SOPHOS

2023 网络安全现状：攻击敌手的业务影响

2023 年 1 月和 2 月，对 14 个国家 3,000 名负责 IT/网络安全的领导者进行的一项独立研究的结果。

研究方法

为了研究 2023 网络安全的现实业务影响，Sophos 委外了一项对 14 个国家 3,000 名负责 IT/网络安全的领导者的独立调查。所有受访者来自拥有 100 到 5,000 名员工的组织。Vanson Bourne 于 2023 年 1 月和 2 月开展调研。

3,000
受访者

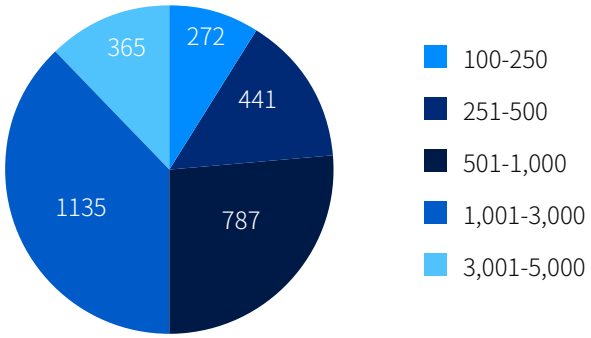
100-5,000
雇员

14
国家

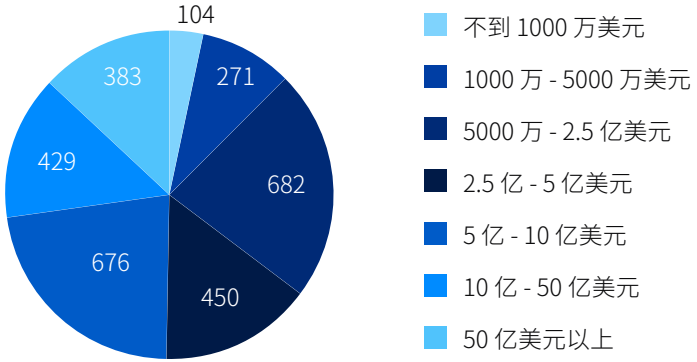
1000 万美元以下 - 50 亿美元以上
年收入

23 年 1 月/2 月
开展研究

按组织规模划分的受访者（员工数量）



按组织规模划分的受访者（年收入）



按国家划分的受访者

国家	受访者人数	国家	受访者人数
美国	500	英国	200
德国	300	南非	200
印度	300	法国	150
日本	300	西班牙	150
澳大利亚	200	奥地利	100
巴西	200	新加坡	100
意大利	200	瑞士	100

执行摘要

情况：攻击敌手不断加快速度，防御者无法跟上脚步

研究揭示，当前的现实是攻击敌手和防御者在不同发展速度的网络安全体系前行。攻击敌手通过自动化、网络犯罪“即服务”模式、隐蔽模仿和适应，不断加快速度发展，现在可以大规模执行广泛的复杂攻击。94% 的组织去年遇到某种形式的网络攻击，所有公司（无论规模或收入）都应假定他们将在 2023 年成为攻击目标。

受专业知识不足，过量的警报，花过多时间用于事件响应所影响，防御者无法跟上脚步。运营威胁侦测与响应对于大多数组织来说都存在困难，93% 的组织发现执行关键安全操作任务存在挑战。

调查安全警报是一个普遍问题。平均来说，所有警报中只有不到一半 (48%) 得到调查以判定是否恶意行为迹象；而大多数组织企业在识别 (71%) 和排定优先级 (71%) 要调查的警报/事件方面举步维艰。对于需要调查的警报，100-3,000 名员工的组织平均用时 9 小时完整侦测、调查和响应流程，而 3,001-5,000 名员工的组织则需要 15 小时。

运营方面，防御者对流程缺乏信心，安全工具配置错误是 2023 年排名最高的感知安全风险。超过一半 (52%) 的 IT 专业人员表示，网络威胁现在过于复杂，组织无法自行处理，而在小型企业（100-250 名员工）中则上升到 64%。

业务影响：局势带来财务、运营和资源方面的后果

这个双速度体系对更大范围的组织具有显著影响。网络事件的直接财务影响巨大并且众所周知，中小型组织扑救勒索软件攻击的平均成本达到 140 万美元[1]。但这些事件清理成本只是一部分。

IT 程序交付能力有所下降，55% 的受访者称，处理网络威胁对IT 团队在其他项目上的工作产生负面影响。网络安全紧迫而不可预测的性质还影响以业务为焦点的工作：64% 希望 IT 团队花更多时间处理战略问题，花更少时间处理紧急事故。

侦测、调查和修复安全警报所用的时间还在资源成本方面带来显著财务影响。

这现状还给员工带来沉重负担。57% 的 IT 专业人员表示，担心组织受网络攻击有时候让他们彻夜难眠；而在 3,001-5,000 名员工的组织中达到 65%。考虑到招聘、培训和挽留此领域员工的高昂成本，这些影响为业务带来额外挑战和成本。

1 2022 勒索软件现状，Sophos

建议：加快防御者的步伐，领先攻击敌手

要让防御者在 2023 年实超前攻击者，需要综合但直接的方法。首先，组织需要建立可以缩放的事件响应流程，通过减少攻击面和需要关注的警报数量来实现，并利用专业服务优化响应时间。

