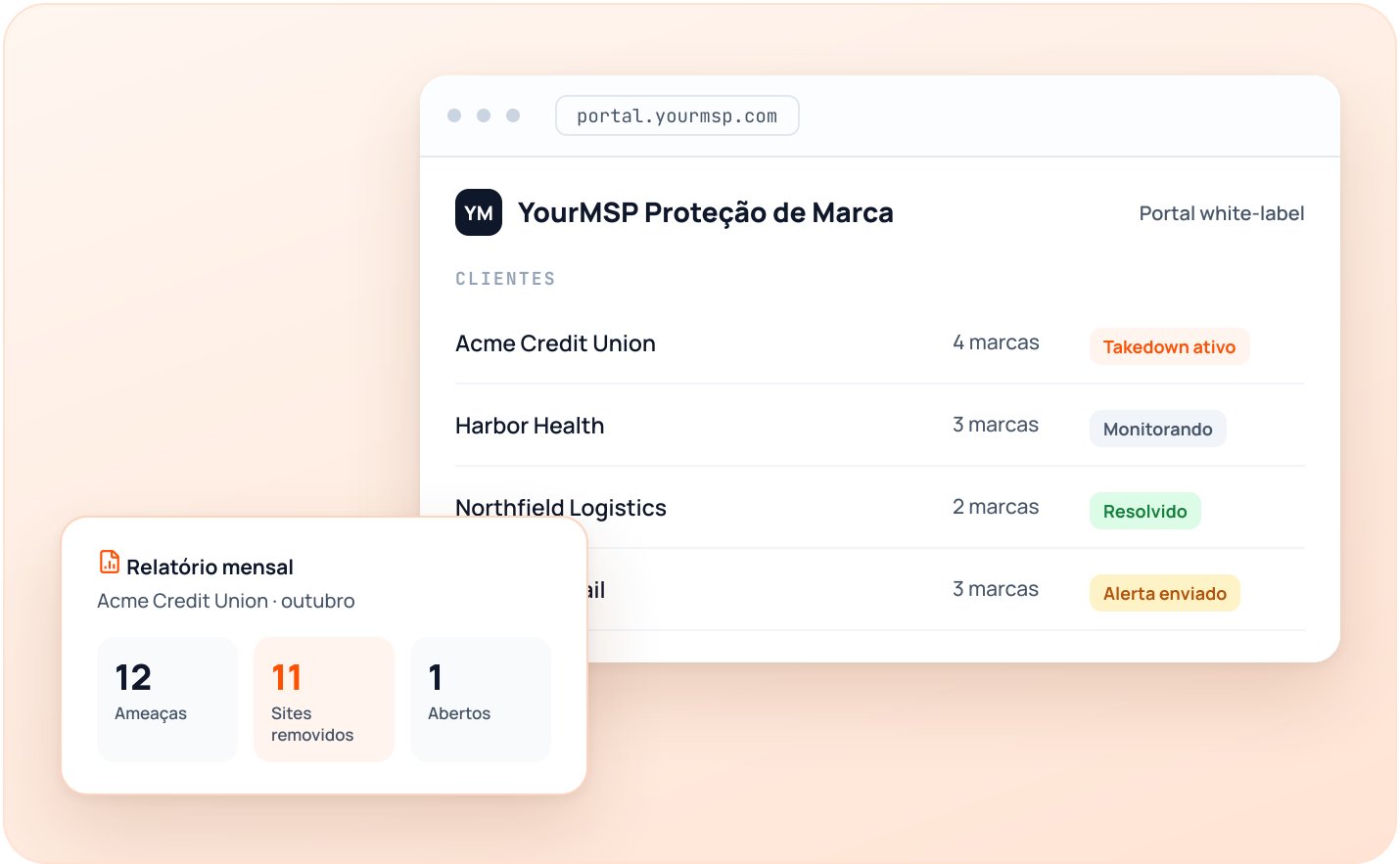
PARA MSPS E MSSPS

Proteção de marca, com a sua marca.

