
CSC
Domain Security
Report 2026

Introduction

For the sixth consecutive year, CSC explored the state of domain security by evaluating the security posture of the Forbes Global 2000 companies. We analyzed the adoption of domain security measures used to mitigate cyber risks found in the Global 2000 companies' domain ecosystem that lay outside a company's firewall, as well as incidences of potential online brand abuse, and infringement by third parties.

This year, we compared the domain security practices of Global 2000 companies with those of the world's top 100 unicorns. While there are some similarities, one of our key questions was whether these newer companies—many in the technology and AI sectors—have adopted a stronger domain security stance. The report reveals what we found.

With the growth of cyber attacks on multinational companies such as the Global 2000, CSC continues to raise the awareness of strong domain security. Threats can arise from all areas of a company's IT infrastructure, however most attacks utilize a domain name to infiltrate systems. Making sure you have a solid security stance has never been more important.

Summary of key findings

Unicorns show strong adoption in key domain security measures around DNS records but lag in other areas that could become critical oversights as they mature

For domain security measures that rely on domain name system (DNS) records such as domain-based message authentication, reporting, and conformance (DMARC), sender policy framework (SPF), DomainKeys identified mail (DKIM), DNS security extensions (DNSSEC), and certificate authority authorization (CAA) records, we observed higher adoption among unicorns, even up to 100% using SPF for their email authentication protocols. Yet only 1% employ DNS redundancy and close to 90% of the unicorns are on a single infrastructure on the cloud.

Five out of eight domain security measures had higher adoption among unicorns than the Global 2000

Unicorns showed greater adoption than the Global 2000 in all DNS record-related measures such as DMARC (96.0% vs 79.8%), DNSSEC (16.8% vs 10.8%), and CAA records (33.0% vs 11.4%). This suggests that teams managing the domain names for unicorns are likely IT professionals with good knowledge of security protocols available within DNS that don't incur much cost for the company. This is an encouraging trend for companies driving (tech) innovation that more mature companies could emulate.

The disparity in registry lock adoption between Global 2000 companies using enterprise-class vs consumer-grade registrar is over 6x

Registry locks offer one of the strongest defenses against hijacking as it prevents unauthorized changes to your domains and DNS even if your registrar account is compromised. Due to the resources required to support this service, most consumer-grade registrars are unable to offer it, and that's evident in the data that companies using enterprise-class registrars show 6x more adoption and stronger security postures. We also saw in our recent report, "The SSL Landscape," that 60% of large corporations were using three or more secure sockets layer (SSL) providers, expanding their risk. Enterprise-class providers can give companies a better handle on their digital landscape, and ensure their supply chain has the same strong security posture, as we've seen how much damage this has caused companies in the past year.[1]

APAC has shown the largest growth between 2024 and 2025, but still lags behind EMEA and the Americas in total adoption

We see greater improvement in adoption rates over the past year among APAC companies, however in terms of actual adoption, APAC still lags behind other regions that are at least 15 percentage points ahead.

The semiconductors and banking industries show the most significant rise in overall scores over the past year

Both increased their rankings by five places each over the last year. The rapid growth in these two industries—fueled by the rise in artificial intelligence (AI) and FinTech—coupled with more stringent cybersecurity demands, could explain the better security postures observed.

The external attack surface is where the domain ecosystem lives

As cyber threats become more AI-powered, attacks continue to rise. This makes domain security an important part of a company's highest-level cyber risk assessment, which must include a company's domain ecosystem as a real vulnerability to the attacks shown in Figure 1. Compromised or hijacked legitimate domains or malicious domain registrations are used to enable all the attacks in Figure 1.

