
CSC
2026年度
域名安全报告

引言

CSC连续六年通过评估福布斯全球企业2000强的安全状况，来审视域名安全态势。我们分析了这些企业在公司防火墙之外的域名生态系统中，为降低网络风险而采取的域名安全措施，以及第三方对线上品牌造成的潜在滥用与侵权事件。

今年，我们对全球2000强企业与全球百强独角兽企业的域名安全实践进行了对比。虽然两者在某些方面存在相似之处，但我们关注的核心问题之一是：这些新兴企业（尤其是科技和人工智能（AI）领域的公司）是否在域名安全方面采取了更强有力的措施。本报告呈现了我们的主要发现。

随着针对全球2000强等跨国企业的网络攻击日益增多，CSC持续致力于提升企业对强域名安全的重要性认知。威胁可能来源于企业IT基础设施的各个环节，但大多数攻击都通过域名渗透系统。确保建立稳固的安全防护措施，其重要性比以往任何时候都更为突出。

重要研究结果摘要

独角兽企业在围绕DNS记录的关键域名安全措施上表现出强劲的采用率，但在其他方面仍显滞后，这些方面随着企业发展可能演变为重大疏漏

对于依赖域名系统（DNS）记录的域名安全措施，例如基于域名的消息认证、报告和一致性（DMARC）、发件人策略框架 (SPF)、域名密钥识别邮件（DKIM)、DNS安全扩展 (DNSSEC) 以及证书颁发机构授权 (CAA) 记录，我们观察到独角兽企业的采用率普遍更高，其中甚至有高达100%的企业使用SPF作为电子邮件认证协议。然而，仅有1%的企业部署了DNS冗余，近90%的独角兽企业仍依赖单一云基础设施。

在八项域名安全措施中，独角兽企业有五项的采用率都高于全球2000强企业

在所有与DNS记录相关的措施中，百强独角兽企业的采用率均高于全球2000强企业，具体如下（百强独角兽vs全球2000强企业：DMARC (96.0% vs 79.8%)、DNSSEC (16.8% vs 10.8%)、CAA记录 (33.0% vs 11.4%)。这表明，为独角兽企业管理域名的团队，很可能由精通DNS安全协议的IT专业人士组成，而这些措施几乎不会给企业带来高昂成本。对于推动技术创新的企业而言，这是一个令人鼓舞的趋势，也为成长型企业提供了可借鉴的做法。

采用企业级和消费级注册商的全球2000强企业在注册局锁采用率上的差距超过6倍

注册锁是防范域名劫持的最强防御手段之一，即使注册商账户遭入侵，也能阻止对域名及DNS的未授权更改。由于该服务需要一定资源支持，多数消费级注册商无法提供。数据显示，使用企业级注册商的企业采用率高出6倍，安全防护能力也更强。我们在近期发布的《SSL发展态势》报告中也指出，60%的大型企业同时使用三家或以上安全套接字层 (SSL) 证书提供商，其风险随之增加。企业级提供商能够帮助企业更好地掌控数字环境，并确保其供应链也具备同样强健的安全防护。过去一年，这类安全漏洞给企业带来的损失有目共睹。[1]

2024年至2025年间，亚太地区的域名安全措施采用率增幅最大，但整体采用率仍落后于欧洲、中东和非洲地区以及美洲

在我们的见证下，过去一年，亚太企业的采用率虽有显著提升，但就实际采用情况而言，仍落后于其他地区至少15个百分点。

过去一年，半导体和银行业的整体评分增幅最为显著

过去一年，这两大行业的排名均上升了五位。得益于AI和金融科技的兴起，这两大行业迅猛增长，加之网络安全要求日益严格，或能解释其安全态势的改善。

域名生态系统存在于外部攻击面之上

随着AI技术愈加成为网络威胁的助力手段，各种攻击也在不断增加。这使域名安全成为了公司最高级别网络风险评估中重要的一环，公司的域名生态系统成为此类评估中不可或缺的元素，也是切实存在的可能遭受攻击的漏洞，如图1所示。被入侵或劫持的合法域名或恶意域名注册均可用于实施图1所示的所有攻击。