Kit para parceiros MSSP de proteção de marca.

Como empacotar, vender e entregar proteção de marca e takedowns para os seus clientes.



SUMÁRIO

O que tem aqui

Tudo o que você precisa para lançar o serviço, da primeira ligação de vendas ao relatório mensal.

01 **A oportunidade** p. 3
Por que a defesa externa da marca combina com os seus serviços.

02 **Empacotar o serviço** p. 4
Três níveis e preços que não punem as denúncias.

03 **Encontrar os clientes** p. 5
Quem mais precisa e como abrir a conversa.

04 **Descoberta** p. 6
As perguntas que revelam a necessidade.

05 **Objeções** p. 7
O que os clientes dizem e como responder.

06 **Onboarding em uma semana** p. 8
O que pedir a cada cliente.

07 **Autorização** p. 9
O que você pode fazer pelos clientes e o que exige aprovação.

08 **Modelo de autorização** p. 10
Um termo para adaptar com advogados.

09 **Entregar em escala** p. 11
Takedowns para mais de 50 clientes.

10 **Relatar resultados** p. 12
O relatório mensal de uma página que renova contratos.

QUEM LÊ CADA PARTE

01
Comercial
Seções 01–05: empacotar, prospectar, descobrir, responder

02
Onboarding
Seções 06–08: escopo, autorização, assinatura

03
Entrega
Seções 09–10: operar em escala, relatar

COMO USAR ESTE KIT

As tabelas e listas foram feitas para copiar nas suas propostas e processos. O termo de autorização também está disponível como download editável.

SEÇÃO 01

01 A oportunidade

Os clientes compram cada vez mais segurança como serviço, e os ataques aos clientes deles acontecem fora da rede que você monitora.

US$ 39,5 bi

SEGURANÇA GERENCIADA, 2025

Mercado de serviços de segurança gerenciada em 2025, crescendo 11,1% ao ano até 2030.

Fonte: MarketsandMarkets

~15% crescimento que a Canalys previu para **serviços de segurança gerenciada** em 2025

Canalys, via MSSP Alert

85% das empresas do Reino Unido que identificaram um ataque sofreram **phishing**

Governo do Reino Unido, 2025

A lacuna fora do firewall

O QUE O SEU SOC VÊ, E O QUE NÃO VÊ

Sites falsos não têm dono

Dentro da rede

O que você já monitora

- Endpoints e servidores
- Gateways de e-mail
- Identidade e logins
- Firewalls e logs

Fora da rede

Onde os atacantes usam a marca do seu cliente

Sites de phishing	No ar	Domínios imitadores	Novo
Perfis falsos nas redes	No ar	Executivos falsos	Observar
Falsos números de suporte	No ar	Logins copiados	Novo

Por que combina com um MSSP

Amplia o que você vende

A metade externa do mesmo trabalho de segurança.

É contínuo

Monitoramento e takedowns todo mês.

Os resultados aparecem

Um site que caiu é fácil de mostrar.

Amplia a relação

Para marketing, jurídico e atendimento.

SEÇÃO 02

02 Empacotar o serviço

Três níveis cumulativos. Recomende o do meio: é o que inclui takedowns.

Monitorar

Clientes menores, ou um primeiro passo

- ✓ Domínios imitadores e sites de phishing
- ✓ Alertas com evidências
- — Alertas nos navegadores (Safe Browsing)
- — Takedowns gerenciados com acompanhamento
- — Monitoramento de redes sociais
- — Monitoramento de executivos (VIP)

Relatório: alertas

RECOMENDE ESTE

Proteger

Clientes com login ou pagamentos

- ✓ Domínios imitadores e sites de phishing
- ✓ Alertas com evidências
- ✓ Alertas nos navegadores (Safe Browsing)
- ✓ Takedowns gerenciados com acompanhamento
- — Monitoramento de redes sociais
- — Monitoramento de executivos (VIP)

Relatório: alertas, takedowns, tempos

Defender

Bancos, varejo, executivos visíveis

- ✓ Domínios imitadores e sites de phishing
- ✓ Alertas com evidências
- ✓ Alertas nos navegadores (Safe Browsing)
- ✓ Takedowns gerenciados com acompanhamento
- ✓ Monitoramento de redes sociais
- ✓ Monitoramento de executivos (VIP)

Relatório: tudo, mais revisão trimestral

Preços que não punem as denúncias

Evite

Por alerta

Os clientes pedem para filtrar mais, e ameaças reais escapam.

