SOPHOS

网络安全：人类挑战性

26 个国家 5,000 名 IT 经理的独立调查结果

Sophos 白皮书 2020 年 10 月

介绍

网络安全熟练专业人员的作用从未如此重要过。虽然自动化和技术进步在加强企业网络防御方面发挥了重要的作用，但真正有效的安全计划仍然需要专家人士的加入。

网络攻击的日益加剧是安全专家重要性得以提升的重要原因。
所有网络威胁背后都是一个网络罪犯，现在的高级攻击往往结合最新技术与实际在线黑客攻击。人为主导的攻击，还需利用人们的专业技术加以防范。

本白皮书全面介绍全球网络安全技术现状和资源的全新观点，揭示 IT 团队在实现人为主导的网络安全时面临的现实情况，探讨企业如何应对面对的挑战。

本文还阐述沦为勒索软件受害者的企业与其日常网络安全做法之间关系的独特见解。

关于调研

2020 年 1 月到 2 月，Sophos 委托专业调研公司 Vanson Bourne 对 26 个国家的 5,000 名 IT 经理进行调研。Sophos 不参与受访者地调选，所有回答完全匿名。

国家	受访者数量
澳大利亚	200
比利时	100
巴西	200
加拿大	200
中国	200
哥伦比亚	200
捷克共和国	100
法国	300
德国	300

国家	受访者数量
印度	300
意大利	200
日本	200
马来西亚	100
墨西哥	200
荷兰	200
尼日利亚	100
菲律宾	100
波兰	100

国家	受访者数量
新加坡	200
南非	200
西班牙	200
瑞典	100
土耳其	100
阿联酋	100
英国	300
美国	500

在每个国家，50% 的受访者来自员工 100 到 1,000 人的企业，其余 50% 来自员工 1,001 到 5,000 人的企业。受访者来自公共和私人的多个领域。

行业领域	受访者数量
IT、科技和电信	979
零售、分销和运输	666
制造生产	648
金融服务	547
公共领域	498
商业和专业服务	480
建筑与房地产	272
能源、石油/天然气和公用设施	204
媒体、休闲和娱乐	164
其他	542

行政摘要

IT 团队在多场战役中展现出成果

- **IT 团队熟练掌握打补丁。**四分之三的 IT 团队在补丁程序发布后一周内，给台式机、服务器、应用程序和联网资产打补丁。服务器和联网资产打补丁的速度最快，39% 的受访者在 24 小时内完成。
- **预防是当务之急。**IT 团队平均近一半的时间 (45%) 用于预防，30% 的时间用于侦测，剩余 25% 用于应对。
- **IT 经理时刻追上网络安全最新信息。**大部分人表示他们 (72%) 及其团队 (72%) 足以因应网络安全威胁，甚至领先一步。仅 11% 认为他们大幅落后。

改善网络安全需要人才 – 但人才不足

- **迫切需要人为主导的威胁追踪。**48% 的受访者已经在安全程序中加入人为主导的威胁追踪，另有 48% 计划在一年内加入。
- **缺乏网络安全技能直接影响防护能力。**超过四分之一 (27%) 的经理表示，找到和挽留熟练 IT 安全专业人员是实现 IT 安全的最大挑战，54% 认为这是主要挑战。

企业正在改变实现安全的方式

- **外包 IT 安全快速增加。**目前 65% 的企业外包部分或全部 IT 安全工作。到 2022 年这一数字将增加至 72%。完全内部员工处理的企业百分比将从 34% 下降至 26%。
- **提高运行效率是一个关键优先事项。**四成 (39%) 的受访者表示，提高运行效率和可缩放性是其 IT 团队今年的最主要优先工作之一。

勒索软件受害者对于没有受害企业表现出不同的行为和态度

- **勒索软件受害者更多接触来自第三方的感染。**去年 29% 受勒索软件攻击的企业允许 5 家或更多供应商直接连接其网络 – 而只有 13% 的没有受勒索软件攻击的企业这样做。
- **勒索软件摧毁专业人员的信心。**受勒索软件攻击和未受攻击的企业相比，前者 IT 经理感觉在网络威胁方面“远远落后”的比例是后者的近 3 倍 (17% 与 6%)。
- **受到攻击加快人为主导的威胁追踪的实施。**43% 的勒索软件受害企业计划在 6 个月内实施人为主导的追踪，而未受攻击的企业只有 33%。
- **受害企业了解到熟练安全专业人员的重要性。**超过三分之一 (35%) 的勒索软件受害企业表示，招聘和挽留熟练 IT 安全专业人员是网络安全方面的最大挑战，未受攻击的企业则只有 19% 这样认为。

