

374.2 million resolving domains



The Top 1000 companies

THE STATE OF EMAIL INFRASTRUCTURE 2026

Who Really Runs Business Email?

The Keyhole Effect: what 374M domains reveal about global email infrastructure beyond the world's largest employers.

The keyhole effect

Who runs corporate email depends almost entirely on where you look. Enterprise studies see the world's largest companies. This report also measures the 374 million domains around them.

53.8%

of corporate mail domains are run by hosting companies, registrars and other named providers.

Microsoft and Google together run 24%. Base: 115.2M corporate mail domains.

9:1

Microsoft to Google in the MX records of the Top 1000 companies.

Across 115.2M corporate mail domains the two are level: Microsoft 11.92%, Google 12.16%.

0.8% vs 97.8%

DMARC enforcement at two brands of the same hosting group, 1&1 and Strato.

Near-identical publication (94.2% and 98.7%), opposite enforcement.

73.3% vs 14.2%

DMARC enforcement: Top 1000 companies against mail domains with a named provider.

37.6% vs 2.34%

Behind a dedicated email security gateway: Top 1000 companies against all corporate mail domains.

Enterprise rankings are not wrong. They describe a keyhole, and this report describes the building around it.

Sources: Datazag Observatory, snapshot of 8 October 2026; Datazag mail records of the 2,000 largest listed companies by number of employees.

Executive summary

Who runs corporate email depends almost entirely on where you look. Enterprise market-share studies look through a keyhole. Among the 1,000 largest listed companies by number of employees, Microsoft appears in nine MX records for every one of Google's.

Across all 115 million corporate mail domains, the two are level, and together they handle just 24%. Most of the business internet, 53.8%, runs on hosting companies and registrars.

We call the gap between those two pictures **the keyhole effect**. It shapes deliverability, security defaults and vendor risk models alike.

How we measured

We measured both ends with one method. The Datazag Observatory's snapshot of 374.2 million resolving domains was taken on 8 October 2026. The mail records of the 2,000 largest listed companies by number of employees¹ come from the same snapshot. Later attribution work on the long tail uses the 11 October publish and is marked where it appears.

CONTENTS

	At a glance, how to read this research and key findings	2
01	Microsoft dominates big business. The wider internet tells another story.	6
02	There is no single global email market	9
03	The overlooked giants of business email	10
04	Why enterprise email security looks different	12
05	DMARC adoption is not DMARC protection	13
06	The millions of mail domains hiding in plain sight	16
07	What it means	19
	Research populations and methodology	20
	What this measures and what it does not · Sources	21

¹ Company sample: the 2,000 largest listed companies by number of employees, ranked using data from [CompaniesMarketCap.com](https://www.companiesmarketcap.com) (downloaded 12 October 2026). Mail records are Datazag DNS observations of 8 October 2026. All company figures are Datazag aggregates; no company-level results are published.

How to read this research

Every figure counts **domains**, not organizations, mailboxes or messages. One company can hold hundreds of domains, and one mailbox can serve a whole domain. A provider's share describes how much of the namespace it carries, not its revenue or seat count.

Four populations. Every share in this report names one.

Resolving domains

The Observatory corpus

374.2M

Mail domains, named provider

Primary MX names a cataloged operator

141.2M

Corporate mail domains

Take mail, have a website and SPF, not parked

115.2M

Top 1000

The 1,000 largest listed companies by number of employees | 1,000 companies

Security gateway

A filtering service named in a domain's MX records, in front of the mailbox. Proofpoint is an example.

Mailbox provider

Where the mail is actually held. Exchange Online is an example. Counting MX endpoints alone mistakes a gateway for this.

Why Microsoft is 32.6% in one place and 11.9% in another. The first is a share of the Top 1000 companies. The second is a share of 115.2M corporate mail domains. Always read a share with its population.

Figures are from the 8 October 2026 snapshot. Full methods and caveats: pages 20–21.

The research doesn't end with this report

This report captures a fixed October 2026 snapshot. The Datazag Observatory is updated daily. Explore current provider shares, follow authentication adoption, and download the aggregate data as Parquet for tools such as DuckDB.

[Explore the live Observatory →](#)



Scan to explore

What we found, and why it matters

01 Microsoft dominates big business. At internet scale, it is level with Google.

Google runs 12.16% of corporate mail domains and Microsoft 11.92%. Counting Microsoft mailboxes behind gateways, the two stay within half a point. Among the Top 1000, Microsoft appears in 32.6% of MX records and Google in 3.7%. Including mailboxes behind gateways, Microsoft rises to 60.9% on strong evidence.

Why it matters: market-share studies built on large enterprises give ESPs, security vendors and analysts a misleading picture of the wider internet.

02 Hosting companies are the overlooked giants of business email.

They handle 53.8% of corporate mail domains, against 24% for Microsoft and Google together. The IONOS group (1&1 and Strato) runs 13.2 million mail domains. GoDaddy and Namecheap run more than 10 million each. None appears in a Top 1000 list.

