Principal Brief // two-minute read

DOMAIN & DNS | HOSTING & INFRASTRUCTURE | THREAT MODELING

Your Domain Vendors Have New Owners

> *In fifteen months a payment network bought a major threat-intelligence vendor and its DNS history, and private equity took two large registrars and the firm that guards corporate domain portfolios. The logos did not change. The owners did.*

WHAT HAPPENED

Permira took Squarespace private in October 2024 with the former Google Domains book of about 10 million registrations inside it. Mastercard bought Recorded Future for $2.65 billion in December 2024, with SecurityTrails and DNS Spy, which record which domain pointed where, and when. In September 2025 CVC agreed to a majority stake in Namecheap at a $1.5 billion valuation. In December 2025 Markmonitor passed to private-equity-owned Com Laude.

WHY IT REACHES YOU

These vendors hold different things: public records of your infrastructure, private registrar accounts, and, if your team uses an intelligence platform, a log of what it searched for. The service may be identical under the new owner; the incentives are not. A payments company scores fraud with what it sees; a private-equity owner is paid on the relationship. Your contract decides what either may do.

THREE THINGS TO TAKE FROM THIS

1

Map control, not logos

Recorded Future, SecurityTrails, and DNS Spy are one Mastercard stack. Two feeds under one parent are no longer independent counterparties.

2

Your searches are intelligence too

An intelligence platform learns what you are investigating, not only what the threat is. Its own policy says query data steers its product.

3

Acquisition is a review trigger

Nothing has to change on day one. Affiliate access, permitted uses, retention, conflicts, and exit rights deserve a second look when the owner changes.

DO THIS

- [ ] **YOU, THIS QUARTER**
  List the registrar, brand-protection provider, and intelligence feeds for each company and the office, with the ultimate parent of each.
- [ ] **YOU, WITH YOUR FAMILY OFFICE**
  Read the change-of-control, affiliate, and data-sharing clauses in those contracts; confirm lock and privacy on every domain.
- [ ] **YOU, WITH YOUR SECURITY LEAD**
  Ask each intelligence vendor in writing what it keeps of your searches, who in the group can see it, and whether it can be switched off.

NOT THE STORY YOU MAY HAVE HEARD

This brief does not say any owner has misused customer data or combined datasets, or that the products changed. It does not say domain intelligence is now one asset class; payments and private-equity buyers had different reasons. It says the governance perimeter around your information moved, and that is a contract question.

HOW SURE WE ARE

High on the deals, the four-layer stack, and the vendor's own statement that it collects and uses query data. Moderate on how the new owners will change pricing, data handling, or service, which is not yet observed.

THE FULL COMMAND BRIEF FOLLOWS: THE CONSOLIDATION ARC, FOUR INFORMATION CLASSES, THE OWNERSHIP TABLE, AND POSTURE BY FUNCTION.

CB-052

The Vendor Map Is Not the Control Map

"Domain-security products changed owners. The product names conceal the resulting concentration, incentives, and information exposure."

> *Domain intelligence used to be a security tool bought by a security operations center. Between October 2024 and December 2025 a run of ownership transactions moved key layers of it inside a payment network and private equity: Mastercard bought a major threat-intelligence vendor and, with it, a passive-DNS history service; one private-equity firm took a large registrar and host private with the former Google Domains book inside it, and another agreed to take a majority stake in one of the largest retail registrars; a private-equity-backed registrar bought the corporate brand-protection house that holds many large companies' domain portfolios. The vendor map you buy from is no longer the control map, and the control map is now part of the threat model. For a principal, the protected person at the center of a security program, the question is not who the logo says is watching your infrastructure. It is who owns them now, what each service learns from being used, and where that knowledge can travel inside the new owner.*

BLUF. The brands that protect corporate domains and map adversary infrastructure increasingly sit inside larger corporate groups. Mastercard completed its $2.65 billion acquisition of Recorded Future in December 2024, taking with it SecurityTrails' passive DNS history and DNS Spy's change monitoring. In October 2024 Permira completed its take-private of Squarespace, which had bought Google Domains' roughly 10 million registrations the year before, so a registrar book that arrived under a Google product now sits under private equity. In September 2025 CVC Capital Partners agreed to acquire a majority stake in Namecheap, a registrar with about 11.5 million .com domains, at a $1.5 billion valuation including debt. In December 2025 Newfold Digital completed the sale of Markmonitor, the corporate registrar and brand-protection firm, to Com Laude, owned by PX3 Partners. None of this establishes misuse or an immediate change in service. It changes the governance perimeter: a parent may now control several products that appear independent, and those products hold different classes of information, registrar records, infrastructure observations, customer queries, analyst annotations, and submitted indicators.