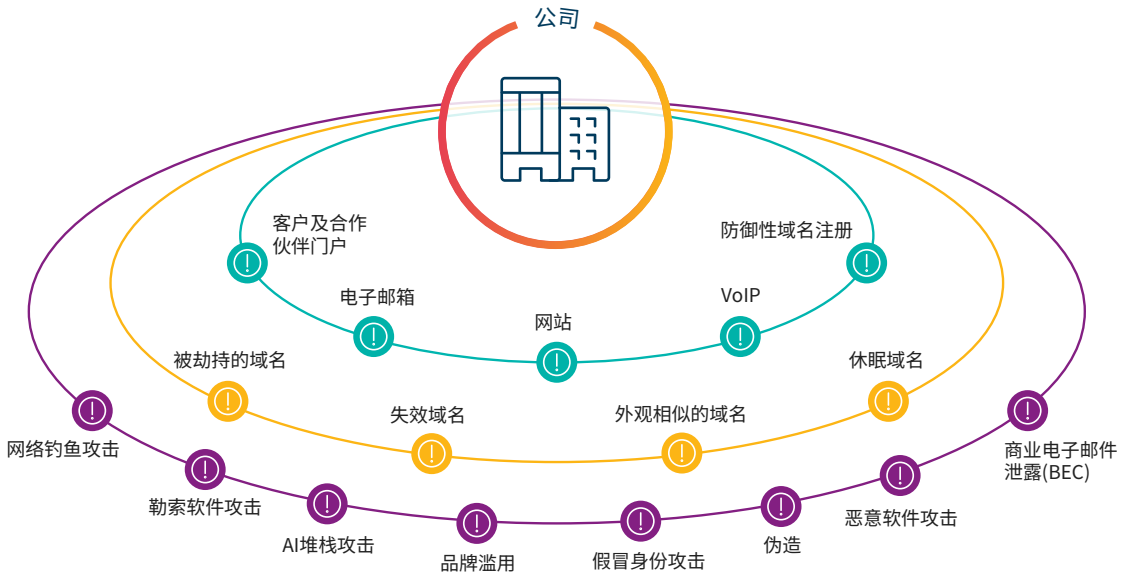


图1:域名生态系统体系

域名安全定义

全球企业的各种事务都要依靠互联网实现，包括网站、电子邮件、身份验证、IP语音(VoIP)、客户门户、提供商应用以及您的整个供应链。互联网是企业外部受攻击面的一部分，需要持续进行监控，以防范网络犯罪和欺诈。随着网络风险不断提高，各个企业和网络保险公司在量化风险和降低其破坏能力方面面临着更大的挑战。这意味着域名是企业网络安全状况的关键要素，因为互联网和域名对企业基础设施和业务连续性至关重要。

→ 遭到入侵或劫持的合法域名

网络犯罪分子会破坏任何未加保护的域名。企业应采用分层防御的深度防御策略来防止域名劫持。

→ 被劫持的子域名

对于子域名劫持这种攻击方式，网络犯罪分子会通过控制不再使用的合法子域名来托管恶意内容，以针对公司进行网络钓鱼或恶意软件攻击。他们会利用被目标公司遗忘的DNS记录（悬空DNS），以指向其自己的内容。

→ 休眠域名

网络犯罪分子可能会注册并持有品牌域名，使其处于闲置状态，以备在网络钓鱼或恶意软件攻击中使用这些域名。休眠域名通常会逃避初步检测，因为它们尚未显示出任何表明域名被注册用于发动攻击的迹象——例如，通常会触发警报的活跃MX（电子邮件）记录。

→ 恶意域名注册

域名诈骗组合伎俩和同形文字假冒域名层出不穷，很容易被网络钓鱼者和恶意第三方利用。这些虚假域名注册的目的是是利用消费者对目标品牌的信任，发起令人信服的网络钓鱼攻击，或进行其他形式的数字品牌滥用。

→ 新近失效的品牌域名被第三方重新注册

企业可能会因为成本压力而选择放弃之前注册的防御性域名。网络犯罪分子会趁机而动，立即出于恶意目的重新注册这些域名。他们会不断寻找可用的品牌域名，并以此作为武器。

研究结果与分析：全球 2000 强企业采用域名安全措施的情况

在本次分析中，CSC调查了全球2000强企业对五项关键域名安全措施的采用情况，分别为：DMARC、DNS冗余、注册局锁、CAA记录和DNSSEC。然后，我们按照行业和地区对采用率进行了深入分析。

