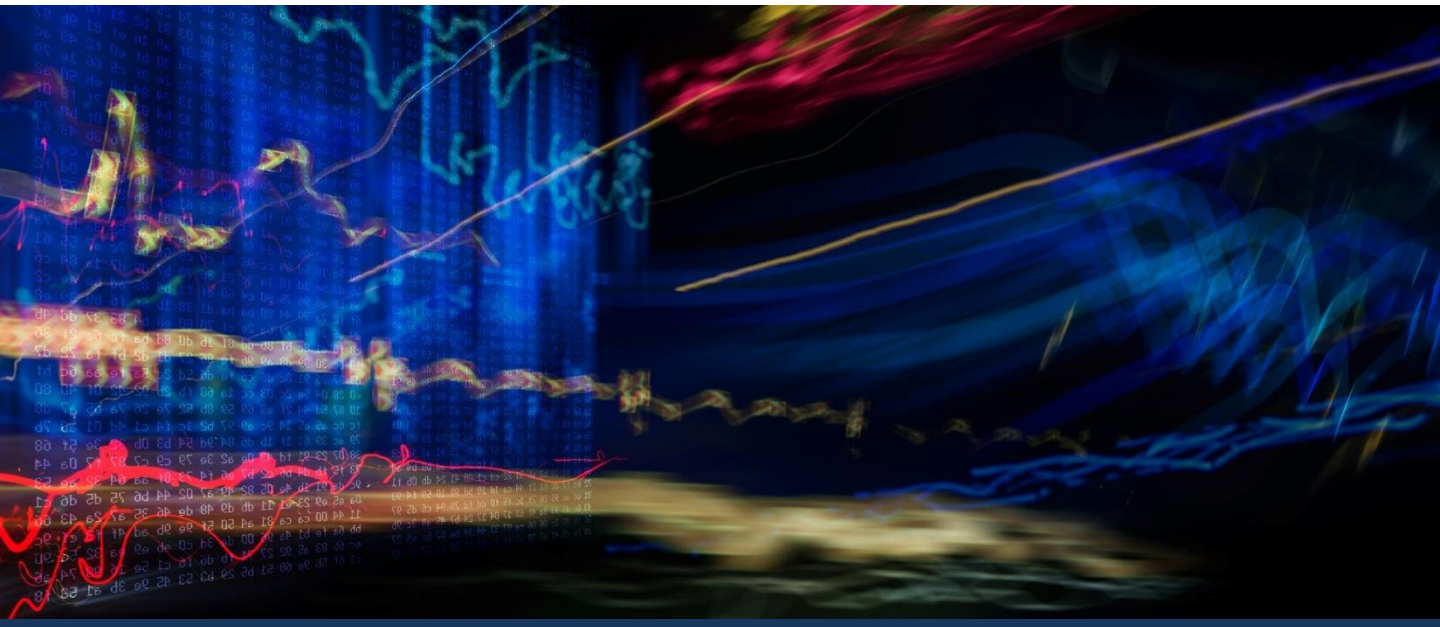


网络安全监控趋势

ESG 资深首席分析师 **Jon Oltsik**，

2016 年 8 月

目录

执行摘要

2016 年，思科系统公司委托 Enterprise Strategy Group (ESG) 对 200 名了解或负责其组织内网络安全和安全分析的 IT 及网络安全专业人员进行调查研究。74% 的受访者声称他们直接参与购买网络安全产品，而其余 26% 的受访者表示他们能够影响网络安全产品的采购。

调查受访者位于北美地区，来自不同规模的公司：25% 的受访者就职于员工数量达到 3000-4999 人的组织，31% 的受访者就职于员工数量达到 5000-9999 人的组织，18% 的受访者效力于员工数量达到 10000-19999 人的组织，27% 的受访者为拥有 20000 名及以上员工的组织工作。受访者包括来自各个行业和政府部门的人员，参与人次最多的行业包括制造业 (19%)、金融服务业（银行、证券、保险等）(13%)、信息技术业 (12%)、医疗卫生业 (11%) 和零售/批发业 (11%)。注意：由于四舍五入的原因，本报告所含数字的总计可能不会达到 100%。

该研究项目旨在评估当前大家在实施与人员、流程和技术相关的网络安全监控时采取的做法和遇到的难题。此外，受访者还被问及他们未来将采取何种战略规划不断增强网络安全监控实践。根据收集到的数据，本文得出了以下结论：

大家已充分理解网络安全遥测技术的价值。调查受访者表示，他们将网络安全监控运用于各种情景中，其中包括“搜寻”恶意活动、检测安全漏洞及自动执行补救任务。网络安全专业人员也意识到，网络安全监控的成功取决于安全团队与网络运营团队之间的奋力合作，并认识到未来的网络安全监控工作必须扩展到云。总而言之，网络安全专业人员似乎能够意识到网络安全监控的价值，并对如何提高网络安全性有明确的想法。

