ISSUE 01 / FIELD GUIDE

THE MARKETING ATTACK SURFACE

How to secure the agencies, platforms, data and technology behind your marketing



CONTRIBUTING CYBERSECURITY PERSPECTIVE

CYTEK

39.0997° N / 94.5786° W • 2026

Your marketing agency is part of your cybersecurity perimeter.

Modern marketing is no longer contained inside the marketing department. It runs on a sprawl of connected systems, and the people who operate those systems increasingly sit outside your building, at an agency, a contractor, a freelancer, or a platform partner.

That sprawl is what makes modern marketing fast, and it is also what makes marketing a security problem, because access granted for speed is rarely reviewed for risk.

What marketing actually touches

On a typical engagement, the marketing function, meaning the internal team and its outside partners together, holds credentials to some or all of the following:

- **CRM** and everything in it: contacts, deal history, notes, exports
- **Customer data**: lists, segments, uploaded audiences, enrichment files
- **Advertising accounts** with live payment methods attached
- **Analytics** and the tag manager that can inject arbitrary script into every page
- **The website**, its CMS, and often its hosting
- **DNS**: the single highest-leverage record set your company owns
- **Email** sending domains, authentication records, and automation platforms
- **Social** accounts, business managers, and the identities behind them
- **Marketing automation** with read/write access back into the CRM
- **AI tools**, increasingly, with data pasted into them and OAuth grants left open

> **Any one of those, on its own, is a reasonable thing to give an agency. All of them together, held by a third party you have never security-reviewed, is a different proposition entirely.**

The argument

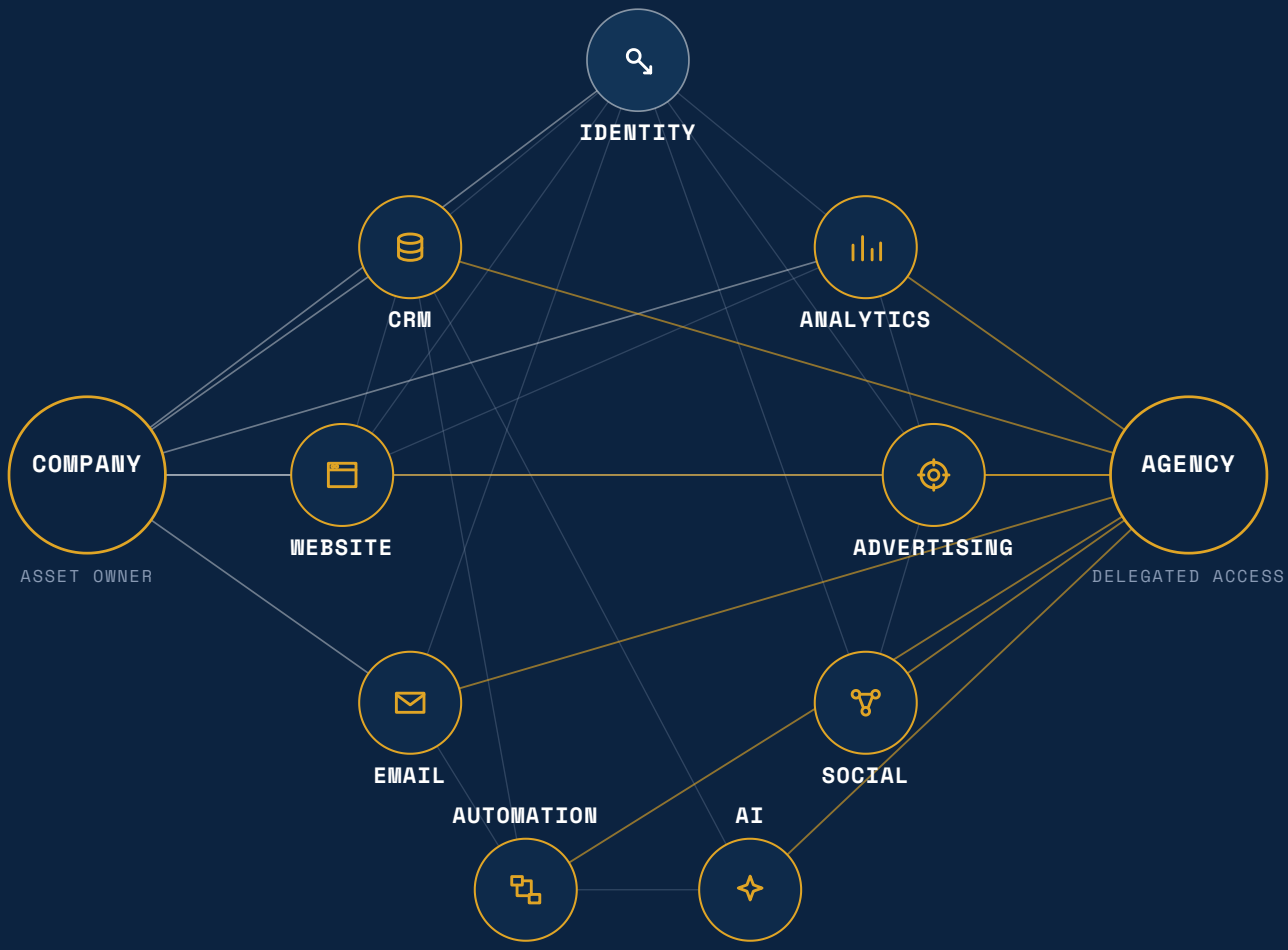
You do not need your agency to be a cybersecurity company. Demanding that would be theatre, producing a binder of policies that changes nothing about your actual exposure.