IT 团队在多场战役中展现出成果

从积极的一面开始：IT 团队不断设法领先每一个网络安全的层面。他们能够一次成功实施多个防御措施，保护企业防御种种威胁。

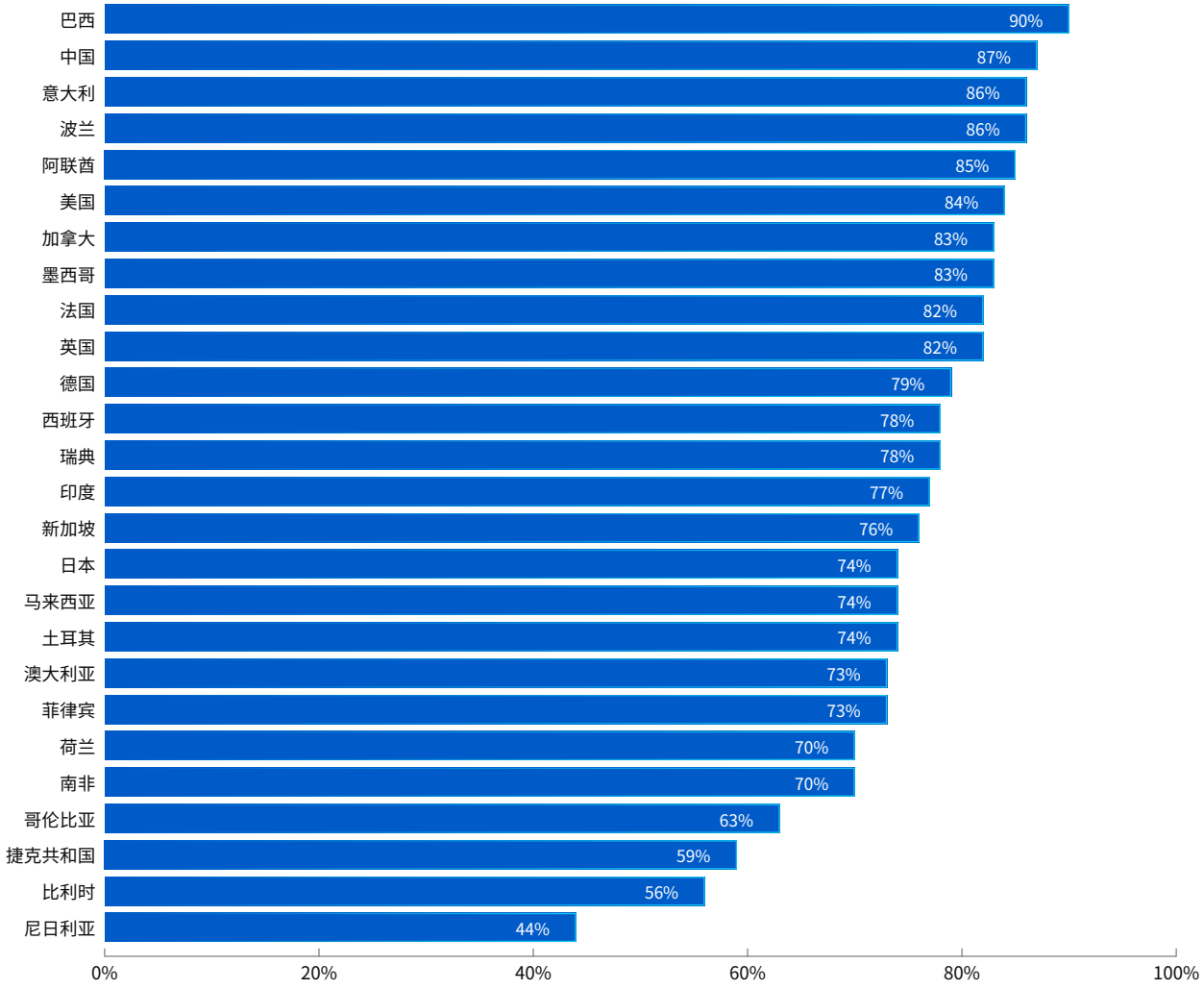
IT 团队熟练掌握打补丁

“尽早打补丁。勤打补丁”是安全专家的共识，IT 团队牢记于心。受访者警惕快速打补丁的需要，许多受访者在发布后 24 小时内应用补丁，四分之三的受访者在发布后一周内完成。服务器和联网资产打补丁的速度最快，39% 的受访者在 24 小时内完成。

	24 小时内打补丁	一周内打补丁	一个月内打补丁
台式机	36%	41%	14%
服务器	39%	38%	14%
应用	36%	40%	15%
联网资产	39%	38%	14%