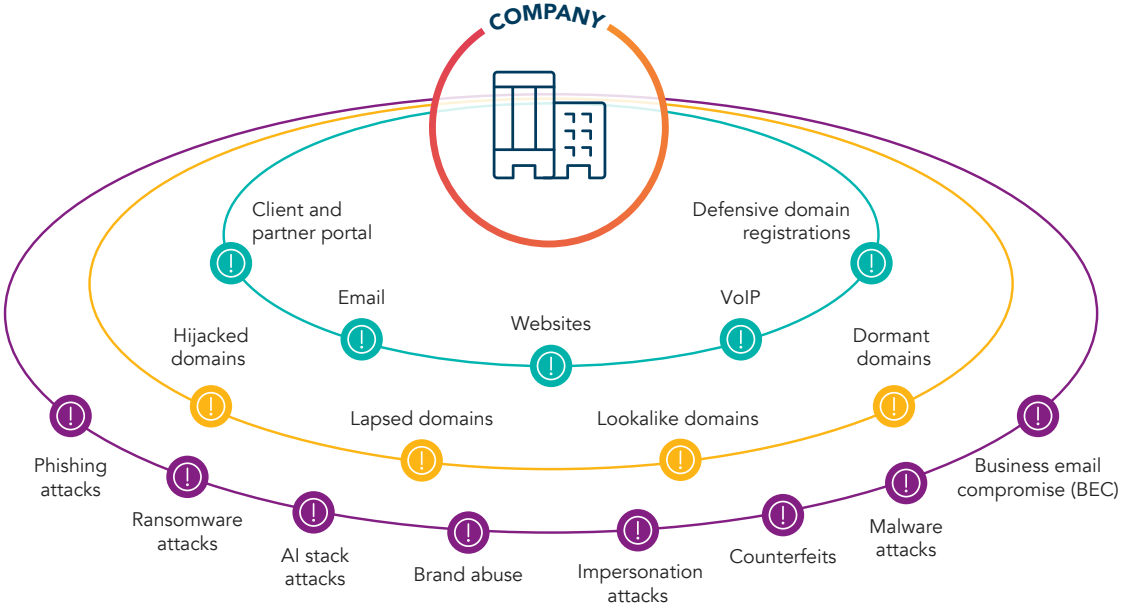
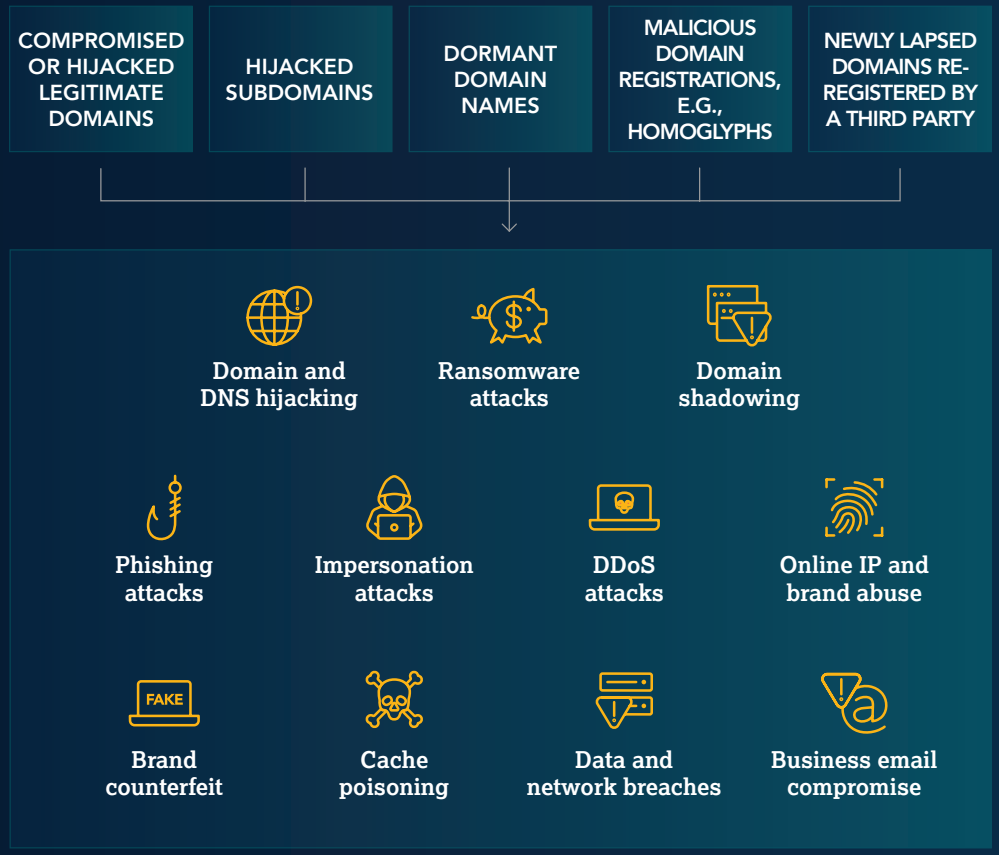


Figure 1: The galaxy of the domain name ecosystem

Domain security defined

Global businesses rely on the internet for everything—websites, email, authentication, voice over IP (VoIP), client portals, supplier applications, and your entire supply chain. The internet is part of an organization's external attack surface and needs to be continuously monitored for cybercrime and fraud. As cyber risks continue to increase, organizations and cyber insurers face greater challenges in quantifying them and addressing their capacity for harm. This means domain names are crucial elements of an organization's cybersecurity posture because the internet and domain names are essential to business infrastructure and continuity.



→ Compromised or hijacked legitimate domains

Cybercriminals will compromise any domains left unsecured. Companies should start with a layered, defense-in-depth approach to protect against hijacking.

→ Hijacked subdomains

A subdomain hijack is an attack where cybercriminals gain control of a legitimate subdomain that's no longer in use to host malicious content to target companies with phishing or malware attacks. They do this by exploiting forgotten DNS records (dangling DNS) to point to their own content.

→ Dormant domain names

Cybercriminals may register and hold onto branded domains, keeping them dormant until they're ready to weaponize them in a phishing or malware attack. Dormant domains often escape initial detection because they don't immediately have any of the indicators of a domain registered to launch an attack—e.g., an active MX (email) record, which would usually raise a red flag.