The governing frame is four maps. The service map is what an organization believes it buys. The control map is who ultimately owns it. The observation map is what each service learns through collection, queries, uploads, support, and integrations. The decision map is where those signals could affect fraud scoring, security ratings, product development, pricing, or account treatment. An acquisition does not prove that information moved from one map to another. It changes the institutional possibility, the economic incentive, and the governance boundary, and it does so before the product interface changes at all. A vendor acquisition is therefore not only a procurement event. It is an intelligence-governance event.

An intelligence service observes two environments at once: the threats in its dataset, and the priorities of the customers searching it.

THE SIGNAL // THE CONSOLIDATION ARC

FOUNDATION LAYER · 2020 TO 2022

SecurityTrails acquired DNS Spy, a DNS change-monitoring service, in 2020, and Recorded Future acquired SecurityTrails in January 2022, bringing passive DNS history, DNS change monitoring, and infrastructure history under one roof. Neither transaction drew wide attention. Together they built the base of what became the Mastercard DNS-visibility stack.

PAYMENTS LAYER · SEP TO DEC 2024

Mastercard announced the acquisition of Recorded Future from Insight Partners for $2.65 billion in September 2024 and completed it in December. Recorded Future's threat intelligence, and SecurityTrails' DNS visibility beneath it, now sit inside a payment network alongside fraud scoring and transaction monitoring.

REGISTRAR LAYER · 2023 TO OCT 2024

Squarespace acquired Google Domains' roughly 10 million registrations when Google exited the registrar business in 2023, then went private to Permira in a deal completed on 17 October 2024 at about $7.2 billion, with founder Anthony Casalena rolling equity and staying as chief executive. Millions of registrants who chose a Google product now hold their domains, and their renewal relationship, with a private-equity-owned registrar and host. It is the first of the two registrar moves in this arc and the one most likely to touch a principal's personal or family domains.

REGISTRAR LAYER · SEP 2025

CVC Capital Partners came to terms to acquire a majority stake in Namecheap, first reported by the Wall Street Journal on 12 September 2025, valuing the registrar and hosting company at $1.5 billion including debt, with founder Richard Kirkendall retaining a significant holding. Namecheap held about 11.5 million .com registrations and operates the Spaceship registrar. The agreement would put one of the largest retail registrars under private-equity control; completion has not been confirmed in the public record as of this revision.

BRAND-PROTECTION AND INFRASTRUCTURE LAYERS · DEC 2025

In December 2025 HYAS was broken up rather than bought: threatER completed the purchase of HYAS Protect, the protective-DNS product, on 11 December, and Silent Push completed the purchase of HYAS Insight, the adversary-infrastructure intelligence product, on 15 December, terms undisclosed on both. HYAS Infosec did not survive as an independent company. This is consolidation within the intelligence market itself rather than a change of sector, and it is the sharper case in this figure: a vendor can be split instead of absorbed, so the layer that blocks traffic for a customer and the layer that tells them what to block can end up under two different owners. On 31 December 2025 Newfold Digital completed the sale of Markmonitor to Com Laude, the corporate registrar owned by London private-equity firm PX3 Partners, a combination PX3 described as a $450 million leader in corporate domain management. Markmonitor manages the domain portfolios and brand-protection programs of many of the world's largest companies.

SINCE PUBLICATION · TO SEP 2026

No further ownership change at these six brands has been announced since this brief first appeared. The pattern continued next door: on 3 August 2026 Visa agreed to buy BioCatch, a behavioral fraud-intelligence vendor, from Permira for $2.4 billion, the second card network to put a security-intelligence vendor on its balance sheet. Annex A carries that and the wider ownership map; this brief stays with the domain layer.

SO WHAT The companies that register your domains, hold your brand portfolio, and record your infrastructure's history changed owners in fifteen months. The logos did not, and the logos are what your vendor inventory records.

