# DNS投资回报率：
# 降低风险与明智投资指南

# DNS安全商业论证：成本、风险缓释与投资回报率

对于大型企业而言，保障域名系统 (DNS) 基础设施的安全是业务刚需。DNS故障可能会导致严重的宕机、法律责任风险以及声誉损害。尽管如此，在更广泛的网络安全战略中，域名安全却经常被忽视。

本洞见白皮书通过阐明故障成本，并提供如何有效阐明风险与投资回报率 (ROI) 的实用方法，帮助决策者构建更具说服力的DNS安全商业论证。

## 忽视DNS安全的真实代价

DNS安全故障可能引发一系列连锁反应，其影响范围远远超出初始宕机带来的损失。虽然宕机期间的收入损失往往是最直观的成本，但合规风险、法律支出以及声誉损害等间接影响更难以量化，并且长期来看，其代价往往更为高昂。

网络安全领域的负责人日益将基于域名的威胁视为实质性的业务风险，而非孤立的技术问题。在《首席信息安全官（CISO）2025年展望》中，70%的受访者预计安全威胁将持续上升，不仅如此，98% 的受访者预测未来三年内威胁将进一步增加。[1]随着威胁形势不断加剧，企业需优先部署能够保障系统可用性、客户信任及业务连续性的基础性安全控制措施。

> *我曾见过团队为恢复DNS中断而通宵达旦，事后却被追问为何企业未能提前部署更强有力的防护机制。因此，DNS安全应被视为一项前瞻性、可规划的投资，而非事后补救措施。*
>
> **Mark Flegg**
> *CSC 安全产品和服务高级总监*

