SOPHOS
Cybersecurity delivered.

2022 医疗勒索软件现状

31 个国家中型企业 5,600 名 IT 专业人员的独立（不知道供应商情况下）调查结果，包括 381 名来自医疗行业的受访者。

介绍

Sophos 对前线工作的医疗行业 IT 专业人员的现实勒索软件体验，揭示更加具有挑战性的攻击环境。加上勒索软件给受害者带来的财务和运营负担不断增加，报告还透露勒索软件与网络保险之间关系的新见解，包括保险在推动网络防御变革中扮演的角色。

关于调研

Sophos 委托研究机构 Vanson Bourne 对 31 个国家的中型企业（100-5,000 名员工）的 5600 名 IT 专业人员开展独立（不了解供应商的）调查，其中包括 381 名来自医疗行业的受访者。调查在 2022 年 1 月到 2 月之间进行，受访者根据去年的经历进行回答。

攻击加剧，复杂性和影响增加

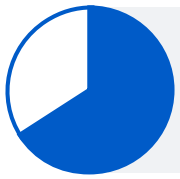
66% 的医疗企业在去年受到勒索软件攻击，2020 年为 34%。一年内增长了 94%，说明对手明显更加擅长大规模开展最有效的攻击。这很可能也体现了勒索软件即服务模式正在不断取得成功，通过降低建立和部署攻击需要的技能水平，大幅扩大勒索软件可达到的范围。[注：勒索软件攻击定义为一个或多个设备受到攻击影响，但不一定加密。]

如果比较所有调查行业的勒索软件攻击盛行程度，医疗行业的攻击频率达到全球平均 66%。

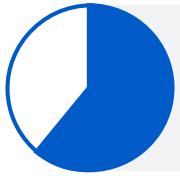
在数据加密率方面，达到 61% 加密率，优于全球平均值 65%，说明医疗更善于在勒索软件攻击中阻止数据加密。医疗行业的加密率也相比去年（2020 年为 65%）下降。

遇到纯勒索攻击的受害者百分比，即数据未加密，但企业受泄露数据威胁而被勒索赎金，从 2020 年的 7% 降低至 2021 年的 4%。这个好迹象的一个原因可能是更多医疗企业现在选择网络保险，这需要更高网络安全防御增强。我们将在本报告稍后部分探讨这一趋势。

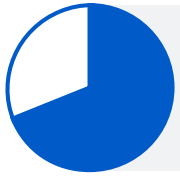
成功勒索软件攻击的增加是越来越广泛威胁环境的一部分，对医疗行业的影响超过任何其他行业。医疗行业的网络攻击数量增加最多 (69%)，网络攻击复杂性增加最多 (67%)，而各行业平均值分别为 57% 和 59%。在此类网络攻击影响方面，医疗是受影响第二大的行业 (59%)。全球平均值为 53%。



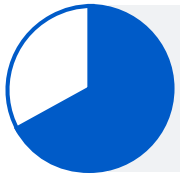
66%
去年受到勒索软件攻击



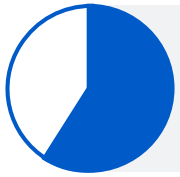
61%
攻击导致数据被加密



69%
网络攻击数量增加，所有行业中最高



67%
网络攻击复杂性增加，所有行业中最高



59%
网络攻击影响增加，所有行业中第二高

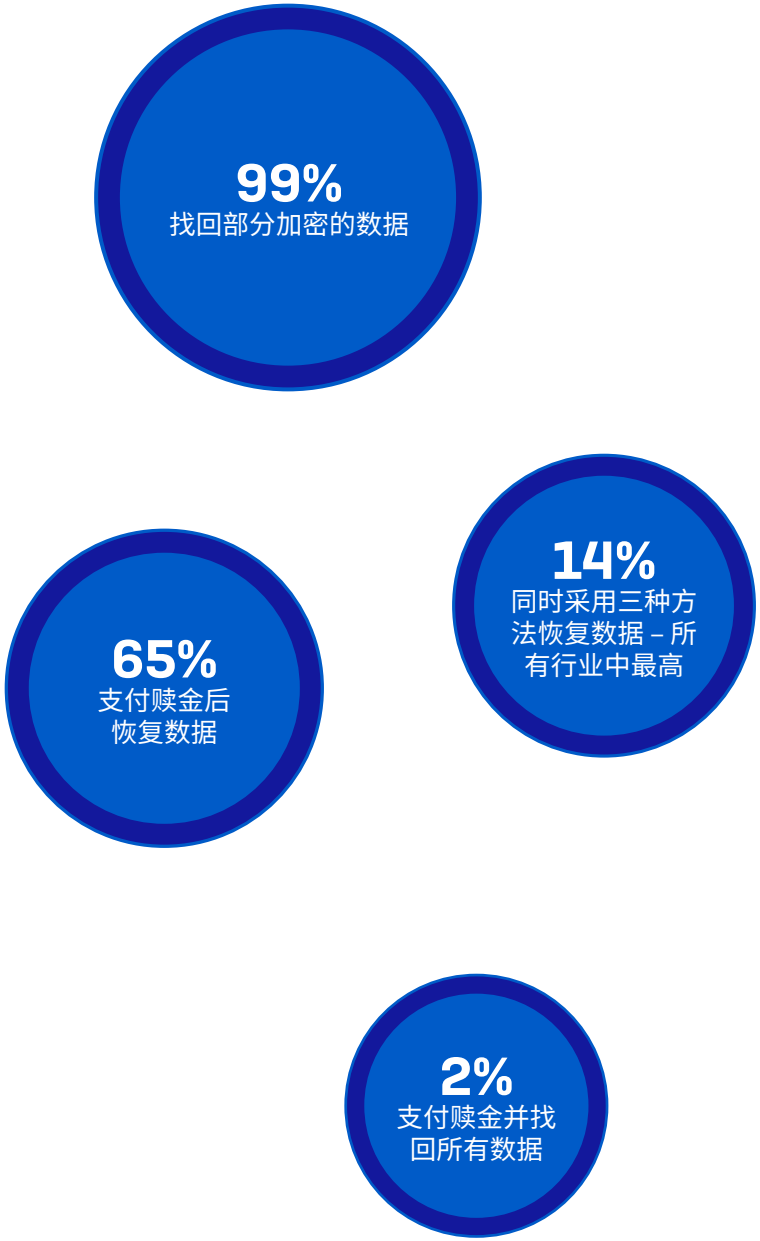
医疗行业在攻击后恢复数据的能力提高

随着勒索软件更加流行，企业应对攻击后果的能力提高。去年 99% 受勒索软件攻击的医疗企业现在都找回了一些加密数据，比去年的 93% 显著增加。

备份是用于恢复数据的头号方法，72% 的数据被加密的医疗企业采用。同时，61% 称支付数据以恢复数据，33% 称利用其他方式恢复数据。这些数字反映了一个事实，许多医疗企业采用多种恢复方法，提高恢复并运行的速度与效率。事实上，整体来说，约一半 (52%) 企业数据被加密的受访者采用多种方法恢复数据。

医疗排名第一 (14%)，同时使用所有三种方法恢复加密的数据：备份、赎金支付和其他方式，全球平均值为 7%。医疗非常依赖数据可用性以实现业务运营的连续性。缺少即时数据可拖延患者治疗，造成灾难性后果。医疗行业尝试利用所有可用方法恢复数据的举动可以理解。