→ Malicious domain registrations

There are endless domain spoofing permutations and homoglyphs that are easily used by phishers and malicious third parties. The intent of these fake domain registrations is to leverage consumer trust in the targeted brand to launch convincing phishing attacks or other forms of digital brand abuse.

→ Newly lapsed branded domains re-registered by a third party

Companies may choose to lapse previously defensively registered domain names due to cost pressures. Cybercriminals wait for this and immediately re-register these domain names for malicious purposes. They're constantly on the lookout for available, branded domains they can weaponize.

Findings and analysis: Global 2000 adoption of domain security measures

In this analysis, CSC looked at the adoption of five key domain security measures across the Global 2000 list—namely DMARC, DNS redundancy, registry locks, CAA records, and DNSSEC. We then performed a deep analysis into the adoption levels across industry groups and regions.

Trends in adoption of domain security measures (2020-2025)

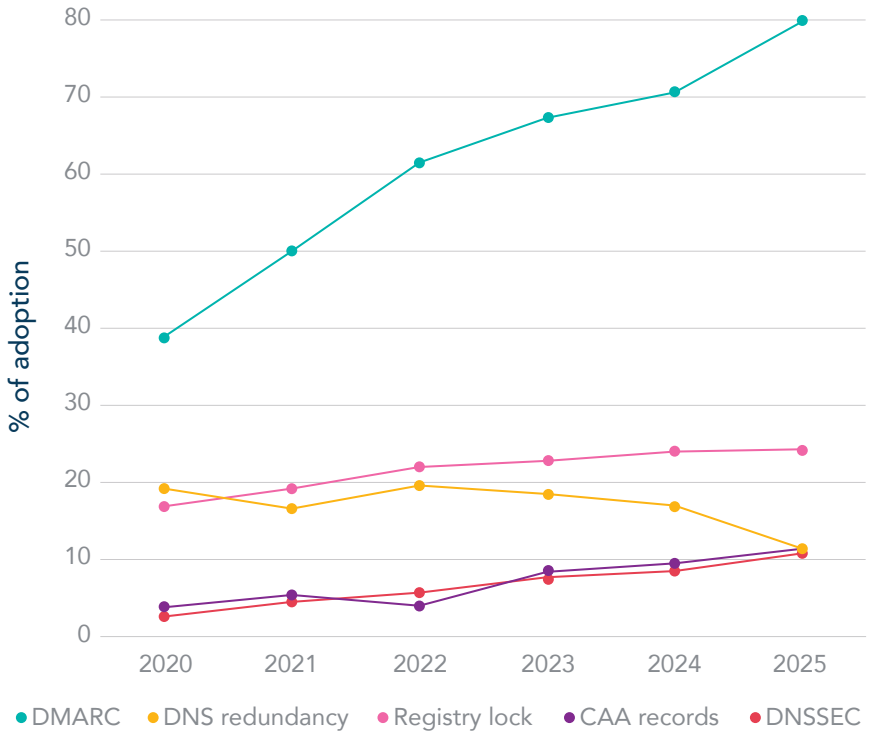


Figure 2: Global 2000 adoption of the five key domain security measures, 2020-2025

DMARC has the fastest growth

It's no surprise given all the news about phishing attacks—including their increase in volume and complexity—that DMARC adoption has risen quickly from 39% in 2020 to 80% in 2025 (Figure 3). We have also seen a drive in DMARC adoption due to NIS2 coming into effect in October 2024, which places more emphasis on cybersecurity for companies operating in the European Union. Of the remaining 20% still lagging in adoption, 85% are from APAC across all industries, which is consistent in our observations on regional adoption.

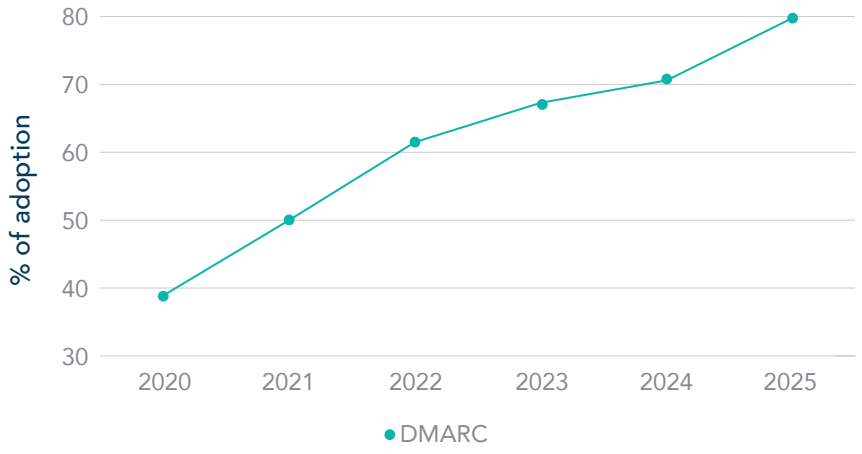


Figure 3: DMARC adoption rates 2020-2025

What is NIS2?