# 直接成本与间接成本：日益扩大的连锁反应

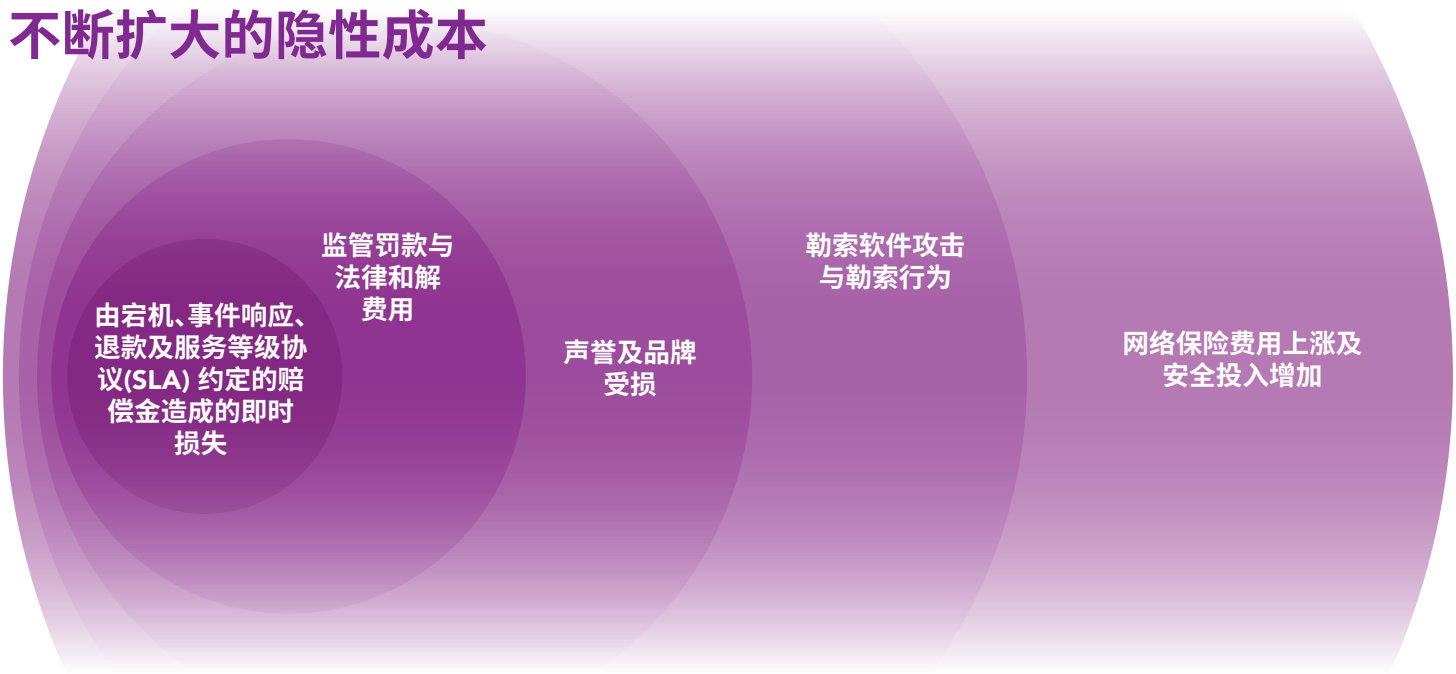
直接成本是指关键服务中断时即时发生且可量化的支出，例如：

**宕机损失**——包括运营中断、交易失败以及客户流失

**紧急IT支持与事件响应**——由内部 IT 团队或外部专家开展故障诊断与服务恢复工作

**退款与服务等级协议（SLA）违约金**——因违反 SLA 而需向客户或合作伙伴支付的赔偿

## 不断扩大的隐性成本




然而，正如Splunk的一份报告所揭示，直接成本仅是这场财务冲击的第一波影响。[2]随着连锁效应向外扩散，隐藏在表面之下的间接成本开始不断累积，其规模甚至可能超过最初的直接支出。

**监管罚款与法律和解费用**——在受监管行业中运营的企业，可能因服务中断或数据泄露而面临合规违规与法律诉讼。

**声誉及品牌受损**——客户信任的流失可能对市场地位、客户留存及收入增长产生长期影响。此外，企业可能还需要安抚利益相关方、回应投资者关切，并对事件响应工作保持透明度。

**勒索软件或勒索要求**——如果攻击者篡改 DNS 设置以重定向流量或阻断访问，企业可能遭遇财务勒索企图。

**网络保险费用上涨及安全投入增加**——DNS 故障（尤其是涉及安全漏洞时）会导致保险公司评估出更高的风险敞口，从而推高保险费用。

# 追求“五个九”的系统可用性，并提出更具战略性的问题

对于企业而言，对系统可用性要求极高。“五个九”原则（即99.999% 的系统可用性），意味着每年的停机时间不超过 5 分钟。许多企业将其作为可靠性基准，但不同服务提供商及服务等级的 DNS 服务承诺存在差异。在实践中，服务提供商的真实运行表现，尤其是在高负载或遭受攻击情况下的表现，往往比理论的系统可用性目标更具参考价值。

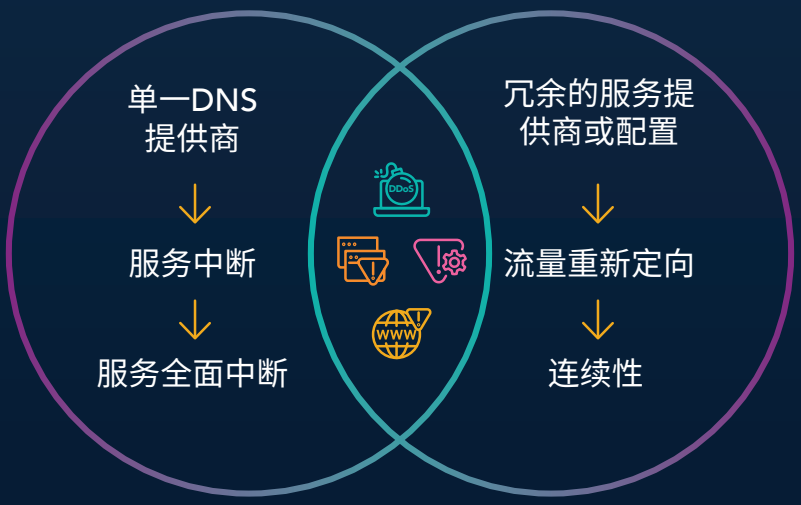
如今，许多企业依赖云端基础设施及第三方平台来支撑面向客户的服务、内部应用程序以及业务关键型工作流。尽管这些服务提供商能够提升系统的可扩展性与性能，但也可能引入运营风险，尤其是在可用性依赖单一提供商、单一区域或单一配置的情况下。DNS韧性规划应纳入冗余策略，以确保在服务中断、配置错误或上游服务降级等情况下仍能维持可用性。