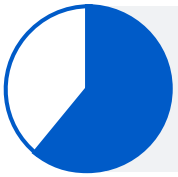
支付赎金几乎总是能找回部分数据，但支付后恢复数据的百分比下降。2021 年支付赎金的医疗企业平均仅找回 65% 的数据，比 2020 年的 69% 降低。同样，2021 年只有 2% 支付赎金的企业找回全部数据，比 2020 年的 8% 下降。



医疗行业最有可能支付赎金

医疗行业最有可能支付赎金，61% 的数据被加密的受访者承认支付赎金，而各行业平均值为 46%。该数字相比 2020 年 34% 支付赎金几乎增加一倍。相比所有其他行业，医疗行业攻击的数量和复杂性增加最高，背后的一个可能原因是支付并克服其在应对此类攻击中的准备不足的倾向性高。

我们将在本报告后面了解的其他原因，包括勒索软件不仅影响加密数据库和设备，而且影响医疗企业的运营和业务收入，使其忙于追求正常。最后，我们在本报告将看到的，医疗行业的高攻击补救成本（第二高的行业，185 万美元），可能迫使医疗机构支付赎金而不是用于补救成本。



61%
医疗行业赎金支付率

医疗支付的赎金最少

医疗行业的支付量虽然位于前列，但实际支付金额排在末尾。整体来说，医疗在所有提到的行业中，平均赎金支付最低（约 19.7 万美元）。因此，虽然医疗企业支付赎金的次数多，但赎金金额相对小。这些低赎金金额可能由众多医疗企业的财务有限推动，尤其是公共医疗。他们没有更多的钱供攻击者榨取。

值得注意的是，虽然医疗是支付赎金最低的行业，但 2021 年医疗行业支付的整体赎金金额相比 2020 年增长 33%。

更详细了解医疗赎金支付，60% 的赎金金额小于 5 万美元。仅 3 名受访者表示其企业支付 100 万美元或更多。这与其他受访企业的趋势相反，去年支付 100 万美元或更多赎金的受害者比例增加近两倍，从 2020 年的 4% 增加至 2021 年的 11%。同时，支付不到 10000 美元的百分比从 2020 年的三分之一 (34%) 降低至 2021 年的五分之一 (21%)。

19.7 万美元

医疗行业平均赎金支付，各行业最低

33%

医疗行业赎金支付相比去年增加

60%

医疗行业赎金金额低于 5 万美元

勒索软件对医疗行业具有巨大的商业和运营影响

赎金总额只是一部分，勒索软件造成的影响远远不只加密数据库和设备。去年 94% 受勒索软件攻击的医疗企业表示，最大的攻击影响其运营能力。此外，在私营医疗企业中，90% 表示导致其丧失业务或收入。

在所有行业中，2021 年企业纠正最近勒索软件攻击影响的平均成本为 140 万美元，比 2020 年的 185 万美元有所下降。这可能体现了网络保险的盛行和影响，保险公司能够更好地通过事件响应流程快速有效引导受害者，降低补救成本。

但是，在医疗行业中，平均补救成本从 2020 年的 127 万美元增长至 2021 年的 185 万美元。实际上，医疗行业与各行业平均值相比，在纠正勒索软件攻击平均成本方面排名第二（185 万美元与 140 万美元）。本报告前面已经介绍，勒索软件对医疗企业的攻击在去年几乎翻倍（2021 年 66%，2020 年 34%）。这可能是医疗企业保障网络保险方面远远落后其他行业的原因之一，我们在本报告后面将更加详细介绍。缺乏网络安全专业知识，医疗物联网设备的大量使用，存在漏洞的传统系统，以及 24/7 全天候运营的性质（导致无法快速补救漏洞系统）继续影响医疗行业，推高整体补救成本。

去年 44% 受到攻击的医疗企业用一周时间从最重大的攻击中恢复，25% 用时一个月，这个时间对于大多数企业来说都很长。高等教育和中央/联邦政府的恢复最慢，约五分之二需要一个月以上来恢复。

此外，一些企业继续信任无效的防御。去年未受到勒索软件攻击，并且预计未来不会受到攻击的医疗企业受访者中，77% 依赖的方法无法阻止企业受到攻击：50% 提到备份，43% 提到网络保险作为预计不会受到攻击的理由，还有一部分同时选择二者。虽然这些有助于从攻击恢复，但无法在第一时间阻止。

94%
勒索软件攻击影响其运营能力

90%
勒索软件攻击导致失去业务/收入

185 万美元
医疗行业补救攻击的平均成本，各行业中第二高

一周
从攻击恢复的平均时间

77%
相信不阻止攻击的方法

医疗企业更加难以获得网络保险

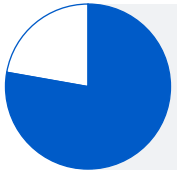
在所有行业中，83% 的企业取得针对勒索软件的网络保险。相比之下，仅 78% 的医疗企业承保，46% 表示保单中有豁免或例外项。考虑到医疗行业勒索软件事件发生率高，此承保不足将导致许多企业承担攻击的全部成本。

能源、石油/天然气和公用设施很可能投保最多 (89%)，之后是非常接近的零售业 (88%)。生产制造排名最后，仅 75% 投保。

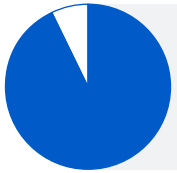
93% 有网络保险的医疗企业表示，去年投保过程发生改变，更加难以获得网络保险。51% 称需要达到的网络安全水平现在更高，45% 表示保单更加复杂，48% 表示提供网络保险的公司减少，46% 表示过程用时更长，34% 表示更昂贵。

这些变化与勒索软件紧密相关，是网络保险索赔的最大因素之一。近年来，赎金攻击增加，赎金和赔付成本激增。因此，一些保险公司离开市场，因为已无法盈利。留下来的公司努力降低风险和暴露。他们还显著提高价格。

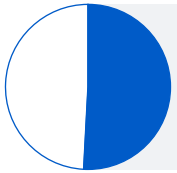
由于提供网络保险的企业减少，这是卖方市场。他们说了算，在承保客户方面精挑细选。建立可靠的网络防御将显著提高企业获得需要保险的能力。