但是，22% 的受访者承认用超过一周时间应用台式机补丁，尼日利亚、比利时和捷克受访者用时最长。

在发布一周内对台式机打补丁的受访者百分比

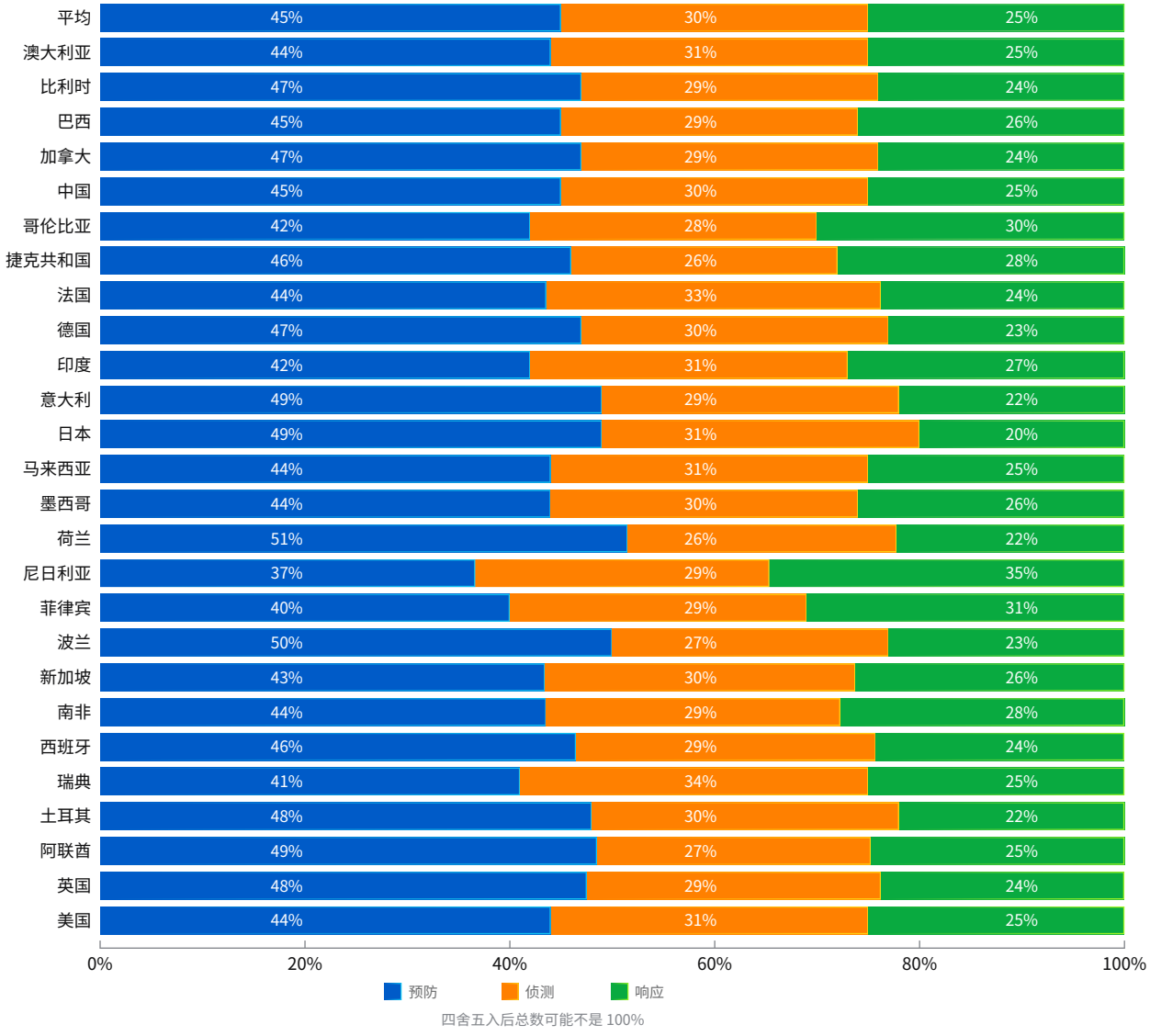


优先预防

IT 团队平均近一半的时间 (45%) 用于预防，30% 的时间用于侦测，剩余 25% 用于应对。数据揭示了一些地区性差异：在受访国家中，荷兰 IT 团队用于预防的时间最多 (51%)；瑞典 IT 团队用于侦测的时间最多 (34%)；尼日利亚企业用于应对的时间最多 (35%)。

平衡用于预防和侦测的时间是合理的网络安全方法，将大量时间用在应对通常意味着无法阻止事件发生。大量时间用于应对说明企业遇到大量事件，在很晚才发现事件，或者同时出现这两种情况。

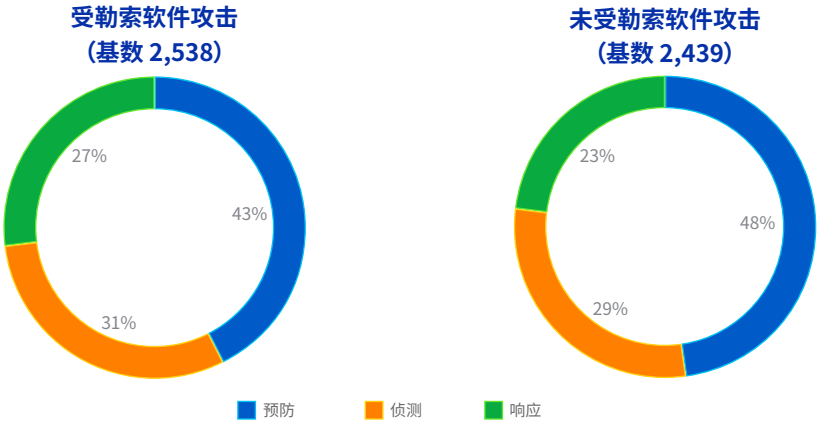
在预防、侦测和应对之间划分时间



四舍五入后总数可能不是 100%

勒索软件受害者用于预防的时间较少，用于应对的时间较多

51% 的受访者承认，他们的企业在过去 12 个月遭受勒索软件攻击。沦为勒索软件受害者的企业对侦测与应对的关注多于非受害企业。反过来，没有受勒索软件攻击的企业比受害者企业用在预防的时间更多。



对预防的更多关注可能帮助非受害企业预防了攻击：强大的防御总是从最好的防护开始。同时，勒索软件受害者对于复杂多阶段性质的高级攻击更加警惕，因此将更多资源用于发现和应对预示攻击即将来临的信号。

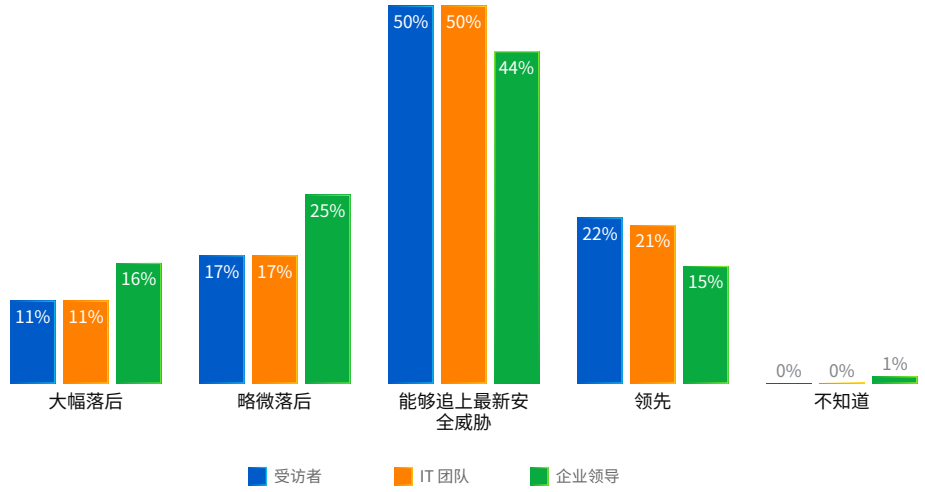
有关如何识别勒索软件攻击者已经将您作为目标的更多信息，请阅读 SophosLabs 文章将要受到攻击的 5 个信号。

IT 经理时刻追上网络安全最新信息

虽然网络安全威胁快速变化，但 IT 专业人员认为他们一直时刻了解网络最新的最新信息。大多数 IT 经理表示他们 (72%) 及其团队 (72%) 足以应对网络安全威胁，甚至领先一步。28% 的 IT 经理认为自己落后，17% 认为略微落后，只有 11% 认为自己大幅落后。

这些数据的背后是显著的地区性差异：波兰、墨西哥和土耳其受访者认为自己最领先网络威胁（分别为 39%、34% 和 31%），而尼日利亚 (60%)、瑞典 (57%) 和德国 (49%) 认为自己最落后。值得注意的是，这些数据是受访者的感受（因此很可能存在文化影响），并不是实际情况的真实衡量。

与时俱进的受访者如何看待他们企业的人与网络威胁



IT 经理通常自信他们及其团队保持最新，41% 的 IT 经理认为他们的企业领导者落后（25% 略微落后，16% 大幅落后）。这一差距可以从许多方面理解 – 企业领导者很少从事网络安全专业 – 但是这突显了 IT 团队让领导了解网络安全风险及相关投资请求所面临的挑战。