*“企业在其他领域均会为故障做充分预案，例如多区域部署、数据备份以及故障切换系统。但在DNS领域，这一原则却常常被忽视，仍被视为“够用即可”，依赖单一提供商或单一配置。而对于所有数字服务均依赖的基础能力而言，这种假设本身具有高度风险。*

**Mark Flegg**
*CSC安全产品和服务高级总监*

# 单点DNS风险与弹性 DNS 架构对比

综合来看，这些风险进一步说明，DNS安全应被视为企业风险降低策略的核心组成部分，而非次要的 IT 事项。此外，《首席信息安全官（CISO）2025年展望》报告显示，首席信息安全官已将域名与 DNS劫持列为未来三年最主要的潜在威胁之一。[3]




DNS在保障网站、电子邮件及内部应用程序可用性方面发挥着基础性作用，但其防护往往仍显不足。相关风险不容忽视，主要包括：

**分布式拒绝服务（DDoS）攻击：**恶意攻击者通过高流量攻击瞄准DNS基础设施，压垮服务器资源并引发服务中断。

**提供商服务中断：**若企业依赖单一 DNS 提供商，一旦该提供商发生宕机，将可能面临服务全部中断的风险。

**配置错误：** 简单的配置错误，例如不当的 DNS 记录修改，可能会导致整个服务中断。

**域名劫持：**在注册商层面发生未经授权的更改，可能导致流量被重定向，从而引发声誉与安全风险。

# DNS故障成本量化

对于企业希望通过评估并阐明 DNS 安全风险带来的财务影响，年度损失期望（ALE）公式提供了一种结构化的损失量化方法。该方法有助于网络安全负责人将技术风险转化为以业务为核心的财务表达，从而更有力地支持对DNS安全的前瞻性投入决策。

ALE公式的定义如下：

**SLE × ARO = ALE**

**单一损失期望（SLE）：**单次DNS故障造成的财务影响，包括直接成本以及在可能情况下的间接成本。

**年度发生率（ARO）：**此类事件在一年内预计发生的次数估算。

**年度损失期望（ALE）：**因DNS安全故障导致的预计年度财务损失。

通过基于企业风险状况计算SLE与ARO，企业可以得出ALE数值——这一指标为量化潜在财务风险提供了具体方法，并为 DNS 安全的预防性投资提供决策依据。

> *许多企业难以量化 DNS 相关威胁的成本，从而使安全投入更难获得合理的商业论证。ALE公式为财务风险提供了一种实用模型，有助于决策者理解主动式DNS安全措施对业务的实际影响。*

**Mark Eggleston**
*CSC首席信息安全官*

# 阐明 DNS 安全的商业价值

尽管对基于域名的威胁防范意识不断提升，但许多企业仍然感到准备不足。《首席信息安全官（CISO）2025 年展望》显示，仅有22%的受访者表示已部署适当工具以应对基于域名的威胁。[4] 风险与应对风险之间的这一差距，正是以ROI为导向的 DNS 安全举措最具说服力的价值所在。

