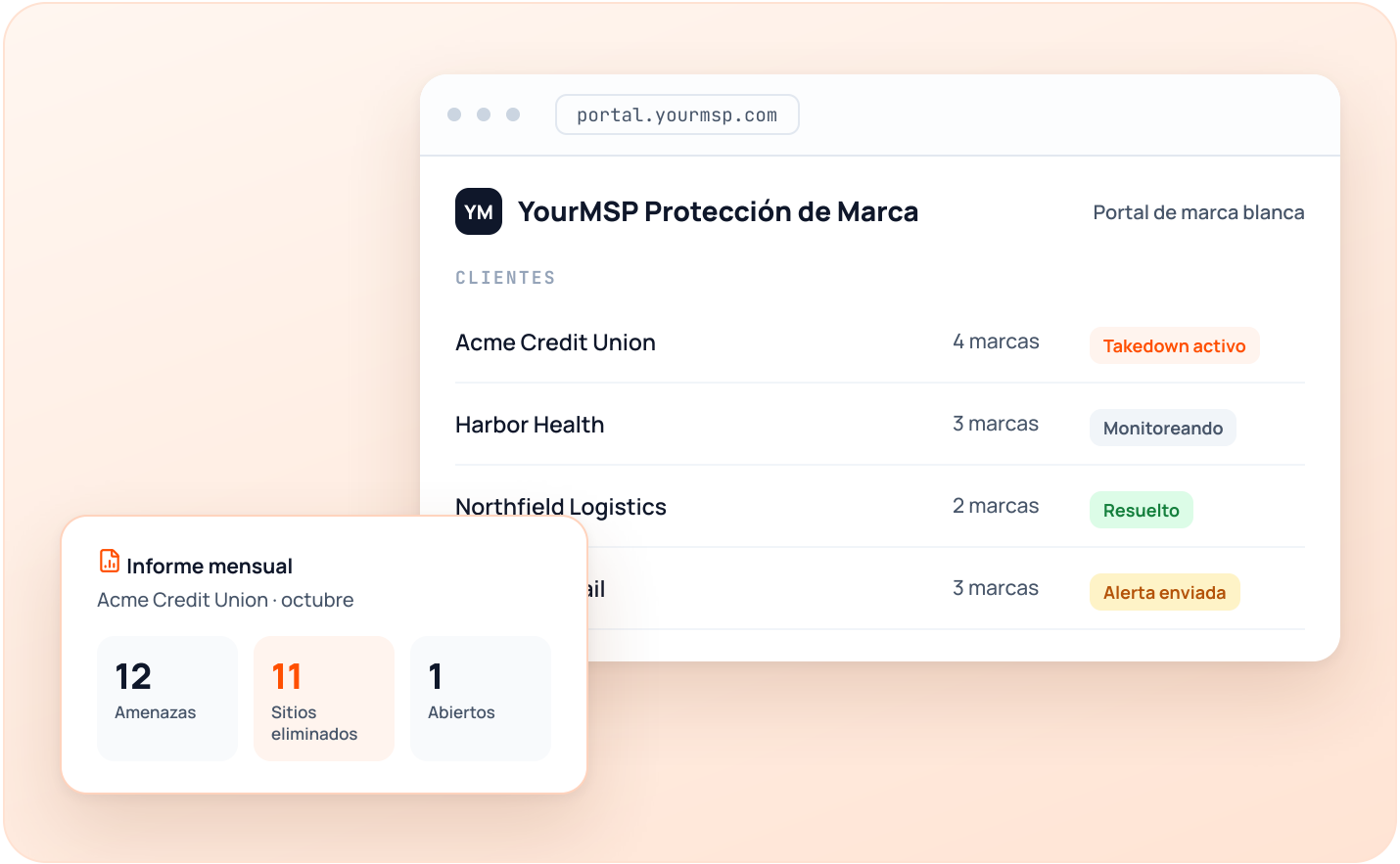
PARA MSP Y MSSP

Protección de marca, con tu marca.

Kit para partners MSSP de protección de marca.

Cómo empaquetar, vender y entregar protección de marca y takedowns a tus clientes.



CONTENIDO

Qué incluye

Todo lo necesario para lanzar el servicio, desde la primera llamada de venta hasta el informe mensual.

01 **La oportunidad** p. 3
Por qué la defensa externa de marca encaja en tus servicios.

02 **Empaquetar el servicio** p. 4
Tres niveles y precios que no castigan los reportes.

03 **Encontrar los clientes** p. 5
Quién lo necesita más y cómo abrir la conversación.

04 **Descubrimiento** p. 6
Las preguntas que revelan la necesidad.