Network and Information Security Directive 2 (NIS2) is the European Union's new cybersecurity law—Directive (EU) 2022/2555—that was adopted on December 14, 2022. It sets stricter requirements than previous directives to ensure a higher common level of cybersecurity across all EU member states. It outlines obligations, particularly for critical entities under Critical Entities Resilience Directive (CER)—Directive (EU) 2022/2557—including organizations in the energy, transport, healthcare, banking, finance marketing infrastructure, digital infrastructure, and public administration sectors. These organizations must take concrete steps to manage cyber risks, protect systems, respond promptly to incidents, and abide by national cybersecurity strategies. Incident reporting is mandatory, while sharing of threat intelligence is encouraged. Regulators are also empowered to audit, enforce compliance, and impose fines on organizations for breaches.

Such focus on cybersecurity at the national level is met by similar responses in governments around the world that have also adopted similar directives for critical industries in their respective countries. For instance, in Australia, the 2023-2030 Australian Cyber Security Strategy, includes a new Cyber Security Act 2024 and amendments to the Security of Critical Infrastructure Act (SOCI Act) that mandates minimum security standards, introduces mandatory reporting, and clarifies rules and obligations in risk management and data security. Companies that operate internationally will need to align their security practices with these rising global standards.

Decline in DNS redundancy

DNS redundancy dipped slightly compared to last year, this is partly due to CSC's methodology changing over the previous year, but in the underlying data there is still a slight decline. This has led to an overall percentage change of 6% year on year, where companies are prioritizing DNS redundancy. DNS redundancy is a critical component in any organization's core infrastructure, and we're seeing adoption for this security measure decreasing, which could be attributed to companies needing to plan for increasing cost and resource allocation. Many companies are also turning to a single infrastructure on the cloud, for cost savings, scalability, data accessibility, and more. On the one hand, being on the cloud provides a globally distributed system, but it still has the same potential risks if parts of the system are taken offline. The only way to truly mitigate risks on DNS is by establishing two robust independent networks for redundancy (dual infrastructure).

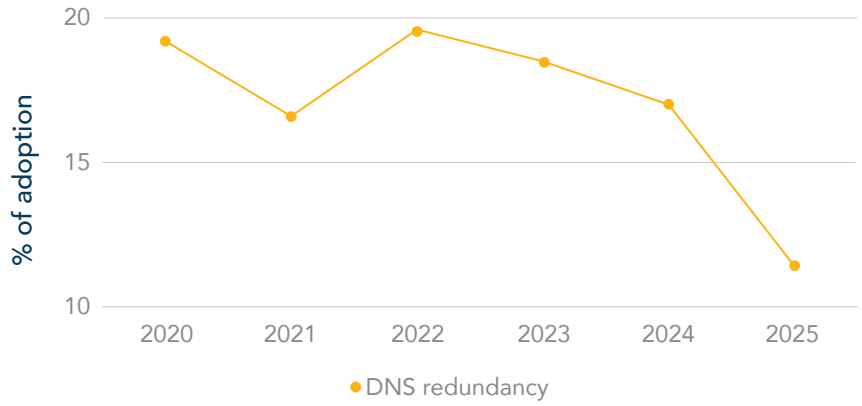


Figure 4: DNS redundancy adoption rates 2020-2025

Watch our webinar to uncover why DNS has emerged as the biggest single point of failure in today's digital ecosystem.

Security measures such as registry lock, DNSSEC, and CAA records have been growing steadily but slowly

Adoption rates of registry locks rose marginally to 24% in 2025. We also observed that companies that use enterprise-class registrars also use registry lock more frequently at 53% in 2025. With increasing pressure to tighten cybersecurity, more registries are offering locks on their domain extensions to enable end-to-end domain name transaction security—mitigating human error and third-party risk.

As a company's domain portfolio is constantly changing, CSC uses a predictive-modeling algorithm that assesses over 20 domain name attributes to identify whether that domain is conducting business-critical work for company operations and online brand, and recommends vital domains that should be locked. With the rise in AI, we continue to advocate for strong domain security posture as a trust signal. This is especially relevant as a company's AI stack that uses application programming interfaces (APIs) and plugins all rely on domains and DNS to function.

While still low, the percentage of companies deploying DNSSEC has quadrupled over the past six years to 11% in 2025. DNSSEC works by providing authentication and data integrity to DNS queries and responses, which in turn prevents cybercriminals from redirecting internet traffic to malicious websites, such as phishing websites. In some countries, the adoption of DNSSEC is greater than 67%. However, it remains lower in large organizations. Some of this is due to the maintenance of updating keys required in a more complex organizational structure, but it remains a security measure all critical domains should be adopting.