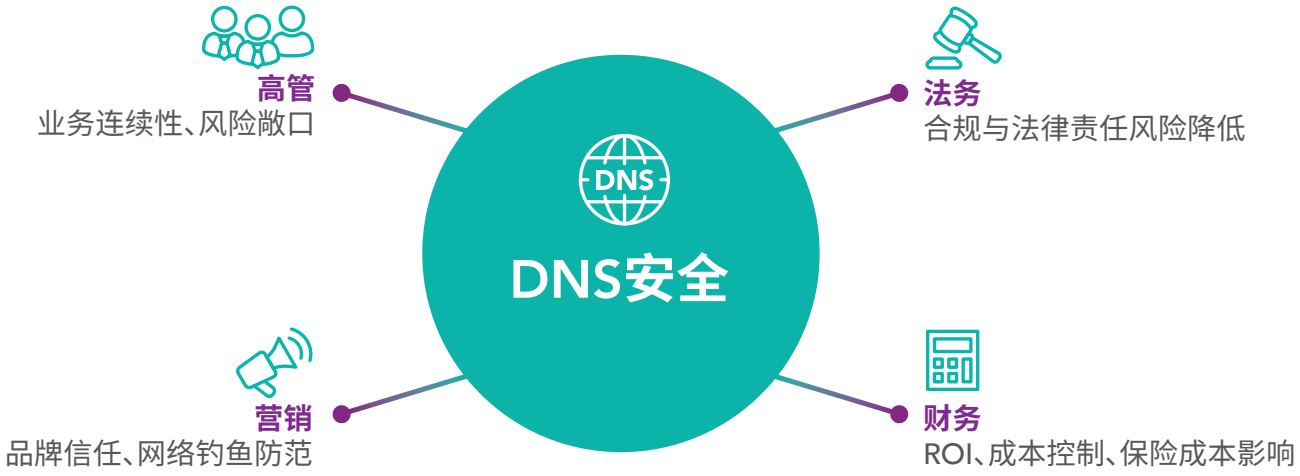
为获得资金支持，网络安全负责人必须将 DNS风险转化为业务影响，从而将域名安全与系统可用性、客户信任、合规风险以及运营韧性紧密关联。

> *DNS最初并非为应对当今的威胁环境而设计，但它仍然是我们依赖的将客户、员工及合作伙伴引导至正确目的地的关键系统。因此，DNS安全应获得与其他核心安全控制措施同等程度的重视。*

**Mark Flegg**
*CSC安全产品和服务高级总监*

## 理解受众：有的放矢的沟通策略

为了争取DNS安全投入，网络安全负责人必须确保沟通内容与不同利益相关者的优先事项保持一致。安全团队可能更关注技术风险，而其他部门则各自关注不同的业务目标、财务考量及运营挑战。将DNS安全与各团队的自身利益相结合，有助于提高获得其支持的可能性。



## 高管：DNS安全对业务影响

财务表现、风险管理和市场竞争力是高管层的核心关切。由于DNS对系统可用性至关重要，它同时也是业务连续性与灾难恢复的核心能力，而这两项正是高层领导关注的两大优先事项。将DNS定位为战略性投资，而不仅仅是 IT 支出，有助于将其与更广泛的企业韧性建设相衔接。

> *董事会成员并不关注DNS本身，而更关注品牌保护与整体网络安全风险。沟通时应避免过多技术细节，转而以商业价值与业务影响为核心进行表达。如需入门参考，可关注《华尔街日报》等媒体对网络安全议题的商业化解读方式。*
>
> **Mark Eggleston**
> *CSC首席信息安全官*

## 法务团队：监管合规与法律责任风险降低

企业法务团队优先关注行业监管合规性以及法律责任风险的降低。包括《通用数据保护条例（GDPR）、《加州消费者隐私法案》（CCPA）以及《网络与信息安全指令》（NIS2）在内的多项数据隐私与安全框架，均要求实施强有力的安全控制措施，以保护敏感信息安全。如果缺乏完善的DNS安全防护，企业将面临数据泄露、网络钓鱼攻击以及未经授权的域名转移风险，这些情况都可能引发法律诉讼或监管处罚。

