网络安全特别报告

中小企业

小而弥坚

中小企业如何加强防御能力，抵挡当今威胁

CISCO

53% 的中型企业曾遭遇安全攻击

高达

5000 个

平均安全警报数量达到 5000 个

中型企业调查的安全警报仅占所有警报的 55.6%

29% 的中型企业表示，安全攻击导致的损失在 10 万美元以下。20% 的企业表示损失达到 1,000,000-2,499,999 美元

许多中小企业亟需像大型企业一样，实施更加高效的网络安全实践。

中小企业 (SMB) 活力十足，已然成为业界创新的支柱和奋进的典范。与其他更具规模的企业相比，他们行动更敏捷，也更具拼搏精神，但也面临着一样严峻的网络威胁。

面对当今的网络威胁形势，所有组织无论大小，都面临着遭到攻击的风险。越来越多的攻击开始将目标瞄准中小企业[1]，而且通常将其作为开展更大规模攻击的跳板。攻击者认为，中小企业安全基础设施和安全实践不够成熟，而且缺乏足够的专业人员来管理和响应威胁，因此更容易被攻破。[1]

许多中小企业才刚刚意识到自己对网络犯罪者如此有吸引力。他们往往是在遭遇攻击之后，才发现这一点，但已为时过晚。对这些企业来说，就算可以从攻击中恢复，也需要付出艰巨工作和高昂成本（视攻击的性质和范围而定）。本报告将介绍小型组织面临哪些风险，以及与其他企业相比，小型组织应该如何应对安全问题，并对 2018 年及将来提供少许指导意见。

根据《思科 2018 年安全能力基准研究》，超过一半 (54%) 的网络攻击造成的经济损失超过 50 万美元，包括（但不限于）收入损失、客户流失、商机流失和付现成本。损失之大，足以让毫无准备的中小企业永久关停。

作为佐证，商业服务监督局 (BBB) 最近执行的一项研究[2]也说明了在遭遇严重的网络攻击后，中小企业要想从中恢复，会面临多大的经济困难。BBB 对北美地区的小企业主询问的一个问题是：“如果你们永久无法访问重要数据，那么还能在多长时间内保持盈利？”大约只有三分之一 (35%) 的受访者表示，他们继续盈利的时间会超过三个月。大多数受访者认为，他们会在一个月内停止盈利。

需要指出，我们对中小企业 (SMB) 的定义是：小型企业是指员工人数少于 250 人的企业，中型企业是指员工人数在 250-499 人之间的企业。本报告的内容涵盖这两种规模的企业。

我们对《思科 2018 年安全能力基准研究》（以下简称“基准研究”）中的 SMB 受访者结果进行分析。该基准研究深入探讨了业界当前使用的安全实践，并且将完整结果与近三年的情况进行了比较。

我们的中小企业数据涵盖 26 个国家/地区的 1816 名受访者。

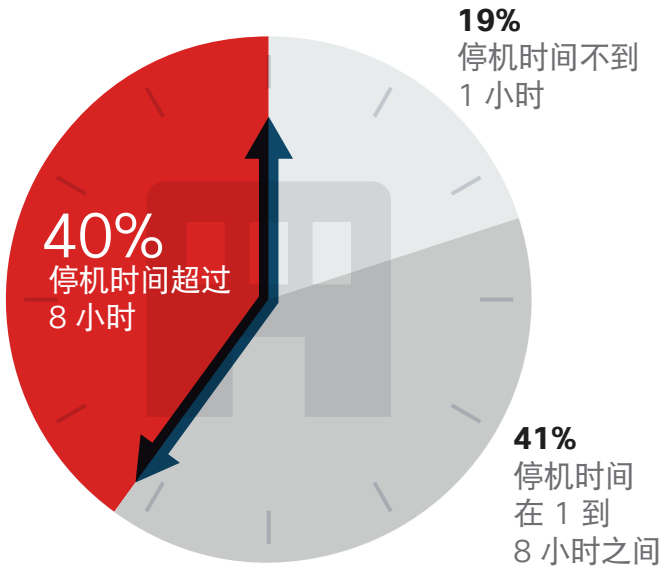
1 《中小企业面临的网络威胁及其解决方案》，Vistage Research Center，2018 年。
与思科和国家中端市场调研中心 (NCMN) 联合编制。可从以下网址获取：
https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/。
2 《2017 年北美小企业的网络安全现状》，BBB，2017 年。可从以下网址获取：
https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf。

网络攻击对员工开展业务有何影响?

任何 IT 管理员都无法妄下定论。系统停机会严重降低员工工作效率和企业盈利能力，这是企业遭遇网络攻击后必须面对的重大问题。基准研究调查发现，40% 的受访者（来自 250-499 名员工的企业）在去年因为严重的安全攻击而经历了 8 个小时或更长时间的系统停机（图 1）。思科对大型企业（拥有 500 或更多员工的企业）的研究样本同样呈现类似结果。区别在于，遭遇攻击后，大型企业能够比中小企业更快地恢复，因为大型企业拥有更多的响应和恢复资源。