大型组织会收集大量网络安全数据，并对其进行处理和分析。要实现网络安全监控，就必须大量地收集、处理和分析数据源（包括防火墙日志、VPN 日志、来自网络设备的日志和代理日志）。通常，网络安全监控数据可在线保留 60 天以上，并且 10% 的组织会将这些数据在线保留一年或更长时间。这些数据的总量是非常大的，如果要实现它们的价值，就必须使数据形成结构，并对其进行有效整理。

网络安全监控实践仍然问题重重。大多数 (72%) 组织认为，过去两年里，由于恶意软件数量、网络流量以及恶意软件复杂性的增加等种种原因，导致攻击者能够避开传统的网络安全控制实施攻击，从而使网络安全监控变得越来越困难。更糟糕的是，大型组织还报告了一些网络安全监控挑战，其中包括网络盲点、网络安全团队与网络运营团队之间的沟通问题以及及时数据收集相关的问题。鉴于这一系列问题，在某些情况下，网络安全监控并不像预期的那样有效或高效。

CISO 为未来几年制定了积极的网络安全监控计划。绝大多数 (91%) 组织计划在未来两年内增加网络安全监控方面的开支。此外，CISO 还制定了大量网络安全监控计划，其中包括加强网络安全培训、将网络安全监控与其他网络和安全技术相集成，以及投资新的网络安全监控工具。

基于此项目中收集和分析的研究数据，ESG 认为网络安全监控正处于转型期间。大型组织必须转向用于集成并提供内置情报的网络安全监控架构。

网络安全监控情景分析

ESG 研究结果显示，80% 的调查受访者表示，网络安全监控对其组织的整体网络安全战略至关重要，而 17% 的调查受访者表示，网络安全监控对其组织的整体网络安全战略非常重要（但并不至关重要）。为什么网络安全监控如此重要？因为它是许多用例和目标不可或缺的一部分。例如，42% 的受访者表示，他们最重要的网络安全监控目标是主动查询网络或“搜寻”可疑行为，35% 的受访者使用网络安全监控来检测安全漏洞，34% 的受访者的目标是使用基于网络的威胁检测自动执行补救任务（见图 1）。鉴于以上各种安全用例，网络安全监控可以说是网络安全的基础技术。

图 1

最重要的网络安全监控目标

关于通过监控网络活动来实现安全，您认为对您的组织来说，下列哪项是最重要的目标？（受访者百分比，N=200，可选三项）

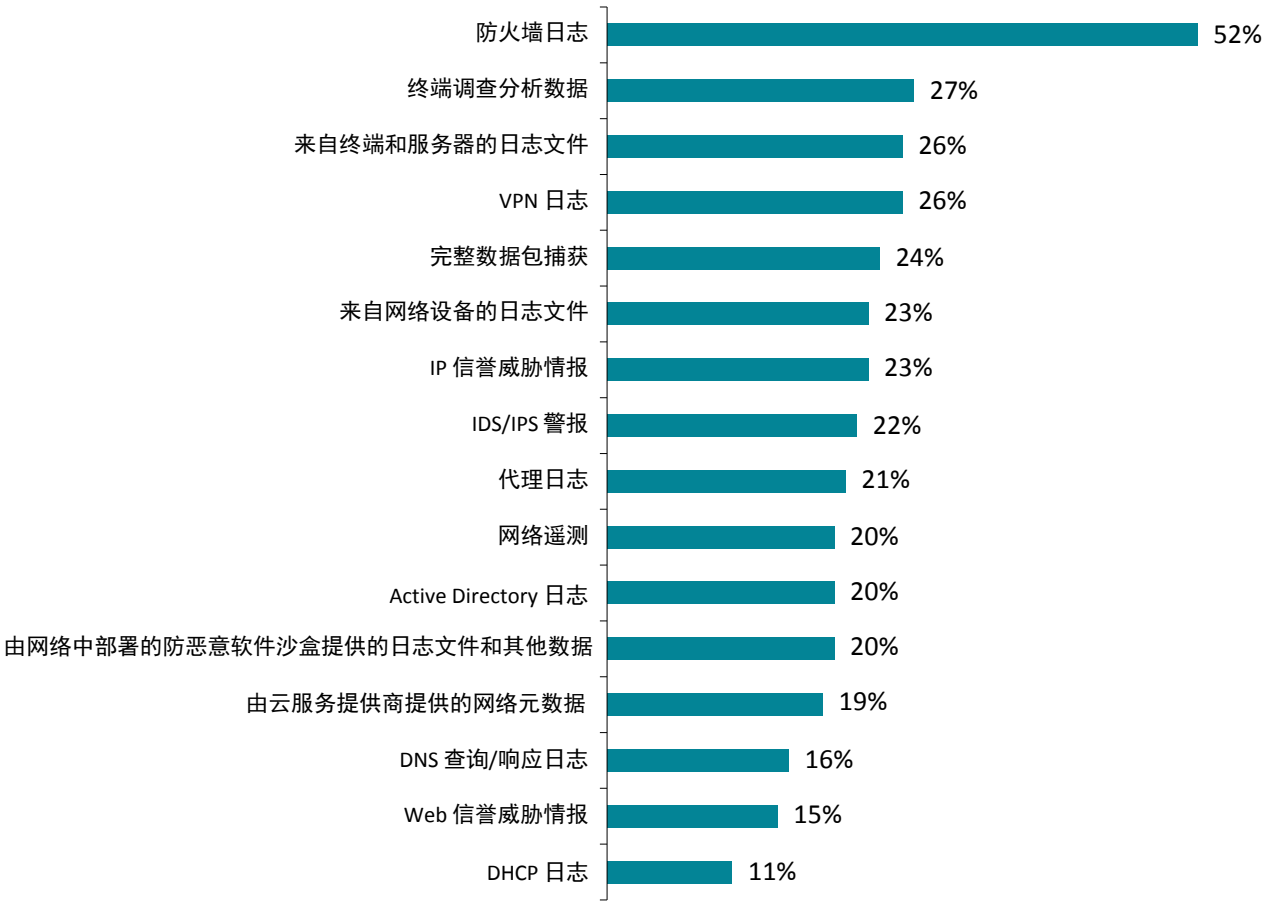
ESG 数据还显示，网络安全监控涵盖了许多有助于检测和响应异常网络行为的技术。当被问及哪种技术发挥的作用最大时，超过一半 (52%) 的受访者表示是防火墙日志，27% 的受访者认为是终端调查分析数据，另外 26% 的受访者认为是来自终端和服务器的日志数据。此处还值得一提的是网络监控的作用 - 24% 的受访者指出是完整数据包捕获，而 20% 的受访者提到网络遥测数据（见图 2）。71% 的组织将网络安全监控数据在线保留 60 天或更长时间，而 10% 的组织将数据在线保留一年以上。此外，25% 的组织认为，将网络安全监控数据在线保留更长的时间会很有益处。