78%
医疗行业的勒索软件网络保险



93%
去年投保过程改变

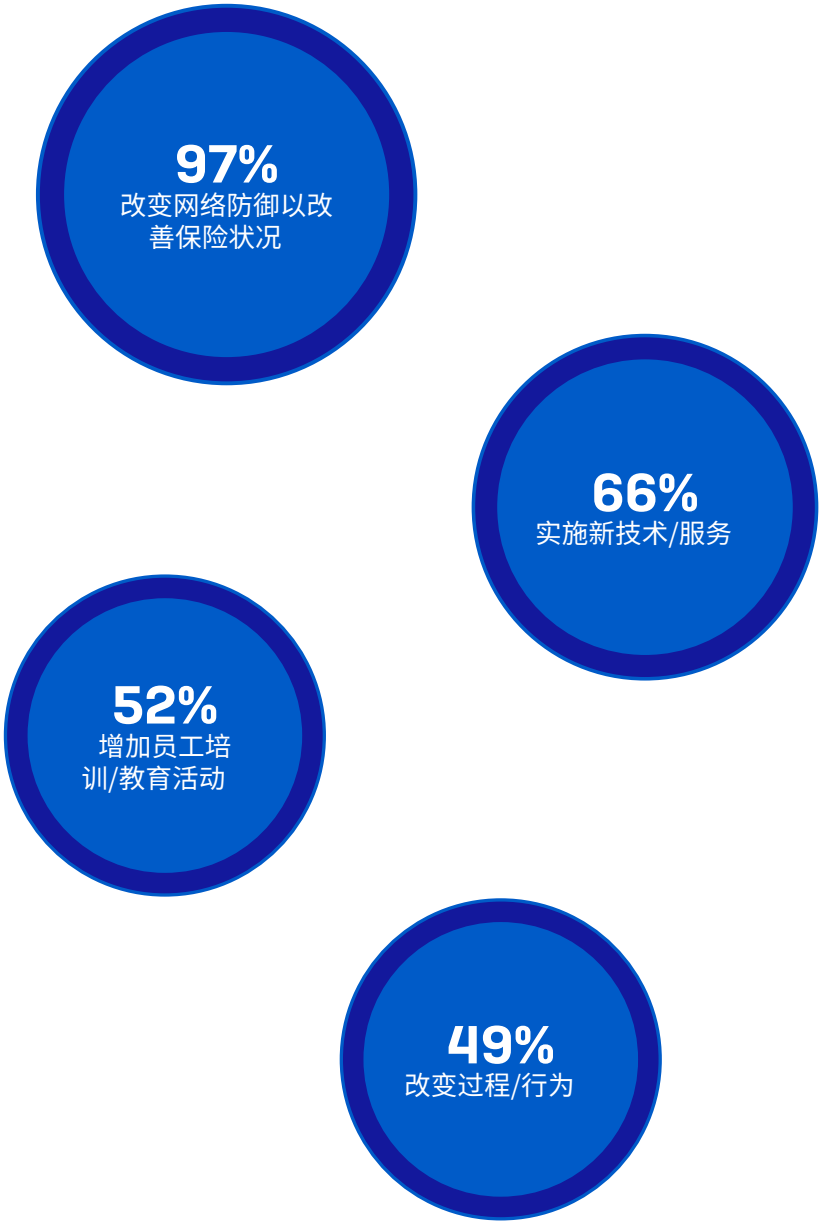


51%
获得网络保险需要的网络安全水平现在更高

网络保险推动网络防御的改进

随着网络保险市场的艰难化，投保更加困难，97% 有网络保险的医疗企业改变网络防御，提高网络保险水平。66% 实施新的技术和服务，52% 增加员工培训和教育工作，49% 改变流程和行为。

网络保险市场的艰难化很大一部分是勒索软件赔付增加的结果，正在成为网络防御增强的推动功能。

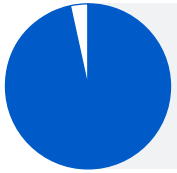


网络保险赔付几乎所有勒索软件索赔

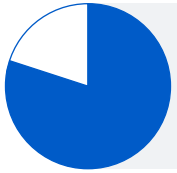
令人安慰的是，对于网络保险，97% 受勒索软件攻击并且网络保险承担勒索软件的医疗企业表示，保单支付了最重大的攻击。81% 的受访者称，保险公司支付清理成本，即让企业再次运行产生的成本。反过来，47% 称保险公司支付赎金。在所有行业的网络保险支付内容方面，调研显示，相比 2020 年调研结果，保险公司支付的清理成本增加，赎金支付减少。

但是，不同行业的赎金赔付差异巨大。最高赔付率出现在低等教育（K-12/小学/初中）53%，州/地方政府 49%，医疗 47%。最低赔付率出现在生产制造 30% 和金融服务 32%。值得注意的是，赎金支付率最低的行业同时也是从事件恢复速度最快的企业，突出了灾难恢复准备工作的重要性。

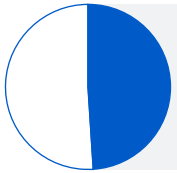
值得记住的是，虽然网络保险将帮助企业恢复以前的状态，但并不能做到“更好”，即，投入更好的技术和服务以解决导致攻击的缺陷。



97%
医疗行业的网络保险赔付率



81%
保险公司在医疗行业支付清洁成本



47%
保险公司支付赎金

结束语

企业面临的勒索软件挑战继续增长。直接受勒索软件影响的医疗企业比例在去年几乎增加一倍：从 2020 年的三分之一以上增加到 2021 年的三分之二。

面对这一近标准化，医疗企业在面对攻击后果方面做的更好：几乎所有企业都找回一些加密数据，近三分之二能够利用备份恢复数据。

同时，支付赎金后恢复的加密医疗数据比例平均下降至 65%。

医疗的平均赎金支付最少（19.7 万美元）。

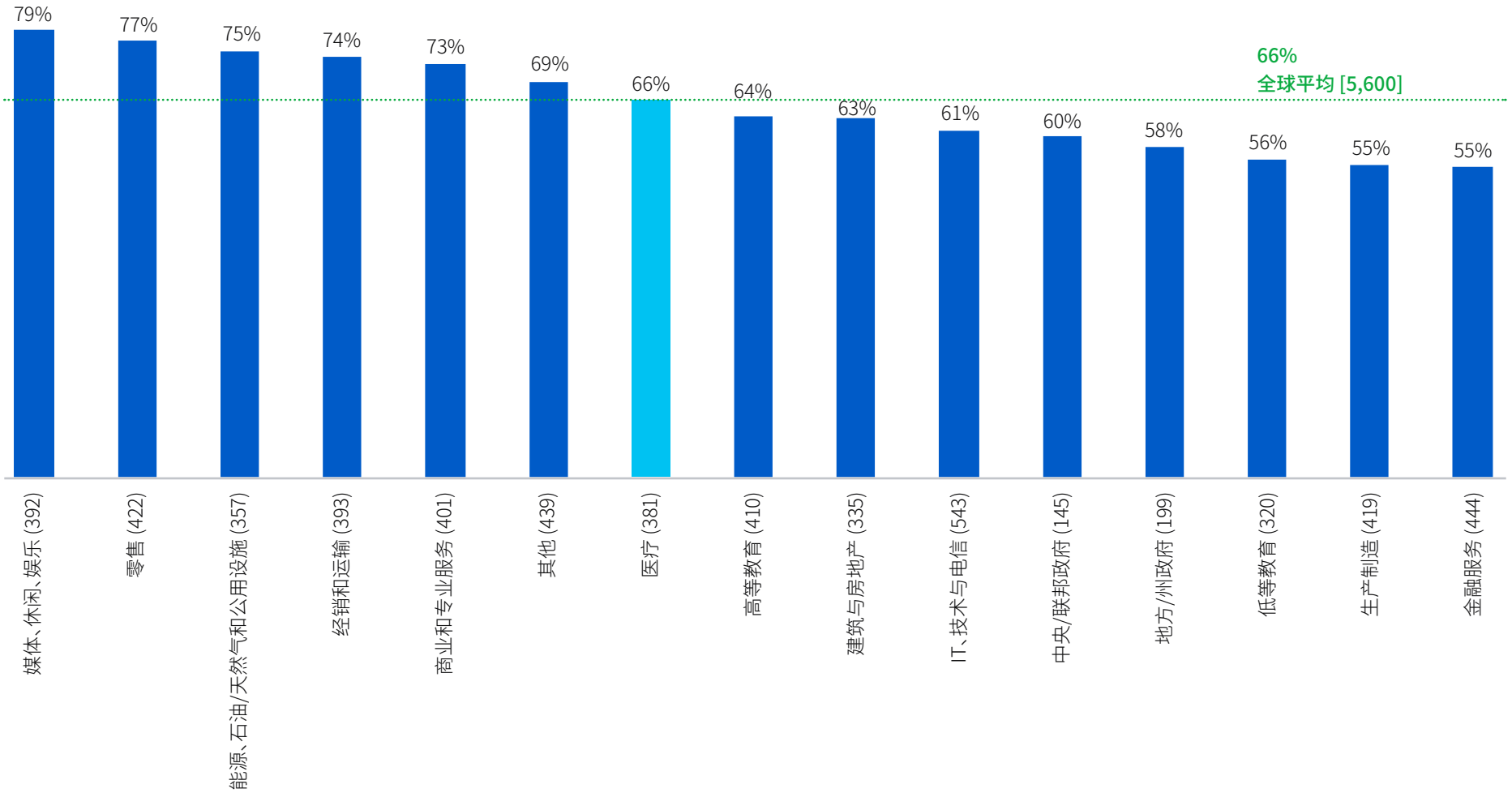
勒索软件影响医疗运营、业务和收入。大多数医疗企业选择投保网络保险，降低与此类攻击相关的财务风险。对于他们来说，保险公司在几乎所有索赔中支付部分费用是一个欣慰的消息。但是，企业获得保险的难度更大。这推动几乎所有医疗企业改变其网络防御，改善网络保险状况。