05 **Objeciones** p. 7
Qué dicen los clientes y cómo responder.

06 **Incorporación en una semana** p. 8
Qué pedir a cada cliente.

07 **Autorización** p. 9
Qué puedes hacer por tus clientes y qué requiere aprobación.

08 **Plantilla de autorización** p. 10
Un acta para adaptar con abogados.

09 **Entregar a escala** p. 11
Takedowns para más de 50 clientes.

10 **Informar resultados** p. 12
El informe mensual de una página que renueva contratos.

QUIÉN LEE CADA PARTE

01
Ventas
Secciones 01–05: empaquetar, prospectar, descubrir, responder

02
Incorporación
Secciones 06–08: alcance, autorización, firma

03
Entrega
Secciones 09–10: operar a escala, informar

CÓMO USAR ESTE KIT

Las tablas y listas están pensadas para copiarlas en tus propuestas y procesos. El acta de autorización también se puede descargar por separado, editable.

SECCIÓN 01

01 La oportunidad

Los clientes compran más seguridad como servicio, y los ataques a sus clientes ocurren fuera de tu red.

39.5 mil M

USD · SEGURIDAD GESTIONADA, 2025

Mercado de servicios de seguridad gestionada en 2025, con 11.1% de crecimiento anual hasta 2030.

Fuente: MarketsandMarkets

~15% crecimiento que Canalys previó para los **servicios de seguridad gestionada** en 2025
Canalys, vía MSSP Alert

85% de las empresas del Reino Unido que detectaron un ataque sufrieron **phishing**
Gobierno del Reino Unido, 2025

La brecha fuera del firewall

LO QUE VE TU SOC, Y LO QUE NO

Los sitios falsos no tienen dueño

Dentro de la red

Lo que ya monitoreas

- Endpoints y servidores
- Gateways de email
- Identidad y accesos
- Firewalls y logs

Fuera de la red

Donde los atacantes usan la marca de tu cliente

Sitios de phishing	Activo	Dominios imitadores	Nuevo
Perfiles falsos	Activo	Directivos falsos	Vigilar
Soporte falso	Activo	Logins copiados	Nuevo

Por qué encaja en un MSSP

Amplía tu oferta
La mitad externa del trabajo de seguridad.

Es continuo
Monitoreo y takedowns todos los meses.

Los resultados se ven
Un sitio eliminado es fácil de mostrar.

Amplía la relación
A marketing, legal y atención al cliente.

SECCIÓN 02

02 Empaquetar el servicio

Tres niveles acumulativos. Recomienda el del medio: es el que incluye takedowns.

Monitoreo

Clientes pequeños, o un primer paso

- ✓ Dominios imitadores y sitios de phishing
- ✓ Alertas con evidencia
- — Advertencias en navegadores (Safe Browsing)
- — Takedowns gestionados con seguimiento
- — Monitoreo de redes sociales
- — Monitoreo de directivos (VIP)

Informe: hallazgos

RECOMIENDA ESTE

Protección

Clientes con logins o pagos

- ✓ Dominios imitadores y sitios de phishing
- ✓ Alertas con evidencia
- ✓ Advertencias en navegadores (Safe Browsing)
- ✓ Takedowns gestionados con seguimiento
- — Monitoreo de redes sociales
- — Monitoreo de directivos (VIP)

Informe: hallazgos, takedowns, tiempos

Defensa

Bancos, retail, directivos visibles

- ✓ Dominios imitadores y sitios de phishing
- ✓ Alertas con evidencia
- ✓ Advertencias en navegadores (Safe Browsing)
- ✓ Takedowns gestionados con seguimiento
- ✓ Monitoreo de redes sociales
- ✓ Monitoreo de directivos (VIP)

Informe: todo, más revisión trimestral

Precios que no castigan los reportes

Evitar

Por alerta

Los clientes piden filtrar más, y se escapan amenazas reales.

Evitar

Por takedown

Los clientes dudan en aprobar eliminaciones, y los sitios siguen activos más tiempo.

Usar este

Por alcance, takedowns incluidos

Se cobra por marcas, dominios y directivos protegidos. Todo lo encontrado se elimina.

REGLA PRÁCTICA

Un cliente que debe aprobar un cargo por cada takedown tiene sitios de phishing activos todo el fin de semana. Cobra por alcance e incluye cada takedown.

SECCIÓN 03

03 Encontrar los clientes

No todos los clientes encajan igual. Empieza por los que los atacantes ya copian.

Quién lo necesita más

Logins o pagos

Bancos, retail, SaaS, logística: las páginas que copian los atacantes.