采用域名安全措施的趋势（2020年-2025年）

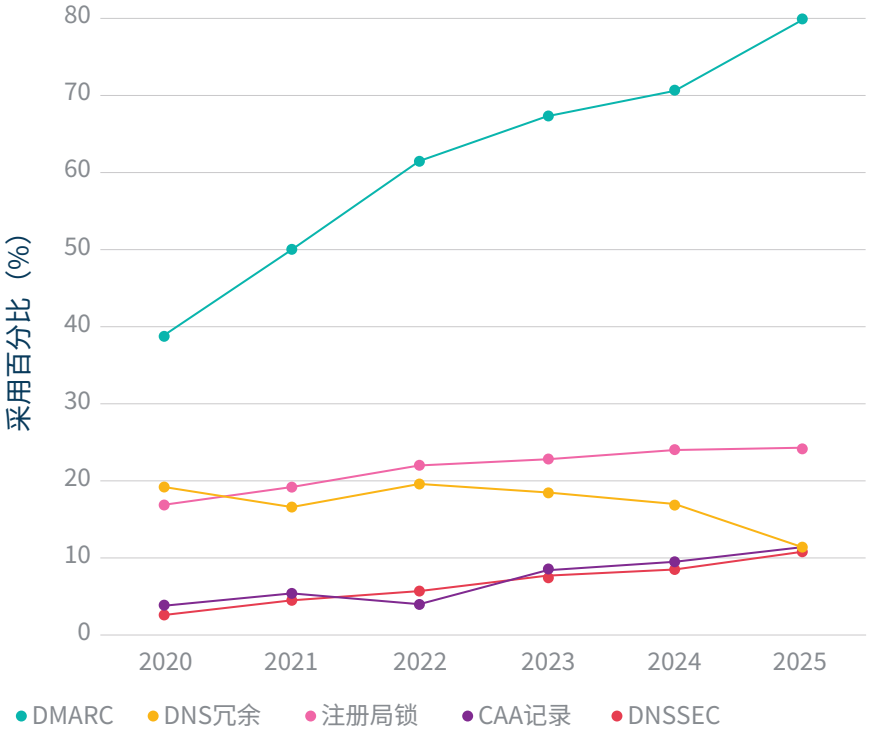


图2：全球2000强企业对五大关键域名安全措施的采用情况（2020年-2025年）

DMARC见证最快增长

鉴于网络钓鱼攻击的各种报道频频登上头条，攻击数量和复杂程度与日俱增，DMARC的采用率从2020年的39%迅速上升到2025年的80%（图3），这并不令人意外。我们还观察到，随着NIS2于2024年10月生效，欧盟境内运营的企业需要强化网络安全防护，这也推动了DMARC的采用。在尚未采用DMARC的20%企业中，有85%来自亚太地区，覆盖各行各业，这与我们对区域采用情况的观察一致。

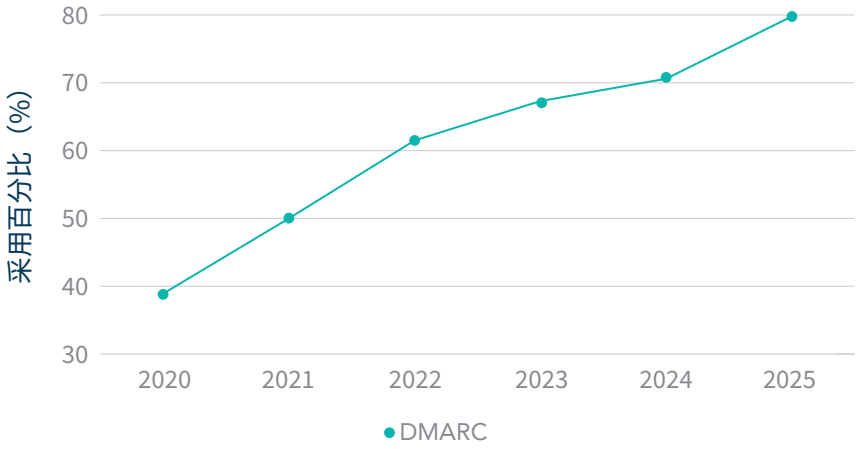


图3：2020年-2025年DMARC采用率

什么是NIS2?

《网络与信息安全指令2》（NIS2）是欧盟于2022年12月14日通过的新网络安全法规——指令(EU)2022/2555。该指令对网络安全要求更为严格，旨在提升欧盟成员国的整体网络安全水平。指令明确了相关义务，尤其针对《关键实体韧性指令》(CER)——指令 (EU)2022/2557下的关键实体，包括能源、交通、医疗、银行、金融市场基础设施、数字基础设施以及公共行政等领域的组织。这些组织必须采取切实措施来管理网络风险、保护系统、及时响应事件，并遵循国家网络安全战略。事件报告为强制性要求，同时鼓励共享威胁情报。监管机构也被赋予审计、强制执行和对违规组织处以罚款的权力。

欧盟在国家层面如此重视网络安全，也促使全球其他国家政府纷纷效仿，为本国关键行业制定类似指令。例如，澳大利亚在《2023 年-2030年澳大利亚网络安全战略》中，纳入了新的《2024年网络安全法》和对《关键基础设施安全法》的修订。《关键基础设施安全法》规定了最低安全标准、引入了强制报告机制，并明确了风险管理和数据安全方面的规则和义务。跨国经营的企业需确保自身的安全实践与这些日益提升的全球标准保持一致。

DNS冗余下降

与去年相比，DNS冗余略有下降，部分原因在于CSC的研究方法较去年有所调整，但基础数据显示确实存在轻微下滑。这导致优先采用DNS冗余措施的企业数量整体同比下降6%。DNS冗余对任何企业的核心基础架构来说都是重要组成部分，但我们发现，这种安全措施的采用率在下滑，原因可能是企业面临不断增加的成本和资源分配压力，需要合理筹划。出于节约成本、提升可扩展性和增强数据可访问性等考虑，许多企业正转向单一云端基础设施。云端部署虽可构建全球分布式系统，但一旦系统某些部分离线，仍存在同样的潜在风险。要切实降低DNS风险，唯有建立两套强健独立的网络以实现冗余（即双基础设施）。

