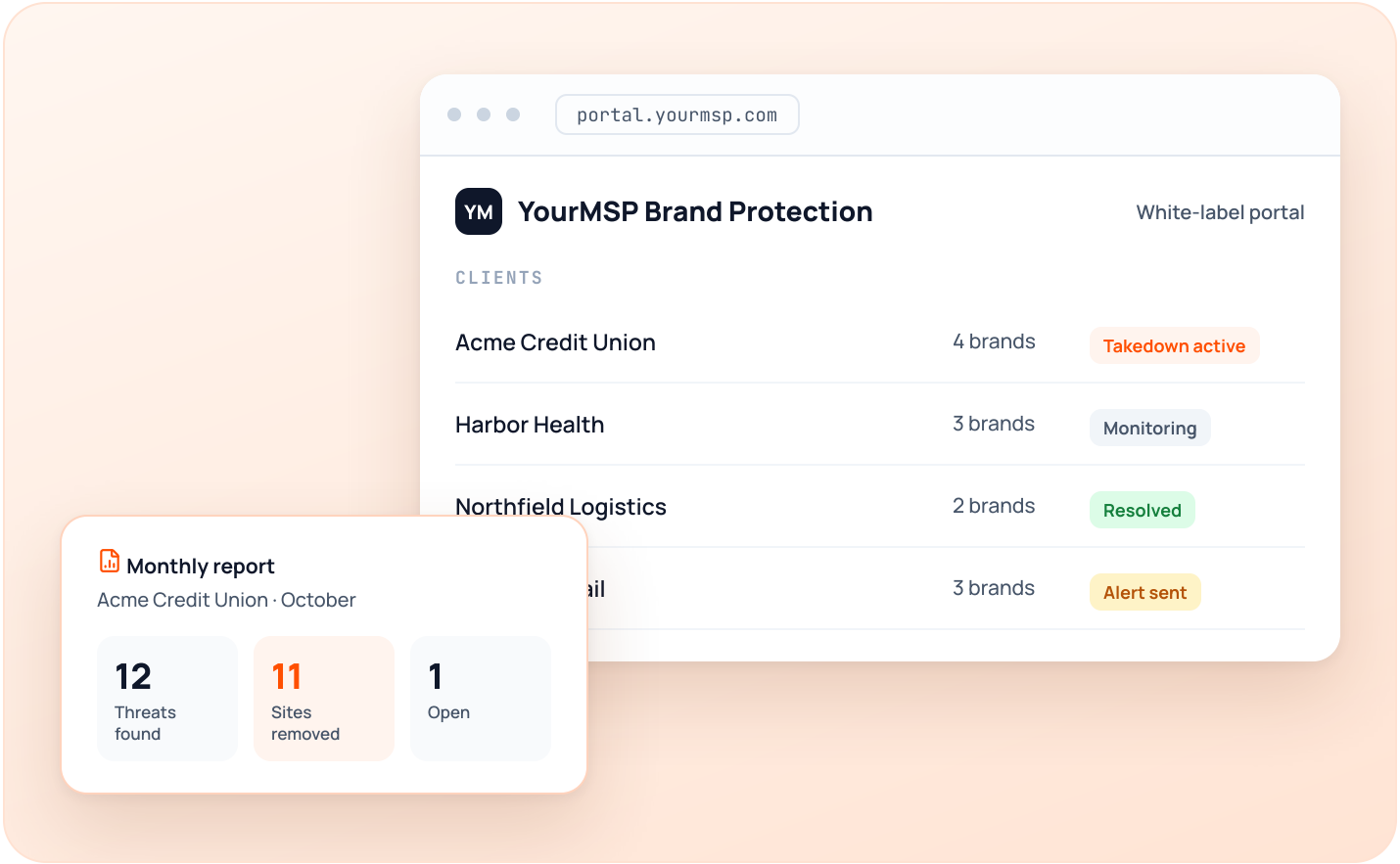
FOR MSPS AND MSSPS

Brand protection, under your brand.

The MSSP Brand Protection Partner Kit.

How to package, sell and deliver brand protection and takedowns for your clients.



CONTENTS

What's inside

Everything you need to launch the service, from the first sales call to the monthly report.

01 **The opportunity** p. 3
Why external brand defense fits your services.

02 **Package the service** p. 4
Three tiers, and pricing that doesn't punish reporting.

03 **Find the right clients** p. 5
Who needs it most, and how to open the conversation.

04 **Discovery** p. 6
The questions that surface the need.

05 **Objections** p. 7
What clients say, and how to answer.