Why it matters: outside the large-enterprise market, hosting providers and registrars play a much greater role in email infrastructure than enterprise rankings suggest.

03 Dedicated gateways are an enterprise layer.

37.6% of Top 1000 companies route mail through one, against 2.34% of corporate mail domains.

Why it matters: rankings that count MX endpoints credit gateways with mail that Microsoft holds. They also miss how little of the internet sits behind one.

04 DMARC adoption is not DMARC protection.

73.3% of Top 1000 domains enforce DMARC at quarantine or reject. Across mail domains with a named provider, 14.2% do.

Why it matters: security assessments should distinguish DMARC publication from enforcement, while recognizing that enforcement is only one part of email security posture.

05 Provider defaults appear to set the outcome.

SiteGround customers publish DMARC at 96.3% and enforce at 1.6%; Hostinger customers at 85.6% and 1.1%. Two brands in one group show it best: 1&1 enforces on 0.8% of its domains, Strato on 97.8%.

Why it matters: changes to default authentication policies at major hosting providers could affect millions of domains, without each customer configuring its own policy.

CHAPTER 01

Microsoft dominates big business. The wider internet tells another story.

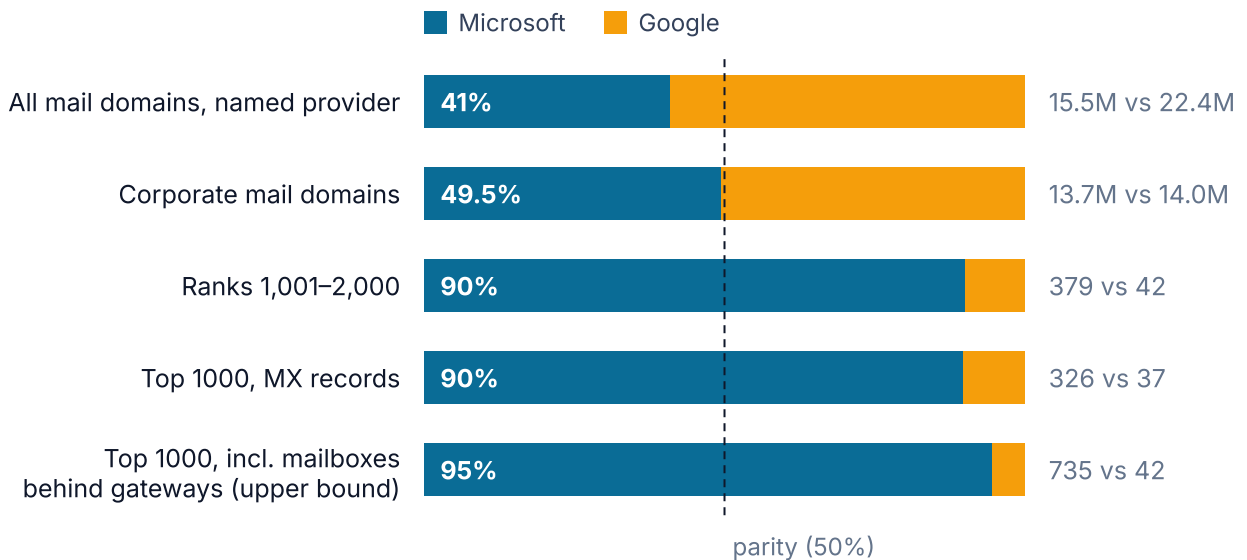
The narrower the lens, the more Microsoft dominates.

Across all mail domains with a named provider, Google runs 44% more domains than Microsoft: 22.4 million against 15.5 million. At the corporate filter, the two are level. In the Top 1000, Microsoft accounts for 90% of the companies that use either platform in MX, and 90% in the next 1,000. Counting mailboxes inferred behind gateways, that rises to as much as 95%. That is an upper bound: it includes companies identified only by a Microsoft tenant token.

FIGURE 1

Microsoft's share of Microsoft-plus-Google mail rises from 41% to 95% as the lens narrows

Microsoft and Google as shares of the domains or companies the two run together, 8 October 2026



Source: Datazag Observatory, 8 October 2026; Datazag Top 1000 mail records, 8 October 2026. The upper bound counts companies identified only by a Microsoft tenant token.

[View latest data →](#)

Two views of email infrastructure, measured on the same day

The underlying DNS observations are consistent, but the populations and attribution measures are not identical. The report distinguishes MX-set membership, primary MX classification and mailbox inference.