What you need is narrower and far more achievable: **make sure your agency does not become the easiest path into your company.** Attackers are economically rational, and they work down the chain until they reach the link with shared logins, no MFA, a former employee's account still active, and an OAuth token granted in 2022 that nobody has looked at since.

This guide closes that gap with fifteen specific controls, most of which take an afternoon and none of which require a security program.

THE MODERN MARKETING ATTACK SURFACE

FIG. 01



OWNED BY THE COMPANY

SYSTEM-TO-SYSTEM TRUST

REACHABLE BY THE AGENCY

SHARED — THE ACTUAL SURFACE

Every edge is a credential, a token, or a trust relationship. The surface lives in the connections between these systems as much as in the systems themselves.

WHO HAS THE KEYS?

Almost every marketing breach begins with somebody holding access they should never have had.

SECTION 01 OF 04

Access is the whole game.

If you fix nothing else in this guide, fix access. It is the layer that makes every other control meaningful, and where most real-world marketing compromise happens.

Least privilege, in practice

Least privilege has a reputation as an ideal nobody reaches. In marketing systems it is unusually tractable, because the platforms already model it well:

- An agency running paid media needs to build and edit campaigns, with no rights to add users, change billing, or export your customer list.
- A content team needs to draft and publish pages, with no server, plugin or DNS access.
- An analytics contractor needs to read reports and configure events, rarely property admin and almost never the tag manager's publish right.

For each partner, name the smallest role that covers their contracted work. Occasionally elevating access costs far less than a standing over-grant.

Individual accounts, always

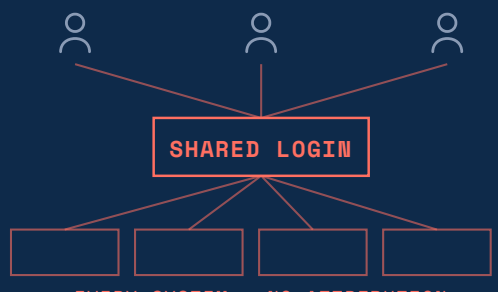
Shared logins are the most common finding in an access review, and they fail three ways at once: **no attribution**, because the audit log records one username; **no offboarding**, because the credential outlives every departure; and **no real MFA**, because a shared second factor is a shared secret with extra steps.