鉴于不同组织的不同做法，大型组织应寻找可以收集、处理和分析来自众多数据源的数据的网络安全监控技术。此外，CISO 还希望与此类网络安全监控供应商合作：他们具有成熟的生态系统，能够与业界合作伙伴进行协调，并将不同的工具整合到集成网络安全解决方案中。

图 2

最重要的网络监控数据源

在您的组织目前收集的所有网络监控数据源中，哪些最能帮助您的组织检测并响应正在发生的异常网络行为和/或网络攻击？（受访者比例，N=200，可选多项）



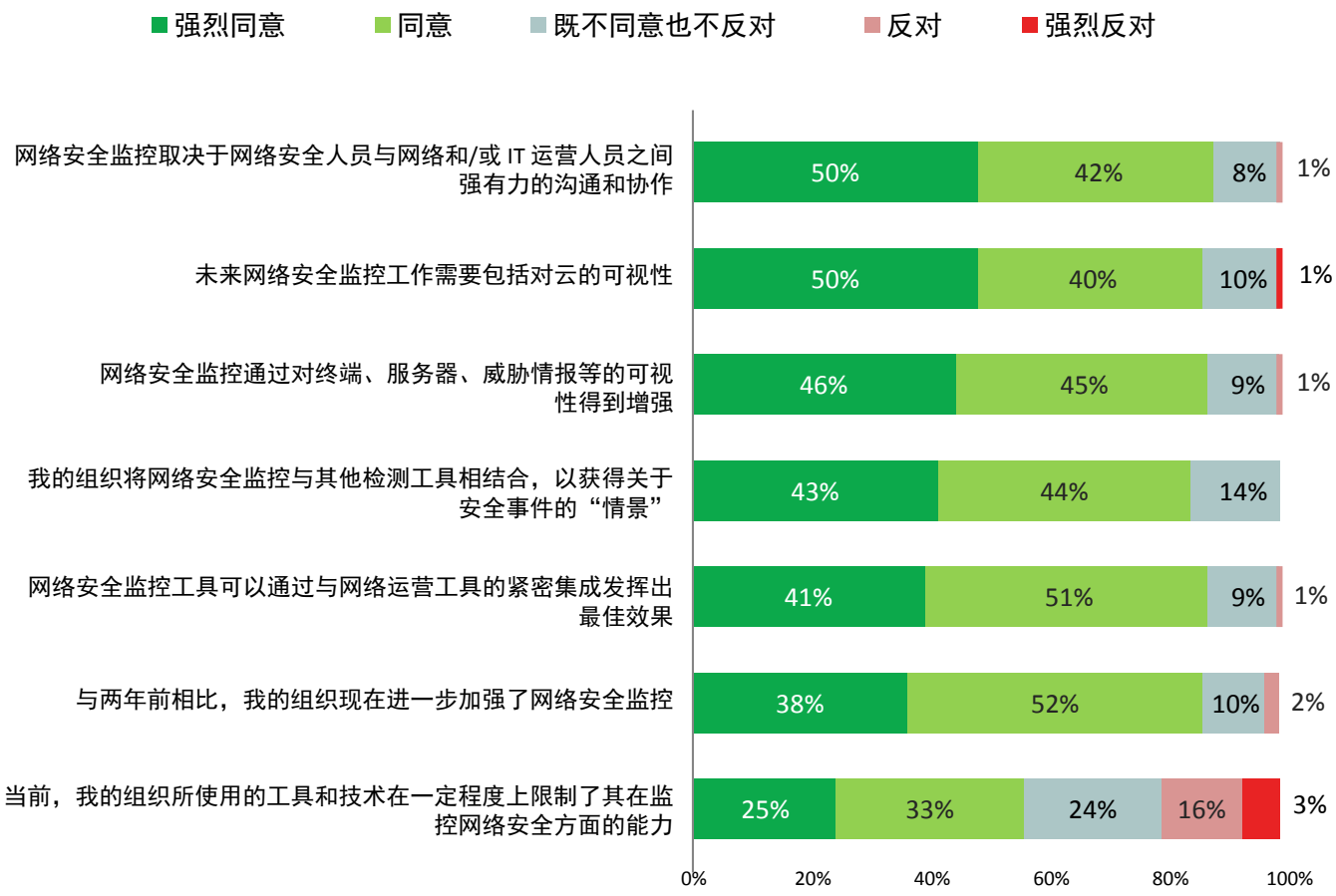
ESG 发现，网络安全和 IT 专业人员受访者对网络安全监控技术和其组织的整体网络安全监控状况持有一些强烈的意见（见图 3）。例如：