Evite

Por takedown

Os clientes hesitam em aprovar remoções, e os sites ficam mais tempo no ar.

Use este

Por escopo, takedowns incluídos

Preço pelas marcas, domínios e executivos protegidos. Tudo o que é encontrado é removido.

REGRA PRÁTICA

Um cliente que precisa aprovar uma cobrança por takedown tem sites de phishing no ar o fim de semana inteiro. Cobre por escopo e inclua todos os takedowns.

SEÇÃO 03

03 Encontrar os clientes

Nem todo cliente se encaixa igual. Comece pelos que os atacantes já copiam.

Quem mais precisa

Login ou pagamentos

Bancos, varejo, SaaS, logística: as páginas que os atacantes copiam.

Marca conhecida

Se os clientes confiam no logo, os atacantes vão usá-lo.

Executivos visíveis

Copiados em golpes de investimento, emprego e pagamento.

Reclamações

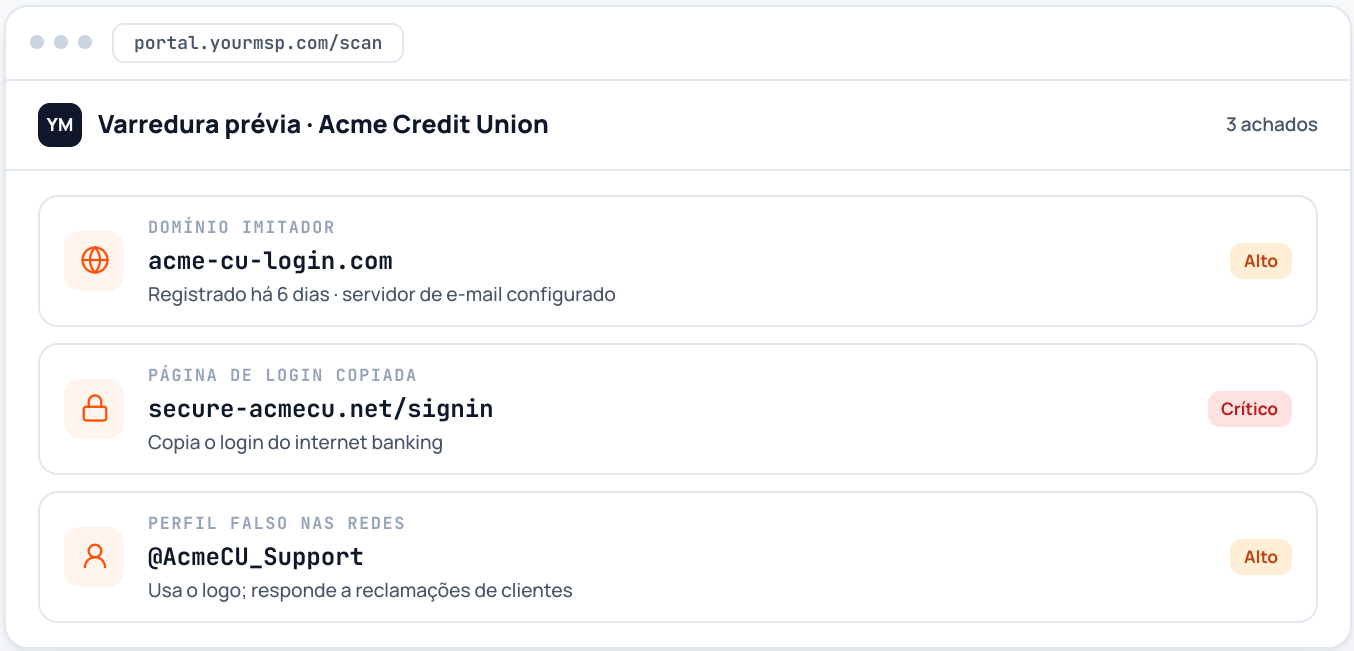
“Recebi uma mensagem estranha de vocês”: já é um alvo.