> **If a vendor says they need a shared login because their team is small, they are telling you they have not built a way to manage access.**

Who owns the account

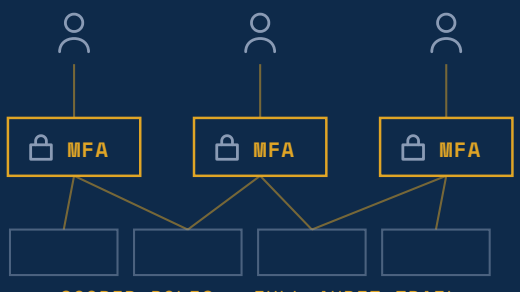
This is the most expensive control to fix retroactively. Ad accounts, analytics properties, the domain and the CMS should be **owned by your company**, with the agency granted access. When the agency owns the asset, you cannot revoke their access and the historical data is theirs. Ask early, while everyone is friendly.

✕ THE DEFAULT



One leak reaches every system.

✓ THE MODEL



One leak stops at one person's scope.

> **Your marketing agency is part of your security perimeter whether you treat it that way or not.**

[Contributor Name] [TITLE]

CYTEK

The organizations that get this wrong are rarely careless. They are usually working from an old map, one drawn when the security perimeter matched the building and the marketing department was a place rather than a network of relationships.

What we see in practice is that marketing accumulates access faster than any other business function and reviews it least often. A campaign needs a tool, the tool needs a connection, the connection needs a token, and the token outlives the campaign by several years. No single decision in that chain was a bad one, which is how the exposure assembles itself unnoticed.

Marketing systems are also trusted systems. Your tag manager can execute code on every page of your website, your email platform can send as your domain, and your CRM holds every customer you have. These carry the same blast radius as core infrastructure while almost never being governed like it.

The fix is to treat the relationship as infrastructure, which means inventorying what it touches, scoping what it can do, and reviewing it on a schedule. None of that requires treating your agency as a threat. It is ordinary operational hygiene, and it usually decides whether an incident stays contained.



CONTRIBUTED PERSPECTIVE · CYTEK

MARKETING DATA IS COMPANY DATA.

The list in your email platform is the same list a regulator will ask you about.

SECTION 02 OF 04

The list is the liability.

Marketing data gets handled as a working asset when it is in fact a governed one. It is copied into spreadsheets, uploaded to platforms, pasted into tools, and shared over whatever channel was convenient, and every copy that gets made is indefinite exposure.

What is actually in scope

- **Customer and prospect lists**: often the company's most complete contact database
- **PII**: names, emails, phone numbers, addresses, and sometimes far more
- **Lead data** including form submissions, call recordings and chat transcripts
- **Behavioral data**: on-site activity, engagement history, inferred attributes
- **Analytics** identifiers that are personal data in most modern privacy regimes
- **Uploaded audiences**: customer lists pushed into ad platforms for matching

Minimize, then retain deliberately

Do we need this field? Marketing collects what is easy to collect, and every extra field is one you must protect, disclose and delete on request. Shortening a form is that rare security control which also improves conversion.

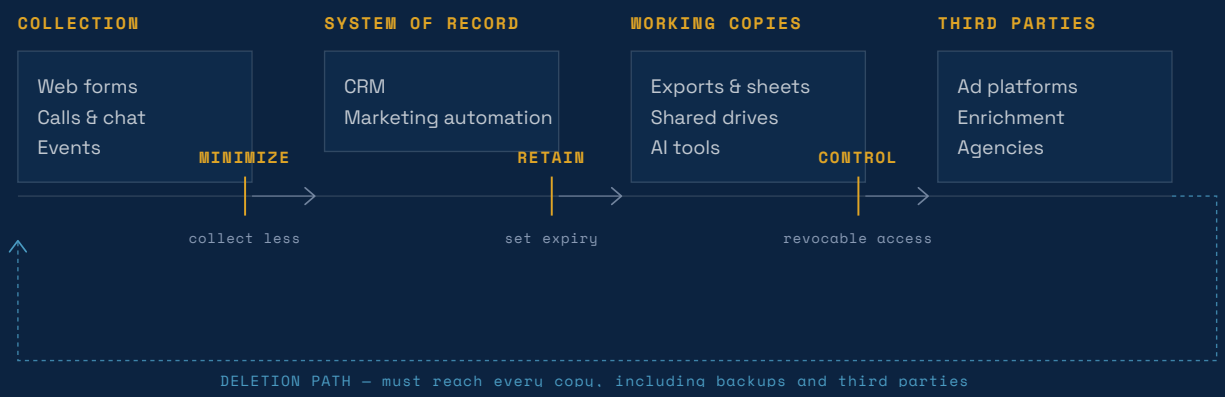
When does this expire? Most marketing data has no retention policy, which means the policy is *forever*. A list from a 2019 campaign has quietly become an unexamined liability with a decreasing chance of ever producing revenue.