勒索软件攻击摧毁 IT 专业人员的信心

深挖数据我们可以发现，勒索软件攻击严重破坏 IT 经理及其团队的信心，超过任何业务影响。

去年遭受勒索软件攻击企业的 IT 经理感觉“大幅落后”网络威胁的数量，几乎是未遭受攻击的企业 IT 经理的三倍（17% 与 6%）。这降低了 IT 经理对 IT 团队和企业领导者的信心，如下表所示。

	大幅落后于网络威胁 (%)	追上网络威胁(%)
IT 经理（受访者）		
受勒索软件攻击	17%	43%
未受勒索软件攻击	6%	57%
IT 团队（受访者感受）		
受勒索软件攻击	15%	43%
未受勒索软件攻击	6%	58%
企业领导者（受访者感受）		
受勒索软件攻击	20%	39%
未受勒索软件攻击	11%	49%

此外，务必记住，这些回答是受访者的感受，而不是实际情况衡量。受勒索软件攻击是一个现实考验，这样的经历导致勒索软件受害者对情况有了更准确的理解。

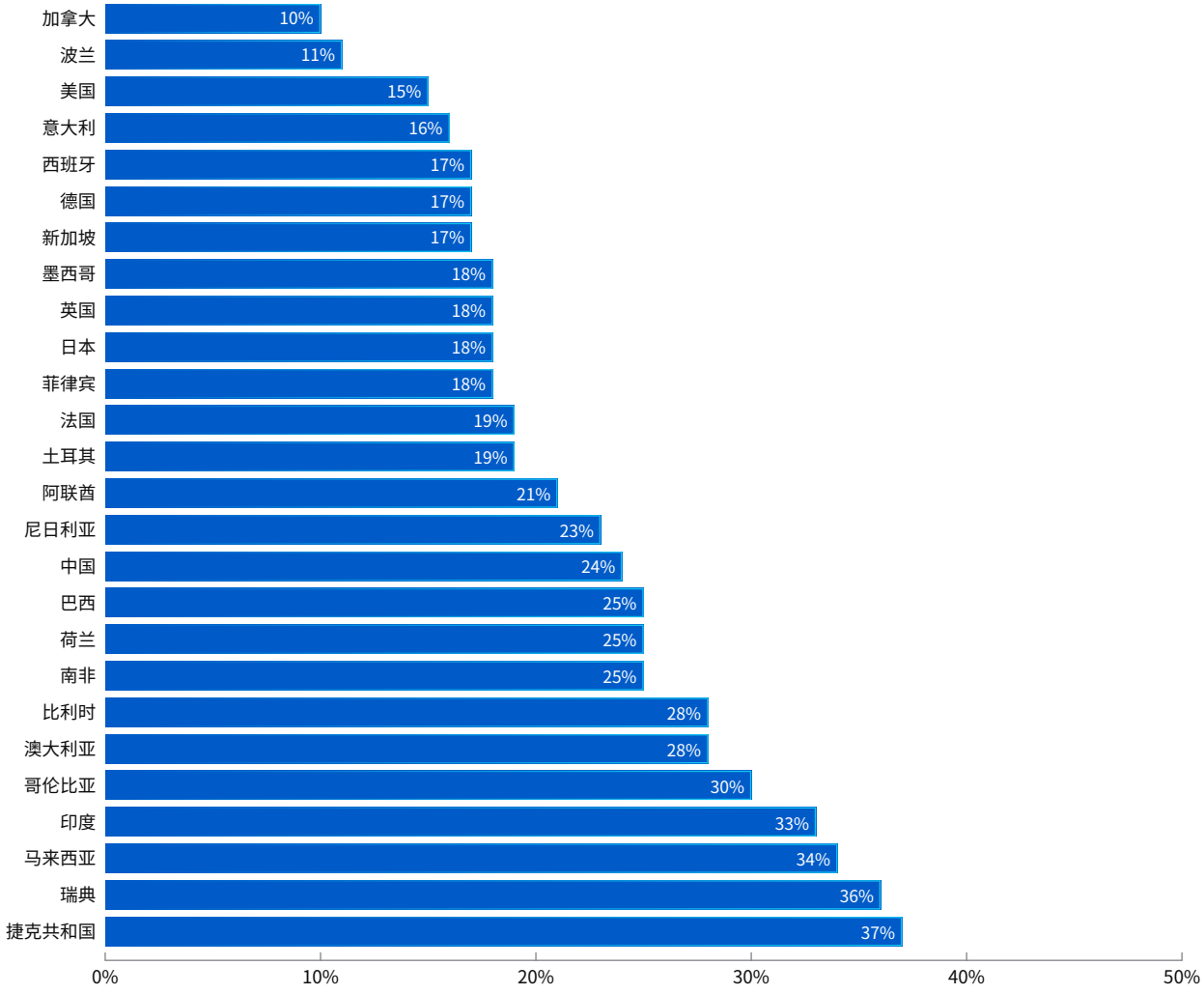
改善网络安全需要人才 – 但人才不足

尽管IT团队在很多情况下都能成功阻抑各种攻击，但要取得全面胜利，仍任重而道远。IT 领导者及其团队做出了最大努力，但网络威胁仍然是存在的挑战 – 仅仅略多于一半的受访者 (51%) 表示，减小网络攻击风险是来年的优先关注方面。从 IT 团队面临的广泛安全挑战来看，理由很明显。

IT 团队面临不断增加的网络攻击，威胁来自于多个方向，针对不同的目标。正如上文提到的，51% 的受访者去年受到勒索软件攻击，网络罪犯在 73% 的攻击中成功加密数据*。云安全是另一个挑战，70% 将数据或工作放在公共云的企业去年遇到安全事件**。

IT 团队面临的另一个挑战是保护可以直接连接其网络的第三方企业，例如会计服务或 IT 提供商。受访者平均有 3 个供应商可以连接其系统。但是，五分之一的受访者 (21%) – 捷克、印度、马来西亚和瑞典达到三分之一（或更多）– 允许 5 个或更多供应商连接。反过来，在加拿大和波兰，仅十分之一的受访者有 5 个或更多供应商远程访问。