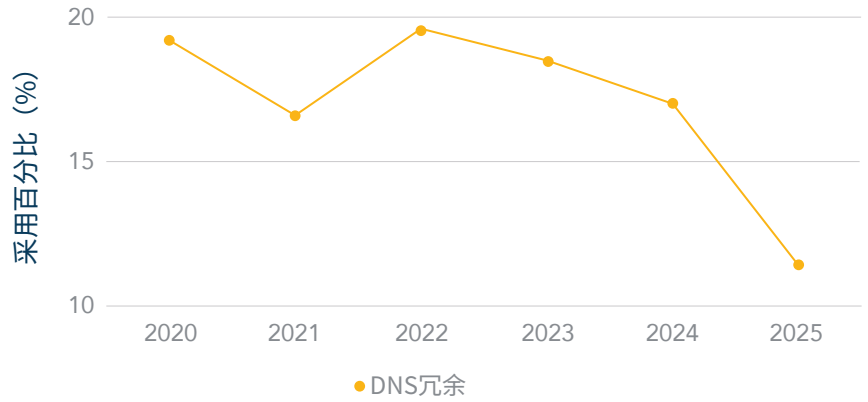


图4：2020 年-2025年DNS冗余采用率

欢迎观看我们的网络研讨会，了解为何DNS已成为当今数字生态系统中最关键的单点故障。

注册局锁、DNSSEC和CAA记录等安全措施稳步增长，但增速仍然缓慢

2025年，企业对注册局锁的采用率小幅上升至24%。我们还发现，使用企业级注册商的公司也更频繁地使用注册局锁，在2025年，后者占前者的比例为53%。随着加强网络安全的压力日益增大，越来越多的注册商开始为其域名扩展提供锁定功能，以实现端到端域名事务的安全性，从而减少人为错误和第三方风险。

公司的域名组合不断变化，为此，CSC使用预测性建模算法，评估域名的20多个属性，以确定该域名是否对公司运营和线上品牌具有关键的商业意义，并就应锁定的重要域名提出建议。随着AI的迅猛发展，我们持续倡导以稳健的域名安全态势作为企业信任的象征。这尤其重要，因为企业的AI堆栈依赖应用程序编程接口（API）和插件，而这些功能的正常运行完全依赖于域名和DNS。

尽管部署DNSSEC的公司比例仍偏低，但过去六年来已增长三倍，到2025年达11%。DNSSEC的工作原理是为DNS查询和响应提供身份验证和数据完整性，从而防止网络犯罪分子将互联网流量重定向到网络钓鱼网站等恶意网站。部分家的DNSSEC采用率已超过67%，但在大型企业组织中，采用率仍相对较低。部分原因在于，企业组织架构越复杂，密钥更新维护的难度就越大，但这仍是所有关键域名必须执行的重要安全措施。

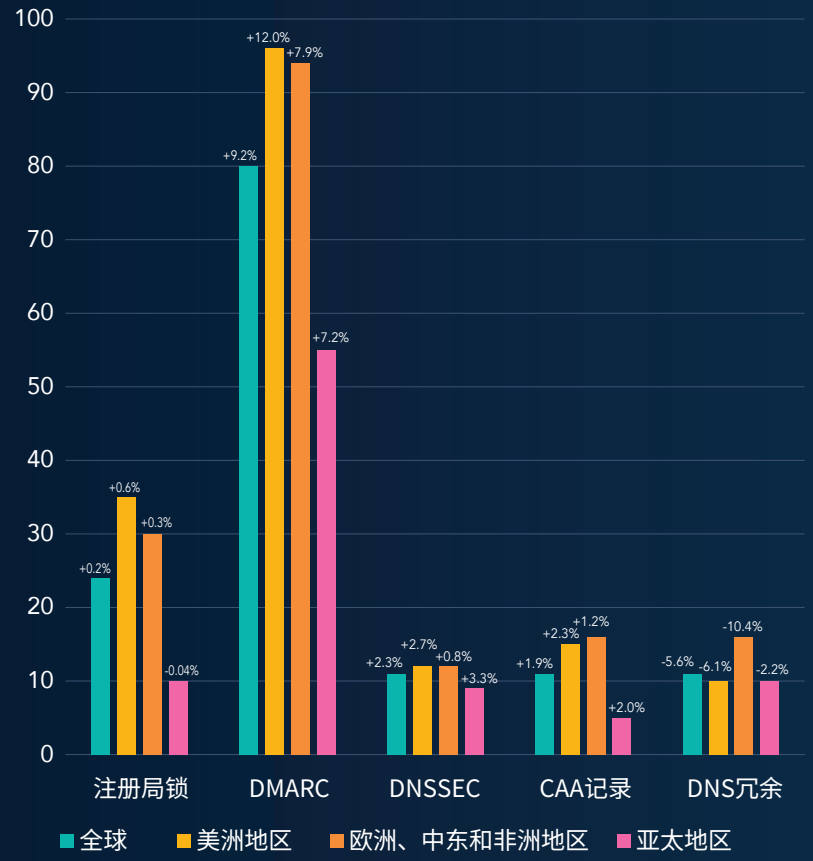
最后，CAA记录的采用率在2025年再次提升，已达到11%。CAA记录允许公司指定特定证书颁发机构（CA）作为其公司域名的数字证书颁发机构。此举可防止网络罪犯使用未授权的CA获取新数字证书，这会导致他们的请求失败，同时公司也会收到相关的警报。CAA记录的另一大优势在于，公司可以强制执行合规性，确保员工仅使用已获授权的服务提供商。在我们近期发布的《SSL发展态势》报告中，超过60%的大型企业使用超过三家的提供商，其中一企业甚至使用了13家提供商。报告还指出，欺诈网站最常使用的提供商往往也是被企业使用频率最高的提供商。随着AI堆栈的自动化程度不断提升，对SSL管理的审查力度亟需加强。