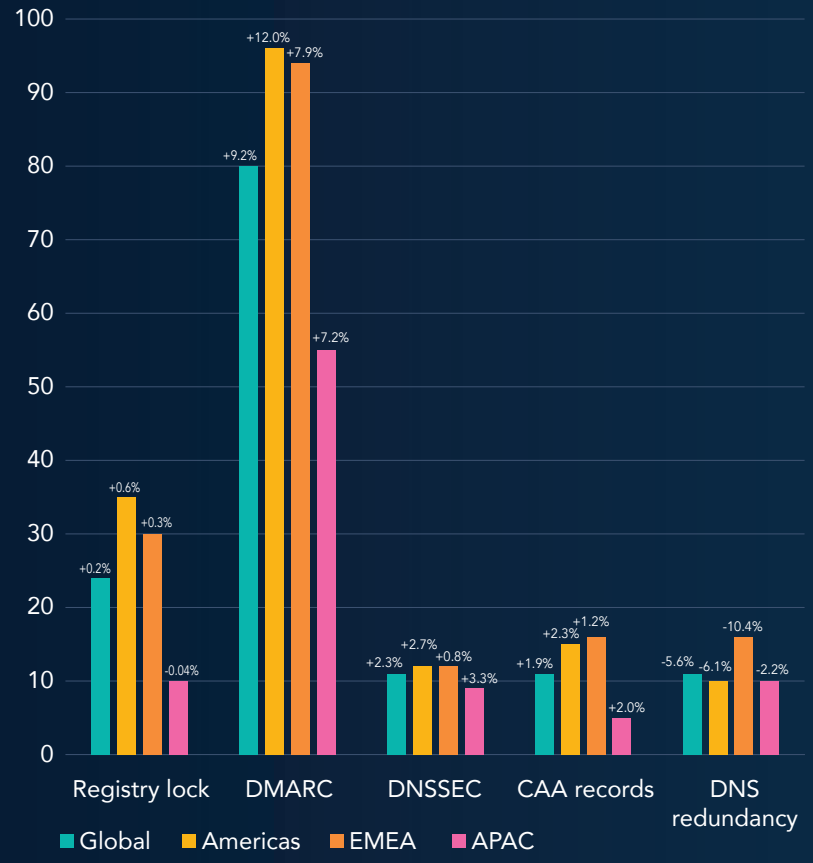
Lastly, the use of CAA records increased again to 11% in 2025. CAA records allow companies to designate specific certificate authorities (CA) to be the issuers of digital certificates for their company's domains. This prevents cybercriminals from using a non-authorized CA to gain a new digital certificate, as their request will fail, and the company will receive an alert. The additional benefit of CAA records are that companies can enforce compliance so that staff only use providers that have been authorized. In our recent report, "The SSL Landscape," we saw over 60% of large corporations use more than three providers, with one using 13 providers. The report also highlighted that providers most prominently used by fraud websites also corresponded with the highest used. Greater scrutiny of SSL management is needed, especially as AI stacks are also becoming more autonomous.

DNSSEC has quadrupled adoption in six years, however only 11% of Global 2000 companies have it integrated into their most critical domain names.

Domain security measures

By region

APAC has shown the largest growth in domain security adoption between 2024 and 2025 but still lags behind EMEA and the Americas in total adoption.



+/- % change from previous year

Figure 5: Domain security adoption by region

By industry

IT software and services remain as the top performing industry in 2025.

Industry classification	2025 rank	2024 rank
Semiconductors	6	11
Banking	11	16
Technology hardware and equipment	13	5
Aerospace and defense	16	8

The highest performance industries continue to be those that rely heavily on the internet for their business operations such as IT software and services and media. We also saw banking and semi-conductors increase their standing further over the last year. The rapid growth in these two industries—fueled by the rise in AI and FinTech—coupled with more stringent cybersecurity demands, could explain the better security postures observed. For the lowest performing industries, we continue to see industries such as construction, mining, and utilities. What's interesting is that many of the low performing industries are also classed as critical industries, particularly in the NIS2 Directive. This may mean that, over the coming year, those industries will take their domain security more seriously, especially with the increased attacks on these types of industries.

↑ HIGHEST PERFORMING INDUSTRIES

- IT software and services
- Media
- Retailing
- Business services and supplies
- Telecommunications services

↓ LOWEST PERFORMING INDUSTRIES

- Construction
- Materials
- Food markets
- Utilities
- Food, drink, and tobacco

Domain security measures by registrar type

For this report, we analyzed the trend of domain security adoption with respect to the type of domain registrar used by the companies that make up the Global 2000.

Many companies have a misconception that all registrars are the same. There's misplaced trust put into consumer-grade registrars that may not prioritize or even offer domain security measures, which can impact a company's overall security posture. This is especially apparent for the adoption of registry locks, as most consumer-grade registrars don't support them.

Enterprise-class registrars

An enterprise-class registrar specializes in working with corporations and brand owners that require advanced business practices, capabilities, expertise, and support staff in relation to domain and DNS management, as well as security, brand and fraud protection, data governance, and cybersecurity. To find out more about how using an enterprise-class registrar can help mitigate domain hijacking, dangling DNS, and domain impersonators, download our "Domain Security Checklist."

Consumer-grade registrars

A consumer-grade registrar is geared for domain services, websites, and email, for personal use, entrepreneurs, and small businesses that are just getting started. Many do not offer domain security services, which also reduces adoption.