然后，需要实施适应性防御，根据情况自动调整。这样可以减慢攻击敌手，为防御者争取到响应时间。

最后，还需要建立良性的循环，结合技术与人类专业知识来加速防御，提升速度、效力和影响。这些措施组合在一起，加快防御者的速度，领先敌手。

此方法成功的核心是利用第三方专家。好消息是组织已经采取混合网络安全方法，94% 的公司与外部专家合作以某种方式扩大他们的运营规模。随着攻击敌手加大力度，引进专门的安全运营专业知识越来越重要。

重要发现

94% 的组织去年遇到某种形式的网络攻击

数据外泄是 2023 年的头号安全顾虑

93% 发现执行关键安全操作任务存在挑战

48% 的安全警报得到调查

15 小时是 3,001-5,000 名员工的组织用来侦测、调查和响应警报的时间中位数

安全工具配置错误是 2023 年排名最高的感知安全风险

52% 表示，网络威胁现在过于复杂，组织无法自行处理

55% 表示，处理网络威胁对IT 团队的其他项目工作产生负面影响

64% 希望 IT 团队花更多时间处理战略问题，花更少时间处理紧急事故

57% 的 IT 专业人员失眠，担心组织受到网络攻击

2023 年网络威胁：前线的现实

2023 年最高网络威胁顾虑

99% 的 IT 专业人员担心 2023 年网络威胁影响其组织。数据外泄（外部攻击者盗窃）位列 IT 专业人员最担心影响其组织的威胁名单第一名，紧随其后的是网络钓鱼（包括鱼叉式网络钓鱼）。勒索软件占据前三名。

务必记住，这三个威胁往往互相关联：网络钓鱼电子邮件通常开展攻击，引致数据外泄和勒索软件。

网络威胁	表示这是最大顾虑的受访者百分比
数据外泄（外部攻击者盗窃）	41%
网络钓鱼（包括鱼叉式网络钓鱼）	40%
勒索软件	35%
网络勒索	33%
拒绝服务攻击 (DDoS)	32%
商务邮件受骇	31%
主动敌手攻击（人为键盘攻击者）	30%
移动恶意软件	30%
加密货币挖矿	22%
擦除程序	16%
其他	0%
我不担心我组织在 2023 年受任何网络威胁影响	1%
不知道	0%

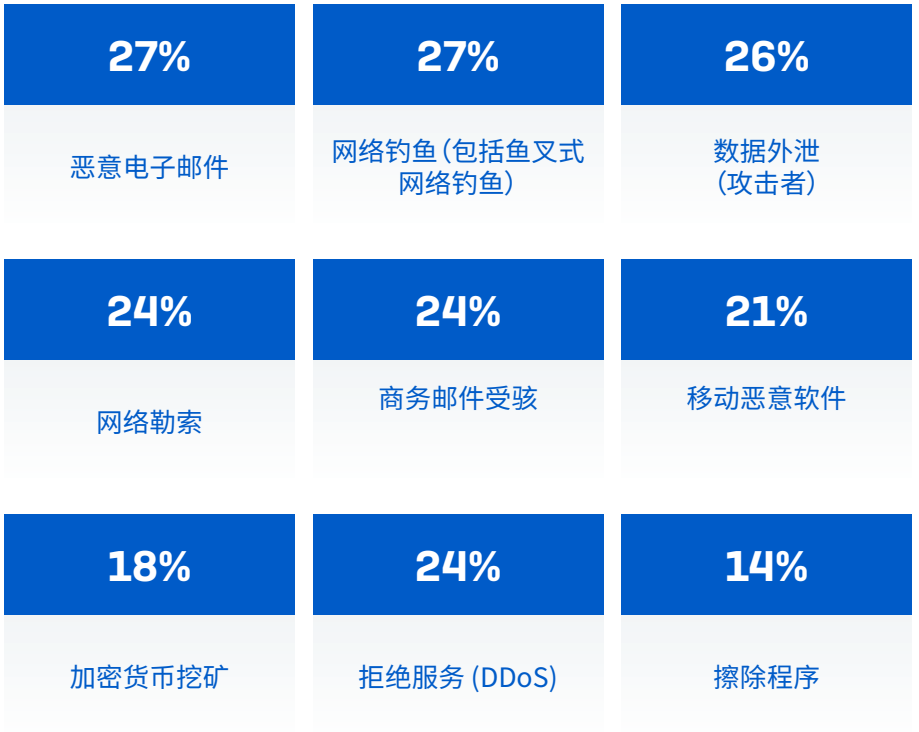
考虑 2023 年，您最担心的影响您组织的网络威胁是什么？(n=3,000)

攻击敌手现在大规模执行多种攻击

IT 专业人员的顾虑非常符合前线正在发生的现实，94% 的组织去年遇到至少一次网络攻击。虽然勒索软件是报道最多的攻击，但攻击敌手大规模执行多种攻击。这种攻击的宽度和深度为防御者带来沉重且日益增长的挑战。

数字的背后是网络罪犯经济的专业化，包括“即服务”模型的增长，包括“访问权即服务”、“网络钓鱼即服务”和“诈骗即服务”。网络犯罪操作的进化降低了潜在网络罪犯的进入壁垒。[有关更多信息，请参阅 Sophos 2023 年网络威胁报告。]