无论您是否寻找投保，优化网络安全都是所有企业必须做的工作。我们的五个重要提示：

- 在环境中的所有点确保高质量防御。检查安全控制，确保仍能满足您的需求。
- 主动追踪威胁，这样可以在对手发起攻击前进行阻止 – 如果您没有时间或内部技能，请联系专家 MDR 网络安全服务。
- 寻找并弥补安全漏洞，加固您的环境：没有打补丁的设备，不受保护的计算机，开放的 RDP 端口等。扩展侦测与响应 (XDR) 非常适合此用途。
- 为最坏的情况做好准备。了解如何发生网络事件应怎么办，需要联系的人。
- 制作备份，练习从备份恢复。您的目标是备份和快速运行，中断最少。

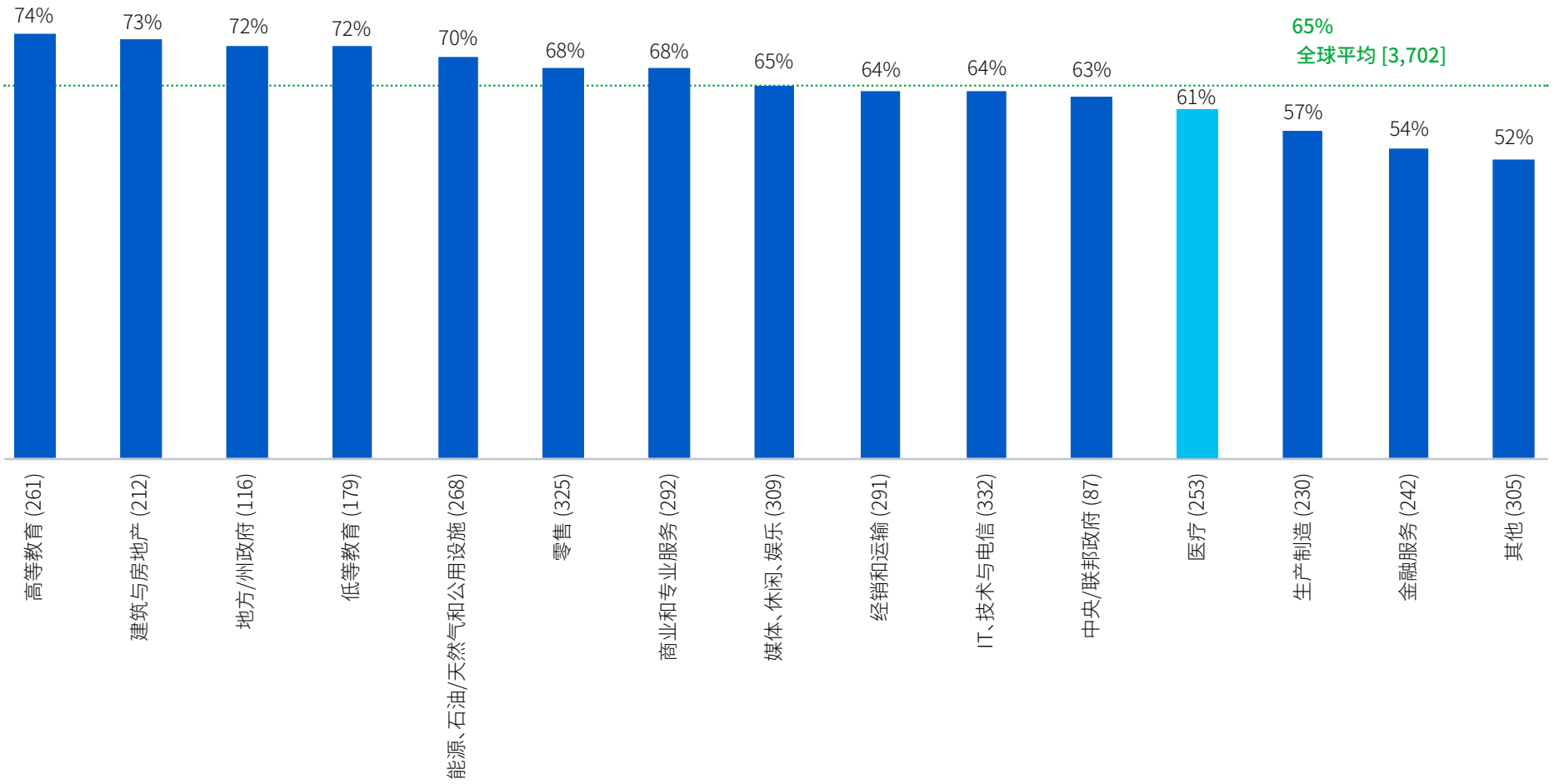
有关各个勒索软件组的详细信息，请参见 Sophos 勒索软件威胁情报中心。

医疗行业的位置：按行业划分的勒索软件攻击



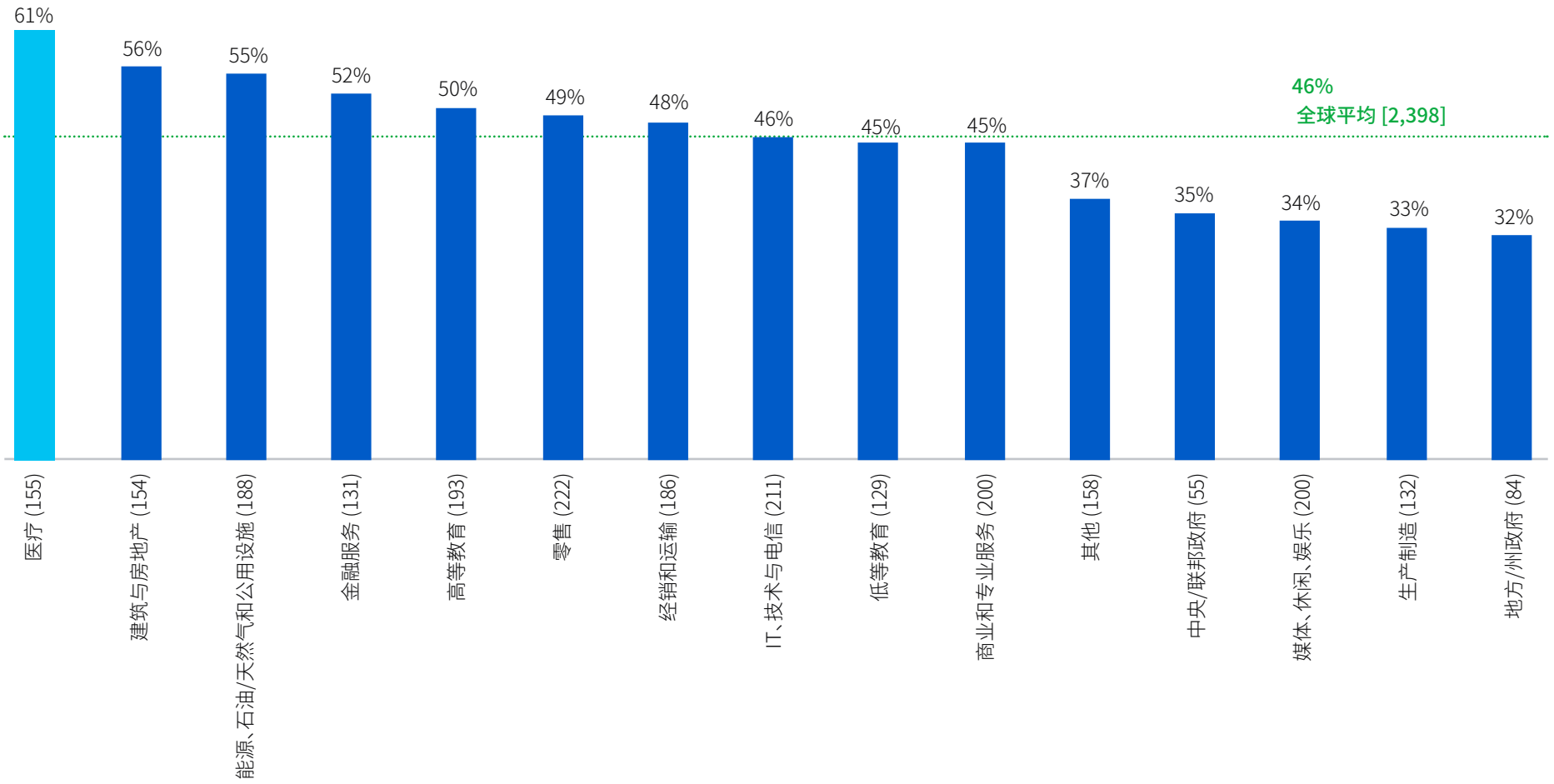
去年您的企业受到过勒索软件攻击吗？[n=5,600]

医疗行业的位置：数据加密率，按行业划分



网络罪犯是否在最重大勒索软件攻击中成功加密您企业的数据？(n=3,702 去年受勒索软件攻击的企业)：是

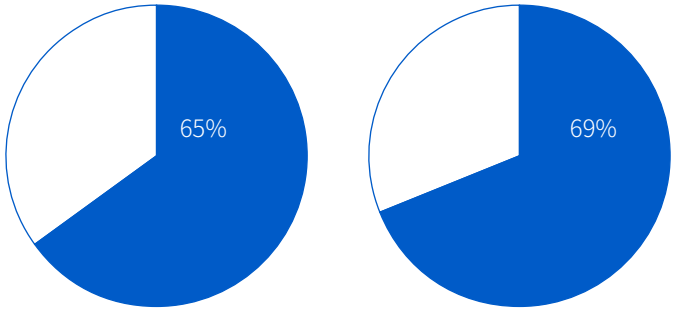
医疗行业最有可能支付赎金



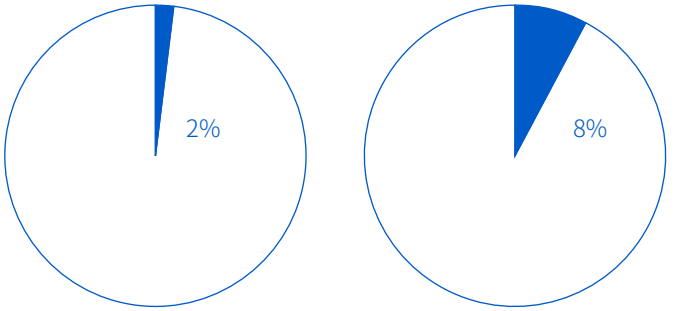
您的企业在最重大勒索软件攻击中找回了数据吗?
(n=2,398 数据被加密的企业):是,我们支付赎金并找回数据