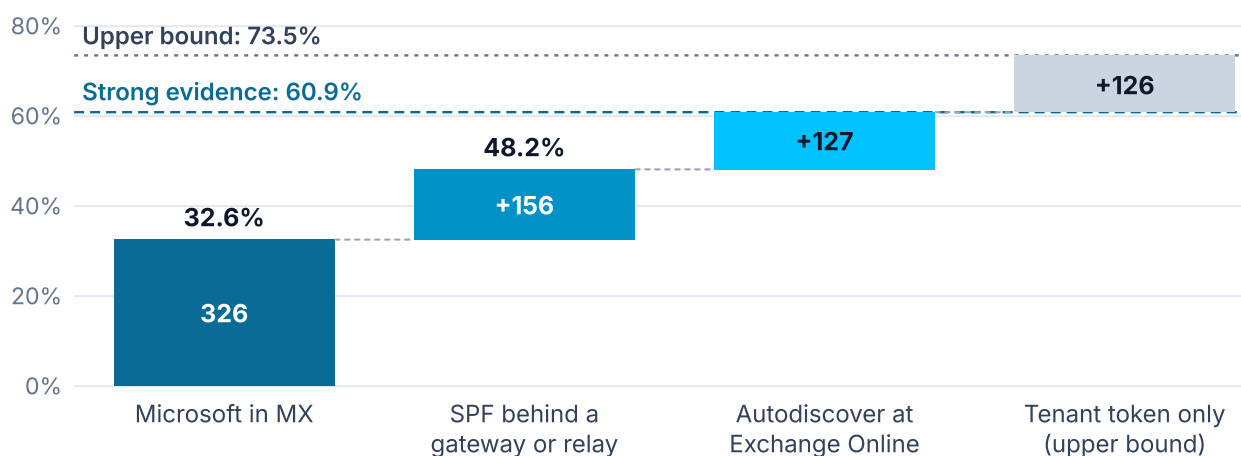
Measure	Top 1000	Observatory population
Microsoft in MX	32.6%	11.92% of corporate mail domains
Google in MX	3.7%	12.16% of corporate mail domains
Behind a dedicated security gateway	37.6%	2.34% of corporate mail domains
Enforcing DMARC (quarantine or reject)	73.3%	14.2% of mail domains with a named provider
DMARC at <code>p=none</code> , share of publishers	18.7%	65.2% of publishers with a named provider

Looking behind the gateway

Looking behind gateways and relays raises Microsoft's count from 326 to as many as 735 companies, in four tiers of evidence, strongest first.

FIGURE 2

Microsoft 365 in the Top 1000: 32.6% by MX, 60.9% on strong evidence, 73.5% at most



Cumulative share of the Top 1000 companies. Source: Datazag Top 1000 mail records, 8 October 2026.

Autodiscover tells Outlook and phones where the mailbox lives, so the first three tiers are strong evidence of Microsoft-hosted mailboxes. The token tier proves only that a tenant exists, which Teams-only and sign-on-only tenants also show. So 73.5% is an upper bound.

Google Workspace, by contrast, appears in the MX records of 37 companies (3.7%, the figure used throughout). SPF evidence behind gateways adds 5 more, for 42 at most.

Why the Top 1000 leans to Microsoft

These are large, long-established groups with central IT departments, many of which ran Windows and Exchange on their own servers long before the cloud. For estates like these, Microsoft 365 is the natural next step, and enterprise agreements sell it alongside the rest of the Microsoft stack. These are also the buyers that enterprise analyst firms track.

The next 1,000: just as Microsoft-heavy, less defended

Microsoft's lead does not fade down the list. Ranks 1,001–2,000 are, if anything, more Microsoft-heavy than the Top 1000. On security they sit between the Top 1000 and the population: fewer gateways, less DMARC enforcement.

Measure	Ranks 1–1,000	Ranks 1,001–2,000
Microsoft 365, MX evidence	32.6%	37.9%
Microsoft 365, strong evidence (MX, SPF or autodiscover)	60.9%	66.3%
Microsoft 365, upper bound (incl. tenant token)	73.5%	74.0%
Google Workspace, MX evidence	3.7%	4.2%
Self-hosted	9.9%	9.8%
No MX found on any mapped domain	0.5%	0.8%
Behind a security gateway	37.6%	33.7%
Publishes DMARC	90.2%	88.9%
Enforces DMARC	73.3%	67.7%
p=none , share of publishers	18.7%	23.8%

Gateway use falls by a tenth, and DMARC enforcement by more than 5 points, within a single step down the list, while Microsoft's share holds. The keyhole effect is as much about security posture as about platform choice. Across the 2,000 companies, 3 could not be mapped to a mail domain and are counted as no MX.

CHAPTER 02

There is no single global email market

A global figure hides national markets as completely as a Top 1000 list hides the long tail.

Across 115.2 million corporate mail domains, who runs the mail changes sharply from one country-code TLD to the next. Among the 12 largest, Microsoft leads only in `.au`, `.ca` and `.nl`. Even `.uk` runs more corporate mail on IONOS. Continental Europe, Russia and Japan run on national hosting companies.