## 营销与品牌团队：声誉保护与网络钓鱼防范

营销团队负责品牌声誉、客户信任及数字化互动，而这些均可能受到DNS相关威胁的影响。将DNS安全定位为品牌保护策略，而不仅仅是 IT 部门的事务，有助于提升其与营销团队的相关性与共鸣。

> *域名安全已超越传统网络安全范畴，其核心在于保护整个数字生态系统免受欺诈性网站的侵害。尽管首席信息安全官可能将其视为次要风险，但对营销与品牌团队而言却是首要优先事项。*
>
> **Mark Eggleston**
> *CSC首席信息安全官*

## 财务与采购：成本效益、ROI及保险益处

财务决策者与采购团队通常基于成本、效率及可量化的ROI来评估各类投资。展示域名安全风险对财务影响的一种有效方式，是引用新闻头条中的真实案例。有时，仅仅转发一个近期安全事件的链接，就足以让财务团队直观理解投入不足所带来的实际后果。完善的DNS防护还可降低业务中断发生频率，从而提升财务稳定性。

将DNS安全定位为业务赋能因素，而不仅仅是技术防护手段，有助于获得更广泛的企业支持，并确保 DNS 防护被视为战略优先事项。

# ROI论证：为主动式 DNS 安全构建商业论证

为DNS安全争取投入不仅需要强调风险，还需要展示可量化的财务与运营收益。首席信息安全官和网络安全负责人必须将安全问题转化为清晰的业务价值，说明对 DNS 安全的投入如何降低成本、优化运营流程并减少财务风险敞口。

安全预算的增长并不总是与网络风险同步。在《首席信息安全官（CISO）2025 年展望》中，仅有 7% 的受访者表示其预算在 2024 至 2025 年间显著增长，而 80% 的受访者则表示仅有适度增长。[5]

在此环境下，DNS投资需要体现可量化的风险降低效果及对运营韧性的提升价值。

## 通过风险缓释与效率提升降低成本

稳健的DNS安全态势有助于实现更广泛的网络风险降低，从而帮助企业在网络保险提供方维持良好记录，并符合广泛认可的安全框架。尽管网络安全保险保单通常不针对DNS提供专项折扣，但加强域名防护能够体现良好的网络安全治理水平，并降低整体威胁风险。

企业也在优先采用可重复、可扩展的方法，尤其是在响应速度至关重要的场景中。《首席信息安全官（CISO）2025 年展望》显示，50%的受访者已制定并定期测试事件响应计划，另有 50% 表示已采用基于AI的监控与维权解决方案。[6]DNS安全通过提升可见性、加快风险缓释速度，并在发生中断时增强业务连续性，与这一向运营成熟度演进的趋势相契合。

自动化在减轻域名安全运营的人工负担方面发挥关键作用，涵盖从DNS配置管理到新兴威胁监测以及事件响应的各个环节。这一点在数字证书管理中也日益重要：随着 CA/Browser Forum 规则在2029年前持续调整，证书生命周期将不断缩短。届时，企业可能需要更频繁地更新安全套接字层（SSL）与传输层安全（TLS）证书，未来平均每年约需完成 8 次续期。在此背景下，自动化续期工作流将成为防止证书过期与业务中断的关键保障。

## 使用财务模型量化DNS风险

高管和财务团队对数据驱动的决策反应最为积极。网络风险量化（CRQ）模型，例如年度损失期望公式或信息风险因素分析（FAIR™）框架，有助于企业评估DNS相关攻击、系统宕机或 DNS劫持事件可能造成的潜在财务损失。通过应用这些模型，网络安全负责人可以用量化数据说明：主动投入能够有效避免更为严重的财务损失。

开展基于场景的风险评估，是进一步呈现DNS 故障可能引发的业务中断与财务影响的另一种有效方式。通过构建真实攻击场景模型，企业能够直观识别DNS安全薄弱所带来的隐性成本。