THE PRODUCT SEES MORE THAN THE THREAT

Passive-DNS services observe infrastructure. Registrars hold account, registrant, billing, and portfolio information. Intelligence platforms may also record what their customers search, investigate, annotate, upload, and monitor. These are different information classes with different contractual and operational protections (Figure 1). Together they can reveal both an organization's external exposure and what its defenders currently care about. Recorded Future's privacy policy, updated 10 August 2026, lists "logs of browser extension queries and other usage data" among what it collects and says the company "uses unattributed Customer Data to develop & improve our offerings," including as "a signal to our teams regarding what type of data to improve, what research to pursue." That is not misuse. It is confirmation that query exhaust is a real information category, not a hypothetical one.

YOUR SEARCHES ARE ALSO INTELLIGENCE

A bank, a family office, or a security team searching repeatedly for one infrastructure cluster may reveal an active investigation, a suspected compromise, a contemplated transaction, a newly identified adversary, or a weakness it has not disclosed. Mastercard has said the Recorded Future acquisition can enhance its cybersecurity services, identity products, real-time fraud scoring, and AI models. That supports a convergence argument without any speculation about improper data combination: the parent has named the internal products that could benefit from what the subsidiary learns. Query handling deserves the same scrutiny as the intelligence feed itself.

OWNERSHIP CHANGES THE GOVERNANCE PERIMETER

An acquisition does not prove that datasets have been combined. It changes who has the authority and incentive to propose that combination, which affiliates sit inside the corporate boundary, and which internal products could benefit from the resulting signals. Under a payments parent the candidate use is fraud and identity scoring; under private equity it is pricing, cross-sell, and the value of the customer relationship at exit. Those questions exist the day the deal closes, before any visible product change. What the owner and its affiliates may actually do is set by the contract, the service architecture, the privacy policy and data-processing terms, applicable law, subprocessor arrangements, and the customer's own configuration. The contract is one control among several, and it is the one the customer can read.

DIVERSIFICATION CAN BE COSMETIC

Separate product names do not guarantee independent ownership, infrastructure, governance, or exit risk. Recorded Future, SecurityTrails, and DNS Spy are three names and one Mastercard stack. Two feeds under one parent may provide different data, but they are no longer fully independent counterparties. Some Recorded Future customers compete with Mastercard in fraud, identity, payment, or risk services, while others are important Mastercard partners; a financial institution with a direct Mastercard relationship may now have several risk functions concentrated within one corporate group. Measure diversification at the ultimate-parent and operating-dependency level, not by counting logos.

CAPABILITY IS NOT CONTROL (A SIDEBAR)

Owning the intelligence stack does not secure the operational stack. In January 2025 researcher Philippe Caturegli disclosed that one of Mastercard's own nameserver records had read akam.ne instead of akam.net since June 2020; he registered the misspelled domain for $300 and received hundreds of thousands of DNS queries a day before Mastercard corrected it on 14 January 2025. The point belongs beside this brief rather than inside its argument: a company can hold four layers of DNS visibility and still carry a five-year typo in its own zone. Mastercard said there was no risk to its systems.

FIGURE 1 // FOUR INFORMATION CLASSES A DOMAIN-SECURITY VENDOR MAY HOLD, AND WHY OWNERSHIP MATTERS FOR EACH

INFORMATION CLASS	EXAMPLE	HOW IT IS OBTAINED	WHY OWNERSHIP MATTERS
OBSERVED INFRASTRUCTURE DATA	Passive DNS history	External sensors and public network activity	Coverage, enrichment, combination with other datasets, retention
REGISTRAR CUSTOMER DATA	Registrant, account, billing, portfolio records	Supplied through the customer relationship	Confidentiality, access, transfer, affiliate sharing
CUSTOMER QUERY DATA	Domains, actors, incidents, infrastructure investigated	Generated when analysts use the platform	Reveals investigative priorities and undisclosed concerns
CUSTOMER-SUBMITTED MATERIAL	Notes, indicators, files, annotations	Uploaded or created inside the service	May expose incidents, targets, and analytic conclusions

FIGURE 2 // THE CONSOLIDATION, IN NUMBERS

$2.65B

Mastercard's acquisition of Recorded Future, announced Sep 2024, completed Dec 2024.

MASTERCARD, 2024

$1.5B

Namecheap valuation, including debt, in CVC's agreement for a majority stake.

WSJ VIA DOMAIN NAME WIRE, 12 SEP 2025

4

Layers deep: Mastercard to Recorded Future to SecurityTrails to DNS Spy.