Top 12 country-code TLDs by corporate mail domains, 8 October 2026

ccTLD	Corporate mail domains	Microsoft 365	Google	Gateway	Other named providers	Leading provider
<code>.de</code>	8.18M	7.9%	1.5%	1.2%	76.5%	IONOS (31%)
<code>.uk</code>	4.25M	19.4%	8.7%	3.1%	59.9%	IONOS (23%)
<code>.nl</code>	2.48M	15.7%	4.7%	2.7%	50.6%	Microsoft (15%)
<code>.ru</code>	2.09M	0.2%	0.8%	0.1%	76.2%	Beget (24%)
<code>.fr</code>	2.01M	7.6%	4.4%	1.9%	69.5%	OVHcloud (35%)
<code>.it</code>	1.86M	5.7%	6.0%	1.1%	67.3%	Aruba.it (37%)
<code>.br</code>	1.76M	5.9%	9.1%	0.4%	43.4%	Locaweb (12%)
<code>.pl</code>	1.59M	2.7%	3.3%	0.2%	63.7%	aftermarket.pl (12%)
<code>.ch</code>	1.52M	10.3%	3.3%	1.0%	65.8%	HostPoint (24%)
<code>.au</code>	1.43M	40.3%	16.1%	4.6%	22.1%	Microsoft (38%)
<code>.ca</code>	1.15M	28.3%	15.0%	3.2%	36.9%	Microsoft (27%)
<code>.jp</code>	1.03M	3.0%	6.4%	1.0%	55.5%	Xserver (19%)

Microsoft and Google shares include mail behind a gateway. Generic TLDs such as `.com` carry no country and are left out. Outside the top 12, Google leads in `.co` (33%) and `.in` (18%). The full split covers 101 ccTLDs and 63 hosting countries, each with at least 10,000 corporate mail domains.

The takeaway: deliverability and security rules cannot be applied globally without accounting for where each market's mail is actually hosted.

CHAPTER 03

The overlooked giants of business email

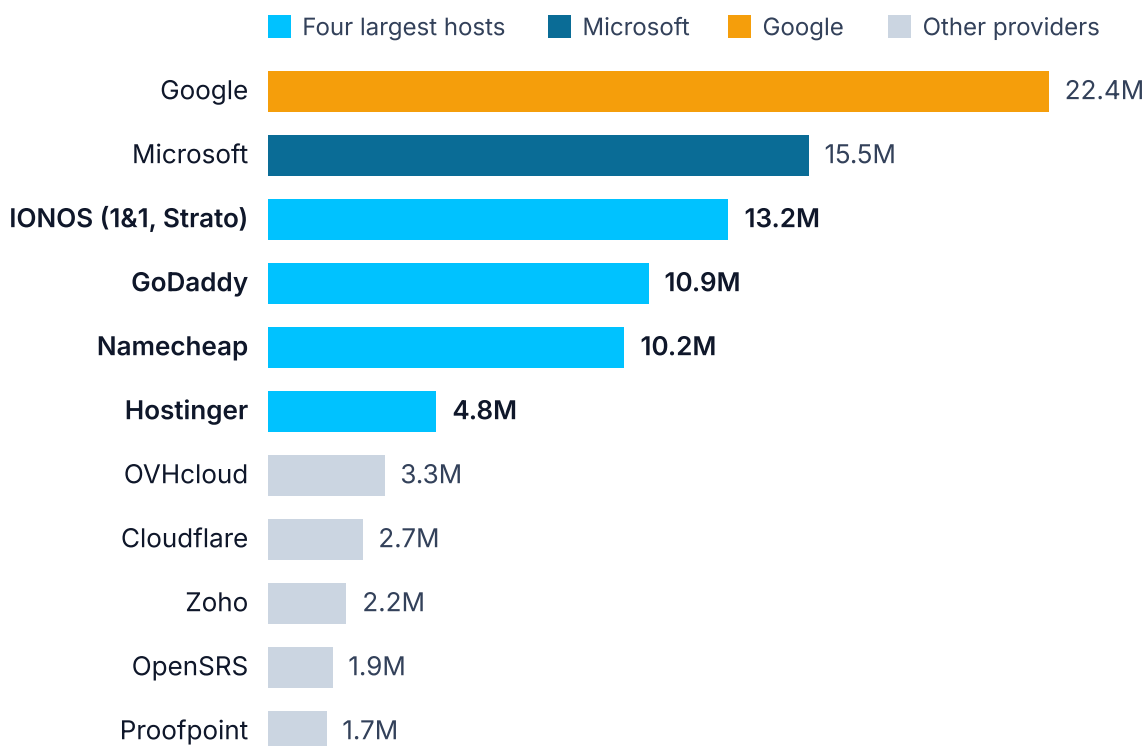
Microsoft and Google together run 24.05% of corporate mail domains: 27.7 million of 115.2 million.

Behind them, hosting companies and registrars run mail at the same scale. Their customers never chose an email platform as a separate purchase.

FIGURE 4

Four hosts and registrars together outrun Microsoft and Google by volume

Mail domains by primary MX provider, 8 October 2026. Highlighted: the four hosts and registrars, 39.2M together.



Source: Datazag Observatory, mail providers, 8 October 2026. Providers counted by operating group.

[View latest data →](#)

Together, the IONOS group (1&1, Strato), GoDaddy, Namecheap and Hostinger run 39.2 million mail domains. That is more than Microsoft and Google combined on the same count (38.0 million).

The mechanism is the bundle

A small business registers a domain or buys hosting, and the provider's mail is switched on with it. The alternative is a separate Microsoft 365 or Google Workspace subscription, billed per user. For a sole trader, a shop or a local practice, the bundled mailbox is often the only one they ever have.