Companies that rely on enterprise-class capabilities have a higher adoption of domain security measures

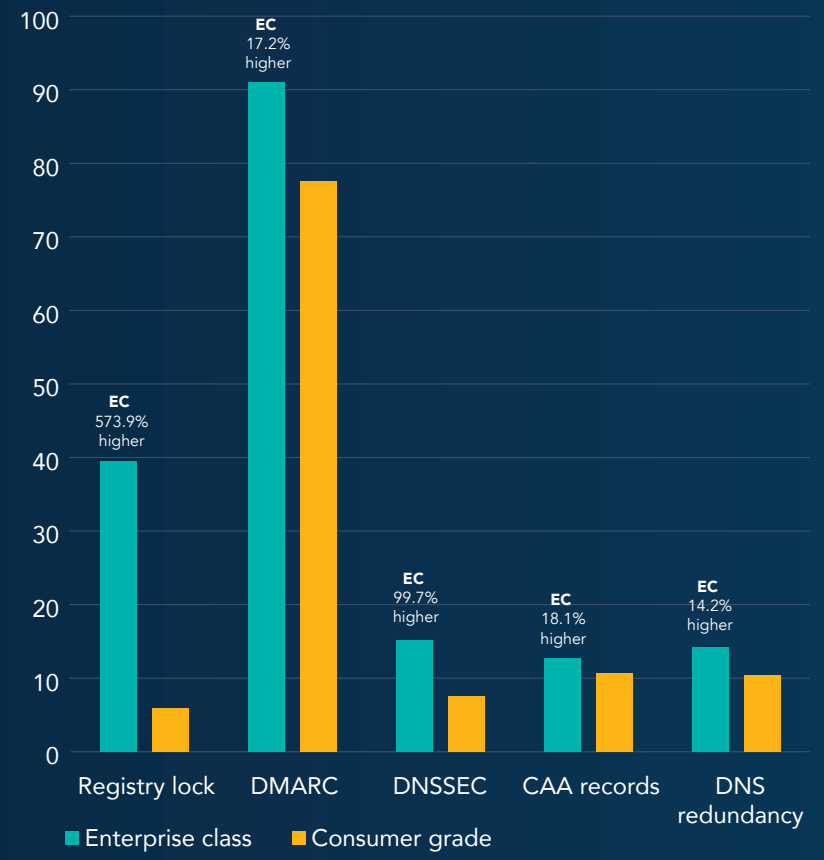


Figure 6: Maturity level of security measures—enterprise-class (EC) vs consumer-grade (CG) registrars

Domain security posture

Looking at the importance of an expanded list of eight key security measures that we grouped according to a company's domain security risk level, CSC derived an average score for each company. This average makes up the company's security score with a higher score denoting a stronger security posture—meaning companies are at less risk of domain security threats.

Key domain security measures:

- Enterprise-class domain registrar
- Registry lock (MultiLock)
- CAA records
- DNS redundancy
- DNSSEC
- Sender policy framework (SPF)
- DomainKeys identified mail (DKIM)
- DMARC

Domain security risk levels

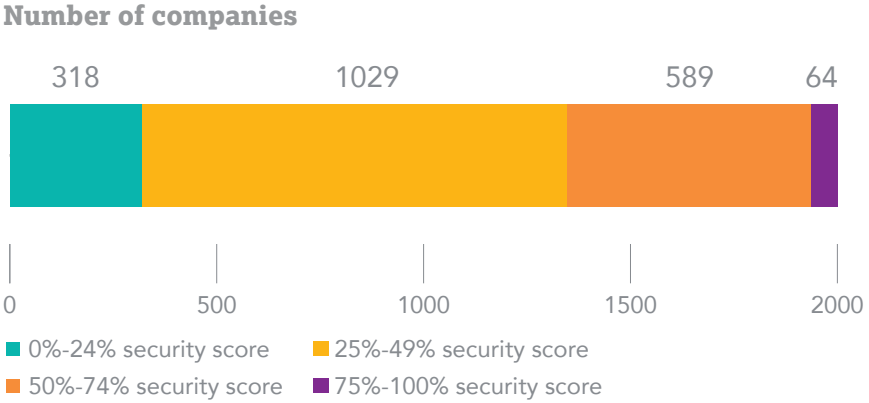


Figure 7: Domain security scores and associated domain security risk levels of Global 2000 companies

> 67% of all Global 2000 companies have less than half of the recommended security measures implemented.

↑ HIGHEST PERFORMING COMPANIES

There is only one company that has a 100% score, similar to last year's report. Only eight companies have a score of seven out of eight, a third less than last year.

↓ LOWEST PERFORMING COMPANIES

Eighty-seven companies have a domain security score of zero, an improvement from last year's number of 107. These companies are primarily from the Asia-Pacific region, making up 87% of the zero-score companies.

Suspicious or malicious domain activity targeting the Global 2000

We identified and analyzed domains containing Global 2000 brand names with more than six characters that were not owned by the brands themselves. The intent of these third-party domain registrations is to leverage the trust placed on the targeted brand to launch phishing attacks, other forms of digital brand abuse, or IP infringement. These lead to revenue loss, traffic diversion, and a diminished brand reputation for the affected brand. There are endless domain spoofing tactics and permutations that can be used by phishers and malicious third parties.