Comece pelo que já existe

A melhor primeira reunião começa com evidências. Antes da ligação, procure domínios imitadores e cópias do site do cliente e leve dois ou três achados. Um domínio real com o nome deles transforma “isso é um problema para nós?” em “o que fazemos com este?”.

LEVE ISTO À PRIMEIRA LIGAÇÃO

Achados de exemplo



Se a varredura não encontrar nada no ar. Também é útil. A conversa vira estar pronto para o primeiro, e os domínios imitadores já registrados que vale monitorar.

SEÇÃO 04

04 Descoberta

Pergunte sobre o processo, não sobre o produto. As lacunas aparecem nas respostas.

01 **Quando um cliente denuncia um site falso, quem cuida?**

Observe: Ninguém definido, ou “marketing” ou “suporte”.

02 **Quanto tempo o último ficou no ar?**

Observe: Dias ou semanas, ou “não sabemos”.

03 **Quem contata a hospedagem e o registrador, e quem cobra?**

Observe: Uma pessoa por e-mail, quando dá tempo.

04 **Vocês sabem dos domínios imitadores antes dos clientes?**

Observe: “Não”, ou “só quando alguém reclama”.

05 **Já se passaram pelos seus executivos nas redes?**

Observe: Sim, ou “provavelmente, nunca olhamos”.

06 **O que acontece numa sexta à noite?**

Observe: Nada até segunda.

07 **Como isso é reportado à diretoria?**

Observe: Não é, ou só depois de um incidente.

Lidere com o resultado

Clientes não compram monitoramento; compram sites falsos que somem. Monte a proposta em torno de três resultados:

01 **Encontrado primeiro**
Ameaças achadas antes que clientes denunciem

02 **Alertado em minutos**
Alertas nos navegadores enquanto a remoção não sai

03 **Removido e reportado**
Fora do ar, com um relatório para compartilhar

SEÇÃO 05

05 Objeções

O que você vai ouvir, e como responder.

CINCO CONVERSAS: O CLIENTE, DEPOIS VOCÊ

Nosso marketing cuida dos sites falsos.

Quanto tempo o último ficou no ar, e quem cobrou a hospedagem? Tiramos o trabalho das mãos deles; não os substituímos.

Já temos segurança de e-mail.

Ela protege as caixas da sua equipe. Isto protege os clientes que recebem um SMS ou anúncio que leva a uma cópia do seu site.

Nunca tivemos problema.

Veja o que a varredura encontrou na sua marca esta semana. Se nada estiver no ar, vale monitorar os domínios imitadores latentes.

Parece caro.

Compare com um incidente: horas de suporte, reembolsos, chargebacks. O preço é por escopo, com takedowns incluídos, sem surpresas.

Não dá para só bloquear os domínios?

Bloquear protege a sua equipe. Os clientes navegam pelos próprios celulares e redes; só um alerta no navegador e um takedown os protegem.

FECHE COM UM PILOTO

Duas semanas com a própria marca

Monitore a marca do cliente por duas semanas e remova o que encontrar. Uma remoção real fecha mais vendas do que qualquer apresentação.

SEÇÃO 06

06 Onboarding em uma semana

Um mesmo checklist para todos os clientes. Onboarding desigual é a primeira coisa que quebra em escala.