06 **Onboard in a week** p. 8
What to collect from every client.

07 **Authorization** p. 9
What you can do for clients, and what needs approval.

08 **Authorization template** p. 10
A charter to adapt with counsel.

09 **Deliver at scale** p. 11
Running takedowns for 50+ clients.

10 **Report the results** p. 12
The one-page monthly report clients renew on.

WHO READS WHICH PART

01
Sales
Sections 01–05: package, prospect, discover, answer

02
Onboarding
Sections 06–08: scope, authorize, sign

03
Delivery
Sections 09–10: run at scale, report

HOW TO USE THIS KIT

The tables and lists are written to be copied into your own proposals and playbooks. The authorization charter is also a separate, editable download.

SECTION 01

01 The opportunity

Clients are buying more security as a service, and the attacks on their customers happen outside the network you watch.

$39.5B

MANAGED SECURITY, 2025

Managed security services market in 2025, growing 11.1% a year to 2030.

Source: MarketsandMarkets

~15% growth Canalys forecast for **managed security services** in 2025

Canalys, via MSSP Alert

85% of UK businesses that identified an attack had experienced **phishing**

UK Government, 2025

The gap outside the firewall

WHAT YOUR SOC SEES, AND WHAT IT DOESN'T

Fake sites have no owner

Inside the network

What you already monitor

- Endpoints and servers
- Email gateways
- Identity and logins
- Firewalls and logs

Outside the network

Where attackers use your client's brand

Phishing sites	Live	Lookalike domains	New
Fake social accounts	Live	Fake executives	Watch
Fake support numbers	Live	Copied logins	New

Why it fits MSSPs

Extends what you sell

The outside half of the same security job.

It's continuous

Monitoring and takedowns run every month.

Results are visible

A site that's gone is easy to show.

Widens the relationship

To marketing, legal and customer support.

SECTION 02

02 Package the service

Three additive tiers. Lead with the middle one: it's the one that includes takedowns.

Monitor

Smaller clients, or a first step

- ✓ Lookalike domains and phishing sites
- ✓ Alerts with evidence
- — Browser warnings (Safe Browsing)
- — Managed takedowns with follow-up
- — Social media monitoring
- — Executive (VIP) monitoring

Report: findings

LEAD WITH THIS

Protect

Clients with customer logins or payments

- ✓ Lookalike domains and phishing sites
- ✓ Alerts with evidence
- ✓ Browser warnings (Safe Browsing)
- ✓ Managed takedowns with follow-up
- — Social media monitoring
- — Executive (VIP) monitoring

Report: findings, takedowns, timings

Defend

Banks, retailers, visible executives

- ✓ Lookalike domains and phishing sites
- ✓ Alerts with evidence
- ✓ Browser warnings (Safe Browsing)
- ✓ Managed takedowns with follow-up
- ✓ Social media monitoring
- ✓ Executive (VIP) monitoring

Report: everything, plus quarterly review

Pricing that doesn't punish reporting

Avoid

Per alert

Clients ask you to filter harder, and real threats get missed.

Avoid

Per takedown

Clients hesitate to approve removals, so sites stay up longer.

Use this

Per scope, takedowns included

Priced on brands, domains and executives protected. Everything found gets removed.

RULE OF THUMB

A client who must approve a fee for each takedown is a client whose phishing sites stay up over the weekend. Price on scope; include every takedown.

SECTION 03

03 Find the right clients

Not every client is an equal fit. Start with the ones attackers already copy.

Who needs it most

Logins or payments

Banks, retailers, SaaS, logistics: the pages attackers copy.

A recognizable brand

If customers trust its logo, attackers will use it.

Visible executives

Copied for investment, recruiting and payment scams.