92% 的受访者强烈同意或同意，网络安全监控取决于网络安全人员与网络和/或 IT 运营人员之间强有力的沟通和协作。这反映了要实现成功的事件响应 (IR)，负责检测安全问题的小组（即安全分析师、调查分析员、SOC 人员等）就必须与负责通过实际技术补救问题的小组（即 IT/网络管理员、网络运营人员等）之间建立有效的工作关系。有鉴于此，网络安全监控工具应同时满足安全团队和网络运营团队的各种要求。

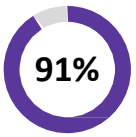
图 3

对于网络安全监控的意见

请在每行中选出一个最能体现您对每项表述的意见的答案。（受访者百分比，N=200）



90% 的受访者强烈同意或同意，未来网络安全监控需要包括对云的可视性。这也是有道理的，因为越来越多的 IT 工作负载和应用正在转向公共云和私有云。网络安全监控工具和流程必须利用对云基础设施的全面可视性来适应这一现实。



91% 的受访者强烈同意或同意，网络安全监控通过对终端、服务器、威胁情报等的可视性得到增强。这一点（以及图3 中的其他点）强调了对“广泛的”网络安全监控视角的需要。换句话说，网络安全监控工具应使用多个数据源，随着安全事件不断演变和遍历网络及资产，提供这些事件的端到端视图。这种“广泛的”可视性应提供实时和历史调查所需的数据。

网络安全监控：至关重要但充满挑战

显然，网络安全监控是一项至关重要的网络安全规程，调查受访者对使网络安全监控工作取得成功所需的人员、流程和技术持有强烈的意见。遗憾的是，要让这些因素很好地协作并非总是件易事。事实上，26% 的调查受访者承认网络安全监控的难度在过去两年中大幅增加，而另外 46% 的受访者声称网络安全监控的难度在过去两年中略微增加。

为什么会出现这种情况？ESG 研究指出（见图 4）：

威胁形势。超过三分之一 (34%) 的受访者认为恶意软件数量的增加导致网络安全监控变得更加困难。27% 的受访者表示恶意软件的复杂性增加可能会导致攻击者避开传统的网络安全控制，从而使监控变得更加困难。26% 的受访者将监控难度的提高归因于可能避开传统控制的针对性攻击数量的增加。似乎可以肯定，大型组织正面临越来越多技术娴熟的网络攻击。