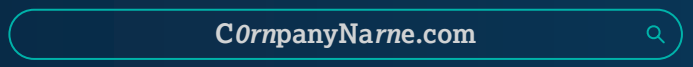
WE INTENTIONALLY FOCUS ON COMMON HOMOGLYPHS AS THEY ARE ONE OF THE MOST EGREGIOUS ATTACK METHODS USED BY THREAT ACTORS

Domain spoofing tactics

Figure 8: Common domain spoofing tactics

Common homoglyphs (fuzzy matches) in .COM domains

Based on frequent observation of use in phishing domains, our analysis included common Latin-character substitutions, for example, using C0rnpanyNarne.com to look like CompanyName.com.



Most popular character substitutions

c → e	0 → 0	m → n	l → I	m → rn
g → q	E → 3	S → 5	B → 8	l → 1

Figure 9: Common homoglyphs (fuzzy matches) in .COM domains

88% OF HOMOGLYPH DOMAINS ARE OWNED BY THIRD PARTIES

Out of the third-party owned domains:

40% have MX records in 2025 compared to 42% in 2024. MX records can be used to send phishing emails or to intercept email. This is a key reason for the growth in DMARC records being added.

HOW ARE THIRD-PARTY DOMAINS BEING USED?

40% point to advertising, pay-per-click ads, or are being used for domain parking.

39% have inactive websites.

32% of all inactive domains have active mail records meaning that even domains that don't resolve to live content can still be used for email activities.

2% point toward malicious content that could damage a brand's reputation and customer confidence.

19% resolve to a live website not associated with the brand owner.

One of the areas companies should be aware of is the use of dormant domains, where third parties carry out mass registrations and keep the names dormant sometimes for a long period. As seen in the results, 32% of third-party domains are inactive but contain MX records, which could easily be activated.

DOMAIN REGISTRARS MOST ASSOCIATED WITH FAKE DOMAIN REGISTRATIONS OWNED BY THIRD PARTIES

- GoDaddy®
- Namecheap™
- Network Solutions

Suspicious and malicious domains: who's being targeted?

INDUSTRY	FAKE DOMAIN THREAT % OF TOTAL
Banking	16.3%
IT software and services	6.6%
Diversified financials	5.8%
Utilities	5.4%
Insurance	5.4%
Construction	5.2%
Oil and gas operations	5.1%
Business services and supplies	4.3%
Capital goods	4.3%
Transportation	4.3%
Consumer durables	4.0%
Retailing	3.6%
Technology hardware and equipment	3.6%
Materials	3.5%
Food, drink, and tobacco	2.8%
Telecommunications services	2.7%
Drugs and biotechnology	2.4%
Healthcare equipment and services	2.4%
Semiconductors	2.3%
Aerospace and defense	1.9%
Trading companies	1.7%
Chemicals	1.7%
Food markets	1.5%
Hotels, restaurants, and leisure	1.3%
Household and personal products	1.0%
Media	0.9%

Domain security insights: are unicorn corporations the dream domain security advocates?

CSC decided this year to make a comparison between the Global 2000 companies—many of which are in long-established industries—against the top 100 unicorn companies. The majority of the top 100 unicorn list are IT companies with many in the AI industry. To keep things simple, we examined the same domain security characteristics against these companies as the Global 2000. Our main goal in the analysis was to ascertain if smaller start-up companies are more attuned to domain security risks and have the ability to implement them than larger established corporations. With many of the unicorns in the AI industry, they display good understanding that the security protocols around their critical infrastructure of domains and DNS is needed and show high adoption in some areas, yet lack in others. Additionally, the AI stack that many of these companies are building will contribute to the broader risks in the supply chain of the companies using them.

What is a unicorn?

A unicorn is a privately owned company with a valuation of over $1 billion. They're usually start ups or relatively new companies, and usually innovative in their industry.

Highlights

Figure 10: Domain security adoption—100 unicorns vs Global 2000

In comparison with the Global 2000 across eight domain security attributes, unicorns have a higher score in five categories. The key areas where they're stronger are email security with higher adoption of SPF, DKIM and DMARC, as well as DNSSEC and CAA records. What all of these have in common is that they're managed through DNS records. This suggests that teams managing the domain names for unicorns are likely IT professionals with good knowledge of security protocols available within DNS that don't incur much cost for the company.

The difference in Global 2000 companies having a higher security stance starts first with more of them using an enterprise-class registrar. Why is this important? Enterprise-class registrars have strong security measures in place, such as training staff against social engineering and two-factor authentication. Companies using consumer-grade registrars have seen activities such as "domain doppleganging" where accounts are hacked and subdomains are set up on legitimate domain names.

The other difference was in registry locks having lower use rates, caused by the fact that many consumer-grade registrars do not offer this service.

With Global 2000 companies using enterprise-class registrars, there's a greater opportunity for their registry lock adoption.