遇到的部分非勒索软件网络攻击，以及报道此类攻击的组织百分比



主动攻击敌手攻击现在很常见

23%
的组织去年遇到涉及主动攻击敌手的攻击

30%
表示主动攻击敌手是他们 2023 年最大网络威胁顾虑之一

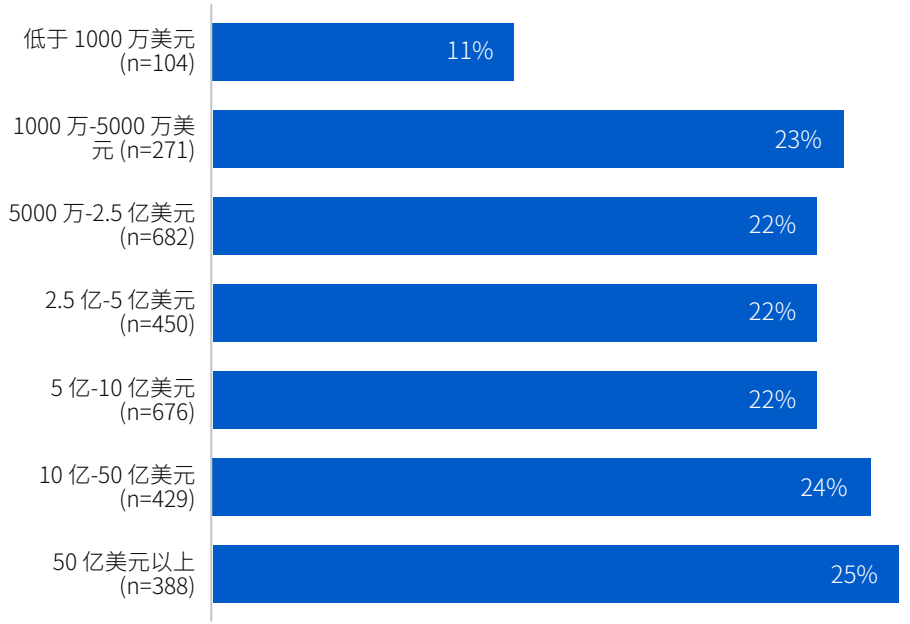
主动攻击敌手是运用实时键盘操作来实时动态调整技术、战术和程序 (TTP) 的威胁操作者，以应对安全技术和防御者操作，并作为避开侦测的战术。此类攻击往往带来毁灭性的勒索软件和数据外泄事件，是最难阻止的攻击。

23% 的受访者称，他们的组织去年遇到涉及主动攻击敌手的攻击。不论组织规模，攻击频率大致保持一致，在所有组织规模划分段内只有 2 个百分点的变化。

有趣的是，对于不到 1000 万美元年度收入的组织，主动攻击敌手攻击的报道率仅 11%，说明攻击者有意锁定收入更多的目标。侦测主动攻击敌手需要很高的技能水平，故很可能实际事件发生率更高。

30% 的受访者称，主动攻击敌手是他们 2023 年最大网络威胁顾虑之一，反映了此类攻击的潜在破坏性。

经历主动攻击敌手攻击，按营收划分

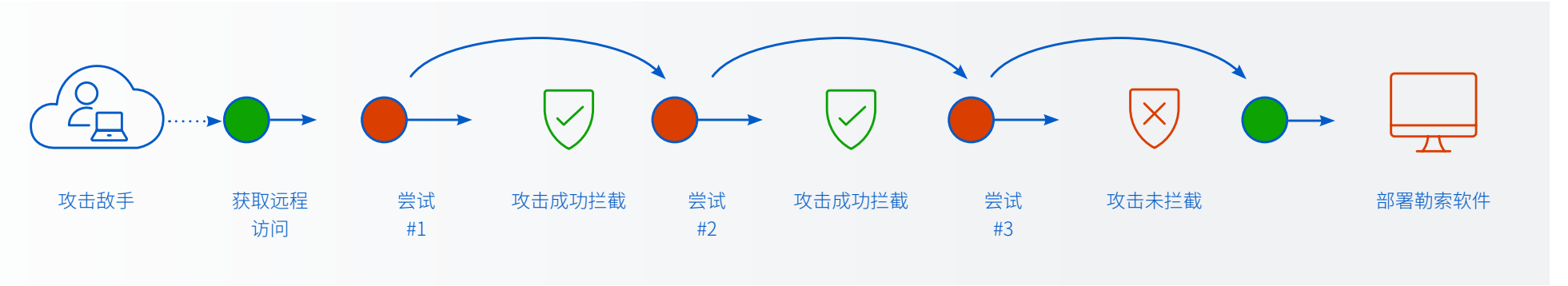


您去年遇到过任何网络攻击吗?遇到过 - 主动攻击敌手（人为键盘攻击者）

了解主动攻击敌手

要理解防御者面临的挑战，务必了解一点，拦截主动攻击敌手不足以阻止他们。这些熟练而难缠的威胁操作者运用多种技术、战术和程序 (TTP) 实现目标，包括：

- 利用安全弱点渗透进入组织，一旦进入网络后横向移动，包括凭据盗窃、未打补丁的漏洞以及安全工具错误配置。
- 滥用防御者运用的合法 IT 工具，避免触发侦测，
- 实时修改攻击以应对安全控制，继续转至新技术直到找到实现目标的方法。



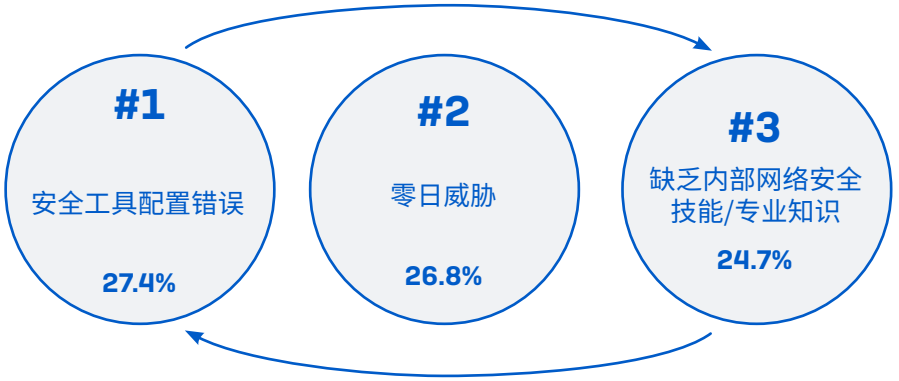
2023年网络安全：防御者现状

最大的网络风险顾虑

安全控制配置错误（例如端点或防火墙解决方案）是最广泛回报的感知安全风险，27.4% 的受访者将其列为前三大网络风险。高排名说明 IT 团队在确保安全控制始终保持正确配置和部署，以及应对攻击敌手利用组织防御漏洞的准备时面临的挑战。