5 个或更多供应商可以直接连接网络的企业百分比



允许第三方供应商连接网络不可避免地带来安全风险，当然也有业务好处。可以连接的供应商越多，IT 团队面临的挑战和工作量越大。

勒索软件受害者更多接触来自第三方的感染

去年遭受勒索软件攻击的企业中，29% 允许 5 家或更多供应商直接连接其网络 – 而没有受攻击的企业只有 13%。9% 的攻击受害者称第三方供应商是进入方法，这无疑是一个主要攻击渠道。

虽然支持外部企业连接您的网络的业务理由有很多，但这样的结果是，保护供应链安全应该是采用此方法的所有人的关键优先工作。强大的网络安全需要成为任何希望连接网络的人的基本条件。

迫切需要人为主导的威胁追踪

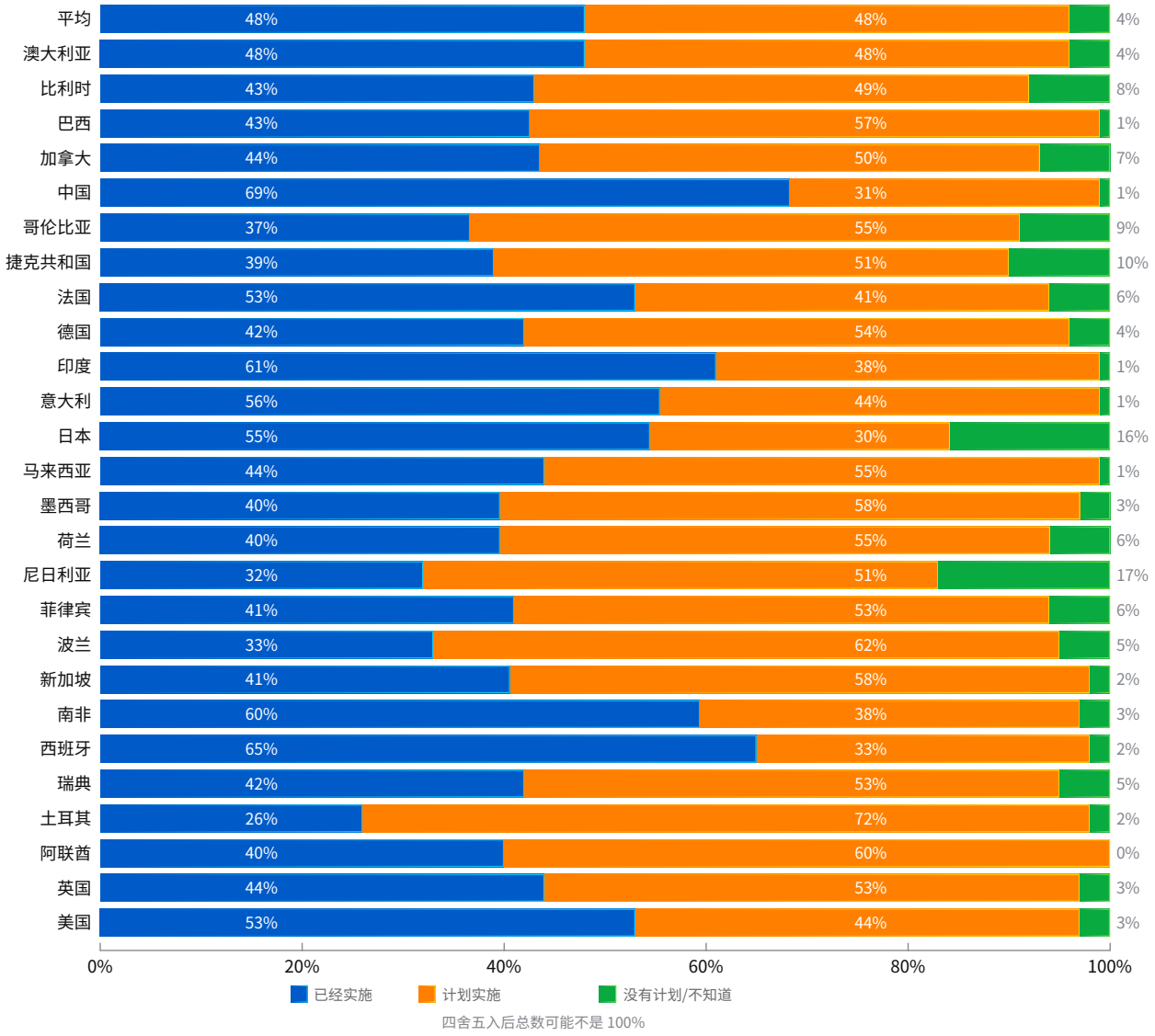
最具破坏性的网络威胁通常涉及人为主导的攻击，往往利用合法工具和进程，如 PowerShell。亲自在线黑客攻击支持攻击者随时修改战术、技术和方法 (TTP)，绕过安全产品和协议。进入受害者网络后，攻击者可以横向移动，窃取数据，安装恶意软件和后门用于未来攻击，部署勒索软件。

虽然技术起到重要作用，尤其是智能自动化技术，但仍然需要专家操作者。阻止人为主导的攻击需要人为主导的威胁追踪。

几乎所有受访者都承认需要此方法：48% 已经在安全过程中加入人为主导的威胁追踪，以识别安全工具（如 SIEM、端点防护、防火墙等）无法侦测的攻击者活动。另有 48% 计划加入。受访者还警惕部署人为主导的追踪的紧迫性，几乎所有 (99.6%) 受访者都希望在来年实施。

人为主导的威胁追踪现状在不同地区差异巨大。69% 的中国受访者已经实施此方法，紧随其后的是西班牙 (65%)、印度 (61%) 和南非 (60%)。反过来，土耳其采用人为主导的威胁追踪的步伐最慢，仅 26% 的受访者已经实施，尼日利亚 (32%) 和波兰 (33%) 仅略微领先。