DNSSEC的采用率
在六年间增长了三倍，
但全球2000强企业中，
仅有11% 将其整合到
最关键的域名中。

域名安全措施

按地区

2024年至2025年间，亚太地区的域名安全措施采用率增幅最大，但整体采用率仍落后于欧洲、中东和非洲地区以及美洲。



相较于上一年的增幅/减幅百分比

图5：按地区划分的域名安全措施采用率

按行业

2025年，IT软件与服务仍是表现最佳的行业。

行业划分	2025年排名	2024年排名
半导体	6	11
银行	11	16
科技硬件与设备	13	5
航空航天与国防	16	8

表现最佳的行业依然是那些高度依赖互联网开展业务的领域，例如IT软件与服务，以及媒体行业。过去一年，银行业和半导体行业的排名也进一步上升。得益于AI与金融科技的蓬勃发展，这两大行业快速增长，加之网络安全要求日益严格，这或能解释其安全态势的改善。表现最差的行业仍为建筑、采矿及公用事业等领域。值得注意的是，许多低表现行业也被列为关键行业，尤其在NIS2指令中。这或意味着，未来一年这些行业会更加重视域名安全，尤其是在针对此类行业的攻击日益增多的背景下。

↑ 表现最佳的行业

- IT软件与服务
- 媒体
- 零售
- 商业服务与用品
- 电信服务

↓ 表现最差的行业

- 建筑
- 材料
- 食品市场
- 公共事业服务
- 食品、饮料和烟草

按注册商类型划分的域名安全措施

在本报告中，我们根据全球企业2000强使用的域名注册商类型，对域名安全措施的采用趋势进行了分析。

很多公司都存在一个误区，认为所有注册商都别无二致，然而，消费级注册商的首先考虑的可能并不是域名安全，甚至不提供域名安全措施，一旦误选了消费级注册商，企业的整体安全状况可能会受到不利影响。这一点在采用注册局锁方面尤为明显，因为大多数消费级注册商都不支持注册局锁。

企业级注册商

企业级注册商专门与各个企业和品牌所有人合作，满足他们对于高级业务实践、功能、专业知识的需求，以及对于域名管理、DNS管理、安全性、品牌保护、欺诈防护、数据治理和网络安全方面的支持团队的需求。如需了解更多关于使用企业级注册商如何帮助防范域名劫持、悬空DNS和域名冒充的详情，请下载我们的“域名安全检查清单”。