零日攻击，即利用以前未知的安全漏洞或软件缺陷的攻击，在前三大安全风险中排名第二，为 26.8%。缺乏内部网络安全技能/专业知识排名第三，25% 的受访者把其列于前三 位。

缺乏技能和安全工具配置错误之间存在直接关系：如果没有时间、知识和经验来正确配置控制，将在防御中产生漏洞。



网络安全风险	前三大顾虑的百分比排名
安全控制配置错误（例如端点或防火墙解决方案）	27%
零日威胁（利用以前未知的攻击技术的威胁）。	27%
缺乏内部网络安全技能/专业知识	25%
盗窃访问权数据和凭据	24%
未受保护的设备（包括未知设备）	24%
缺乏网络安全工具	23%
未修补的漏洞	22%
允许远程用户访问	20%
不安全的无线联网	20%
内部用户（意外）	18%
合作伙伴/供应链	18%
远程访问工具	18%
内部用户（故意）	17%
物联网设备	17%
其他	0%
以上都不是我组织的网络安全风险	0%
不知道	0%

您认为谁/什么是您组织的前三大网络安全风险?排名第一、第二和第三的回答组合 (n=3,000)

警报调查的不同方法

组织调查 **48% 的安全警报**以识别是否是恶意活动迹象

防御者的一个挑战是识别要调查的警报，以及如何运用有限资源发挥最好的效果。

平均来说，所有安全警报的不到一半 (48%) 得到调查以识别是否是恶意活动迹象，而在 3,001-5,000 名员工的组织中上升到 54%。但是，不同方法存在巨大差异：16% 的组织调查四分之三以上的警报（包括 5% 回报有调查所有警报），而 18% 调查四分之一或更少。

从行业来说，中央/联邦政府调查警报比例最低 (39%) (n=89)；而能源、石油/天然气和公用设施行业调查比例最高 (55%) (n=69)。

侦测、调查和响应开销

对于 100-3,000 名员工的组织，侦测、调查和响应警报的时间中位数为 9 小时；对于 3,001-5,000 名员工的组织则为 15 小时，很可能反映了操作环境的复杂程度增加。

调查揭示了不同行业的显著不同，生产制造（15 小时）和能源、石油/天然气和公用设施（18 小时）的组织用时是 IT、技术和电信（6.75 小时）的一倍。

务必注意，大多数警报不会移到响应阶段。大多数攻击将通过安全技术主动拦截，少数警报进行分类进而调查。响应操作还将根据需要修复的事件性质而显著不同，从删除用户收件箱的网络钓鱼电子邮件，到重建整个服务器集群。

侦测、调查和响应警报的时间中位数

活动	100-3,000 名员工 (n=2,460)	3,001-5,000 名员工 (n=350)	IT、技术和电信 (n=98)	生产制造 (n=331)	能源、石油/天然气和公用设施 (n=66)
侦测	3 小时	3 小时	1.5 小时	3 小时	6 小时
调查	3 小时	6 小时	2.25 小时	6 小时	6 小时
响应	3 小时	6 小时	3 小时	6 小时	6 小时
总计	**9 小时**	**15 小时**	**6.75 小时**	**15 小时**	**18 小时**

您的组织侦测、调查以及（必要时）修复潜在事件用多长时间？
（n=2,812 名内部调查警报的受访者）

组织缺乏基本安全操作技能

正如已经看到的，IT 专业人员将缺乏内部网络安全技能/专业知识视为 2023 最大安全风险之一。更深入挖掘，调查表明，大多数组织艰难应对每日核心安全操作任务的实现，93% 将以下至少一个活动评为“具有挑战性”：

- 从杂讯中发现信号（71% 认为具有挑战性）
- 排定需要调查的信号/警报的优先级（71% 认为具有挑战性）
- 获得足够数据以确定信号是良性还是恶性（71% 认为具有挑战性）
- 及时修复恶意警报或事件（71% 认为具有挑战性）
- 确定事件的根本原因（75% 认为具有挑战性）
- 保留准确的调查记录（68% 认为具有挑战性）