相比去年，医疗企业支付赎金后找回的数据更少

支付赎金后恢复的数据百分比

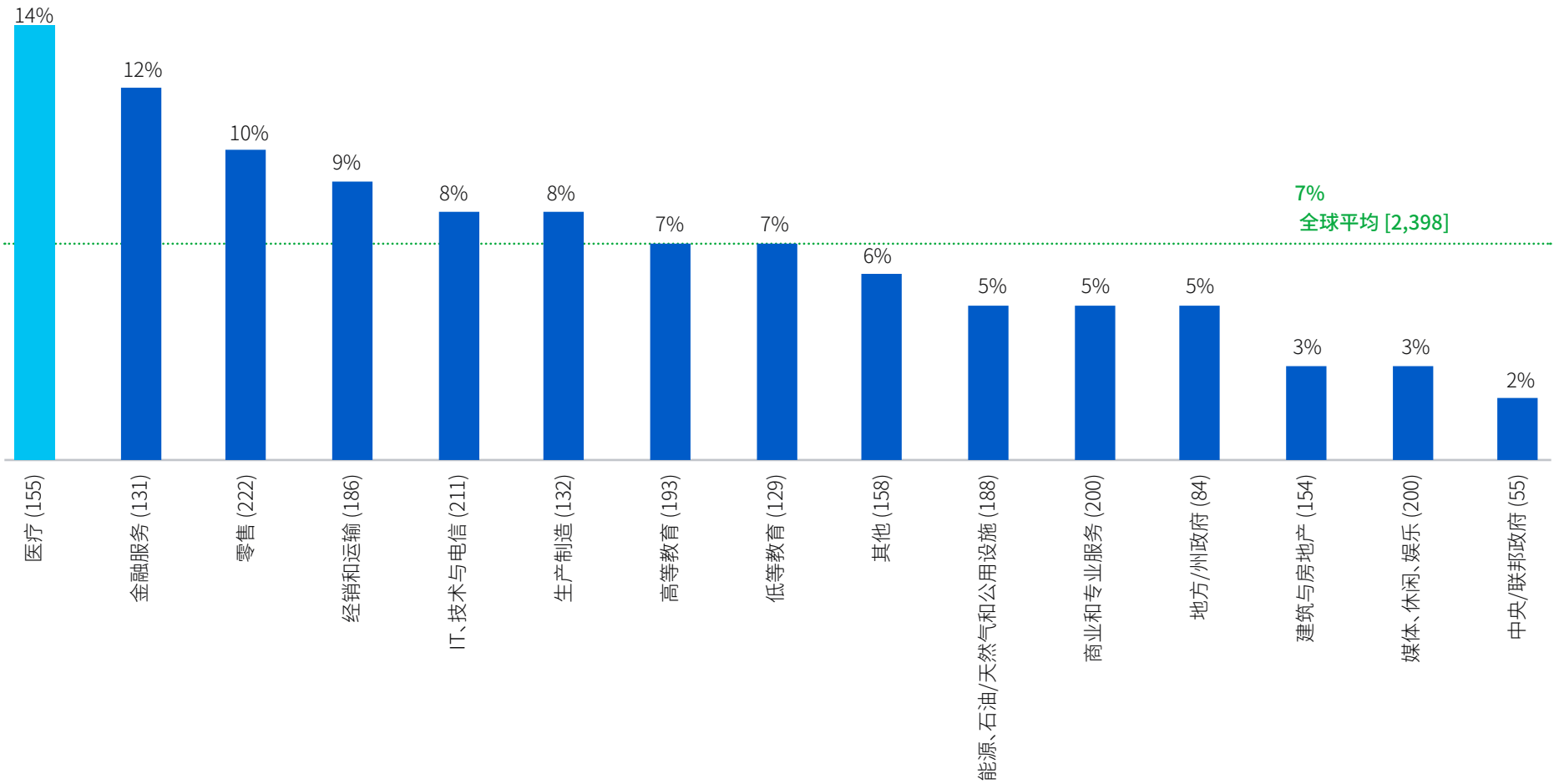


支付赎金后找回所有数据的百分比



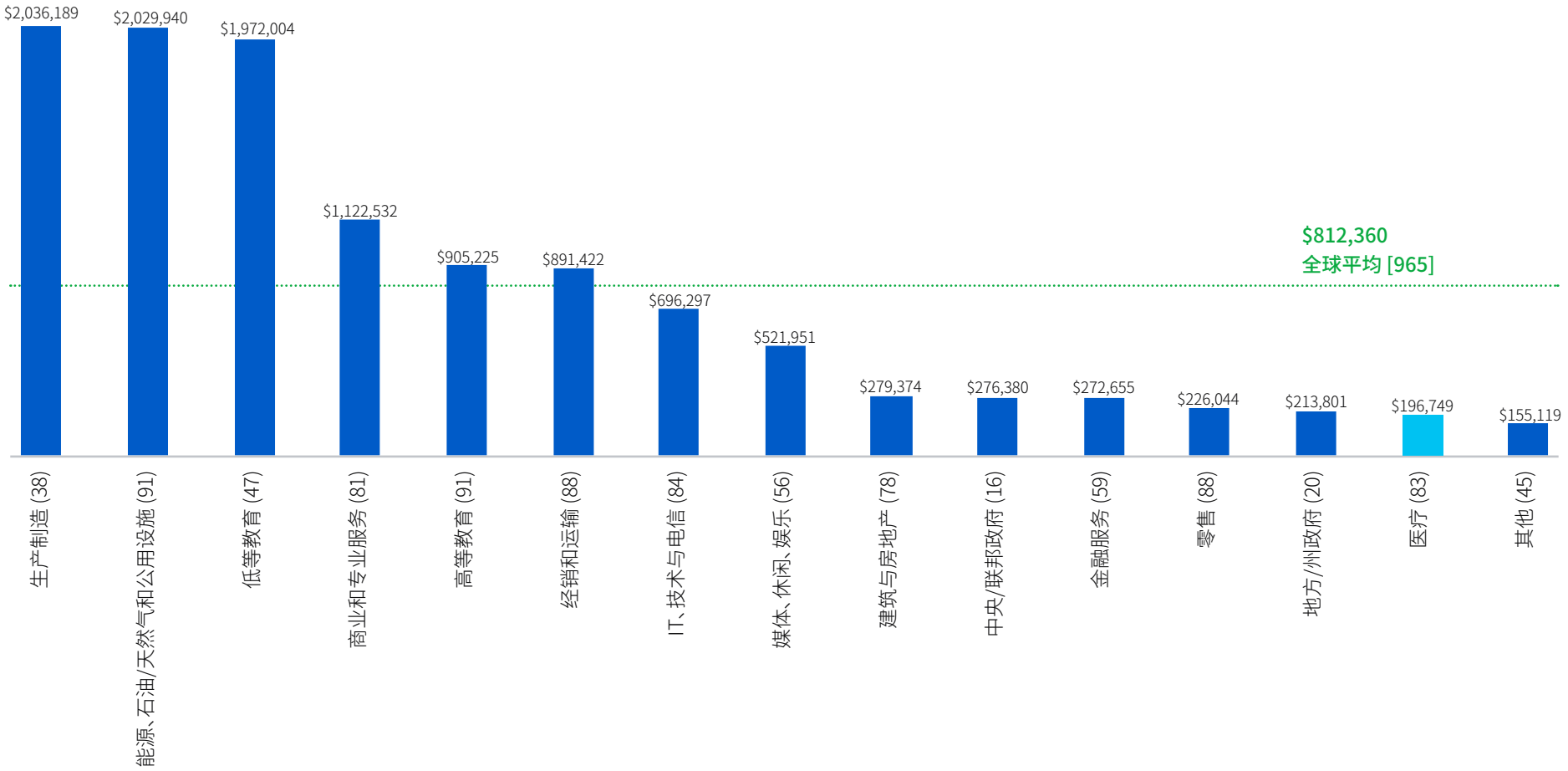
您在最大勒索软件攻击中找回了多少企业数据？