消费级注册商

消费级注册商面向个人、创业者和刚刚起步的小公司提供域名服务、网站和电子邮件。许多消费级注册商不提供域名安全服务，这也导致域名安全措施的采用率降低。

依赖企业级功能的企业采用域名安全措施的比例更高

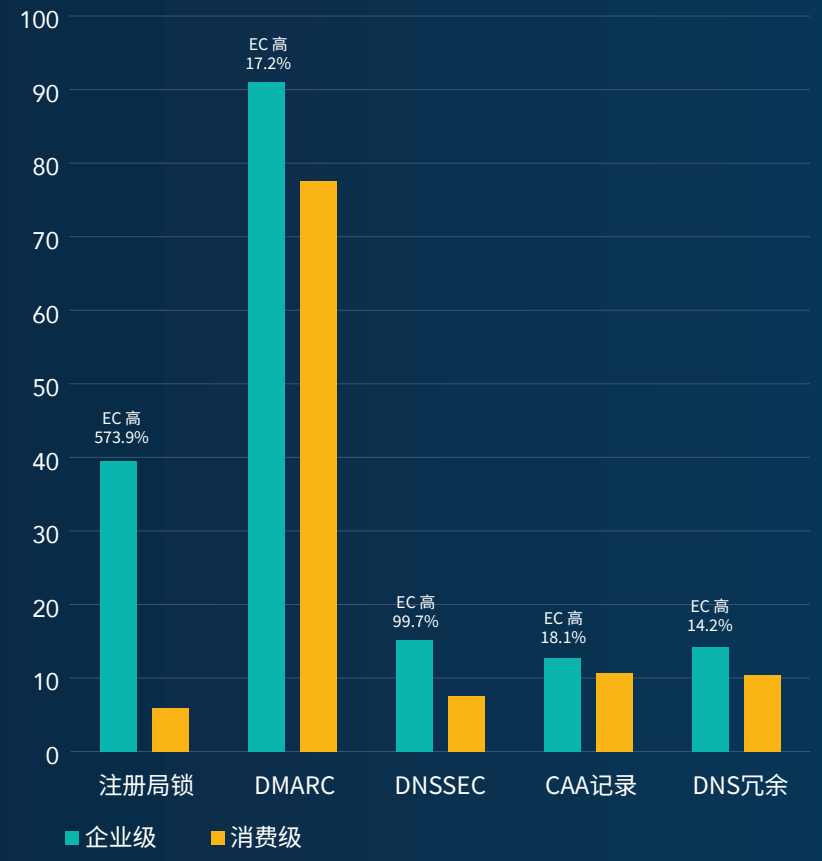


图6：安全措施的成熟度水平——企业级（EC）与消费级（CG）注册商的对比

域名安全状况

CSC根据企业域名安全风险等级，对扩展的八项主要安全措施的重要性进行分组，并为每家企业计算出一个平均分。该平均分构成了企业的安全分数，分数越高，表明企业的安全状况越稳固——这也意味着企业遭受域名安全威胁的风险越低。

主要域名安全措施：

- 企业级域名注册商
- 注册局锁（多重锁定）
- CAA记录
- DNS冗余
- DNSSEC
- 发件人策略框架（SPF）
- 域名密钥识别邮件（DKIM）
- DMARC

域名安全风险等级

公司数量

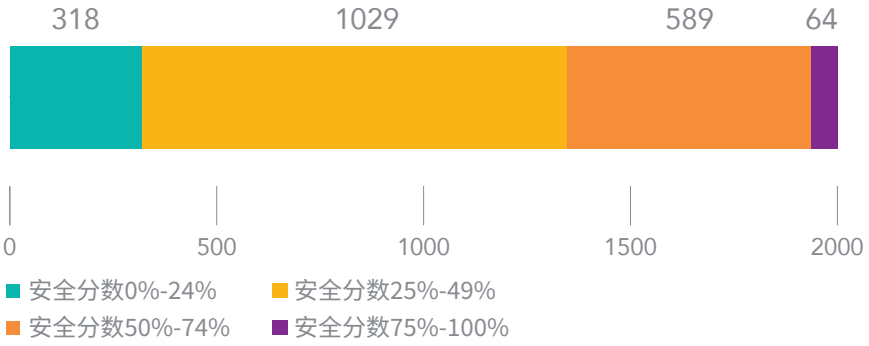


图7：全球2000强企业的域名安全分数和相关域名安全风险等级

67%的全球2000强企业实施的安全措施不到推荐措施的一半。

↑ 表现最佳的公司

与去年的报告类似，只有一家公司的得分是100%。
只有八家公司的得分为7分（满分8 分），较去年减少三分之一。

↓ 表现最差的公司

87家公司的域名安全得分为0，较去年的107家有所改善。这些公司主要位于亚太地区，该地区的公司占0分公司的87% 。

针对全球2000强企业的可疑或恶意域名活动

我们确定并分析了不是由全球2000强企业持有但包含这些企业品牌名称中超过6个字符的域名。这些第三方域名注册的目的是利用人们对目标品牌的信任，发动网络钓鱼攻击、其他形式的数字品牌滥用或知识产权侵权。这些都会给受影响的品牌带来收入损失、流量分流及品牌声誉的下降。网络钓鱼者和恶意第三方可以使用不计其数的域名诈骗战术和组合方法。

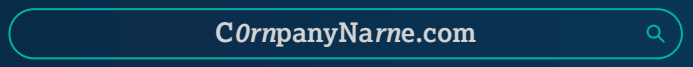
我们特意关注了常见的同形文字，因为它们是威胁发起者使用的最恶劣攻击方法之一

域诈骗伎俩

图8：域名诈骗常见伎俩

.COM域名中常见的同形文字（模糊匹配）

根据对网络钓鱼域名使用情况的密切观察，我们的分析包含了常见的拉丁字符替代字符，例如，使用C0rnpanyNarne.com来仿冒CompanyName.com。



最常见的替代字符

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

图9：.COM域名中常见的同形文字（模糊匹配）

88%的同形文字域名由第三方所有

在第三方所有的域名中：

40% 在2025年有MX记录，而2024年这一比例为42%。MX记录可用于发送网络钓鱼电子邮件或拦截电子邮件。这是DMARC记录增长的其中一个关键原因。

第三方域名会被用于何种目的?

40% 指向广告、按点击付费的广告或用于域名停放。

39% 指向不活跃的网站。

32% 在所有非活跃域名中，32%配置了有效的邮件交换记录，这意味着即使无法解析到有效内容，它们仍可用于电子邮件活动。

2% 指向可能损害品牌声誉和客户信心的恶意内容。

19% 解析到与品牌持有人无关的活跃网站。

企业需警惕的一个方面是休眠域名的使用，第三方批量注册后，往往将域名长期闲置。研究结果显示，32%的第三方域名虽处于非活跃状态，但仍保留MX记录，一旦需要便可轻易激活。

与第三方持有的虚假域名注册活动关联度最高的域名注册商

- GoDaddy®
- Namecheap™
- Network Solutions

可疑和恶意域名：目标是谁?