Past complaints

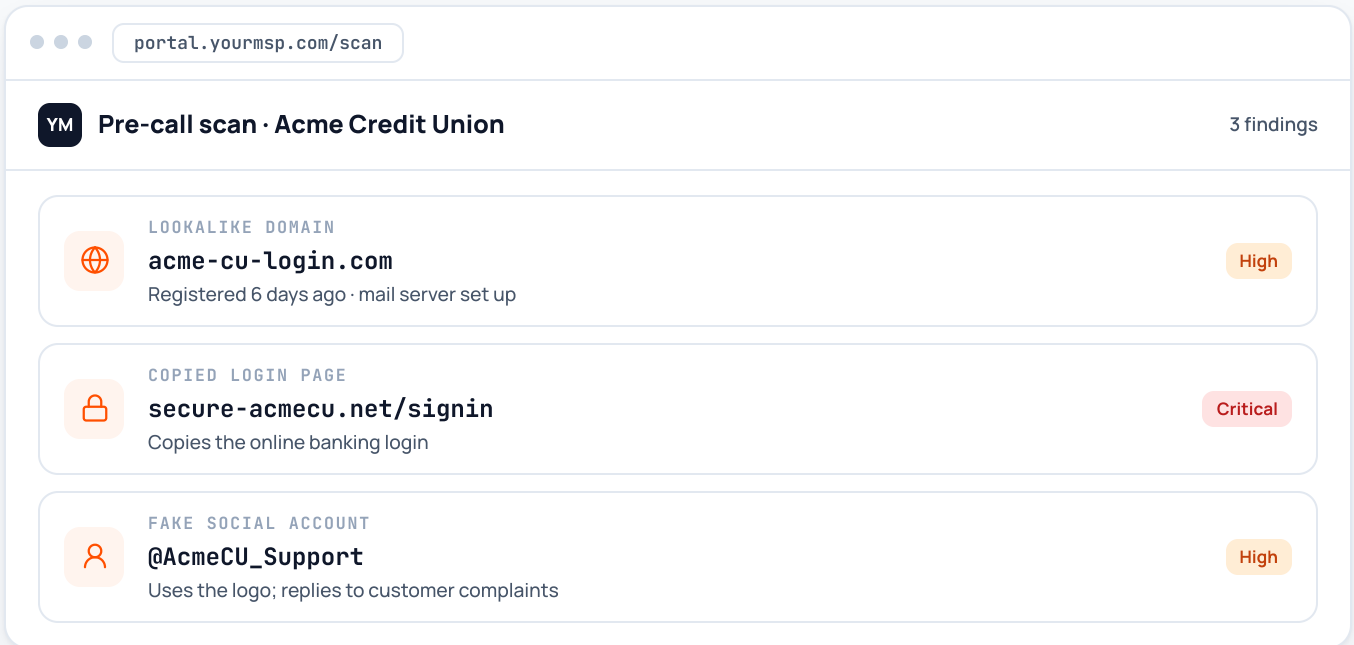
“I got a strange text from you” means it’s already a target.

Open with what already exists

The most effective first meeting starts with evidence. Before the call, scan for lookalike domains and copies of the client’s site, and bring two or three findings. A real domain with their name in it turns “is this a problem for us?” into “what do we do about this one?”.

BRING THIS TO THE FIRST CALL

Example findings



If the scan finds nothing live. That’s useful too. The conversation becomes about being ready for the first one, and about the dormant lookalikes already registered that are worth watching.

SECTION 04

04 Discovery

Ask about the process, not the product. The gaps show up in the answers.

01 When a customer reports a fake website, who handles it?

Listen for: No clear owner, or “marketing” or “support”.

02 How long did the last one stay up?

Listen for: Days or weeks, or “we don’t know”.

03 Who contacts the host and registrar, and who follows up?

Listen for: One person doing it by email, when they have time.

04 Do you know about lookalike domains before customers do?

Listen for: “No”, or “only when someone complains”.

05 Have your executives been impersonated on social media?

Listen for: Yes, or “probably, we haven’t looked”.

06 What happens on a Friday evening?

Listen for: Nothing until Monday.

07 How do you report this to leadership?

Listen for: They don’t, or only after an incident.

Lead with the result

Clients don’t buy monitoring; they buy fake sites that go away. Frame the proposal around three outcomes:

01
Found first
Threats found before customers report them

02
Warned in minutes
Browser warnings while removal is in progress

03
Removed and reported
Offline, with a report the client can share

SECTION 05

05 Objections

What you'll hear, and how to answer.

FIVE CONVERSATIONS: THE CLIENT, THEN YOU

Our marketing team handles fake sites.

How long did the last one stay up, and who followed up with the host? We take the work off their plate; we don't replace them.

We already have email security.

That protects your staff's inboxes. This protects customers who get a text or ad leading to a copy of your site.

We haven't had a problem.

Here's what the scan found on your brand this week. If nothing is live, the dormant lookalikes are worth watching.

It sounds expensive.

Compare it to one incident: support time, refunds, chargebacks. It's priced on scope, takedowns included, so there are no surprises.

Can't we just block the domains?

Blocking protects your staff. Customers browse from their own phones and networks; only a browser warning and a takedown protect them.

CLOSE ON A PILOT

Two weeks on their own brand

Monitor the client's brand for two weeks and take down what you find. A real removal closes more deals than any slide.