（94/25 支付赎金并找回数据的医疗企业）

医疗最有可能利用所有三种方法恢复数据



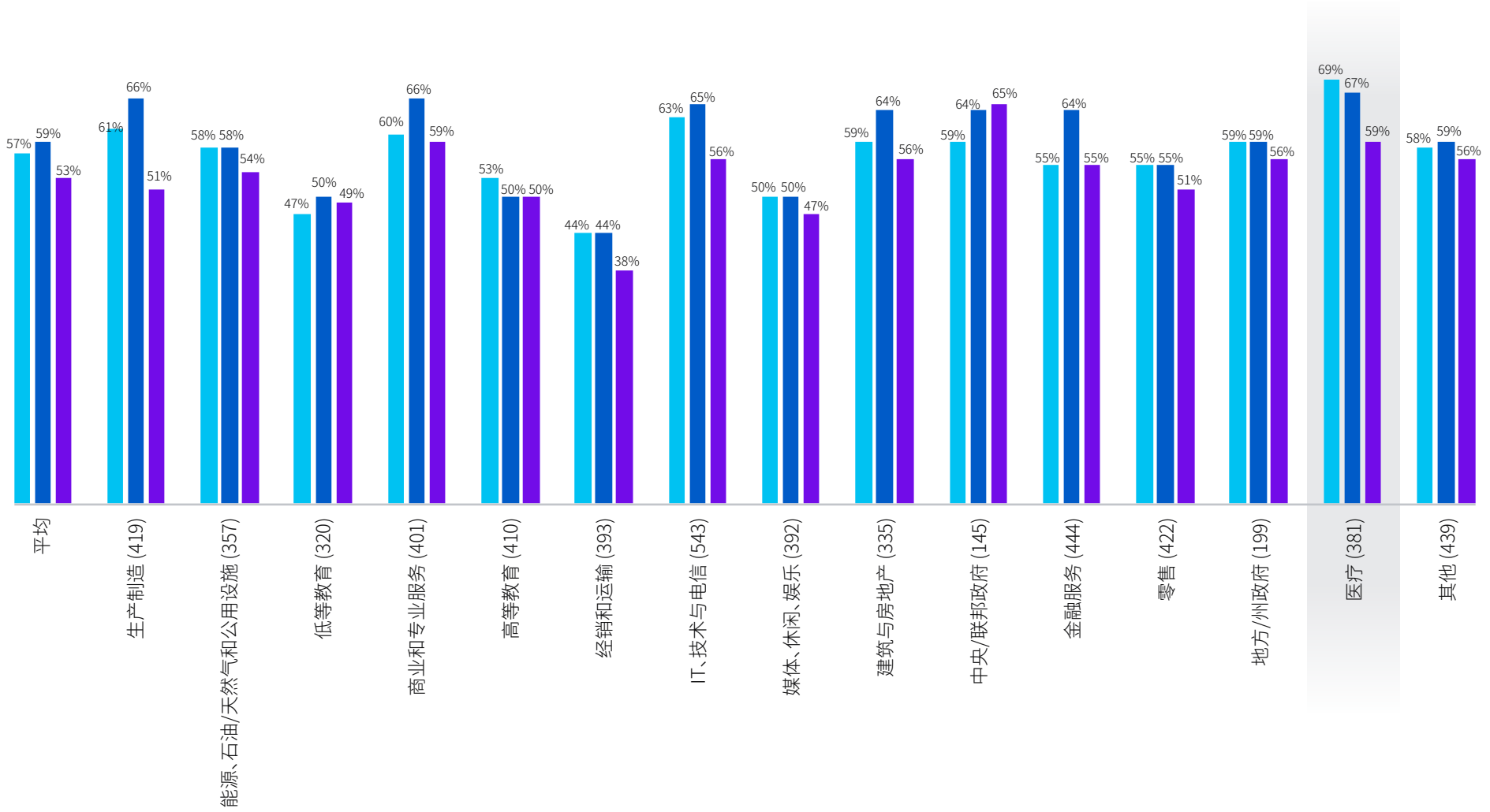
您的企业在最重大勒索软件攻击中找回了数据吗?
(2,398 数据被加密的企业):是的,我们采用所有三种方法(备份、赎金支付和其他方法)找回数据