These counts are mail domains, not organizations or mailboxes. One company can hold hundreds of domains on Microsoft, and one mailbox can serve a whole household's domain. The count measures how much of the namespace each provider carries. That is what matters for deliverability, impersonation and concentration risk.

The inverse of the largest employers

Across corporate mail domains, the whole population is the inverse of the 2,000 largest employers.

Who handles the mail, corporate mail domains		Share
Other named providers, mostly hosting companies		53.8%
No named provider		19.9%
Google		12.1%
Microsoft 365, direct		11.9%
Microsoft 365, behind a gateway		0.5%

Among the 2,000 largest employers, Microsoft 365 handles up to 74% of companies, and more than a third sit behind a gateway. Across 115 million corporate domains, Microsoft handles one in eight, and gateways about one in fifty.

For data analysts and researchers: download the raw data

Get the Observatory aggregates as a Parquet file and run your own queries in DuckDB or Python.

[Download the data →](#)

CHAPTER 04

Why enterprise email security looks different

The gateway is an enterprise layer, and the reason enterprise rankings misread who hosts the mail.

Dedicated email security gateways front 2,701,357 corporate mail domains, 2.34% of the population, across 116 vendors. In the Top 1000 they front 376 companies, 37.6%.

Gateway, Top 1000	Companies	Share
Proofpoint	238	63.3%
Cisco Email Security	47	12.5%
Mimecast	47	12.5%
Trend Micro	18	4.8%
Symantec Cloud Email	10	2.7%
Other	16	4.3%

Behind the 376 gateways

Microsoft in SPF	106
+ Autodiscover at Exchange Online	119
+ Microsoft tenant token only	102
Points to Google	4
Could not be resolved	45

225 to 327

on Microsoft 365

Behind the gateway, the evidence points to Microsoft. A ranking that counts MX endpoints credits all 376 companies to the gateway, and none to the platform that holds the mail.

Across all 2,000 companies, Proofpoint fronts 447 of the 713 that use a gateway (63%). Proofpoint in front of Microsoft 365 is the most common single mail path among the 2,000 largest employers: 393 of them.

Companies that buy a gateway also enforce more. 83.2% of gateway-fronted Top 1000 domains enforce DMARC, against 67.3% of the rest. Across the whole population, Proofpoint's 1.69 million mail domains enforce at 27.4%, nearly double the 14.2% average for named providers. Buying security as a separate product goes with configuring the rest of the mail estate more tightly.

For enterprise and risk teams: portfolio exposure audit

Map your organization's or portfolio's third-party email, gateway and hosting dependencies against the Datazag dataset.

[Request an exposure audit →](#)

CHAPTER 05

DMARC adoption is not DMARC protection

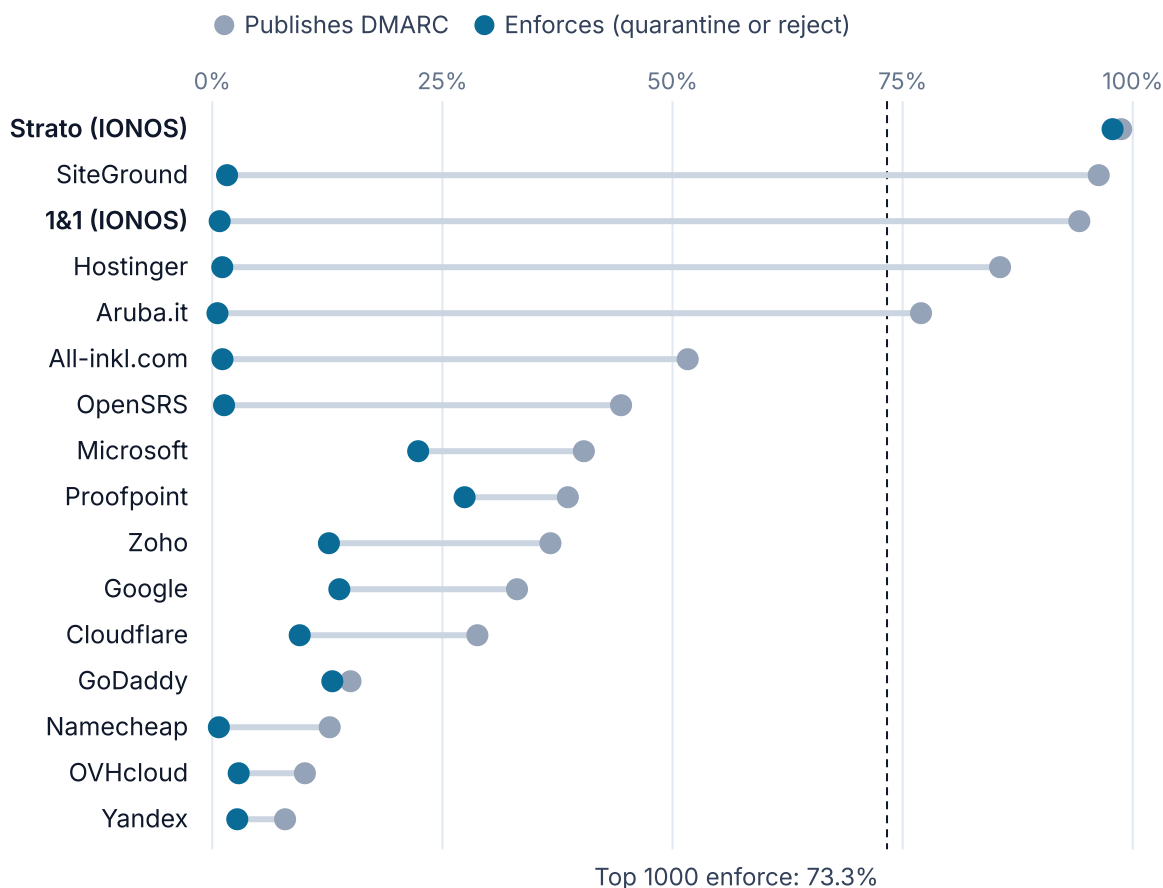
Publishing DMARC and enforcing it are different decisions, made by different people.