93%
认为安全操作具有挑战性

75%
认为难以确定事件的根本原因

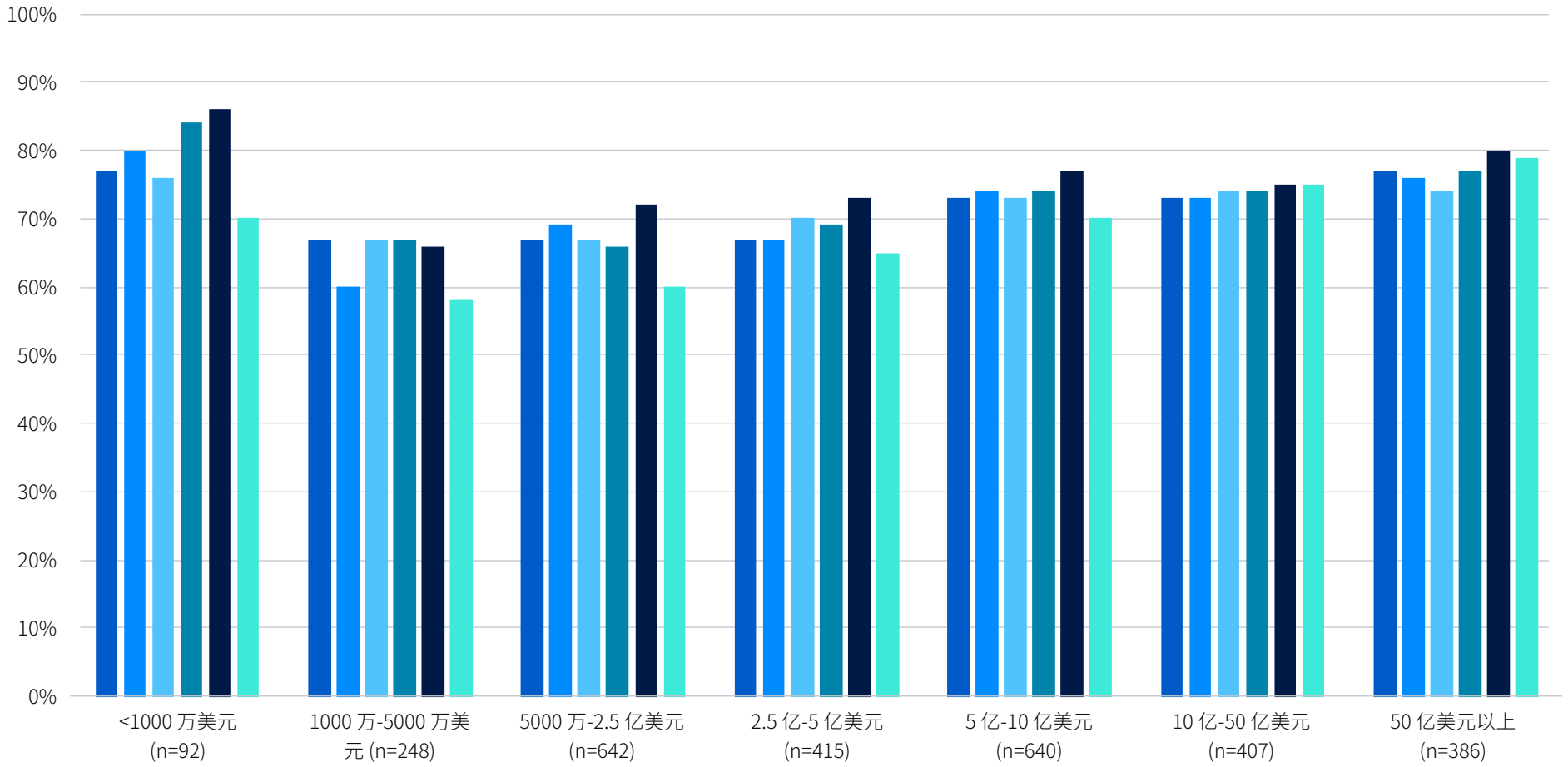
71%
难以识别要调查的警报

确定事件的根本原因是最广泛的问题，75% 的受访者称具有挑战性。

年收入最低（1000 万美元以下）的组织最可能认为安全运行任务具有挑战性，之后是年收入最高（50 亿美元以上）的组织。这两极将面临不同的障碍，组织和系统复杂程度可能在更大规模的组织中起到更大作用。

技能不足带来了多米诺骨牌效应：调查警报需要更长时间，反过来减少团队能力，增加风险暴露。

按收入划分认为安全操作任务“具有挑战性”的组织



组织在调查可疑警报时认为安全操作任务“非常有挑战性”或“有些挑战性”的受访者（n=2,812 名在内部调查安全警报的受访者）

- 从杂讯中识别信号，即了解要调查的信号/警报
- 优先排定要调查的信号/警报
- 获得足够数据以确定信号是良性还是恶性
- 识别事件的根本原因，即攻击敌手如何进入组织
- 及时修复恶意警报或事件
- 保留准确的调查记录