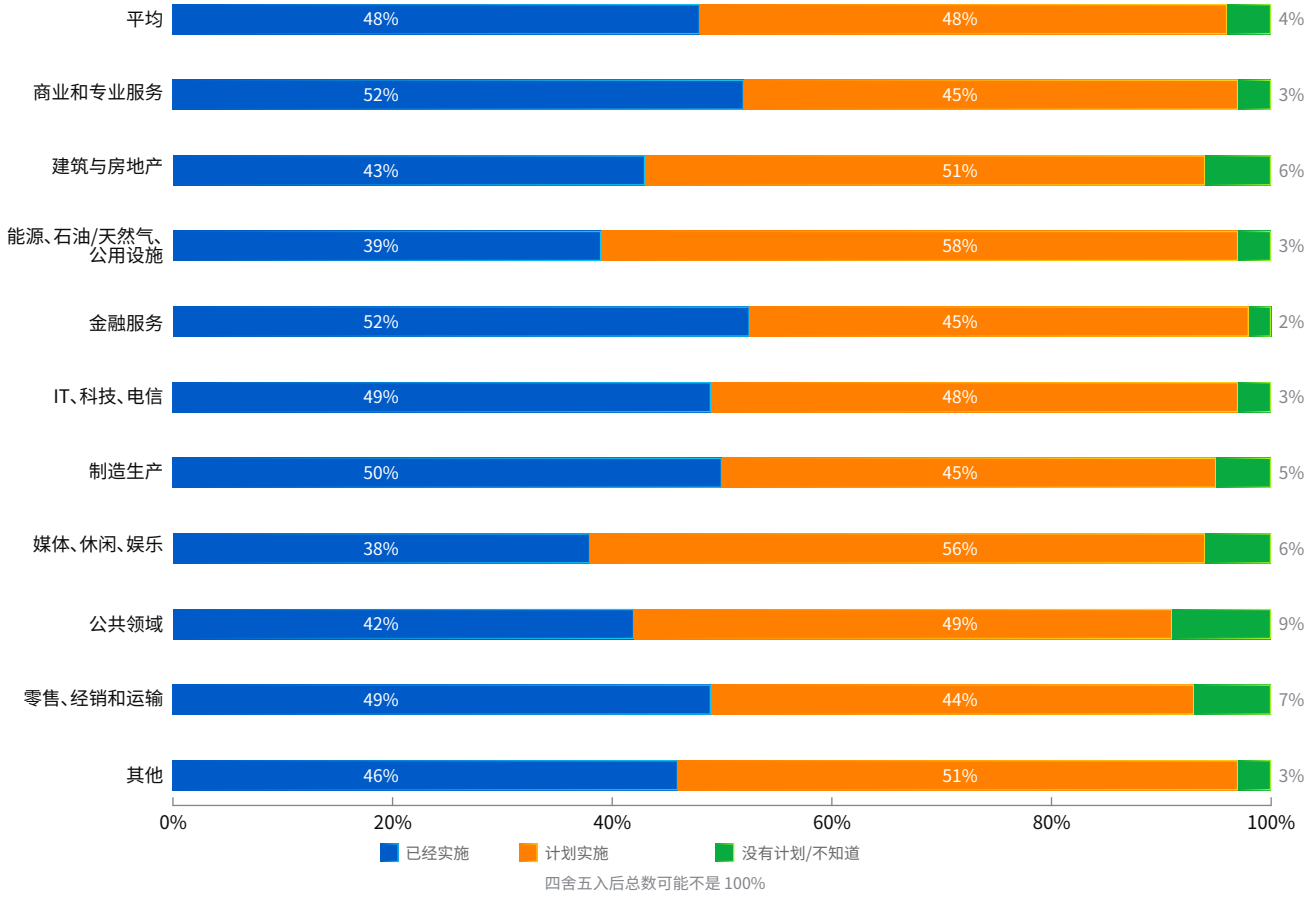
计划加入人为主导的威胁追踪



调查还揭示了不同行业的准备程度。商业和专业服务以及金融服务在实施人为主导的威胁追踪方面领先，每个行业有 52% 的受访者表示其企业已经采用此方法。

相比之下，媒体、休闲和娱乐 (38%) 以及能源、石油/天然气和公用设施领域 (39%) 受访者当前开展人为主导的威胁追踪较少。考虑到能源领域是国家级攻击的潜在目标，对人为主导威胁的脆弱情度令人担忧。

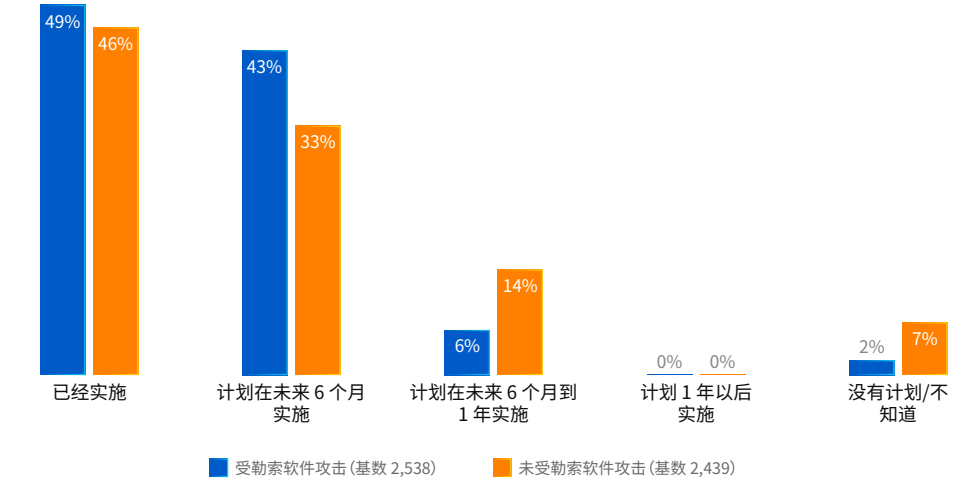
计划加入人为主导的威胁追踪（按行业划分）



受到勒索软件攻击加快人为主导的威胁追踪的实施

受勒索软件攻击对企业加入人为主导的威胁追踪的意愿整体影响非常小，但确实提高了实施的紧迫性。43% 的勒索软件受害企业计划在 6 个月内实施人为主导的威胁追踪，而未受攻击的企业只有 33%。这一数据表明，勒索软件受害者迫切希望避免事件再次发生。

最近遭遇勒索软件事件对实施人为主导的威胁追踪的影响



缺乏网络安全技能直接影响防护能力

81% 的受访者表示，找到并挽留熟练 IT 安全专业人员，是企业实现 IT 安全的主要挑战：54% 表示是重要挑战，超过四分之一 (27%) 认为是最大挑战。

每个国家在招聘熟练 IT 人员方面都遇到困难。在意大利 (94%)、印度 (93%) 以及巴西和哥伦比亚（都为 92%），超过九成的受访者表示，找到并挽留熟练员工是保护企业不受网络威胁的主要障碍。

