ Integración con servicios como Microsoft 365 y Google Workspace.
- ✓ Visualización en tiempo real del flujo de correos.
- ✓ API para integración con sistemas externos (SIEM, DNS, Helpdesk).

INTELIGENCIA ARTIFICIAL Y APRENDIZAJE

- ✓ Detección de patrones de spam mediante IA.
- ✓ Ajuste dinámico de filtros según comportamiento del tráfico.
- ✓ Reducción de falsos positivos (<0.01%).
- ✓ Análisis por reputación y comportamiento anómalo.

CARACTERÍSTICAS TÉCNICAS CLAVE

Categoría	Especificaciones
Tipo de servicio	Basado en nube (SaaS) – sin hardware local
Protocolos compatibles	SMTP, POP3, IMAP
Mecanismos de autenticación	SPF, DKIM, DMARC, BIMI, MTA-STS, TLS-RPT
Protección adicional	Anti-Relay, Anti-Spoofing, Anti-Phishing
Gestión de usuarios	Ilimitados, con grupos y alias configurables
Cuarentena	Espacio seguro con listas blancas/negras integradas
Reportes	XML, CSV y PDF – programables y personalizables
Seguridad	Cifrado SSL/TLS, MFA, registro de actividad y auditoría
Compatibilidad	Google Workspace, Microsoft 365, Zimbra, Postfix, Exim
Escalabilidad	Multi-dominio y multi-usuario con crecimiento automático
Soporte técnico	Local, con atención vía mesa de ayuda y soporte remoto
Normativas de cumplimiento	ISO 27001, GDPR, CCPA, Ley 29733 (Perú)

CARACTERÍSTICAS TÉCNICAS CLAVE

Reducción del 99.9 % de correos spam

Protección proactiva contra malware y phishing

Mejora de la reputación del dominio y entregabilidad

Administración centralizada y control de usuarios

Cumplimiento normativo en protección de datos

Alta disponibilidad y continuidad del servicio 24/7

REQUISITOS Y SOPORTE

Servicio 100 % gestionado en la nube

Actualizaciones automáticas y upgrades incluidos

Asistencia técnica local especializada

Plataforma con acceso mediante autenticación segura MFA

Integración directa con herramientas de seguridad corporativas

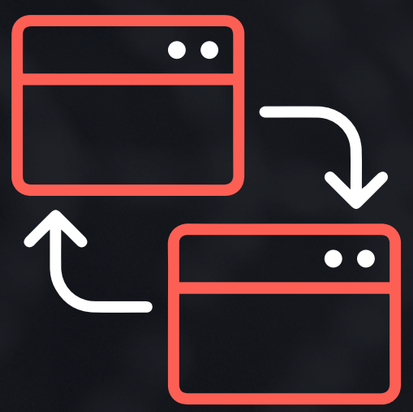
¿POR QUÉ ELEGIR XCITIONE MAIL PROTECT?

TECNOLOGÍA AVANZADA Y ADAPTABLE

Utilizamos los algoritmos más avanzados para ofrecerte una protección inigualable. Innovación constante para mantenernos un paso adelante de los cibercriminales.

SOPORTE EXPERTO Y DEDICADO

Equipo de expertos en ciberseguridad siempre a tu disposición. Asistencia técnica y orientación para ayudarte a sacar el máximo provecho de nuestra plataforma.



EFICIENCIA Y RENDIMIENTO ÓPTIMO

Mejora la eficiencia operativa mediante la gestión centralizada y el servidor de relay seguro. Garantiza un rendimiento óptimo en la entrega de correos electrónicos legítimos.

citione
Mail Protect

www.xcitione.com

PROTECCIÓN DEFINITIVA CONTRA EL CORREO NO DESEADO

994444344