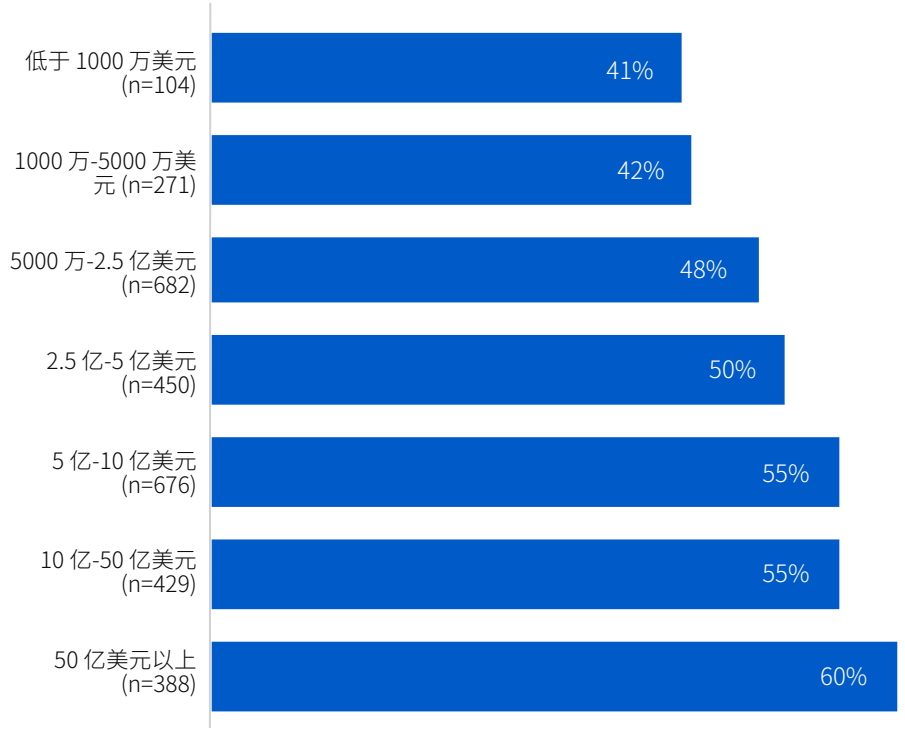
攻击敌手已经超前了防御者

52%
表示网络威胁现在过于复杂，组织无法自行处理

超过一半 (52%) 的 IT 专业人员表示，网络威胁现在过于复杂，组织无法自行处理，而在小型企业 (100-250 名员工) 中则上升到 64%。

随着组织收入增加，内部团队无法跟上脚步。这很可能反映了更高收入组织的内部网络安全环境的复杂程度更高，引入专业安全服务的可能性更大。这还反映出对威胁环境以及防御高级威胁的挑战的理解更为深刻。

网络威胁现在过于复杂，组织无法自行处理



您对下面说法的赞同或不赞同程度如何：网络威胁过于复杂，我们的组织无法自行处理？强烈同意，有些同意（基数在图中）

业务影响

程序交付影响

64%
希望 IT 团队花更多时间处理战略问题，花更少时间处理紧急事件

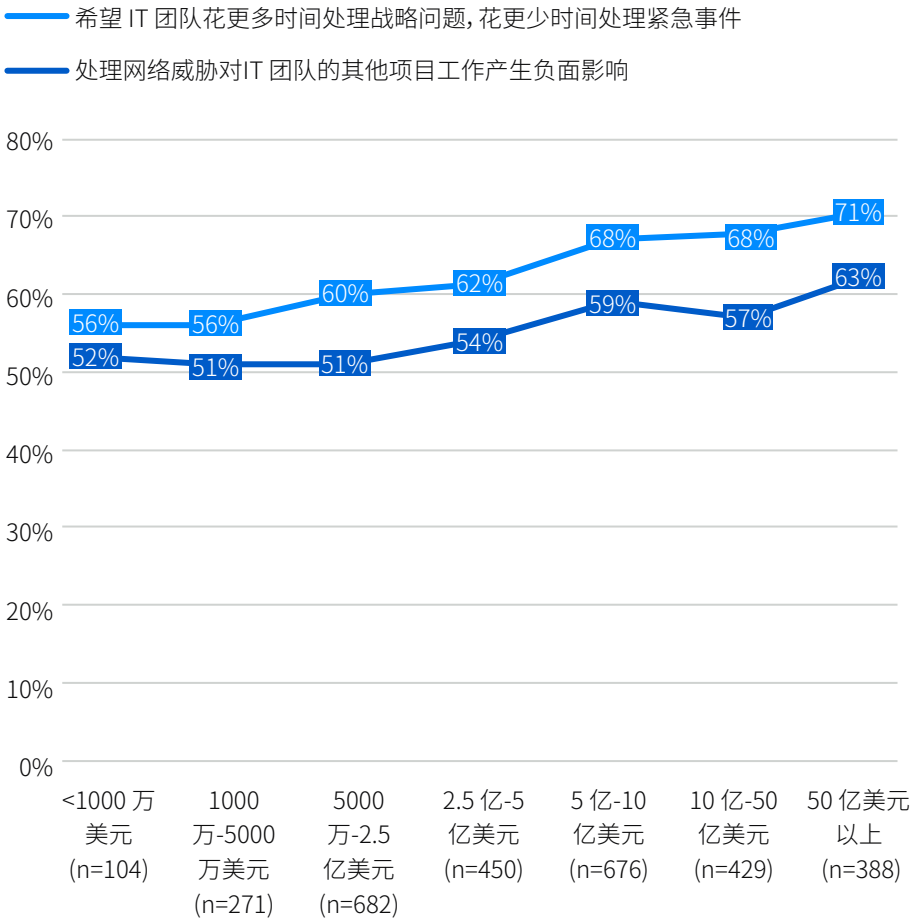
55%
表示处理网络威胁对IT 团队的其他项目工作产生负面影响

对于 60% 的组织来说，网络安全和更广泛 IT 功能关联非常密切：52% 在 IT 团队内有一支网络安全团队，8% 的 IT 团队管理其网络安全。剩余 40% 有单独网络安全和 IT 团队。网络安全需要的时间和工作量对 IT 组织具有重大影响。

超过一半 (55%) 组织表示，应对网络威胁对IT 团队在其他项目上的工作产生负面影响，当中收入最高的组织报告的影响最大。

网络安全紧迫而不可预测的性质还影响以业务为焦点的工作：平均 64% 希望 IT 团队花更多时间处理战略问题，花更少时间处理紧急事件。同样，随着收入增加，对更大范围程序交付的影响也增加。

网络安全对IT 程序交付产生负面影响



您对下面说法的赞同或不赞同程度：处理网络安全事件对IT 团队在其他项目的工作产生负面影响，我希望 IT 团队花更多时间处理战略问题，花更少时间处理紧急事件（基数在图中）

财务影响

具有挑战性的网络安全环境对组织造成多个财务影响。最大的成本发生在重大网络事件中。正如 2022 年 Sophos 勒索软件现状报告所指出的，平均勒索软件修复费用高达 140 万美元。