行业	虚假域名威胁占总数的百分比
银行	16.3%
IT软件与服务	6.6%
多元化金融	5.8%
公共事业服务	5.4%
保险	5.4%
建筑	5.2%
石油和天然气业务	5.1%
商业服务与用品	4.3%
资本货物	4.3%
交通运输	4.3%
耐用消费品	4.0%
零售	3.6%
科技硬件与设备	3.6%
材料	3.5%
食品、饮料和烟草	2.8%
电信服务	2.7%
药物和生物技术	2.4%
医疗设备与服务	2.4%
半导体	2.3%
航空航天与国防	1.9%
贸易公司	1.7%
化学品	1.7%
食品市场	1.5%
酒店、餐厅与休闲	1.3%
家庭与个人用品	1.0%
媒体	0.9%

域名安全洞察：独角兽企业是理想的域名安全倡导者吗？

今年，CSC决定将全球2000强企业（其中多数来自传统行业）与百强独角兽企业进行对比分析。这100家独角兽企业中，绝大多数为IT公司，其中很多来自AI行业。为简化分析，我们使用与全球2000强企业相同的域名安全指标来考察独角兽企业。本分析的主要目标在于确定：相比大型成熟企业，规模较小的初创公司是否对域名安全风险更为敏锐，并具备更强的防护实施能力？许多AI领域的独角兽企业充分认识到围绕关键基础设施（域名和DNS）的安全协议的必要性，在部分领域的采用率较高，但在其他方面仍存在不足。此外，这些企业正在构建的AI堆栈，也可能增加使用这些技术的企业供应链的整体风险。

什么是独角兽企业？

独角兽企业是指估值超过10亿美元的私营企业。它们通常为初创或相对年轻的公司，并往往在所属行业中具有创新性。

要点

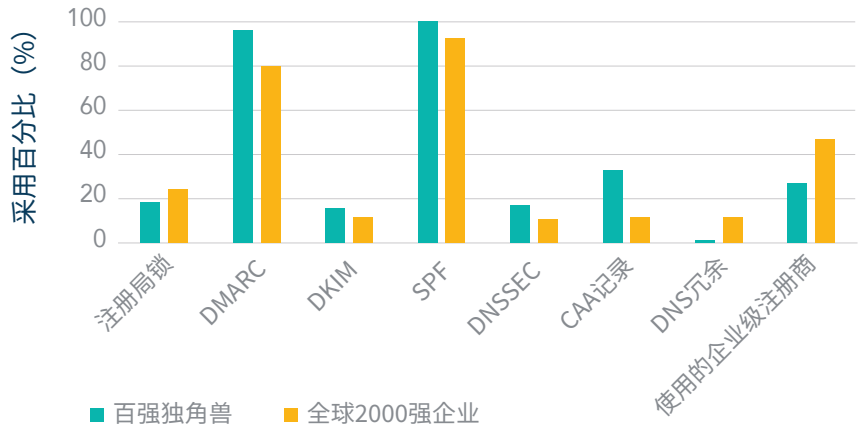


图10：域名安全措施采用情况——百强独角兽与全球2000强企业的对比

在八项域名安全指标的对比中，独角兽企业在五项指标上得分高于全球2000强企业。其主要优势体现在电子邮件安全方面，SPF、DKIM、DMARC，以及DNSSEC和CAA记录的采用率更高。这些措施的共同特点是均通过DNS记录进行管理。这表明，为独角兽企业管理域名的团队，很可能由精通DNS安全协议的IT专业人士组成，而这些措施几乎不会给企业带来高昂成本。

全球2000强企业在安全排名上更高的差异，首先体现在使用企业级注册商的比例更高。这点为何重要？企业级注册商能够实施强有力的安全措施，例如为员工提供防范社交工程攻击的培训以及双因素身份验证。而使用消费级注册商的企业，则常发生“域名仿冒”事件，即黑客入侵账户后，在合法域名下创建子域名。

另一个差异在于注册局锁采用率偏低，这主要因为许多消费级注册商并不提供此项服务。全球2000强企业使用企业级注册商，因此在采用注册局锁方面具备更多机会。

独角兽企业仍处于以市场增长为核心的早期阶段，注册商的选择可能在其业务优先级中排名靠后，或对注册商的差异及其对安全态势的影响缺乏了解。注册商类型对注册局锁的采用率与安全性具有直接响。消费级注册商不支持此类锁定功能，因此独角兽企业在注册商缺乏额外防御措施时，更容易遭受DNS劫持、域名劫持、电子邮件欺骗等攻击。即便独角兽企业拥有精通DNS基础的强大的IT团队，随着运营规模扩大、域名组合日益庞大复杂，若将域名安全托付给第三方注册商而监管不力，也可能带来重大风险——任何事故或停机都将直接影响这些依赖线上运营的企业。