Moving data without leaking it

Customer data should not travel by email attachment, consumer file-sharing link or chat upload, which are the three most common paths in practice. Use an access-controlled destination where permissions can be revoked and access is logged. Encryption matters less than **revocability** here, because an emailed spreadsheet cannot be recalled once it is sent.

Deletion has to be real

Deletion means removed from source systems, from the platforms it was pushed to, from backups on their own schedule, and from every working copy. If your agency cannot describe how they would delete your data, then they cannot delete it, and both your contract and most privacy regimes assume they can.



YOUR WEBSITE IS PRODUCTION INFRASTRUCTURE.

It is code execution, identity, and email deliverability wearing a marketing costume.

SECTION 03 OF 04

A marketing stack is infrastructure.

The website looks like a marketing asset because marketing is what it does. Structurally it is production infrastructure that happens to serve pages, and the access surrounding it reaches further than most people assume.

The CMS and its plugin problem

A CMS with plugin installation rights is a system where a user can execute arbitrary code on your server. An admin role grants the privilege to install software, which is a great deal more than the privilege to edit the website. Separate authoring from administration, keep the plugin inventory short, and treat every plugin as a vendor you did not vet.

DNS is the highest-leverage system you own

Whoever controls DNS controls where your domain points, who can send email as you, and who can obtain a valid certificate in your name. It is the most powerful access in this guide, and it is routinely handed to whoever built the last website.

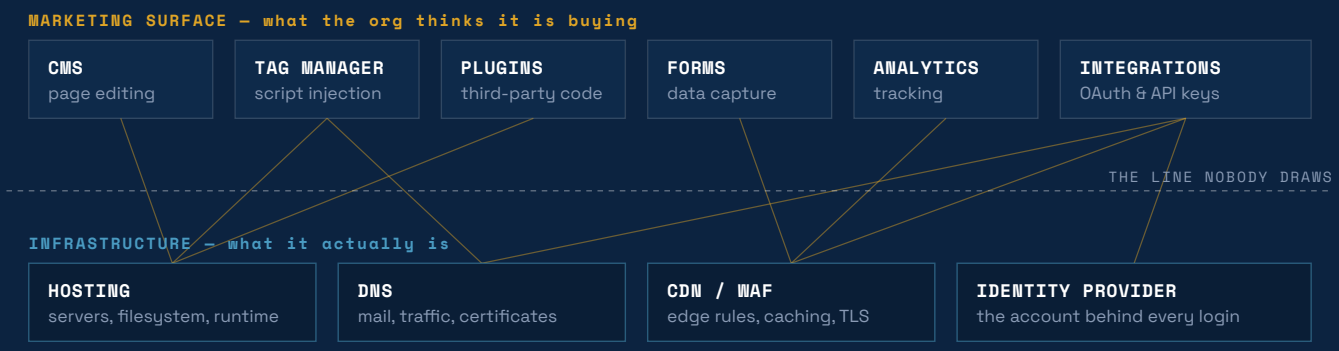
DNS deserves a named internal owner, MFA without exception, registrar lock, and a change process. If your agency needs a record added, they can request it. Standing DNS access for a marketing vendor is very hard to justify.

The tag manager is a code injection tool

Google Tag Manager exists to inject JavaScript into every page of your site without a deploy. That is genuinely useful, and it is also precisely the capability an attacker wants, and it is how card-skimming attacks work. Restrict **publish** rights to a small named group and let everyone else draft. Turn on change notifications, and review the container for tags nobody can account for.