A PRIMEIRA SEMANA

1

DIA 1

Escopo

Marcas, domínios, logos, executivos, perfis oficiais

2

DIA 2

Autorizar

Autorização assinada para denunciar em nome do cliente

3

DIA 3

Linha de base

Primeira varredura: o que existe, o que remover primeiro

4

DIAS 4-5

Operar

Monitoramento, takedowns e relatório mensal

O que pedir a cada cliente

ITEM	POR QUE IMPORTA
Marcas, registros e logos	O que monitorar e o que conta como cópia
Domínios e perfis oficiais	Para nunca denunciar os sites do próprio cliente
Executivos a proteger	Nomes, cargos e perfis oficiais, com consentimento
Autorização assinada	Prova de que você pode denunciar em nome dele (seção 07)
Contatos para aprovações	Quem decide sobre UDRP, notificações e declarações públicas
Destinatários do relatório	Quem recebe o relatório mensal e quem participa da revisão trimestral

ANTES DO PRIMEIRO SITE NO AR

Tenha a autorização assinada antes do primeiro takedown, para ninguém esperar uma assinatura enquanto um site de phishing coleta dados dos clientes do seu cliente.

SEÇÃO 07

07 Autorização

Você não precisa de autorização para denunciar um site de phishing. Precisa para quase tudo ao redor dele.

DENÚNCIA	QUEM PODE FAZER	O QUE PEDEM SOBRE A AUTORIDADE
Site de phishing à hospedagem ou registrador	Qualquer pessoa	Normalmente nada; as evidências é que importam
Google Safe Browsing, SmartScreen	Qualquer pessoa	Nada
Falsificação nas redes sociais	A marca ou seu representante	Podem pedir prova de autoridade
Reclamação de marca a uma plataforma	Titular ou agente autorizado	Registro da marca; autorização para agentes
Notificação DMCA	Titular dos direitos ou agente autorizado	Declaração, sob pena de perjúrio, de que o remetente está autorizado
Reclamação UDRP ou URS	Titular da marca, em geral com advogado	Feita em nome do titular

Pré-aprovado, ou depende do cliente

PRÉ-APROVADO NO TERMO

- Denunciar sites de phishing ao Safe Browsing e SmartScreen
- Denúncias de abuso a hospedagens, registradores e CDNs
- Denunciar perfis falsos nas redes
- Notificações sobre conteúdo copiado do site
- Acompanhamento e escalonamento a registros

EXIGE APROVAÇÃO DO CLIENTE

- Abrir um UDRP ou URS
- Notificações extrajudiciais
- Falar com a imprensa ou publicar
- Contatar autoridades pelo cliente
- Comprar um domínio imitador

SEÇÃO 08

08 Modelo de autorização

O núcleo do termo: escopo, ações pré-aprovadas e o que exige aprovação.

SEÇÕES 3-5 DO TERMO

Versão completa: sentrike.ai/downloads

Autorização de proteção de marca e takedown

Entre [Cliente] e [Prestador] · Vigência a partir de [data]

3. ESCOPO

Marcas e registros de marca: nome, número de registro, órgão (um por linha)
Domínios do Cliente: lista - nunca devem ser denunciados
Perfis oficiais nas redes: plataforma, usuário - nunca devem ser denunciados
Executivos incluídos (com consentimento): nome, cargo, perfis oficiais

4. AÇÕES PRÉ-APROVADAS (sem aprovação adicional)

a. Denunciar sites de phishing e falsificação ao Google Safe Browsing, Microsoft SmartScreen e serviços semelhantes de proteção nos navegadores.
b. Enviar denúncias de abuso a hospedagens, registradores, registros e CDNs, e acompanhar ou escalar até o conteúdo ser removido.
c. Denunciar perfis que se passem pelo Cliente ou pelos executivos indicados.
d. Enviar notificações sobre conteúdo copiado dos sites do Cliente, como agente autorizado do Cliente.

5. AÇÕES QUE EXIGEM APROVAÇÃO POR ESCRITO DO CLIENTE (caso a caso)

a. Abrir um UDRP, URS ou outra disputa de domínio.
b. Enviar notificações extrajudiciais.
c. Contatar autoridades ou a imprensa em nome do Cliente.
d. Comprar ou registrar domínios para o Cliente.
e. Qualquer declaração pública.