Across all 374.2 million resolving domains, 24.2% publish a DMARC record and 12.1% enforce one. Half of all publishers stop at `p=none`, which asks receivers to take no action against spoofed mail.

FIGURE 5

Same group, opposite outcomes: Strato enforces on 98% of its domains, 1&1 on under 1%

DMARC published and enforced, mail domains of 16 large providers, 8 October 2026



Source: Datazag Observatory, DMARC by mail provider, 8 October 2026; Top 1000: Datazag mail records, 8 October 2026.

[View latest data →](#)

The Top 1000 enforce at 73.3%, five times the 14.2% rate across mail domains with a named provider. Only 18.7% of Top 1000 publishers stop at `p=none`, against 65.2% across named providers.

Case study: how provider defaults shape security outcomes

A host can publish DMARC for every customer when the domain is provisioned. The policy it picks is likely to be the one most customers keep.

Two brands in the IONOS group, owned by United Internet, show this in both directions on the 8 October snapshot. The report counts them together as one provider, but their defaults differ. IONOS sells 1&1 to businesses, and Strato to individuals and small projects.

1&1	9.4M mail domains	Strato	3.8M mail domains
Publishes DMARC	94.2%	Publishes DMARC	98.7%
Enforces	0.81%	Enforces	97.8%

Near-identical publication, opposite enforcement. That is the pattern a provider default would produce, and far more plausible than millions of matching individual decisions. Defaults are the explanation the data most strongly supports, though customer mix and migration history may also contribute.

A catalog that merges the two brands reports 28.6% enforcement, a blend that describes neither. Where a host appears to default to `p=none`, enforcement collapses: SiteGround 96.3% and 1.6%, Hostinger 85.6% and 1.1%, Aruba.it 77.0% and 0.6%.

The records are consistent with a template. **Four in five `p=none` records carry no `rua` reporting address.** Domain owners are not even receiving the spoofing reports they would need to move to enforcement.

Where customers set DMARC themselves, enforcement is low and close together: Microsoft 22.4%, Google 13.8%, GoDaddy 13.0%. Proofpoint, whose customers bought security as a separate product, enforces at 27.4%.

A record with `p=none` and no reporting address asks receivers to take no action, and sends no aggregate reports to anyone. It is not identical to having no record, but it protects little more. Yet every adoption statistic counts it as deployment.

Why the gap matters

A DMARC presence count ranks SiteGround's customers among the best protected on the internet. An enforcement count ranks them among the least. A security score, vendor benchmark or underwriting signal built on presence alone largely measures provider defaults. Security assessments should distinguish DMARC publication from enforcement, while recognizing that enforcement is only one part of email security posture.

Publication is not protection. Enforcement is the part of DMARC that asks receivers to act on spoofed mail.

24.2%

of all resolving domains publish DMARC

12.1%

enforce it at quarantine or reject

The same gap on parked domains

Parked domains send no mail and could safely reject everything. Yet only 13.3% publish DMARC, and 88.5% of those sit at `p=none`. Our forthcoming note, *The Compliance Illusion*, covers them in detail.

Get a domain infrastructure report

See your mail providers, DMARC publication and enforcement, and remediation priorities, domain by domain.

[Request a report →](#)

CHAPTER 06

The millions of mail domains hiding in plain sight

32.6 million mail domains, 18.7% of the 173.8 million that operate mail, had no named provider on 8 October.

They are not a hidden giant. Much of this tail runs on third-party infrastructure that the MX name does not reveal.

Primary MX of domains with no named provider		Domains	Share
Under the domain's own name		26,064,618	80.1%
On a third-party domain our catalog does not name		4,173,303	12.8%
Cannot take mail		2,249,680	6.9%

DATAZAG OBSERVATORY INVESTIGATIVE SPOTLIGHT

Dissecting the unnamed tail

79.5%

of domains with apparently self-hosted MX names expose third-party infrastructure through reverse DNS

The infrastructure most often belongs to a hosting operator. Reverse DNS does not by itself show who operates the mail service.