但是，应对网络攻击的财务影响不局限于清理费用。美国 IT 安全专家的平均工资目前差不多达每年 100,000 美元[2]，每次安全警报调查的每小时资源成本非常高。虽然工资根据当地条件而不同，但长时间事件调查过程的财务影响仍然可观。

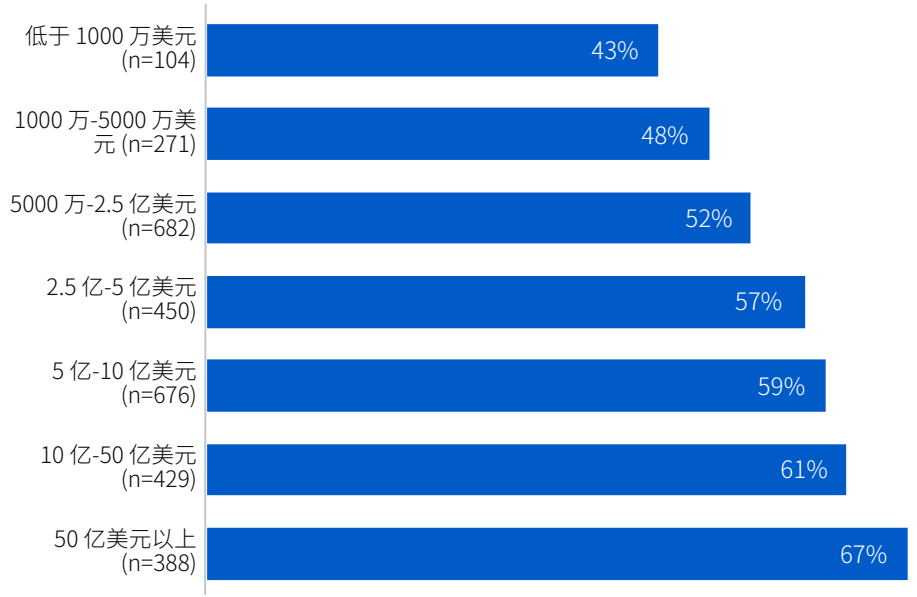
团队影响

57% 的受访者表示，因担心组织受网络攻击有时候让他们彻夜难眠。考虑到招聘和挽留该领域员工的高成本，这是福利和经济顾虑的双重原因。此外还表示，防御者对他们的安全工具没有完全信心。

耗尽是网络安全的一个重要问题。过多警报和过多任务给员工带来巨大压力。压力过大的团队更有可能错过重要信号，进一步加剧压力。最终，人会崩溃。

网络安全担忧让人失眠的可能性随着组织收入增加而稳步增长，年收入不到 1000 万美元的组织为 43%，50 亿美元以上组织则达到 67%。

表示担心组织受网络攻击有时候让他们彻夜难眠的受访者比例



您对下面说法的赞同或不赞同程度：担心组织受到网络安全攻击有时候让我彻夜难眠（基数在图中）

2 根据 2023 年 3 月的 IT 安全专家平均工资，https://www.indeed.com/career/it-security-specialist/salaries

建议

解决这一局面需要直接的三步骤方法：采取更加可缩放的事件响应流程以加速响应时间；利用适应性防御以减慢攻击敌手；创造良性循环以改进防护和降低成本。

这里可以用到“竖起盾牌”类比。阻止先进而持续的攻击敌手需要组织优化防御效力（“盾牌”），包括可以根据情况提升防护水平的环境感知技术。关键在于，他们还需要利用防御争取到的时间，运用人的专业知识解决根本原因。