即使在南非，这个最不可能遇到网络安全员工招聘困难的国家，也有超过六成 (62%) 的受访者称带来主要问题。

招聘和挽留熟练 IT 安全专业人员对企业实现 IT 安全带来的挑战达到什么程度？

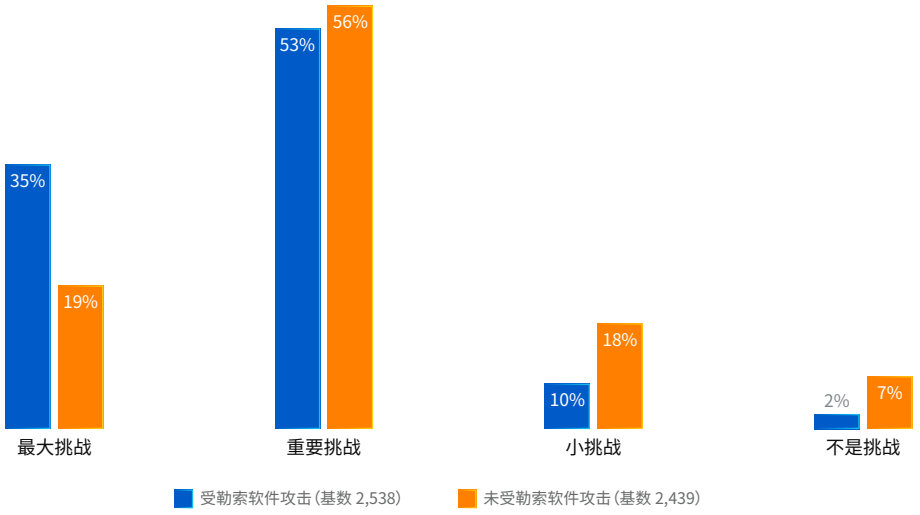
国家	最大的挑战	重要挑战，但不是最大的	小挑战	不是挑战	不知道
平均	27%	54%	14%	4%	0%
澳大利亚	17%	57%	22%	5%	0%
比利时	24%	52%	24%	0%	0%
巴西	45%	47%	6%	3%	1%
加拿大	19%	55%	18%	7%	2%
中国	24%	54%	18%	4%	0%
哥伦比亚	29%	63%	8%	1%	0%
捷克共和国	33%	47%	18%	1%	1%
法国	23%	62%	11%	4%	0%
德国	19%	63%	14%	5%	0%
印度	58%	35%	6%	1%	0%
意大利	28%	67%	5%	2%	0%
日本	35%	44%	17%	4%	1%
马来西亚	26%	54%	16%	4%	0%
墨西哥	27%	62%	6%	6%	0%
荷兰	26%	49%	25%	0%	1%
尼日利亚	32%	51%	16%	1%	0%
菲律宾	40%	49%	8%	2%	1%
波兰	9%	59%	20%	12%	0%
新加坡	17%	72%	10%	2%	0%
南非	22%	40%	19%	19%	0%
西班牙	17%	58%	17%	8%	1%
瑞典	44%	41%	13%	1%	1%
土耳其	30%	52%	9%	8%	1%
阿联酋	22%	62%	15%	1%	0%
英国	14%	64%	20%	2%	0%
美国	26%	49%	17%	8%	0%

勒索软件受害企业以血的教训了解到熟练安全专业人员的重要性

成为网络攻击受害者对网络安全员工的态度具有重要影响。在去年勒索软件受害企业中，超过三分之一 (35%) 的受访者表示招聘和挽留熟练 IT 安全人员是网络安全最大挑战，53% 认为是重要挑战。

反过来，在去年没有受勒索软件攻击的企业中，仅 19% 将其视为最大挑战 – 整个 16 个百分点的差距。

招聘和挽留熟练 IT 安全专业人员是企业实现 IT 安全的挑战



这些态度的差异背后很可能有以下几个因素的影响。首先，在最初遭遇勒索而付出财务、运营和信誉代价的人的眼中，对有限安全技能造成的后果记忆犹新。

此外，勒索软件受害者将始终调查攻击源头。在这样做的过程中，他们将发现导致攻击者能够进入企业并访问其数据的防御漏洞。许多人很可能将发现人才专业技术的不足是成为攻击受害者的原因之一。

招聘是 IT 经理的首要任务

技能不足导致的后果是招聘和挽留员工成为 IT 经理的首要任务。55% 的受访者表示，这是未来 12 个月的焦点方面之一，将减小网络攻击风险降到第二位。（注：受访者可以为此问题选择多个回答）。

企业正在改变实现安全的方式

IT 专业人员对于人才挑战并不意外。多年来一直存在网络安全招聘的问题，经理们优先重视人才令人鼓舞，但这挑战之巨大说明不会很快解决到问题。

从这个角度来看，IT 经理改变实现网络安全的方式，将重点放在提高效率和可缩放性，可以视为对人才挑战的直接应对。

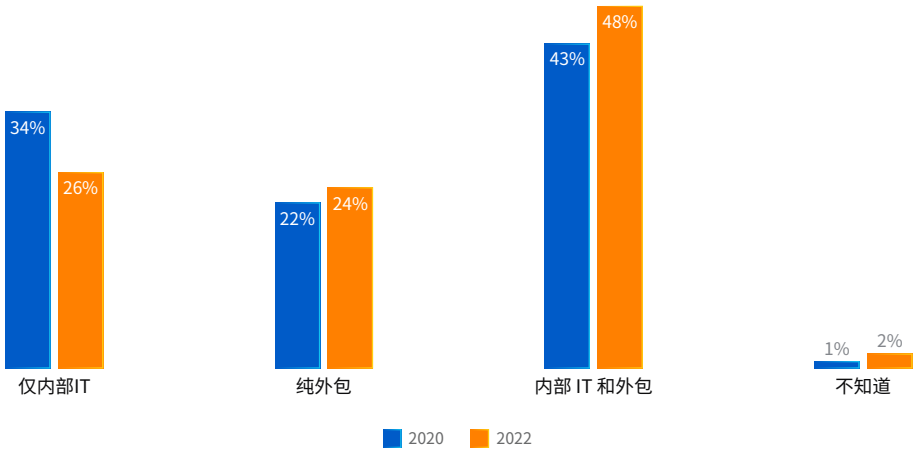
外包快速增长

外包网络安全让企业能够享受到安全专业人员的专业技术，而无需直接招聘他们。由于安全服务提供商培养和发展专业技能的能力强，通常比不这样做的企业能够获得更高的安全能力。