Tracing reverse DNS across 26 million such domains, and researching the 269 largest operators behind them, attributed **8.3 million domains** to named providers in a single pass. The unnamed share fell from 18.7% to 13.6% of mail domains.

Own-domain MX is not the same as self-hosting

An MX under the domain's own name, such as `mail.example.com`, looks like self-hosting. Often it is not. A full-corpus probe on 9 October looked up the reverse DNS of every such MX host.

Own-domain MX, 26.1M domains		Domains	Share
Reverse DNS points to third-party infrastructure, usually a hosting operator		20.75M	79.5%
No reverse DNS		4.60M	17.6%
Reverse DNS under the domain's own name		0.76M	2.9%

Reverse DNS identifies third-party infrastructure behind 20.75 million of the 26.1 million domains whose MX records use their own domain names. This is strong evidence that apparently self-hosted mail frequently depends on external infrastructure. It does not by itself establish who operates the mail service. Distinguishing customer-managed servers from provider-managed mail requires additional attribution.

Why these domains stayed unnamed

Hosting companies sign their servers with infrastructure domains, while catalogs list their brands. The two never match.

THE SERVER'S REVERSE DNS SAYS

`unifiedlayer.com` `eigbox.net`
`host-h.net`

≠

THE CATALOG LISTS

`bluehost.com` `hostgator.com`

The tail is concentrated enough to name

1,840 reverse-DNS domains each serve 1,000 or more of these mail domains, 14.3 million in all. A further 33 third-party MX domains each serve 1,000 or more. Each of the largest 269 was researched on 9 October, covering 9.9 million domains.

Outcome	Domains	Notes
Operator identified and added to the catalog	8.3M	Led by Newfold Digital (Bluehost, HostGator, Network Solutions, Web.com and others), with 2.2M from the tail alone. Then xneelo, o2switch, LWS, World4You, Serverplan, A2 Hosting and Afrihost.
Cloud, VPS or ISP: reverse DNS names the landlord, not the mail operator	0.8M	Mail most likely run by the customer on a rented server. Stays in the tail.
Still under review	0.8M	Includes suspected bulk-mail fleets, left unnamed on purpose.

Unnamed mail domains, before and after attribution

8 October		32.6M
11 October		23.6M

With these operators added, the 11 October publish puts the unnamed tail at 23.6 million domains, 13.6% of 174.2 million mail domains. Domains whose MX sits under their own name fell from 26.1 million to 17.3 million. Newfold Digital, counted as one group, now runs 3.3 million mail domains.

The new attributions were researched from each operator's website, DNS, registration and network ownership. They were not individually confirmed by the operators.

These domains authenticate no worse than the rest: 37.3% publish DMARC and 13.6% enforce, against 40.9% and 14.2% across named providers.

CHAPTER 07

What it means

The keyhole effect changes the answer for anyone who sells to, secures or measures the business internet.



Deliverability teams and ESPs

Most recipient and sender domains outside the enterprise sit on hosts and registrars, not Microsoft or Google. A domain's mail provider and its DMARC enforcement are useful indicators of how its mail is likely to be filtered, and how easily it can be spoofed. Both can be read before the first send.



Email security vendors

The gateway market is concentrated in 2.34% of corporate domains. A vendor's own enforcement column shows whether its estate was bought as security or bundled. The other 97.66% show no dedicated gateway in MX; protection delivered through mailbox APIs is not measured here.



Cyber insurers and MSSPs

The largest correlated mail exposure in most books is the mailbox platform, not the gateway. Severity models should distinguish DMARC enforcement from DMARC presence, because presence largely measures provider defaults. Enforcement is one part of mail security posture, not all of it.



Market analysts

A Top 1000 share and a population share answer different questions. Microsoft leads among the largest companies; Google and the hosts lead across the domain population. Name the population before quoting the share.

Research populations and methodology

Every figure comes from DNS records the domains publish themselves. Nothing is surveyed or taken from a vendor's customer list. Every share names its population, and shares from different populations are never compared directly. The research draws on three dates.

8 October 2026

The Observatory snapshot supplies every population figure. The company mail records were read from the same snapshot.

9 October 2026

A full-corpus probe looked up the reverse DNS of every own-domain MX host. The 269 largest operators it surfaced were researched individually.

11 October 2026

The Observatory publish carries those new attributions. It is used only for the long-tail results, where it is marked.

Population	Domains	Definition
Resolving domains	374.2M	The Observatory corpus
Mail domains with a named provider	141.2M	Primary MX attributed to a cataloged operator
Corporate mail domains	115.2M	Accepts mail, is not parked, resolves a website and publishes SPF
Top 1000	1,000 companies	Ranks 1–1,000 of the company sample ¹ , one mail domain each. Ranks 1,001–2,000 also read.