Backups, APIs and OAuth

- **Backups** off-host, restore-tested, and not writable by the CMS, because ransomware that reaches your site will reach any backup that site can write to.
- **API keys** scoped, rotated, and never committed to a repo or a page template.
- **OAuth grants** are the quiet one, a durable credential that survives password changes and never appears in your user list.



Every diagonal is a credential, token or trust relationship granted for a marketing task.

TREAT MARKETING SYSTEMS LIKE FINANCIAL SYSTEMS.

There is a live payment method attached to your ad accounts and a login that can move it.

SECTION 04 OF 04

Follow the money and the identity.

Advertising platforms are the only marketing systems that spend money directly, and they are governed almost universally with less rigor than a company applies to a corporate card, despite frequently moving more money than one.

Ad accounts are financial systems

Google Ads and Meta Ads combine a spending mechanism, a payment instrument, and your customer data in one console. Apply the controls you would apply to any financial system:

- **Billing separated from operations.** The people running campaigns do not need to change the payment method. Those are different roles and most platforms model them separately.
- **Company-owned payment methods**, because an agency card reimbursed later obscures your real spend and complicates every exit.
- **Spending alerts** at thresholds you would notice, routed to someone internal. Unusual spend is both a fraud signal and a compromise signal.
- **Access reviewed on a schedule**, because agency staffing changes more often than your access list does.

Identity is the real perimeter

Behind every one of these platforms is a Google or Microsoft identity, and that identity is the actual key. Compromise it and platform-level permissions stop mattering, because the attacker has become the user.

This is why **phishing-resistant MFA on the identity provider** is the highest-value control in this document. SMS does not qualify, since it is defeated by SIM swap and increasingly by simple interception. Use an authenticator app at minimum, and hardware keys or passkeys for anyone with privileged access.

Privileged access should be rare and boring

Admin rights should be held by a small number of named people, used deliberately, and reviewed. The usual failure mode is accumulation rather than malice, an admin grant made for a one-week migration in 2023 that nobody removed. Every account with standing admin is a permanent increase in your blast radius.

Account ownership, again

Ownership matters more here than anywhere else in this guide. An ad account owned by your agency, with your money in it and your customer lists uploaded to it, is a problem that only becomes visible when the relationship ends. Verify ownership now, in writing.

Fifteen controls.

15 CONTROLS

These follow the four sections of this guide. None require a security team, and the high-leverage ones close most of the realistic exposure.

ACCESS 05

01 MFA everywhere — HIGH
Phishing-resistant on the identity provider first, then every platform. No SMS.

02 Individual accounts — HIGH
One named login per person. Delete every shared credential.

03 Least privilege — HIGH
Scope each partner to the smallest role that covers their contracted work.

04 Access inventory — FOUNDATIONAL
List every system, who can reach it, and at what level. Review quarterly.

05 Password manager — MED
Org-wide, so the fallback stops being reuse and spreadsheets.

DATA 04

06 Account ownership — HIGH
Company owns every asset; the agency is granted access to it.

07 Data minimization — MED
Drop fields you cannot justify. Shorter forms also convert better.

08 Retention and deletion — MED
Set an expiry per dataset. Verify deletion reaches copies and backups.

09 Written AI policy — MED
Decide what may be pasted into which tools before someone decides for you.

INFRASTRUCTURE 04

10 DNS protection — HIGH
Named internal owner, MFA, registrar lock, change process. No standing vendor access.

11 Tag manager limits — HIGH
Publish restricted to a named few; everyone else drafts. Alerts on.

12 Backups off-host — FOUNDATIONAL
Restore-tested, and not writable by the CMS it protects.

13 API key hygiene — MED
Scoped, rotated, never in a repo or page template.

MONEY & IDENTITY 02

14 OAuth review — HIGH
Audit connected apps on every platform. Revoke what nobody can explain.

15 Spend alerts + IR plan — FOUNDATIONAL
Thresholds routed internally, and a joint plan for hour one.

LEVERAGE HIGH MEDIUM FOUNDATIONAL

Agency security scorecard

Fifteen controls, what each one actually prevents, and where you stand. Print this page and work through it with your agency.