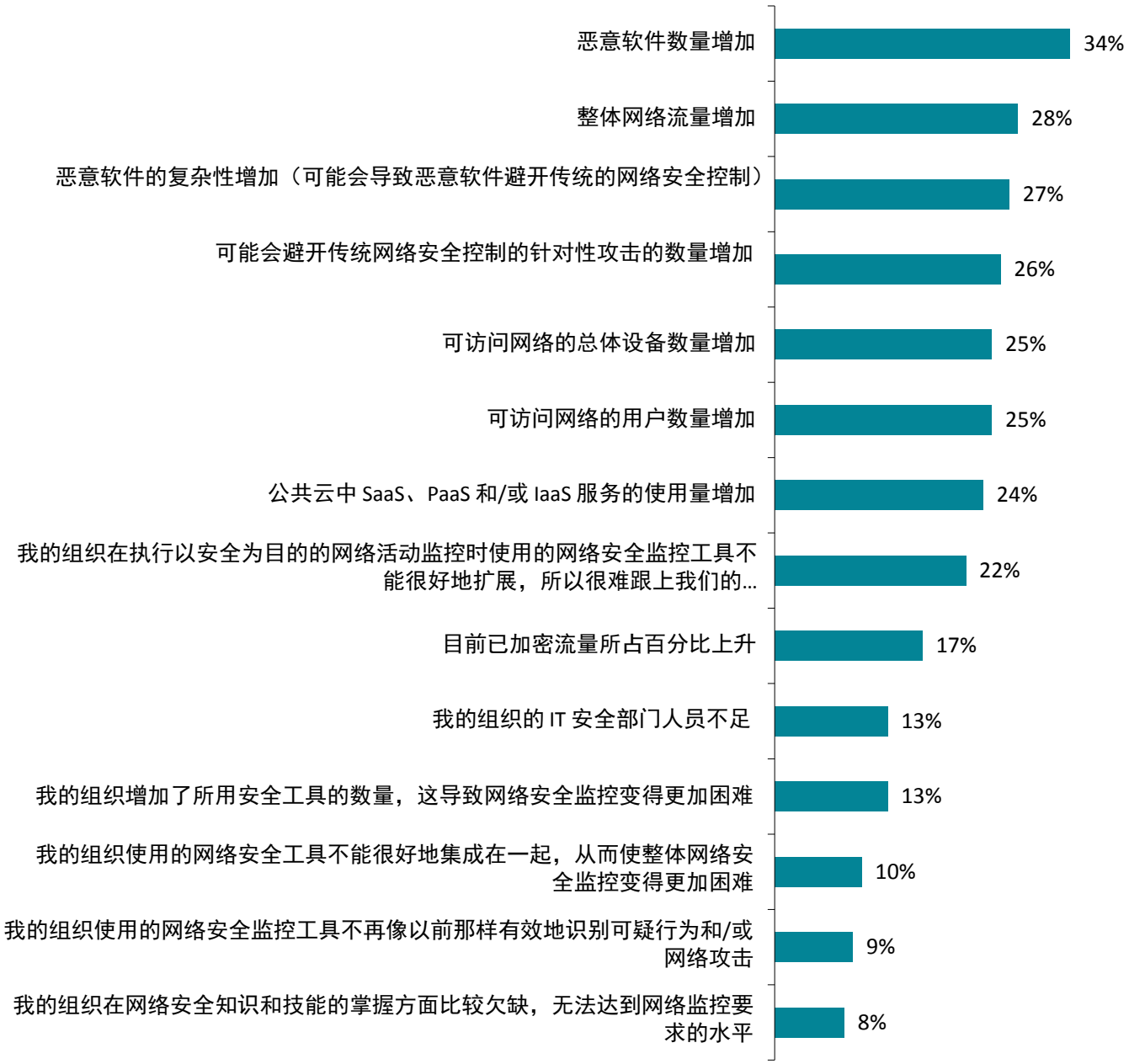
IT 复杂性。请注意，28% 的受访者认为给监控造成难题的是整体网络流量的增加，而 25% 的受访者认为是可访问网络的用户和设备数量的增加。此外，24% 的受访者表示，由于人们越来越多地在公共云中使用 IaaS、PaaS 和 SaaS，网络安全监控变得更加困难。

网络安全监控技术问题。22% 的受访者表示，他们的网络安全监控工具不能很好地扩展。这些工具无法对抗上述威胁形势和 IT 复杂性问题。

图 4

为什么网络安全监控变得愈发困难

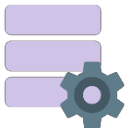
您刚才指出，过去两年来以安全为目的的网络活动监控变得更加困难。在您看来，以下哪些因素使得以安全为目的的网络活动监控变得更加困难？（受访者百分比，N=143，可选三项）



在外部威胁形势使网络安全监控变得更加困难的同时，大型组织还需应对那些促使网络安全监控复杂程度加剧的内部因素（见图 5）。这些挑战包括：

处理网络“盲点”。31% 的组织表示，他们在网络安全监控方面遇到的一大挑战是他们的网络中存在一个或多个盲点，他们对这些区域内的网络安全活动没有足够的可视性。这些盲点在何处？42% 的组织报告在监控网络上的非企业设备时存在盲点，39% 的组织报告在对用户行为进行监控时存在盲点，39% 的组织报告从企业网络流向合作伙伴网络的流量方面存在盲点，39% 的组织表示内部 Wi-Fi 网络上存在盲点。这些盲点给组织带来了一些负面影响，其中包括加剧 IT 风险、降低组织“搜寻”恶意活动的能力以及使组织无法检测到网络中某些区域内存在的恶意行为。

组织问题。29% 的组织承认他们的网络安全团队与网络运营团队之间存在一些沟通和流程问题，这可能会阻碍其网络安全监控能力。这一点很令人担忧，尤其是考虑到 92% 的调查受访者强烈同意或同意，网络安全监控取决于网络安全人员与网络和/或 IT 运营人员之间强有力的沟通和协作。