AI和技术占主导

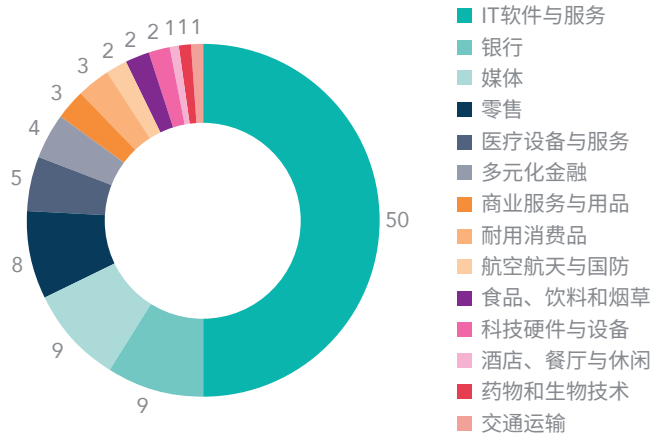


图11：百强独角兽的行业分布

百强独角兽企业中，半数来自IT服务行业，其次是银行业，占比居第二。其中，许多IT服务企业是纯AI公司，大多数银行业企业则为金融科技初创公司，这两类企业均高度依赖互联网来推动业务发展。

谁更安全?

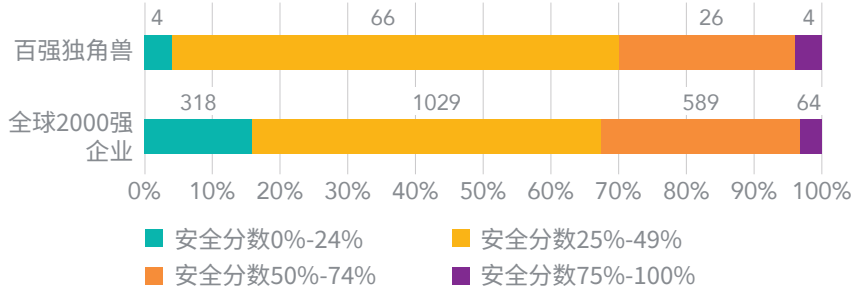


图12：域名安全等级——百强独角兽与全球2000强企业对比

对比全球2000强企业与百强独角兽的域名风险评分，并未发现显著差异。显而易见，低分区的独角兽占比仅为4%，远低于全球2000强企业的15%。但处于中分区的独角兽占比明显更高，这表明它们在某些安全要素（例如邮件安全）上已投入重视，但在更高级的安全协议（如注册局锁和DNS冗余）方面仍存在不足。

结论

全球企业仍在缓慢提升域名安全水平，而大型企业仍有改进空间，需要付出更多努力。我们认为，政府通过NIS2等立法干预，将进一步促使企业加快改进步伐，尤其是在针对跨国企业的网络攻击持续增长的情况下。

独角兽企业已迅速采用围绕DNS安全的域名安全协议，其背后的驱动因素通常是，其IT部门规模较小且更为敏捷，能够迅速做出决策，而无需应对业务遍布全球的企业所面临的复杂情况。不过，它们在DNS冗余、注册局锁和企业级注册商等方面仍存在短板，但随着企业发展成熟以及所使用供应商服务的升级，这种情况可能会改善。未来，独角兽企业需要确保自身域名安全、供应链域名安全以及其所参与的整个供应链体系的安全都得到强化。尽管许多独角兽企业所在的AI行业影响力日益提升，但或许唯有经历重大安全事件或政府干预，才能真正激发紧迫感——也正因此，安全对于推动企业业务发展至关重要。

如果公司不解决域名安全问题，将可能造成灾难性的风险。未受保护的域名会对公司的网络安全状况、数据保护、消费者安全、知识产权、供应链 、收入和声誉构成重大威胁。

企业若不重视域名安全，极易遭受第三方的恶意利用。在瞬息万变的地缘政治环境、日益狡猾的犯罪手法以及AI在恶意网络攻击中的应用下，我们必须共同努力，确保自身成为难以攻破的目标。

查看CSC的主动性和防御性安全措施清单，使用多层次、深度防御的域名安全方法，保护您的域名和品牌。

下载我们的“域名安全检查单”

CSC是值得信赖的优选安全和威胁防范提供商，深受福布斯全球企业2000强和全球最佳品牌100强(Interbrand®)企业的青睐，专注于域名安全和管理以及数字品牌和欺诈防护业务。随着全球越来越多的公司加大投资力度完善安全状况，我们的DomainSec℠平台可以一展身手，帮助这些公司了解他们存在的网络安全漏洞并且保护其在线数字资产和品牌。企业可以凭借CSC的专有技术来增强自身的安全状况，防范针对其在线资产和品牌声誉的网络威胁，从而避免遭受严重的收入损失。CSC还提供在线品牌保护（将在线品牌监控和维权活动相结合），多维度审视防火墙外针对特定域名的各类网络威胁。欺诈防护服务可在攻击的早期阶段打击网络钓鱼，使我们的解决方案更加完善。CSC成立于1899年，总部位于美国特拉华州威尔明顿市，在美国、加拿大、欧洲和亚太地区设有办事处。CSC是一家全球性公司，我们通过聘用所服务行业的业内专家，可为世界各地的客户提供服务。

联系我们

cscdbs.com/cn

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