强大的盾牌至关重要

网络安全技术的质量无比重要，安全控制应该：

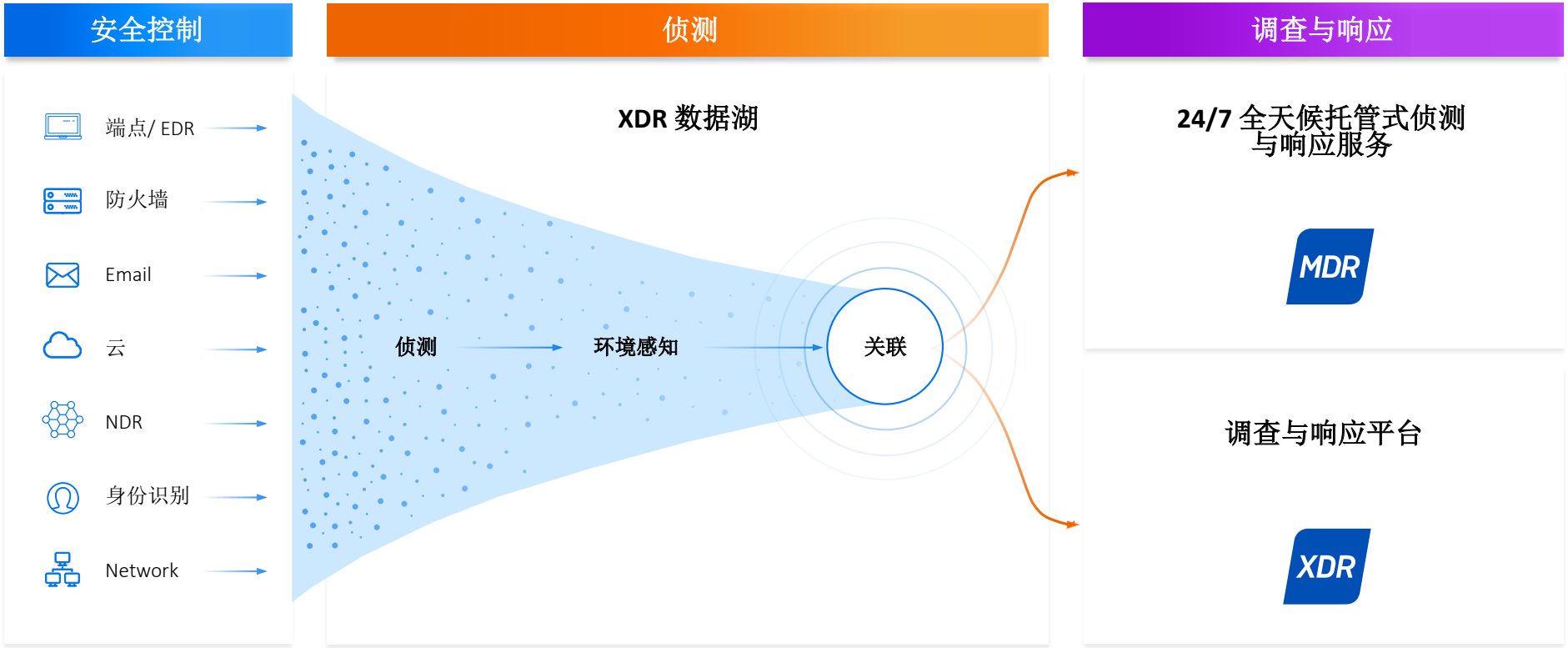
- **优化防御，**在攻击链早期自动侦测和阻止尽可能多的威胁。这样做，可以减少组织的风险，同时释放防御者以集中于更少的事件。
- **减少暴露，**通过确保安全投资正确最优部署，避免配置错误问题来更易实现。
- **打断攻击敌手。**自动侦测和攻击敌手活动的技术令攻击者受挫，同时为防御者争取到时间来消除事件。

借助人和技术解决根本原因

盾牌为防御者争取到宝贵时间，调查并响应攻击。但这无法确保 100% 防御，所以耗时长、信息充分、正确执行的根本原因修复非常重要。

研究表明，攻击敌手不会采取单一路径。利用安全环境的遥测，运用组织已有的安全控制，使防御者能够更快发现和响应威胁，同时增加现有投资回报。

在良性警报中找到恶意活动往往就像大海捞针。通过加入环境深入信息并关联相关警报的扩展式侦测与响应 (XDR) 平台处理信号，使内部防御者能够快速聚焦重要内容。内部团队可以通过 XDR 平台执行调查和响应。或者，组织可以将侦测、调查和响应工作外包给专业托管式侦测与响应 (MDR) 服务。



加快防御者的脚步

当飞轮开始高速转动时，会保持转动下去。飞轮背后的力越大，转动越快。组织可以结合安全技术和人的专业技术，加快网络安全的脚步。全面的安全控制减少防御者需要处理的警报数量，让他们可以集中精力消除攻击和提升安全状态。反过来，这提高安全控制的效力，创造良性的循环。

大多数组织计划采用需要的安全控制和服务

调查表明，大多数组织计划在未来 12 个月内将威胁侦测与响应解决方案加入其安全方案组合。超过四分之三 (78%) 计划在未来一年加入端点侦测与响应 (EDR) 和/或扩展式侦测与响应 (XDR) 工具。

调查和响应复杂网络威胁是一项专业技能，要提供 24/7 全天候覆盖需要至少 5 或 6 个人。缺乏内部网络安全技能/专业知识是 2023 年前三个网络风险之一，许多组织寻找外部专家的支持：44% 的组织计划在未来 12 个月开始与托管式侦测与响应 (MDR) 供应商合作。

计划在未来 12 个月采用侦测与响应解决方案的组织比例

Sophos 可以帮助

Sophos 提供帮助组织加快防御者脚步并领先攻击敌手的服务和技术。我们帮助超过 550,000 家组织防御最复杂的威胁，而Sophos MDR 是全球最受信任的 MDR 服务。

从最强的盾牌开始

我们的端点/EDR、防火墙、电子邮件、网络和云解决方案减慢攻击者，为防御者带来响应需要的时间和信息：

- **优化防御：**Sophos 将 99.98% 的威胁自动拦截在大门外，减少风险，使防御者可以专注于需要人为干预的更少事件。
- **减少暴露：**从第一天起自动部署最优防护设置，消除安全漏洞。内置帐户运行状况检查找出所缺少的软件和配置问题，其可能导致可以避免的感染。
- **打断攻击敌手。**适应性主动对手防护在侦测到“人为键盘”端点入侵时立刻激活更高防御，令攻击者受挫，为防御者争取响应时间。

优化侦测、调查和响应

防御者发现的越多，行动就越快。Sophos 使用整个安全环境的侦测，整合 Sophos 和第三方安全控制的遥测信息来加快侦测和响应，增加现有安全投资回报。

Sophos MDR 服务汇集超过 500 名专家，代表您全天候追踪、调查和响应攻击敌手及其他攻击。平均威胁响应时间仅 38 分钟，Sophos MDR 比内部团队平均时间快得多。或者，组织可以使用 Sophos XDR 平台，包含全部 EDR 功能，直接或与 Sophos MDR 团队协作调查和响应攻击。

无论您的组织处于什么阶段，未来想达到什么水平，Sophos 都可以帮助您加快防御者脚步，领先现在的先进攻击敌手。有关更多信息，请访问 www.sophos.com 或联系安全顾问。

通过 Sophos 实现最优网络安全成果

2023-03-29 (WP-NP)

SOPHOS