¹ Company sample: the 2,000 largest listed companies by number of employees, ranked using data from [CompaniesMarketCap.com](#) (downloaded 12 October 2026). Mail records are Datazag DNS observations of 8 October 2026. All company figures are Datazag aggregates; no company-level results are published.

A further 32.6 million mail domains have no named provider (chapter 06), and 36.9 million parked domains sit outside the corporate filter. Their authentication is the subject of a companion note, *The Compliance Illusion* (forthcoming, October 2026).

Providers are counted by operating group. IONOS includes its 1&1 and Strato brands. Newfold Digital includes Bluehost, HostGator, Network Solutions, Web.com and its other brands. Brands are shown separately only where their behavior differs, as with DMARC in chapter 05.

Mailbox provider or MX endpoint

A domain's primary MX shows who **accepts** its mail. When a security gateway sits in front, that is the gateway, not the platform that holds the mailboxes. Ranking MX endpoints therefore lists Proofpoint and Mimecast as "mail hosts."

The Observatory's corporate figures count a domain under every operator in its MX set, backups included. Its provider ranking gives each domain one provider, by primary MX. Top 1000 comparisons use the same MX-set rule. Separately, we look behind the gateway, using Microsoft tenant verification records, SPF includes and autodiscover, to name the mailbox platform.

What this measures and what it does not

Domains, not organizations or mailboxes

One organization may hold hundreds of domains on one platform. Counts describe the namespace each provider carries, not its revenue or seat count.

MX shows who accepts mail

Corporate figures count every operator in a domain's MX set, backups included, so one domain can count under both a gateway and a mailbox provider. The Top 1000 mailbox view looks behind it and is labeled wherever it is used.

API-based email security is invisible

Products that connect to the mailbox through an API, rather than taking over MX routing, do not appear. Gateway figures are a floor, not a market measurement.

Own-domain MX is not proof of self-hosting

Reverse DNS points to third-party infrastructure for 79.5% of these hosts. That is strong evidence of third-party infrastructure, not proof of who operates the mail service. The operators behind them are being identified but not individually verified.

The corporate filter is constructed

It requires a published SPF record, which a host can set on a customer's behalf, so it is not neutral across markets.

Snapshots

Population figures are from 8 October 2026 (374.2 million resolving domains). The long-tail results in chapter 06 use the 11 October publish, when the corpus was 371.5 million.

Microsoft's hosts

Microsoft's count includes both its Exchange Online hosts and the newer `mx.microsoft` hosts. A re-run on the 8 October snapshot found 23 domains outside it, too few to change any figure.

Headcount is not mailboxes

Companies are ranked by employees, the closest public measure of mail users. Groups with large frontline workforces rank higher than their mailbox count suggests. Each is read on one mail domain.

Sources

[Datazag Observatory: Email](https://observatory.datazag.com/email), snapshot of 8 October 2026. observatory.datazag.com/email

[Datazag Observatory: Mail providers](https://observatory.datazag.com/email/providers), snapshot of 8 October 2026, and publish of 11 October 2026 (long-tail attribution). observatory.datazag.com/email/providers

[Datazag Observatory: DMARC enforcement](https://observatory.datazag.com/email/enforcement). observatory.datazag.com/email/enforcement

Datazag population pass over the Observatory corpus, 8 October 2026 snapshot: corporate mail by country-code TLD; DMARC by 1&1, Strato and Hostinger primary MX host.

The Corporate Mail Path and *The Compliance Illusion*, Datazag research notes (forthcoming, October 2026).

¹ Company sample: the 2,000 largest listed companies by number of employees, ranked using data from [CompaniesMarketCap.com](https://www.companiesmarketcap.com) (downloaded 12 October 2026). Mail records are Datazag DNS observations of 8 October 2026. All company figures are Datazag aggregates; no company-level results are published. Websites: Wikidata (CC0), Datazag research. Autodiscover and tenant tokens probed 13 October, when 17 failed 8 October lookups were re-read.

From internet-wide measurements to intelligence you can use

Datazag continuously observes domains, DNS, email infrastructure, certificates and network routing. It turns them into intelligence organizations can use directly.

The free Datazag Observatory makes aggregate internet measurements available to explore, download and analyze independently. For organizations that need domain-level intelligence, Datazag makes its datasets available through cloud data sharing and marketplaces, alongside APIs, alert feeds and infrastructure reports. The data arrives in the environment teams already use.

Email platforms

Classify customer and recipient domains by their underlying provider.

Security teams

Map infrastructure relationships and authentication weaknesses.

Insurers

Join infrastructure dependencies to their own portfolios to investigate concentration risk.

Where to go next

DATA ANALYSTS AND RESEARCHERS

Download the raw data

Get the Observatory aggregates as a Parquet file and run custom queries in DuckDB or Python.

[Download the data →](#)

ENTERPRISE AND RISK TEAMS

Portfolio exposure audit

Map your organization's third-party email, gateway and hosting dependencies against the Datazag dataset.

[Request an audit →](#)

MEDIA AND PRESS

Media stat pack

Request high-resolution charts, ccTLD breakdowns and data interviews.

[Request the stat pack →](#)