医疗的赎金支付最少



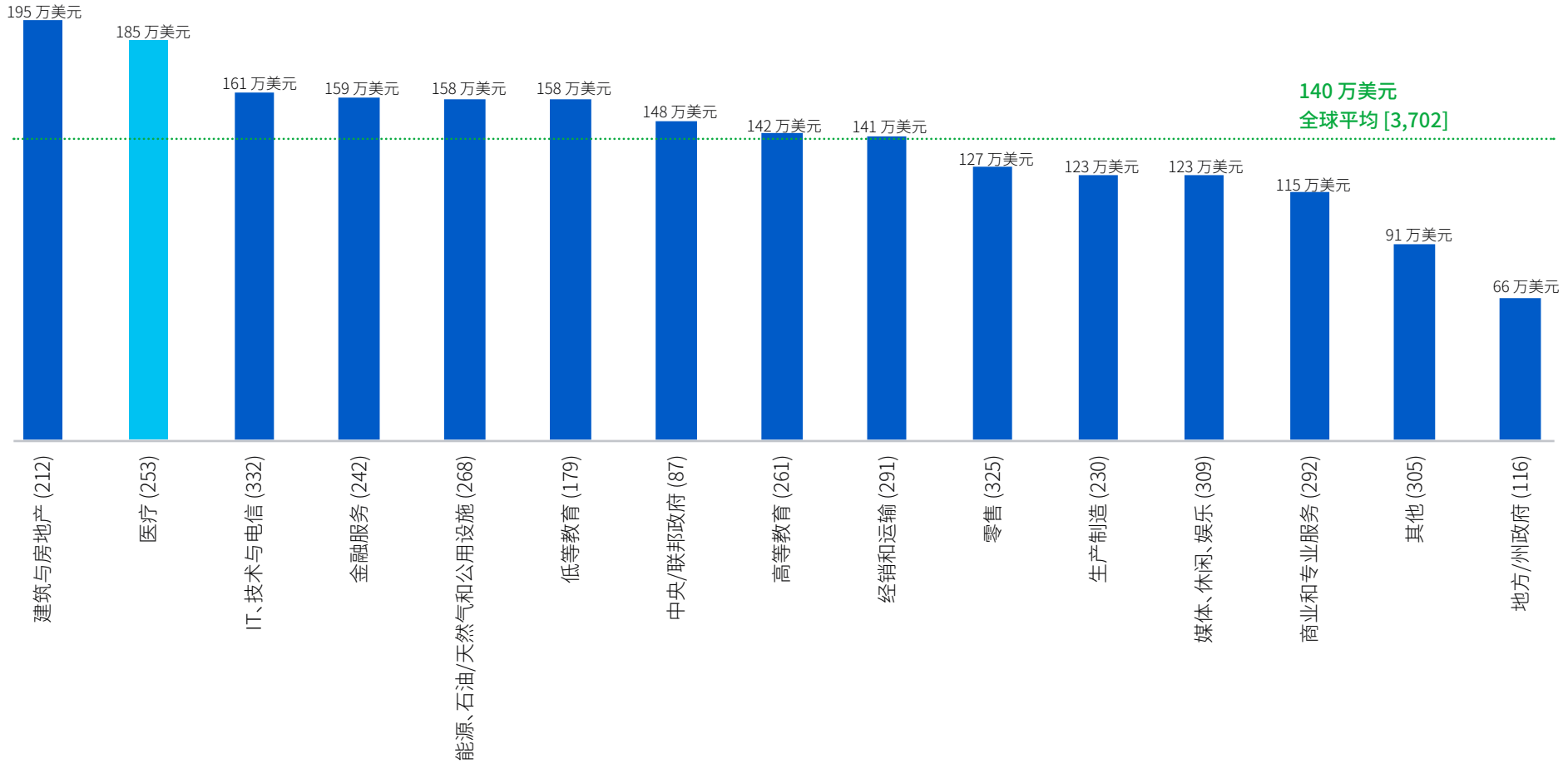
您的企业在最重大勒索软件攻击中支付了多少赎金?美元。图中的基数。不包括“不知道”的回答 注意对于低基数的行业，结果应视为具有指示性。