DEAL ANNOUNCEMENTS, 2020 TO 2024

$2.4B

Visa's agreement to buy BioCatch from Permira: the second card network to buy a security-intelligence vendor.

VISA, 3 AUG 2026 (ANNEX A)

FIGURE 3 // SIX BRANDS, THEIR OWNERS AT PUBLICATION, AND THEIR OWNERS NOW

BRAND	WHAT IT HOLDS	OWNER BEFORE	OWNER NOW
RECORDED FUTURE	Threat intelligence; adversary-infrastructure tracking	Insight Partners (from 2019)	Mastercard (Dec 2024)
SECURITYTRAILS / DNS SPY	Passive DNS history; DNS change monitoring	Recorded Future (from 2022 / 2020)	Mastercard, via Recorded Future
SQUARESPACE (INCL. FORMER GOOGLE DOMAINS)	About 10M registrations from Google Domains; hosting; site builder	Public company; Google Domains until 2023	Permira (Oct 2024)
NAMECHEAP	About 11.5M .com registrations; hosting; Spaceship	Founder-owned	Founder-owned; CVC Capital Partners agreed to acquire a majority stake, Sep 2025
MARKMONITOR	Corporate domain portfolios; brand protection	Newfold Digital	Com Laude, owned by PX3 Partners (Dec 2025)
HYAS	Protective DNS and adversary-infrastructure platform	Independent	Split Dec 2025: threatER (Protect) and Silent Push (Insight)

> **SO WHAT** Read the right-hand column of Figure 3 against your own vendor list. Where a name appears, the counterparty behind your contract is not the one you signed with, and Figure 1 says what it may hold.

THE STEELMAN // THE CASE THAT THIS IS ORDINARY M&A

THE BEST CASE FOR THE OTHER SIDE

+ Consolidation is routine in every software market, and a change of owner does not change what the telemetry measures.
+ Buyers still receive the same passive DNS, registrar, and brand-protection services they always did, so the operational product is unchanged.
+ Four buyers with four different motives do not make a trend, and a payments motive describes only one of them.

Concede that the raw telemetry is the same, that consolidation is ordinary, and that the buyers bought for different reasons. The brief does not need them to share a motive. It needs them to share an effect, and they do: each moved a product that holds one or more of the four information classes in Figure 1 behind a new governance perimeter, with new affiliates, incentives, and integration paths, while the product interface stayed the same. A financial institution with a direct Mastercard relationship may now have several risk functions inside one group; a company whose domain portfolio sits at Markmonitor has a new private-equity owner behind its most sensitive registrar relationship. Those are facts a vendor map by logo will never show, and the day they matter is the day a use is proposed inside the group, not the day the product changes.

ASSESSMENT

FIGURE 4 // ANALYTIC CONFIDENCE BY CLAIM

Key layers of domain intelligence changed owners between 2024 and 2025; the transactions are public.	**STRONG**
The brand-level vendor map no longer shows who controls these services.	**STRONG**
Intelligence platforms collect customer query and usage data and may use it, unattributed, to steer product and research.	**STRONG / THE VENDOR'S OWN POLICY**
Domain intelligence as a whole has become a financial-risk asset class.	**MODERATE / TRUE OF THE TWO CARD-NETWORK DEALS, NOT THE PRIVATE-EQUITY ONES**
How the new owners will change pricing, data handling, or service.	**MODERATE / FORWARD**
A change of owner means the service or the data handling has already changed.	**REJECTED / IT MEANS THE GOVERNANCE PERIMETER HAS**

POSTURE

FOR PRINCIPALS

→ Map control, not logos. For the operating businesses, the family office, and personal domains, list the registrar, the brand-protection provider, and any threat-intelligence or DNS-visibility feed, then write the ultimate parent beside each brand. Figure 3 is the starting list; Annex A extends it.

→ Treat a change of control at one of these vendors as a review trigger, not an alarm. The service may be identical; the questions are affiliate access, permitted uses, retention, integration, conflicts, portability, and exit rights, and what the contract, the data terms, and the architecture let the new owner do.

FOR FAMILY OFFICES

→ Check whether a feed mix that looks diversified is actually independent. Two products under one parent may carry different data, but they are no longer fully independent counterparties. Where the parent is also a direct payments or risk-services counterparty, note the concentration; it is a procurement fact, not a security finding.