Marca reconocida

Si sus clientes confían en su logo, los atacantes lo usarán.

Directivos visibles

Copiados para estafas de inversión, reclutamiento y pagos.

Historial de quejas

“Me llegó un mensaje raro de ustedes” significa que ya es un objetivo.

Empieza por lo que ya existe

La mejor primera reunión empieza con evidencia. Antes de la llamada, busca dominios imitadores y copias del sitio del cliente, y lleva dos o tres hallazgos. Un dominio real con su nombre convierte “¿esto nos afecta?” en “¿qué hacemos con este?”.

LLEVA ESTO A LA PRIMERA LLAMADA

Hallazgos de ejemplo

portal.yourmsp.com/scan

YM **Escaneo previo · Acme Credit Union**

3 hallazgos

DOMINIO IMITADOR

acme-cu-login.com

Registrado hace 6 días · servidor de correo configurado

Alto

LOGIN COPIADO

secure-acmecu.net/signin

Copia el login de la banca en línea

Crítico

CUENTA FALSA EN REDES

@AcmeCU_Support

Usa el logo; responde quejas de clientes

Alto

Si no encuentras nada activo. También sirve. La conversación pasa a estar listos para el primero, y a los dominios imitadores ya registrados que conviene vigilar.

SECCIÓN 04

04 Descubrimiento

Pregunta por el proceso, no por el producto. Las brechas aparecen en las respuestas.

01 **Cuando un cliente reporta un sitio falso, ¿quién lo gestiona?**

Qué escuchar: Nadie claro, o “marketing” o “soporte”.

02 **¿Cuánto tiempo estuvo activo el último?**

Qué escuchar: Días o semanas, o “no sabemos”.

03 **¿Quién contacta al hosting y al registrador, y quién da seguimiento?**

Qué escuchar: Una persona por email, cuando tiene tiempo.

04 **¿Se enteran de los dominios imitadores antes que sus clientes?**

Qué escuchar: “No”, o “solo cuando alguien se queja”.

05 **¿Han suplantado a sus directivos en redes sociales?**

Qué escuchar: Sí, o “seguramente, no lo hemos revisado”.

06 **¿Qué pasa un viernes por la noche?**

Qué escuchar: Nada hasta el lunes.

07 **¿Cómo lo informan a la dirección?**

Qué escuchar: No lo hacen, o solo después de un incidente.

Lidera con el resultado

Los clientes no compran monitoreo; compran sitios falsos que desaparecen. Arma la propuesta en torno a tres resultados:

01
Encontrado primero
Amenazas detectadas antes de que los clientes las reporten

02
Advertido en minutos
Advertencias en navegadores mientras llega la eliminación

03
Eliminado e informado
Fuera de línea, con un informe para compartir

SECCIÓN 05

05 Objeciones

Lo que vas a escuchar, y cómo responder.

CINCO CONVERSACIONES: EL CLIENTE, Y LUEGO TÚ

Nuestro equipo de marketing se encarga de los sitios falsos.

¿Cuánto tiempo estuvo activo el último, y quién dio seguimiento al hosting? Les sacamos el trabajo de encima; no los reemplazamos.

Ya tenemos seguridad de email.

Eso protege los buzones de tu personal. Esto protege a los clientes que reciben un SMS o un anuncio que lleva a una copia de tu sitio.

No hemos tenido problemas.

Esto encontró el escaneo sobre tu marca esta semana. Si no hay nada activo, conviene vigilar los dominios imitadores latentes.

Suena caro.

Compáralo con un incidente: horas de soporte, reembolsos, contracargos. Se cobra por alcance, con takedowns incluidos, sin sorpresas.

¿No basta con bloquear los dominios?

Bloquear protege a tu personal. Tus clientes navegan desde sus propios teléfonos y redes; solo una advertencia en el navegador y un takedown los protegen.

CIERRA CON UN PILOTO

Dos semanas con su propia marca

Monitorea la marca del cliente durante dos semanas y elimina lo que encuentres. Una eliminación real cierra más ventas que cualquier presentación.

SECCIÓN 06

06 Incorporación en una semana

Un mismo checklist para todos los clientes. Una incorporación desigual es lo primero que falla a escala.