SECTION 06

06 Onboard in a week

One checklist for every client. Inconsistent onboarding is the first thing that breaks at scale.

THE FIRST WEEK

1 — DAY 1
Scope
Brands, domains, logos, executives, official accounts

2 — DAY 2
Authorize
Signed authorization to report on their behalf

3 — DAY 3
Baseline
First scan: what exists, what to remove first

4 — DAYS 4–5
Run
Monitoring, takedowns and the monthly report

What to collect from every client

ITEM	WHY IT MATTERS
Brands, trademarks and logos	What to monitor, and what counts as a copy
Official domains and accounts	So the client's own sites are never reported
Executives to protect	Names, roles and official profiles, with their consent
Signed authorization	Proof you can report on their behalf (section 07)
Contacts for approvals	Who decides on UDRPs, legal letters and public statements
Report recipients	Who gets the monthly report, and who joins the quarterly review

BEFORE THE FIRST LIVE SITE

Get the authorization signed before the first takedown, so nobody is waiting for a signature while a phishing site is collecting your client's customers' data.

SECTION 07

07 Authorization

You don't need authorization to report a phishing site. You do for almost everything around it.

REPORT	WHO CAN FILE	WHAT'S ASKED ABOUT AUTHORITY
Phishing site to host or registrar	Anyone	Usually nothing; evidence is what matters
Google Safe Browsing, SmartScreen	Anyone	Nothing
Social media impersonation	The brand or its representative	May ask for proof of authority
Trademark complaint to a platform	Rights holder or authorized agent	Trademark registration; authorization for agents
DMCA notice	Copyright owner or authorized agent	A statement, under penalty of perjury, that the sender is authorized
UDRP or URS complaint	Trademark holder, usually through counsel	Filed in the trademark holder's name

Pre-approved, or needs the client

PRE-APPROVED IN THE CHARTER

- Reporting phishing sites to Safe Browsing and SmartScreen
- Abuse reports to hosts, registrars and CDNs
- Reporting impersonating social accounts
- Notices about copied site content
- Follow-ups and escalation to registries

NEEDS THE CLIENT'S APPROVAL

- Filing a UDRP or URS complaint
- Legal letters or cease-and-desist notices
- Contacting the press or posting publicly
- Contacting law enforcement for the client
- Buying a lookalike domain

SECTION 08

08 Authorization template

The core of the charter: scope, pre-approved actions and what needs approval.

SECTIONS 3–5 OF THE CHARTER

Full version: sentrike.ai/downloads

Brand protection and takedown authorization

Between [Client] and [Provider] · Effective [date]

3. SCOPE

Brands and trademarks: name, registration number, office (one per line)
Domains owned by Client: list - these must never be reported
Official social media accounts: platform, handle - these must never be reported
Executives covered (with their consent): name, title, official accounts

4. PRE-APPROVED ACTIONS (no further approval needed)

a. Reporting phishing and impersonating websites to Google Safe Browsing, Microsoft SmartScreen and similar browser protection services.
b. Sending abuse reports to hosting providers, registrars, registries and CDNs, and following up or escalating until the content is removed.
c. Reporting accounts that impersonate Client or the executives listed above to the platforms concerned.
d. Sending notices about content copied from Client's websites, as Client's authorized agent.

5. ACTIONS THAT NEED CLIENT'S WRITTEN APPROVAL (per case)

a. Filing a UDRP, URS or other domain dispute.
b. Sending legal letters or cease-and-desist notices.
c. Contacting law enforcement or the press on Client's behalf.
d. Buying or registering domains for Client.
e. Any public statement.

For the Client: name, title, date

For the Provider: name, title, date

⚖ **Not legal advice.** Adapt the template with both parties' counsel before it's signed. If the trademarks are held by a separate entity, that entity signs too. The full version adds parties, evidence, contacts, term and a letter of authorization: sentrike.ai/downloads/takedown-authorization-template.txt.

SECTION 09

09 Deliver at scale

Fifty clients work when each is a separate tenant and the repetitive work is automated.

ONE PORTAL, EVERY CLIENT

Illustrative

portal.yourmsp.com

YM **YourMSP Brand Protection** White-label portal

52	17	143	2
Clients	Open cases	Removed this month	Waiting on a client

CLIENT	BRANDS	OPEN CASES	OLDEST	STATUS
Acme Credit Union	4	3	2 days	Takedown active
Harbor Health	3	0	—	Monitoring
Northfield Logistics	2	1	6 hours	Warned
Summit Retail	3	2	1 day	UDRP: approval

What breaks first, and how to avoid it

Inconsistent onboarding

Use one checklist for everyone (section 06).