## 增强威胁情报和风险优先级划分

要领先于不断演变的威胁，就需要持续了解潜在风险。企业若加入特定行业信息共享团体，如美国信息共享和分析中心国家委员会（National Council of Information Sharing and Analysis Centers），可以获得关于新兴 DNS 相关攻击的预警和洞见。

此外，实施持续威胁暴露管理可帮助安全团队优先处理最紧迫的DNS漏洞，确保资源得到高效分配，在高风险情境升级前完成风险缓释。

## 使用我们的DNS成本计算器衡量成本节约效果

理解DNS安全的财务收益，需要清晰的成本模型。以下DNS内部成本计算器提供了一套计算模型，帮助企业评估DNS宕机的真实成本，涵盖交易损失、修复成本以及运营中断等关键变量。

*“评估DNS安全的价值并不一定需要复杂的模型。一旦将DNS宕机映射为真实的业务影响——包括生产力损失、交易损失以及恢复时间成本，这就使ROI 就变得不言自明了。*

**Mark Flegg**
*CSC安全产品和服务高级总监*

| DNS成本节约计算器 | 指标 |
|---|---|
| 管理DNS的员工人数 | 2 |
| 每位工作人员的年薪 | 75,000美元 |
| 福利成本（按员工成本的 30% 左右计算） | 45,000美元 |
| 硬件、软件及网络带宽的年度费用 | 40,000美元 |
| **运行内部DNS的总成本** | **160,000美元** |
| 外部DNS服务的拟定成本 | 50,000美元 |
| **使用外部DNS服务所节省的总成本** | **110,000美元** |

*注意：实际数值仅为示例。*

通过展示可量化的成本节约、运营效率提升以及财务风险敞口的降低，网络安全负责人可以为DNS安全投入构建极具说服力的商业论证，精准契合高管、财务团队以及风险管理人员的优先关注事项。

# 将DNS安全列为业务优先事项

DNS安全是企业网络安全战略中至关重要但常被忽视的组成部分。正如本报告所示，DNS安全故障所带来的影响远不止系统宕机，还包括财务损失、监管处罚以及声誉损害。

除部署技术控制措施外，首席信息安全官及安全负责人还需以商业语言阐述DNS安全价值。通过将沟通重点与高层优先事项保持一致、量化风险并证明ROI，企业能够获得保护其数字资产所需的必要投入。

现在采取主动措施强化DNS安全，有助于预防未来发生代价高昂的安全事件。**立即咨询CSC，获取为贵司保驾护航的定制化解决方案。**

**cscdbs.com**

**以下是赢得高管层对网络安全支持的三个步骤：**

1. 建立关系——理解高管的核心优先事项，采取稳健且具有战略性的沟通方式。
2. 同频沟通——将网络安全界定为治理问题。参考美国公司董事协会（NACD）等机构的指南。
3. 展示进展——通过仪表板或其他清晰的可视化工具，呈现安全投入所带来的实际成效。

**Mark Eggleston**
*CSC首席信息安全官*

## 沟通交流

1 800 927 9800 | cscdbs.com

## CSC 简介

CSC是值得信赖的优选安全和威胁情报提供商，深受福布斯全球 2000 强企业和百大全球最佳品牌（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载体，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。欢迎访问 cscdbs.com。

*[1]CSC，首席信息安全官 (CISO) 2025 年展望，2025 年，https://www.cscdbs.com/en/resources/2025-ciso-cybersecurity-outlook-report/。*

*[2]Splunk，停机的隐性成本，2024 年，https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html。*

*[3]CSC，首席信息安全官（CISO）2025年展望。*

*[4]CSC，首席信息安全官 (CISO) 2025 年展望。*

*[5]CSC，首席信息安全官（CISO）2025年展望。*

*[6]CSC，首席信息安全官（CISO）2025年展望。*



DBS03112026