医疗行业的位置：去年网络攻击体验的改变



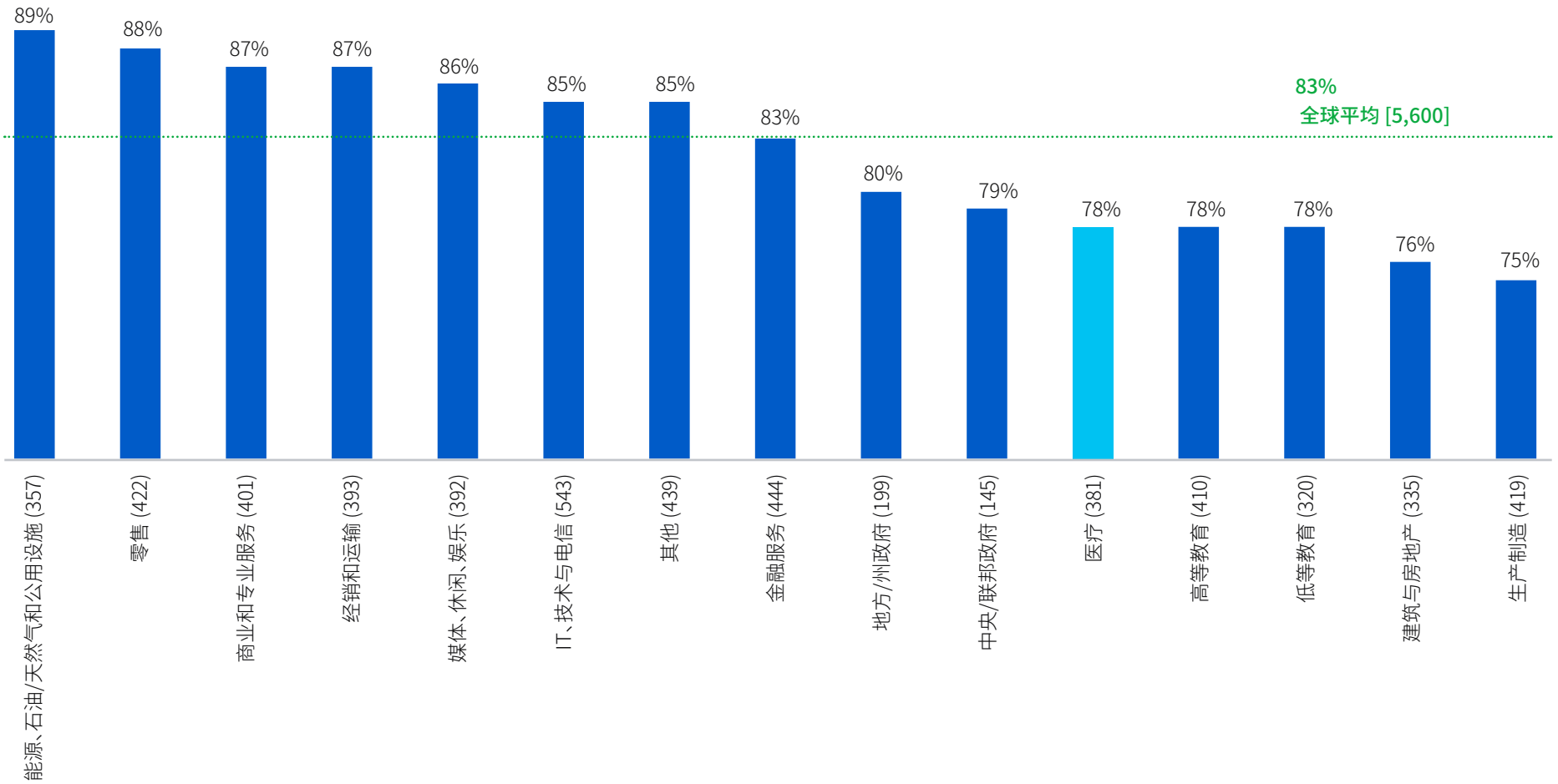
对于量、复杂性和影响，您的企业去年的网络攻击体验有什么改变？(n=5,600)：增加很多，增加了一点

医疗行业勒索软件补救成本高于全球平均值



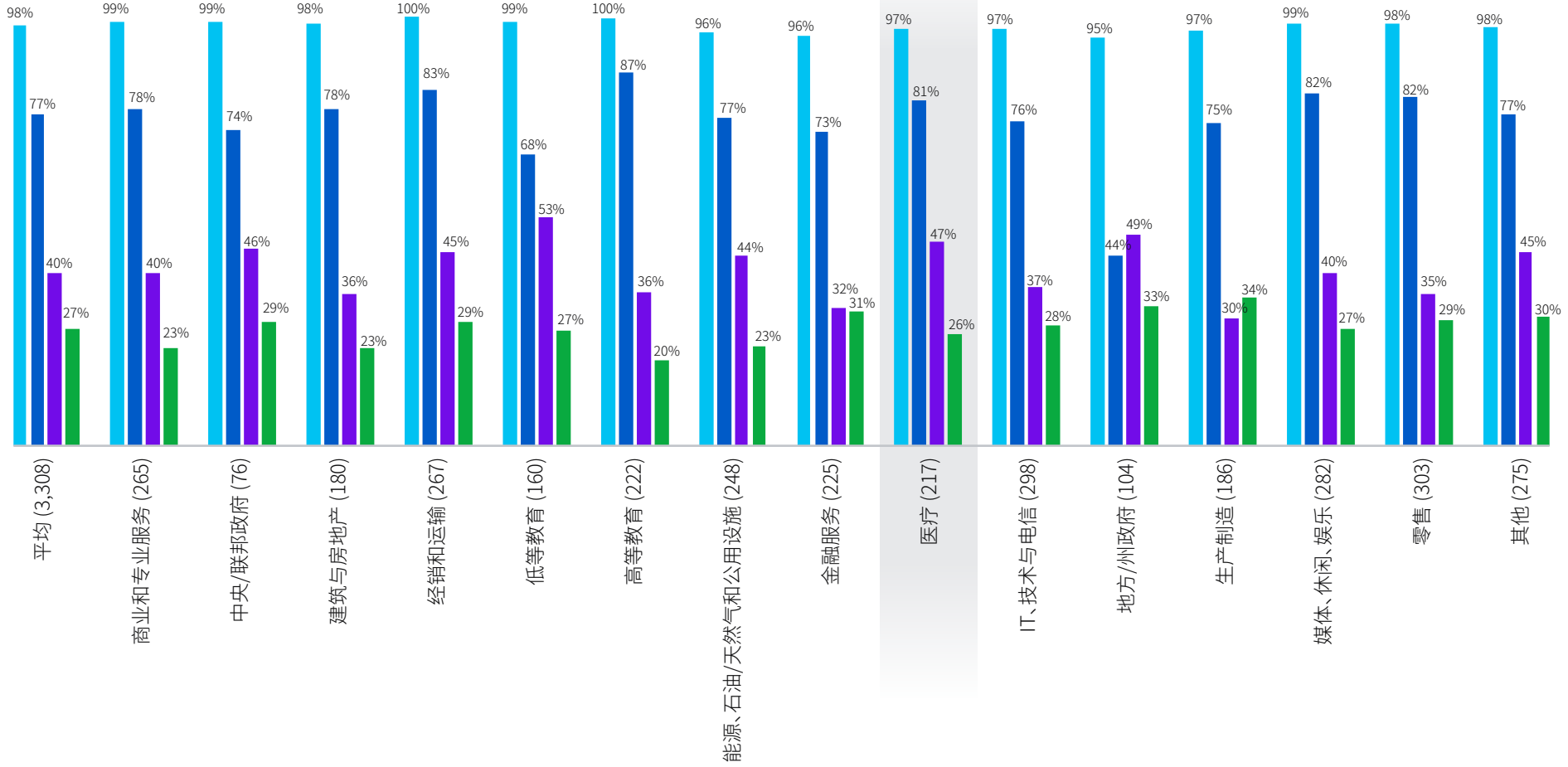
企业纠正最近勒索软件攻击造成的影响（考虑停机时间、人员时间、设备成本、网络成本、失去机会、支付赎金等）的大致成本是多少？（3,702 家企业受到勒索软件攻击）

医疗行业的网络保险投标率低于平均值



如果受勒索软件攻击，您企业是否有网络保险？(图中的基数)。
是；是，但保单有例外/不包括项

医疗行业的位置：网络保险赔付率，按行业划分



网络保险支付您企业受到的最大勒索软件攻击相关费用吗？(n=3,308 去年受勒索软件攻击，网络保险承担勒索软件费用的企业) 是，支付清理成本 (例如企业恢复并运行的成本)；是，支付赎金；是，支付其他成本 (例如停机成本，失去机会等)

保险赔付
保险支付清洁成本
保险支付赎金
保险支付其他成本

了解更多勒索软件以及 Sophos 如何帮助您保护企业安全的信息。

Sophos 为所有规模的企业提供行业领先的网络安全解决方案，实时保护其防御高级威胁，如恶意软件、勒索软件和网络钓鱼。凭借成熟的新一代功能，产品在人工智能和机器学习的支持下，可以有效保护业务数据安全。

2022-5-31 (WP-NP)

SOPHOS