LA PRIMERA SEMANA

1 — DÍA 1
Alcance
Marcas, dominios, logos, directivos, cuentas oficiales

2 — DÍA 2
Autorizar
Autorización firmada para reportar en su nombre

3 — DÍA 3
Línea base
Primer escaneo: qué existe, qué eliminar primero

4 — DÍAS 4-5
Operar
Monitoreo, takedowns e informe mensual

Qué pedir a cada cliente

DATO	POR QUÉ IMPORTA
Marcas, registros y logos	Qué monitorear y qué cuenta como copia
Dominios y cuentas oficiales	Para nunca reportar los sitios propios del cliente
Directivos a proteger	Nombres, cargos y perfiles oficiales, con su consentimiento
Autorización firmada	Prueba de que puedes reportar en su nombre (sección 07)
Contactos para aprobaciones	Quién decide sobre UDRP, cartas legales y declaraciones públicas
Destinatarios del informe	Quién recibe el informe mensual y quién va a la revisión trimestral

ANTES DEL PRIMER SITIO ACTIVO

Consigue la autorización firmada antes del primer takedown, para que nadie espere una firma mientras un sitio de phishing recoge datos de los clientes de tu cliente.

SECCIÓN 07

07 Autorización

No necesitas autorización para reportar un sitio de phishing. Sí para casi todo lo que lo rodea.

REPORTE	QUIÉN PUEDE PRESENTARLO	QUÉ SE PIDE SOBRE LA AUTORIDAD
Sitio de phishing al hosting o registrador	Cualquiera	Normalmente nada; importa la evidencia
Google Safe Browsing, SmartScreen	Cualquiera	Nada
Suplantación en redes sociales	La marca o su representante	Pueden pedir prueba de autoridad
Queja de marca a una plataforma	Titular o agente autorizado	Registro de marca; autorización si es agente
Aviso DMCA	Titular de los derechos o agente autorizado	Declaración, bajo pena de perjurio, de que quien envía está autorizado
Queja UDRP o URS	Titular de la marca, normalmente con abogado	Se presenta a nombre del titular

Preaprobado, o requiere al cliente

PREAPROBADO EN EL ACTA

- Reportar sitios de phishing a Safe Browsing y SmartScreen
- Reportes de abuso a hostings, registradores y CDN
- Reportar cuentas que suplantan en redes
- Avisos sobre contenido copiado del sitio
- Seguimiento y escalamiento a registros

REQUIERE APROBACIÓN DEL CLIENTE

- Presentar un UDRP o URS
- Cartas legales o intimaciones
- Contactar a la prensa o publicar
- Contactar a las autoridades por el cliente
- Comprar un dominio imitador

SECCIÓN 08

08 Plantilla de autorización

El núcleo del acta: alcance, acciones preaprobadas y qué requiere aprobación.

SECCIONES 3–5 DEL ACTA

Versión completa (en inglés): sentrike.ai/downloads

Autorización de protección de marca y takedown

Entre [Cliente] y [Proveedor] · Vigente desde [fecha]

3. ALCANCE

Marcas y registros de marca: nombre, número de registro, oficina (uno por línea)
Dominios del Cliente: lista - nunca deben reportarse
Cuentas oficiales en redes: plataforma, usuario - nunca deben reportarse
Directivos incluidos (con su consentimiento): nombre, cargo, cuentas oficiales

4. ACCIONES PREAPROBADAS (sin aprobación adicional)

a. Reportar sitios de phishing y suplantación a Google Safe Browsing, Microsoft SmartScreen y servicios similares de protección en navegadores.
b. Enviar reportes de abuso a hostings, registradores, registros y CDN, y dar seguimiento o escalar hasta que se elimine el contenido.
c. Reportar cuentas que suplanten al Cliente o a los directivos indicados.
d. Enviar avisos sobre contenido copiado de los sitios del Cliente, como agente autorizado del Cliente.

5. ACCIONES QUE REQUIEREN APROBACIÓN ESCRITA DEL CLIENTE (caso por caso)

a. Iniciar un UDRP, URS u otra disputa de dominio.
b. Enviar cartas legales o intimaciones.
c. Contactar a autoridades o a la prensa en nombre del Cliente.
d. Comprar o registrar dominios para el Cliente.
e. Cualquier declaración pública.

Por el Cliente: nombre, cargo, fecha

Por el Proveedor: nombre, cargo, fecha

⚖ **No es asesoría legal.** Adapta la plantilla con los abogados de ambas partes antes de firmar. Si las marcas pertenecen a otra entidad, esa entidad también firma. La versión completa (en inglés) suma partes, evidencia, contactos, vigencia y una carta de autorización: sentrike.ai/downloads/takedown-authorization-template.txt.

SECCIÓN 09

09 Entregar a escala

Cincuenta clientes funcionan con un tenant por cliente y el trabajo repetitivo automatizado.