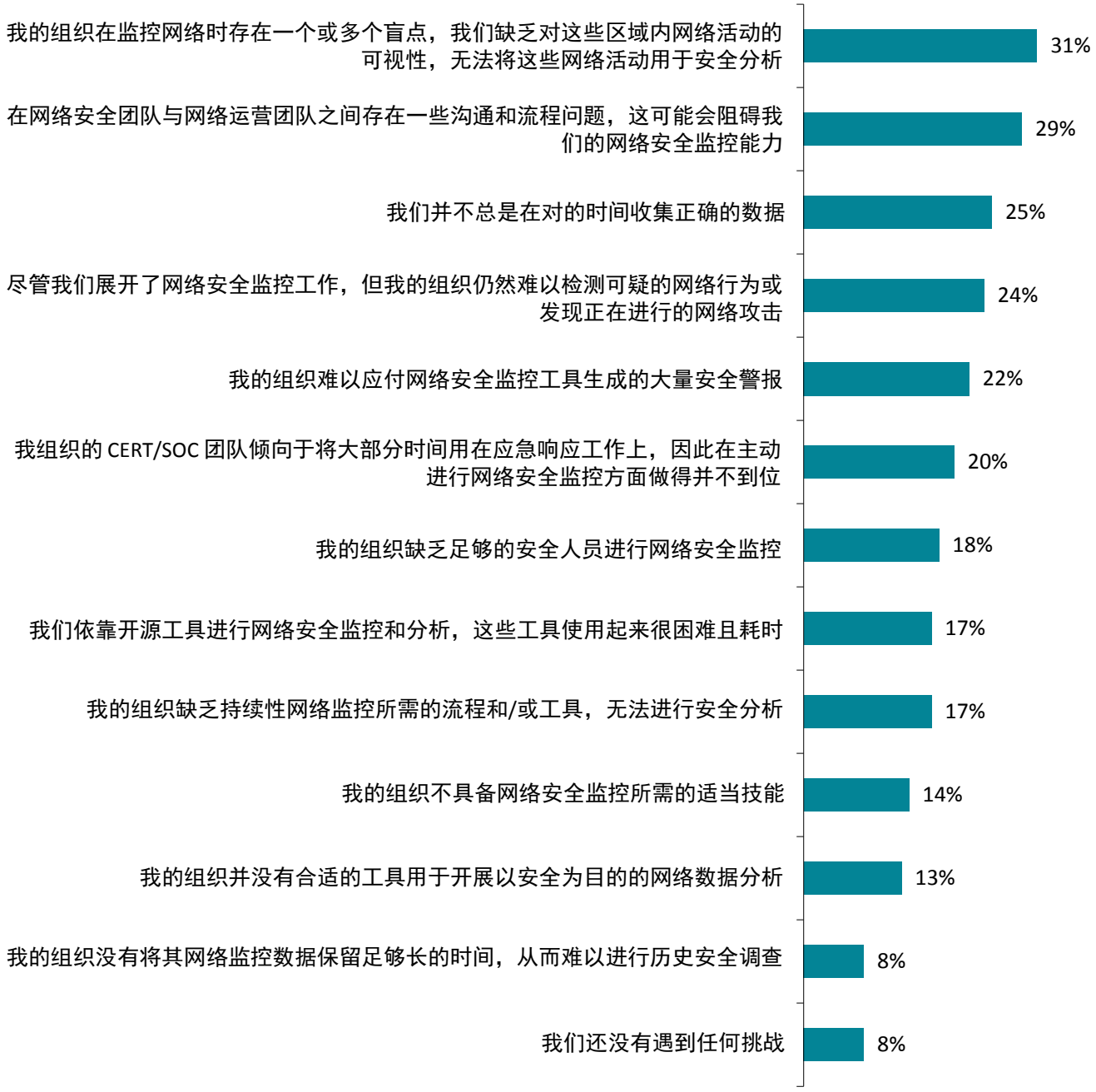
时间性挑战。四分之一 (25%) 的组织表示他们并不总是在对的时间收集正确的数据。这尤其令人不安，因为网络安全监控的目的即在于提供对网络攻击的实时检测。如果没有充足的数据，网络攻击者在网络上“驻留的时间”将延长，这可能会将一个小型安全事件发展为重大的数据泄露事件。

遗憾的是，24% 的调查受访者表示，尽管他们展开了网络安全监控工作，但其组织仍然难以检测可疑的网络行为或发现正在进行的网络攻击。大多数组织都认为网络安全监控对他们来说至关重要，但也有近四分之一的组织承认他们目前的网络安全监控工作效果不大。