→ Read the change-of-control, data-sharing, and affiliate clauses in registrar and brand-protection contracts, and confirm registrar-lock, transfer, and privacy settings on every domain portfolio. Those settings, not the owner's identity, are what protect a domain when the owner changes. Check personal and family domains too: anyone who registered through Google Domains is now a Squarespace customer under Permira, whether or not they noticed the transfer.

→ Ask each intelligence vendor, in writing, what it retains of your queries, annotations, and uploads, for how long, whether affiliates can see it, and whether unattributed use can be switched off. The answer is a term you can negotiate; the silence is a finding.

FOR SECURITY & LEGAL FUNCTIONS

→ Assess Mastercard-stack exposure specifically. Any organization buying Recorded Future, SecurityTrails, or DNS Spy is buying from a payment network's subsidiary. For an institution with a direct Mastercard relationship that is a concentration question spanning threat intelligence, fraud scoring, and transaction processing; for one that competes with Mastercard in fraud, identity, or payment services it is a question of what its investigations reveal to the group. Treat query handling as a control to be verified, not assumed.

→ Brief procurement that ownership at the domain-intelligence layer is an evaluation variable, and track the CVC-Namecheap completion, the Visa-BioCatch close (expected by Visa's fiscal second quarter of 2027), and any post-acquisition changes to these vendors' data and privacy terms. Annex A carries the wider ownership map. CB-053 covers what domain records disclose about their registrants; CB-054 covers predictive infrastructure intelligence. This is intelligence analysis, not legal advice.

CONFIDENCE High on the transactions: the Mastercard, CVC, Com Laude, Silent Push, and Visa deals are announced by the parties, and the Mastercard DNS typo is documented by the researcher and acknowledged by the company. High on the four-layer stack as an ownership chain and on the collection and unattributed use of query data, which is stated in the vendor's own policy. Moderate on any characterization of the whole as financial-risk infrastructure, which fits the two card-network deals and not the private-equity transactions, and on how the new owners will change pricing, data handling, or service. The DNS Spy acquisition date (2020) rests on the parties' contemporaneous statements and is not independently confirmed here.

METHOD Revised edition. First published 2 May 2026; facts re-verified and analysis revised 10 September 2026. The revision replaces the original financialization thesis with the four-map frame (service, control, observation, decision), retitles the brief, separates the information classes a vendor may hold, adds the query-data mechanism from the vendor's own policy, adds the Squarespace and Google Domains transaction, corrects the dates and terms of the Namecheap, HYAS, Markmonitor, and Mastercard-typo items, records the HYAS transaction as the two-buyer breakup it was, adds ownership and information-class tables, moves the wider ownership map to Annex A, and sets the brief to public release. Built from deal announcements and the parties' releases, researcher disclosure, and trade press, cross-read against CB-053 and CB-054.

SOURCES Mastercard and Recorded Future announcements (September and December 2024). Domain Name Wire on the CVC-Namecheap agreement, citing the Wall Street Journal (12 September 2025). threatER on the completed purchase of the HYAS Protect assets (11 December 2025) and Silent Push on the completed purchase of HYAS Insight (15 December 2025). Newfold Digital on the completed sale of Markmonitor to Com Laude (31 December 2025) and PX3 Partners on the agreement. Krebs on Security, "MasterCard DNS Error Went Unnoticed for Years" (22 January 2025). Recorded Future and SecurityTrails statements on the SecurityTrails (2022) and DNS Spy (2020) acquisitions. Permira on the completed acquisition of Squarespace (17 October 2024). Recorded Future privacy policy (updated 10 August 2026). Visa announcement of the BioCatch acquisition (3 August 2026). Mastercard announcement of the Recorded Future acquisition (September 2024).

Scope note: deal values are as announced; the Namecheap figure is an enterprise valuation including debt for a majority stake, not a purchase price, and the transaction was an agreement in principle when reported. Nothing here alleges that any owner has changed how customer data is handled or combined datasets; the brief describes changes in ownership, incentive, and governance perimeter, quotes the vendor's own policy on query data, and directs readers to their contracts and data terms. This is intelligence analysis, not legal advice.

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-052-DOMAIN-FINANCIALIZATION-2026Q2 // XREF **CB-052-A CB-053 CB-054** // ACCESS PUBLIC · PUBLIC-INTEREST RELEASE · REVISED 10 SEP 2026