Pelo Cliente: nome, cargo, data

Pelo Prestador: nome, cargo, data

⚖ **Não é aconselhamento jurídico.** Adapte o modelo com os advogados das duas partes antes de assinar. Se as marcas pertencem a outra empresa, ela também assina. A versão completa (em inglês) inclui partes, evidências, contatos, vigência e uma carta de autorização: sentrike.ai/downloads/takedown-authorization-template.txt.

SEÇÃO 09

09 Entregar em escala

Cinquenta clientes funcionam quando cada um é um tenant e a rotina é automatizada.

UM PORTAL, TODOS OS CLIENTES

Ilustrativo

portal.yourmsp.com

YM **YourMSP Brand Protection** — Portal white-label

52	17	143	2
Clientes	Casos abertos	Removidos no mês	Aguardando o cliente

CLIENTE	MARCAS	CASOS ABERTOS	MAIS ANTIGO	STATUS
Acme Credit Union	4	3	2 dias	Takedown ativo
Harbor Health	3	0	—	Monitorando
Northfield Logistics	2	1	6 horas	Alertado
Summit Retail	3	2	1 dia	UDRP: aprovação

O que quebra primeiro, e como evitar

Onboarding desigual
Use um mesmo checklist para todos (seção 06).

Caixas compartilhadas para respostas de abuso
Guarde as conversas de cada caso junto do caso, por tenant.

Relatórios que ninguém lê
Uma página: ameaças, remoções, tempos, decisões.

Analistas fazendo buscas
Automatize as etapas repetitivas antes de crescer a carteira.

WHITE-LABEL

O cliente vê o seu portal, o seu domínio e o seu relatório; a plataforma faz o trabalho de takedown por trás. Você fica com a relação e o preço.

SEÇÃO 10

10 Relatar resultados

Os clientes julgam um serviço pelo relatório e renovam o que conseguem ver. Mantenha em uma página.

O RELATÓRIO MENSAL — Ilustrativo



O que entra nele

1. **Ameaças encontradas,** por tipo: site de phishing, domínio imitador, perfil falso.
2. **Takedowns concluídos,** e sites ainda em andamento, com a idade de cada um.
3. **Tempo até o alerta e até a remoção:** a mediana e o caso mais lento, que é o que o cliente vai perguntar.
4. **Reincidentes,** e **decisões pendentes** do cliente, como um UDRP.

O que não apresentar como sucesso

- ✕ **"Takedowns solicitados":** uma solicitação não é uma remoção, e os clientes percebem na primeira vez que um site denunciado continua no ar uma semana depois.
- ✕ **Número de alertas sozinho:** mais alertas não é mais proteção.

REVISÃO TRIMESTRAL

Uma vez por trimestre, mostre a tendência: a rapidez com que os sites são sinalizados e removidos, que marcas e canais os atacantes preferem, e o que incluir no escopo a seguir.

O PROGRAMA DE PARCEIROS DA SENTRIKE

Entregue com a sua marca

Os agentes de IA da Sentrike fazem o trabalho de takedown. Você fica com a relação com o cliente.

Revenda

A Sentrike entrega ao seu cliente

- Registro de oportunidades
- Material de vendas
- Participação na receita

MSP / MSSP

Você entrega, com a sua marca

- Portal white-label
- Painel multi-tenant
- Uso e faturamento por tenant

Tecnologia

Seus clientes usam no seu produto

- Acesso completo à API
- Webhooks e eventos em tempo real
- Suporte técnico

TODAS AS MODALIDADES

- Sem compromisso inicial, volume mínimo ou exclusividade
- Você define o preço; a Sentrike não vende direto para as suas contas
- Gerente de sucesso de parceiros, onboarding e suporte prioritário

Inclua proteção de marca nos seus serviços.

Candidate-se ao programa de parceiros e faça um piloto com a marca de um dos seus clientes.

Seja parceiro →

Solicitar acesso

FONTES

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