外包 IT 安全已经成为共识，65% 在一定程度上外包：43% 结合内部和外包安全，22% 完全外包其 IT 安全。调查揭示地区性差异。外包靠前的国家包括中国 (76%)、阿联酋 (74%) 和马来西亚与新加坡（都为 73%），约四分之三的受访者已经外包 IT 安全。另一方面，比利时 (52%)、法国 (54%) 和尼日利亚 (54%) 仅刚过一半的受访者当前正在使用第三方安全提供商。

全球未来 2 年外包趋势将增加，从现在的 65% 增长到 2022 年的几乎四分之三 (72%)。最大的变化是完全内部员工处理的企业百分比：将从 34% 下降至 26%。完全外包 IT 安全和结合内部外包的百分比都将增加。

企业如何实现 IT 安全



全球数据的背后存在一些有趣的地区性差异：

- 西班牙和印度受访者计划仅增加内部 IT 安全管理 – 虽然数字相对较小（西班牙从 34% 增加到 37%，印度从 33% 增加到 34%），但无疑与全球趋势相反
- 在菲律宾，近一半受访者 (48%) 计划到 2022 年完全外包 IT 安全 – 相比目前的 30% 是一个飞跃。计划纯外包策略超过平均值的其他国家包括捷克、尼日利亚和瑞典（都为 35%）以及澳大利亚 (34%)
- 超过六成受访者计划结合内部和外包方法的国家包括中国 (67%) 和墨西哥 (62%)

IT 经理关注提高效率和可缩放性

寻找更充分发挥现有技能的方法是另一个应对 IT 安全专业技术不足的措施。四成 (39%) 的受访者表示，提高运行效率和可缩放性是其 IT 团队今年的最主要优先工作之一。欧洲和日本受访者低于此平均值，中国、马来西亚和南非有半数以上受访者将其纳入优先工作。

结束语

以上见解来自 26 个国家的 5,000 名 IT 经理，揭示了 IT 团队在管理和实现 IT 安全方面面临的挑战。IT 团队赢得许多战役 – 主要通过打补丁和时刻追上网络安全威胁- 但这场战争还远没有获胜。IT 专业人员面临多个方面的挑战：从勒索软件和云安全，到管理可以连接其网络的第三方供应商。

面对人为主导的攻击增长，大多数企业转向人为主导的威胁追踪；到 2020 年底，95% 的受访者希望在一定程度上实施。与此同时，难以招聘和挽留网络安全专业人员成为限制绝大多数企业的因素。去年成为勒索软件受害者的企业尤其警惕技能不足对实现有效网络安全造成的影响。

勒索软件直接经历与 IT 行为之间关系明显。勒索软件受害者受到第三方感染多于其他企业，用于应对的时间更多，说明他们要处理的事件更多。同时，他们的经历使其更加认可熟练网络安全专业人员的重要性，更加迫切实施人为主导的追踪。

在这些挑战之下，看到 IT 团队改变其做法是令人鼓舞的。未来 2 年外包专家的利用将继续增加，到 2022 年近四分之三的企业将在一定程度外包 IT 安全。在许多领域，还将更加关注提高运行效率和可缩放性，以便支持 IT 团队以现有熟练专业人员做到更多。

网络安全不会停滞不前。IT 团队在多个安全方面保持领先值得称赞。考虑到网络安全人才持续短缺，IT 团队将需要找到新的方法，扩大和增强防御，应对不断发展的威胁，尤其是人为主导的攻击的增加。

Sophos 可以帮助做什么

无论要以何种方式管理 IT 安全，我们都可以支持您。

24/7 全天候人为主导的威胁追踪服务

利用 Sophos 托管威胁响应 (Managed Threat Response, MTR)，您的企业将获得威胁追踪和响应专家团队 24/7 全天候保护，代表您主动追踪和消除威胁。这些训练有素的安全专业人员能够侦测并阻止人为主导的高级攻击，阻止其影响您的企业。

了解更多，阅读 MDR 买家指南。

即时事件响应服务

任何遇到作动中攻击事件的企业都可以部署我们的**快速事件响应**服务。我们的事件响应专家团队将快速发现并消除活跃威胁。无论是感染、攻破还是尝试绕过安全控制的未经授权访问，我们都能够发现并阻止。

了解更多

高级 IT 保健和威胁追踪工具

如果您希望自己进行威胁追踪，Sophos 端点侦测与响应 (EDR) 为您提供实现高级威胁追踪和 IT 安全运行保健所需的工具。借助强大的搜索功能，您的团队可以发现并主动解决安全和 IT 保健问题，提升防护水平。

了解更多和免费试用。

下一代网络安全系统

部署 Sophos 下一代网络安全系统的企业都表示 IT 管理开销降低 50%。部署我们市场领先的端点和防火墙解决方案，并通过 Sophos Central 平台管理所有内容，IT 团队可以节约一半用于管理网络安全的时间 – 并且提高安全效果。

了解更多和自己阅读客户案例。

深入的勒索软件研究

SophosLabs 和 Sophos MTR 团队在 Sophos 博客 定期发表最新勒索软件技术研究成果。

* 2020 勒索软件现状由 Sophos 委托，并由 Vanson Bourne 执行的对 5,000 名 IT 经理的全球调查。

** 2020 云安全现状由 Sophos 委托，并由 Vanson Bourne 执行的对 3,521 名 IT 经理的全球调查。

关于 Vanson Bourne

Vanson Bourne 是科技行业独立市场的调研专家。严格的调研原则，以及获得所有行业和所有主要市场的技术与业务职能资深决策者意见的能力，是其强大而可信的研究分析信誉的基础。访问 www.vansonbourne.com

中国（大陆地区）销售咨询
电子邮件: salescn@sophos.com

20-10-05 WPZHCN (DD)

SOPHOS