Shared inboxes for abuse replies

Keep every case's correspondence with the case, per tenant.

Reports nobody reads

One page per client: threats, removals, timings, decisions.

Analysts doing lookups

Automate the repetitive steps before you grow the client list.

WHITE-LABEL

The client sees your portal, domain and report; the platform does the takedown work underneath. You own the relationship and the pricing.

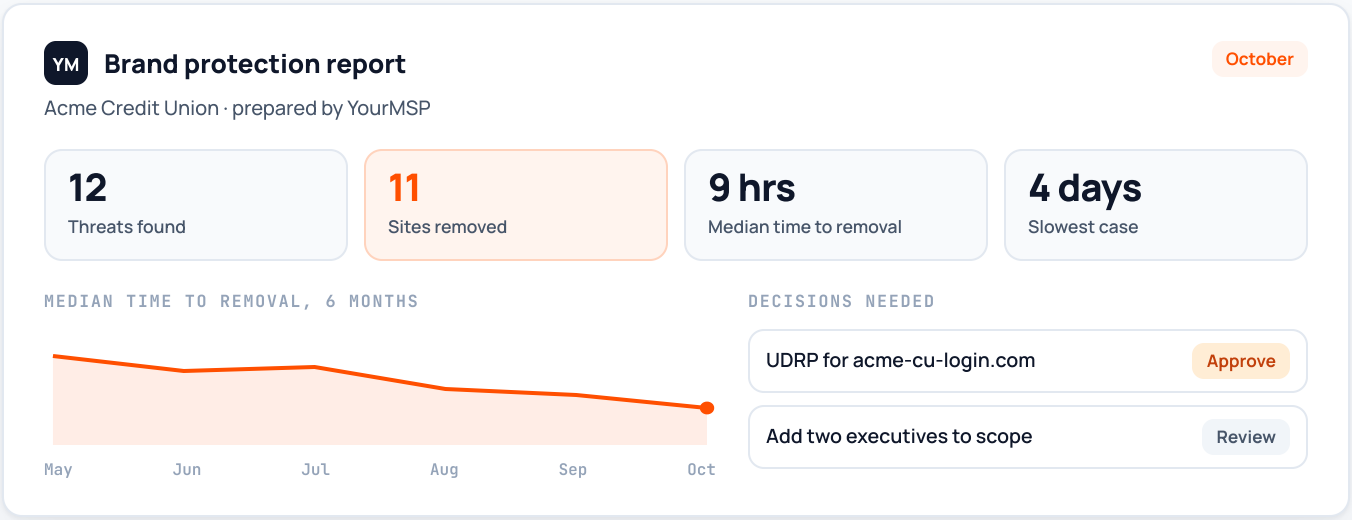
SECTION 10

10 Report the results

Clients judge a service by its report, and renew what they can see. Keep it to one page.

THE MONTHLY REPORT

Illustrative



What goes in it

1. **Threats found,** by type: phishing site, lookalike domain, fake account.
2. **Takedowns completed,** and sites still being worked on, with their age.
3. **Time to warning and to removal:** the median and the slowest case, which is what the client will ask about.
4. **Repeat offenders,** and **decisions needed** from the client, such as a UDRP.

What not to report as success

- ✕ **"Takedowns requested":** a request isn't a removal, and clients learn the difference the first time a reported site is still live a week later.
- ✕ **Alert counts on their own:** more alerts isn't more protection.

QUARTERLY REVIEW

Once a quarter, show the trend: how fast sites are warned and removed, which brands and channels attackers favor, and what to add to the scope next.

THE SENTRIKE PARTNER PROGRAM

Deliver it under your brand

Sentrike's AI agents do the takedown work. You keep the customer relationship.

Reseller

Sentrike delivers to your customer

- Deal registration
- Sales enablement
- Revenue share

MSP / MSSP

You deliver, under your brand

- White-label portal
- Multi-tenant dashboard
- Per-tenant usage and billing

Technology

Customers use it in your product

- Full API access
- Webhooks and real-time events
- Technical support

EVERY TRACK

- No upfront commitment, minimum volume or exclusivity
- You set the price; Sentrike doesn't sell direct into your accounts
- Partner success manager, onboarding and priority support

Add brand protection to your services.

Apply to the partner program and run a pilot on one of your clients' brands.

Become a partner →

Request access

SOURCES

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