图 5

网络安全监控挑战

就网络安全监控而言，您认为下列哪项对您的组织来说是最严峻的挑战？（受访者百分比，N=200，可选三项）



网络安全监控未来战略

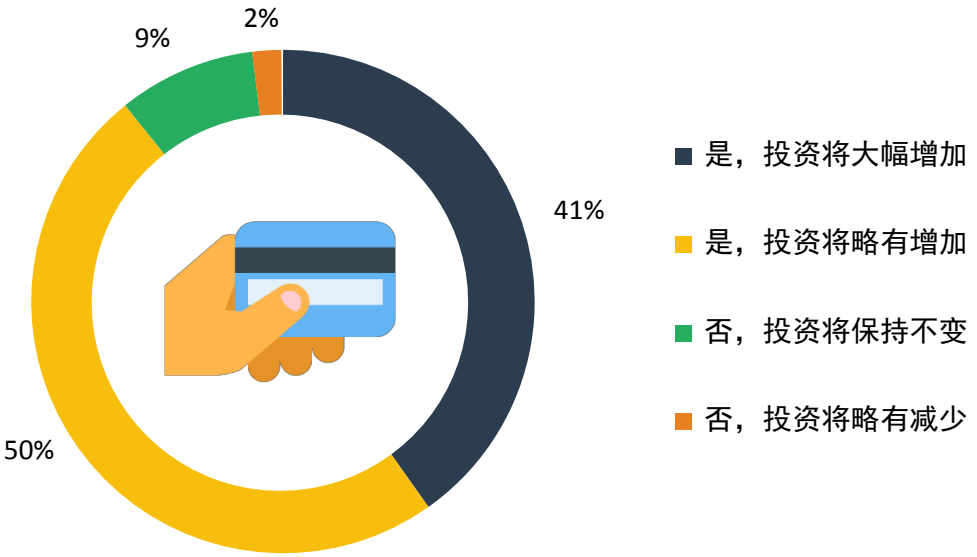
一方面，网络安全专业人员意识到网络安全监控至关重要，他们了解从人员、流程和技术角度来看需要做哪些工作。另一方面，网络安全监控变得越来越困难，且充满了挑战。

许多 CISO 似乎决意要处理这一情况（见图 6）- 41% 的组织表示，他们将在未来两年内大幅增加对网络安全监控的投资，而另有 50% 的组织表示他们会略微增加在这一方面的投资。基于上述薄弱环节和挑战，这些公司将很有可能对技术集成、全面的网络覆盖、增强型威胁检测等领域，以及有助于促进网络安全团队与网络运营团队之间协作与合作的工具进行投资。

图 6

网络安全监控投资

您认为在接下来的两年中您的组织是否会增加其在网络安全监控技术、培训和资源方面的投资？（受访者百分比，N=200）



除了询问有关预算的内容外，ESG 还要求调查受访者指出他们在网络安全监控方面的战略重点。此列表包括(见图 7)：

为现有员工提供更多关于网络安全监控的培训。作为该项目的一部分，ESG 研究还透露，59% 的组织表示轻度或严重缺乏具备坚实网络安全监控技能的人员。认识到这点不足后，许多 CISO 将加强对网络安全和网络运营人员的网络安全监控培训。

将网络监控/威胁检测与网络和安全运营工具集成。ESG 发现大家都对包括网络安全监控在内的所有领域的安全技术集成表现出一定的兴趣。在这种情况下，许多公司都希望将网络安全监控和威胁检测工具与其他技术（如 SIEM、NPM 和事件响应平台）相集成。

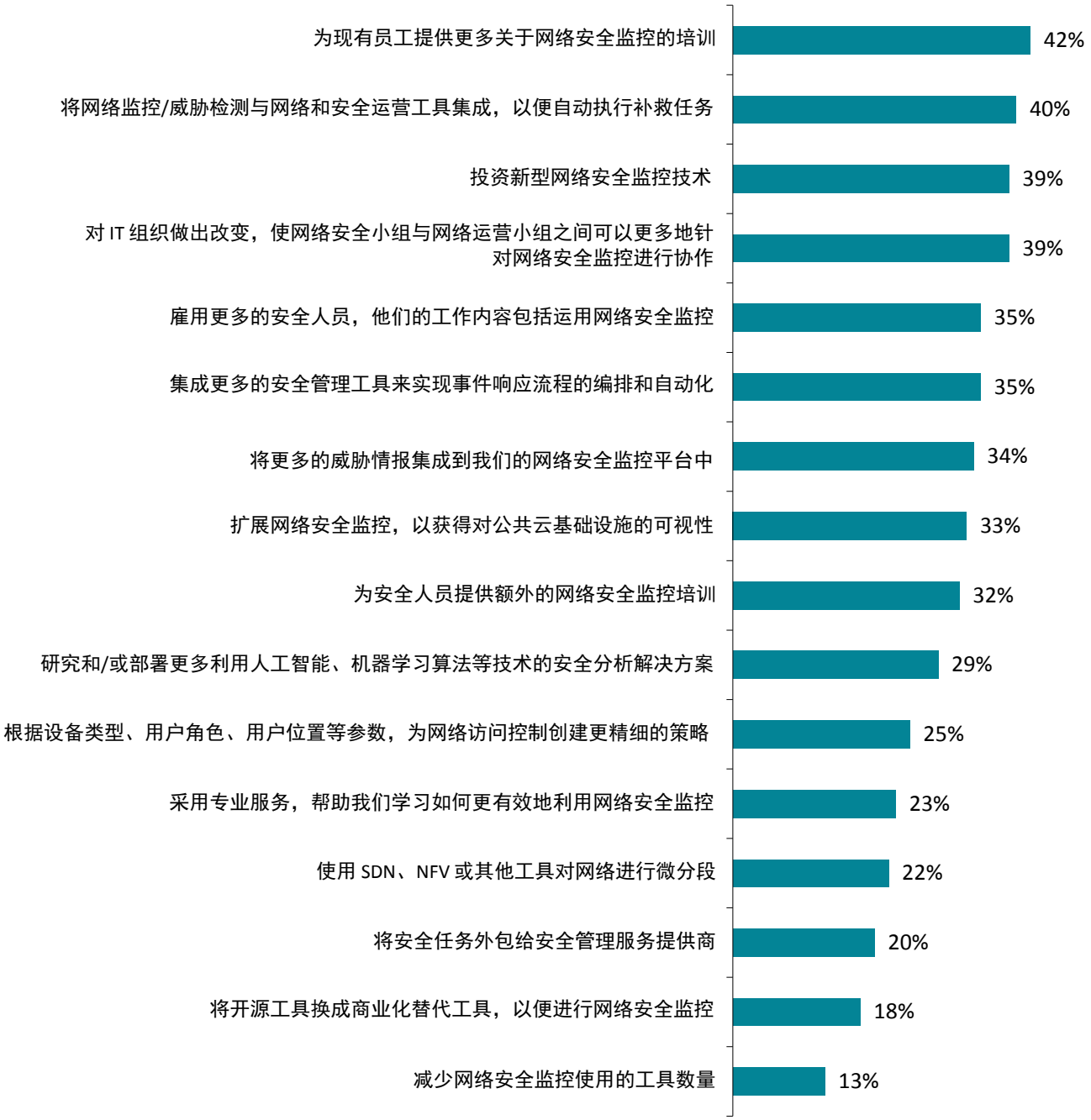
投资新型网络安全监控技术。根据本报告所提供的调查结果，大型组织需要具有可扩展性、易用性和情报分析的网络安全监控工具。CISO 准备投资这些类型的网络安全监控技术。