	CONTROL	WHY IT MATTERS	STATUS		
			YES	PARTIAL	NO
01	**Phishing-resistant MFA everywhere**	One stolen password stops being one breach, which makes this the highest-value control here.	☐	☐	☐
02	**Individual named accounts**	Shared logins destroy attribution, offboarding and MFA at once.	☐	☐	☐
03	**Least-privilege roles**	Caps the blast radius of any single compromised account.	☐	☐	☐
04	**Access inventory, reviewed quarterly**	You cannot secure a list of systems you have never written down.	☐	☐	☐
05	**Password manager, org-wide**	Removes the reuse and the spreadsheet that usually replaces it.	☐	☐	☐
06	**Company owns every account**	Protects your data and your exit, and it costs far less to arrange now than to unwind later.	☐	☐	☐
07	**Documented offboarding, ≤24h**	Departed staff keep access by default unless a process removes it.	☐	☐	☐
08	**OAuth / connected-app review**	Tokens survive password changes and never appear in your user list.	☐	☐	☐
09	**Scoped, rotated API keys**	Limits what a leaked key reaches and how long it works.	☐	☐	☐
10	**Off-host, restore-tested backups**	An untested backup is a hope, and one your site can write to gets encrypted alongside it.	☐	☐	☐
11	**DNS locked, MFA, named owner**	Highest-leverage records you own: mail, traffic, certificates.	☐	☐	☐
12	**Tag manager publish restricted**	Publish rights are arbitrary code execution on every page.	☐	☐	☐
13	**Data minimization and retention**	Shrinks the volume and lifetime of what a breach can expose.	☐	☐	☐
14	**Written AI usage policy**	Decides what may be pasted into tools before someone decides for you.	☐	☐	☐
15	**Joint incident response plan**	Determines whether hour one is contained or chaotic.	☐	☐	☐

REVIEWED WITH _____ DATE _____

10 QUESTIONS TO ASK YOUR MARKETING AGENCY

DILIGENCE

Ask these on the next call. You are listening for whether the answer is specific, because a vague answer is itself the finding.

01	Who currently has access to our marketing systems?
02	Does everyone have their own account?
03	Is MFA required everywhere?
04	What information can your employees access?
05	How do you handle employee offboarding?
06	What happens if one of your employees gets phished?
07	What third-party applications have access to our systems?
08	How do you protect and delete our customer data?
09	What happens to our accounts and data when we terminate the relationship?
10	Can you provide evidence of your security controls?

IN CLOSING

THE SIGNAL TO WATCH

A security policy tells you very little. Policies are easy to produce, and a great many of them were produced to be shown rather than used.

What tells you a great deal is **whether anyone there can answer the access question without going to look.** An agency that knows who has access to what, and can tell you today, manages access as a practice. One that needs a week to assemble the answer has been accumulating access without governing it, and that stays true regardless of what its policy document says.

Start with the inventory. Everything else in this guide follows from knowing what exists.



SEISMICDIGITAL

ABOUT SEISMIC DIGITAL

Seismic Digital is a digital marketing and strategy firm in Kansas City. We build search, paid media, analytics and creative programs for brands in financial services, healthcare, retail and manufacturing, and we operate inside our clients' systems every day, which is why the questions in this guide are ones we hold ourselves to as well.

CYTEK

ABOUT THE CONTRIBUTOR

Cytek provides managed and co-managed IT, cybersecurity, cloud and VoIP services to organizations in Kansas City. Their perspective in this issue reflects what they see across mid-market environments: exposure that assembles itself quietly, through access nobody revisited.

THE SEISMIC DIGITAL EDITORIAL FIELD GUIDE IS A RECURRING SERIES. EACH ISSUE PAIRS SEISMIC'S OPERATING EXPERIENCE WITH A CONTRIBUTING SUBJECT-MATTER EXPERT.