As unicorns are still in their early stages focused on market growth, the choice of registrar could be low among their business priorities, or they could lack the knowledge of the differences between registrars and how it impacts their security postures. Registrar type has a direct influence on registry lock adoption and security—such locks are unsupported by consumer-grade registrars, hence unicorns leave themselves vulnerable to attacks such as DNS hijacking, domain hijacking, email spoofing, and more when their registrar is more easily compromised without the additional layers of defense. Even with a strong IT team with good DNS fundamentals, as unicorns scale in their operations with larger, more complex domain portfolios, an oversight of their domain security in the hands of their third-party domain registrar could bring about great risks, as any incident or downtime directly impacts most of these businesses that operate online.

AI and technology dominate

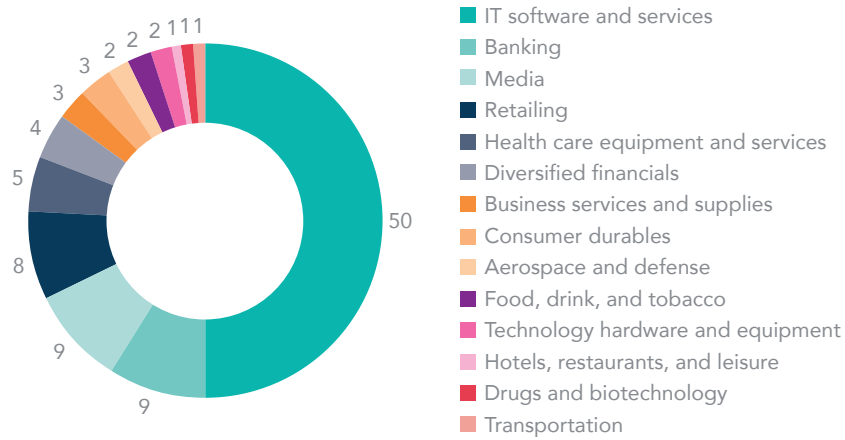


Figure 11: Industry representation among 100 unicorns

Half the companies within the top 100 unicorns are IT services, followed by banking, which comes in as the second highest. Many in IT services are sole AI companies, and most of the banking companies are FinTech start ups, both with heavy reliance on the internet to drive their business.

Who's more secure?

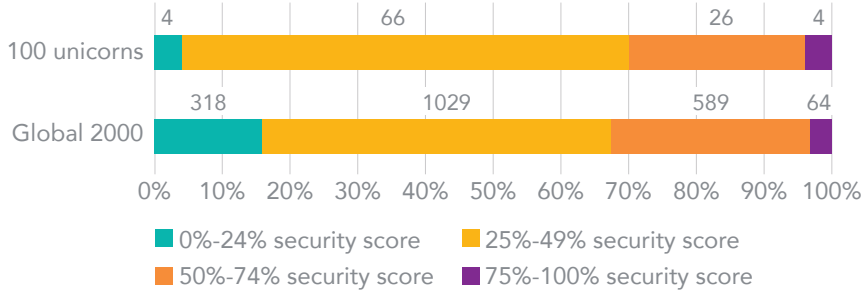


Figure 12: Domain security levels—100 unicorns vs Global 2000

Comparing the Global 2000 domain risk scores against the unicorns doesn't show comprehensive differences. It's apparent that fewer unicorns (4%) are in the low score range compared to 15% among the Global 2000. However, significantly more unicorns sit in the mid-range—showing they're taking certain elements seriously, such as email security, but lacking some of the more advanced security protocols, such as registry lock and DNS redundancy.

Conclusion

Companies continue slowly to increase their domain security, however there's still more work needed for improvement amongst the largest companies in the world. We believe that government interventions with legislations such as NIS2 will create more emphasis on driving these changes quicker, especially as we see a continued growth of cyber attacks against multinational companies.

Unicorns have quickly adopted domain security protocols around DNS security, often driven by smaller more nimble IT departments able to make quick decisions without the complexities of a globally dispersed company. That said, they tend to fall short in areas such as DNS redundancy, registry locks, and enterprise-class registrars, but this may change as the company matures and the vendors they use become more sophisticated. In time, unicorns will need to ensure that both their own domain security, that of their supply chain, and the supply chain they're a part of, are made stronger. It may take a major incident or government intervention to spark urgency despite the growing prominence of AI, the industry in which many of unicorns operate in, showing how security is paramount to driving their businesses forward.

The risk of a company not addressing its domain security can be catastrophic. Unprotected domains pose a significant threat to a company's cybersecurity posture, data protection, consumer safety, intellectual property, supply chains, revenue, and reputation.

If companies do not take the security of their domain names seriously, it can lead to exploitation by third parties. With ever-changing geopolitical systems, more sophisticated criminals, and the introduction of AI into malicious cyber campaigns, we all collectively need to make sure we become hard targets.

View CSC's list of proactive and defensive security measures to safeguard your domains and brands using a multi-layered, defense-in-depth approach to domain security.

Download our "Domain Security Checklist"

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve.

Get in touch

cscdbs.com

[1]cnbc.com/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html

DBS14112025