对 IT 组织做出改变以实现更多协作。如上所述，网络安全监控取决于网络安全团队与网络运营团队之间的共同协作。ESG 研究表明，组织愿意改变组织结构，以促进这种协作。

图 7

网络安全监控的战略计划

您的组织计划在未来 12 至 24 个月内实施以下哪些活动？（受访者比例，N=200，可选多项）



更重要的事实

ESG 研究显示形势较为危险。大家固然都明白网络安全监控的重要性，但网络安全专业人员对如何成功地进行网络安全监控持有着强烈的意见。然而，许多组织并没有采纳他们的建议，导致网络安全监控的工作效果不尽人意。

令人高兴的是，大多数组织了解到这一困境，计划增加网络安全监控开支，并为未来制定更全面的战略。大型组织在着眼于加强网络安全监控时应该：

清楚地意识到网络安全监控与 SIEM 之间的差异，并对两者进行投资。令人惊讶的是，人们对于何时何地使用 SIEM 以及网络安全监控仍然存在一些混淆。这多少是可以理解的，因为 SIEM 在过去十年中一直用于安全分析。然而，鉴于当今的威胁形势，SIEM 应通过其他类型的分析（包括网络安全监控）进行增强。在理想情况下，这两种技术相辅相成，SIEM 专注于事件关联、规则和控制面板，而网络安全监控用于监控流量、连接和基于数据包的内容。安全团队应先清楚地了解每种技术、各自的角色和它们的共同价值，再进行接下来的工作。

让网络运营团队参与进来。虽然网络安全监控技术可能由网络安全团队购买和运营，但也要让网络运营团队参与到相关工作中，例如需求定义、试验项目和升级流程等，这点非常重要。目的是什么？建立这两个团队将共用的共同网络安全监控基础。这样有助于缓解本报告中所披露的沟通/协作问题，同时帮助这两个团队达成各自的目的和目标。这还有助于将网络安全监控转变为策略，并实施到精细网络分段和用户/设备访问控制等领域中。

力争集成。正如 ESG 研究明确显示的那样，网络安全监控的成功高度取决于与其他技术（如终端安全监控、SIEM、威胁管理和威胁情报）的多点集成。还有一点也很重要，即寻找机会集成网络安全监控和网络设备以实现分段和访问控制。这将有助于为安全分析提供全面的视角。

考虑易用性和自动化。由 ESG 于今年早些时候开展的一项研究表明，46% 的组织声称存在网络安全技能短缺问题。[1]遗憾的是，这意味着网络安全组织可能没有足够的人员或时间有效地使用网络安全监控技术。有鉴于此，CISO 应在所有网络安全监控决策中强调易用性。例如，网络安全监控工具应易于安装，并能满足初级安全分析师、经验丰富的调查分析员以及网络运营人员的需求。要解决技能短缺问题，网络安全监控技术还应该能够实现流程和操作的自动化，从而减轻当前需要手动操作的任务。

平衡可视性与实施性。为了支持自动化，网络安全监控应与安全控制本身紧密配合。当网络安全监控工具检测到威胁或漏洞时，它们应该能够使用和修改各种安全控制。例如，当网络安全监控检测到高度可疑的连接时，它应该能够使用网络安全控制来隔离系统、终止连接或创建新的防火墙规则。要实现这些类型的功能，就要依靠上文中所介绍的紧密集成。

[1]来源：ESG 研究报告，*2016 IT Spending Intentions Survey*，2016 年 2 月。