UN PORTAL, TODOS LOS CLIENTES

Ilustrativo

portal.yourmsp.com

YM **YourMSP Protección de Marca** — Portal de marca blanca

52	17	143	2
Clientes	Casos abiertos	Eliminados este mes	Esperando al cliente

CLIENTE	MARCAS	CASOS ABIERTOS	MÁS ANTIGUO	ESTADO
Acme Credit Union	4	3	2 días	Takedown activo
Harbor Health	3	0	—	Monitoreo
Northfield Logistics	2	1	6 horas	Advertido
Summit Retail	3	2	1 día	UDRP: aprobar

Qué falla primero, y cómo evitarlo

Incorporación desigual

Usa un mismo checklist para todos (sección 06).

Buzones compartidos para respuestas de abuso

Correspondencia guardada con cada caso, por tenant.

Informes que nadie lee

Una página por cliente: amenazas, bajas, tiempos, decisiones.

Analistas haciendo búsquedas

Automatiza los pasos repetitivos antes de sumar clientes.

MARCA BLANCA

El cliente ve tu portal, tu dominio y tu informe; la plataforma hace el takedown por debajo. Tú te quedas con la relación y el precio.

SECCIÓN 10

10 Informar resultados

Los clientes juzgan un servicio por su informe y renuevan lo que pueden ver. Que sea de una página.

EL INFORME MENSUAL

Ilustrativo

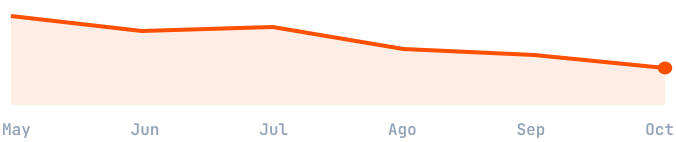
YM **Informe de protección de marca**

Octubre

Acme Credit Union · preparado por YourMSP

12	11	9 h	4 días
Amenazas encontradas	Sitios eliminados	Mediana hasta eliminación	Caso más lento

MEDIANA HASTA LA ELIMINACIÓN, 6 MESES



DECISIONES PENDIENTES

- UDRP para acme-cu-login.com — Aprobar
- Sumar dos directivos al alcance — Revisar

Qué incluye

1. **Amenazas encontradas,** por tipo: sitio de phishing, dominio imitador, cuenta falsa.
2. **Takedowns completados,** y sitios aún en gestión, con su antigüedad.
3. **Tiempo hasta la advertencia y hasta la eliminación:** la mediana y el caso más lento, que es el que el cliente va a preguntar.
4. **Reincidentes,** y **decisiones pendientes** del cliente, como un UDRP.

Qué no presentar como éxito

- ✕ **"Takedowns solicitados":** una solicitud no es una eliminación, y los clientes lo notan la primera vez que un sitio reportado sigue activo una semana después.
- ✕ **Cantidad de alertas sola:** más alertas no es más protección.

REVISIÓN TRIMESTRAL

Una vez por trimestre, muestra la tendencia: qué tan rápido se advierten y eliminan los sitios, qué marcas y canales prefieren los atacantes, y qué sumar al alcance.

EL PROGRAMA DE PARTNERS DE SENTRIKE

Entrégalo con tu marca

Los agentes de IA de Sentrike hacen el trabajo de takedown. Tú te quedas con la relación con el cliente.

Revendedor

Sentrike entrega a tu cliente

- Registro de oportunidades
- Material de ventas
- Participación en ingresos

MSP / MSSP

Tú entregas, con tu marca

- Portal de marca blanca
- Panel multi-tenant
- Uso y facturación por tenant

Tecnología

Tus clientes lo usan en tu producto

- Acceso completo a la API
- Webhooks y eventos en tiempo real
- Soporte técnico

TODAS LAS MODALIDADES

- Sin compromiso inicial, sin volumen mínimo y sin exclusividad
- Tú fijas el precio; Sentrike no vende directo a tus cuentas
- Gerente de éxito de partners, onboarding y soporte prioritario

Suma protección de marca a tus servicios.

Postúlate al programa de partners y haz un piloto con la marca de uno de tus clientes.

Ser partner →

Solicitar acceso

FUENTES

Managed security services market (MarketsandMarkets) www.marketsandmarkets.com/Market-Reports/managed-security-services-mar

Canalys: huge opportunity for MSSPs in 2025 (MSSP Alert) www.msspalert.com/news/canalys-huge-opportunity-for-mssps-in-2025-if-t

Cyber security breaches survey 2025 (UK Government) www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/c

Section 512 of Title 17 (U.S. Copyright Office) www.copyright.gov/512/index.html

WIPO Guide to the UDRP www.wipo.int/en/web/amc/domain-name-disputes/guide