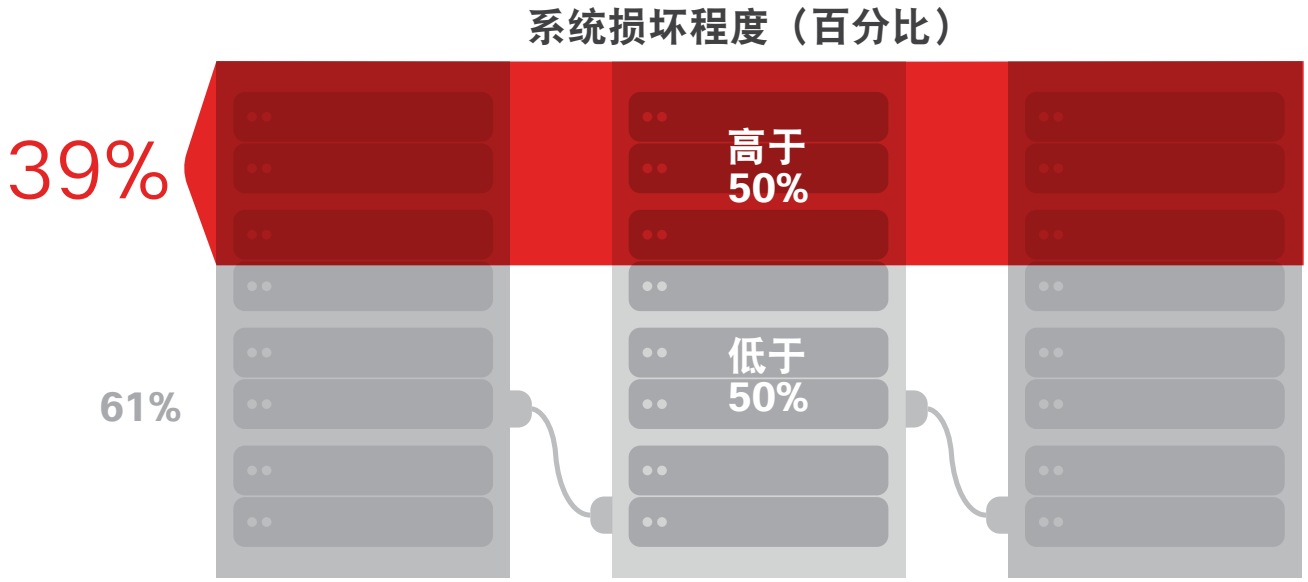
此外，39% 的受访者表示，他们至少一半的系统曾受到严重攻击影响（图 2）。小型企业不太可能拥有多个运营位置或业务部门，其核心系统互连程度更高。当这些企业遭遇攻击时，威胁可以快速轻松地从网络传播到其他系统。

图 1 遭遇严重攻击后的系统停机时间



来源：思科 2018 年安全能力基准研究

图 2 受到严重攻击影响的系统比例



来源：思科 2018 年安全能力基准研究

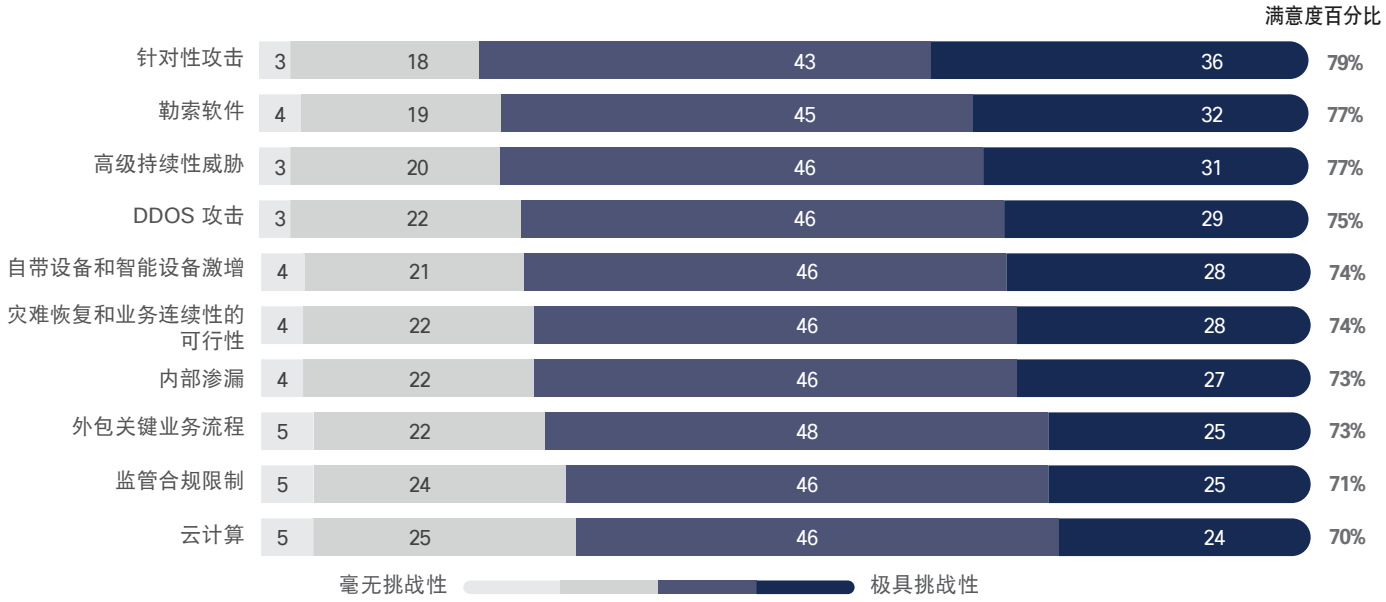
安全问题让人寝食难安

当被问及目前面临的最大安全挑战时，受访者表示最关心以下三个问题：

- 面向员工的针对性攻击（例如，精心设计的网络钓鱼攻击）
- 高级持续性威胁（前所未见的高级恶意软件）
- 勒索软件

众所周知，勒索软件是一种可以加密受害者数据的恶意软件，通常要求受害者交付赎金后才解密数据。勒索软件也会对中小企业造成严重的网络中断和系统停机。（有趣的是，大型企业并未将其列入他们“最关心的 3 大问题”中。）而且，勒索软件会给中小企业带来其他损失：思科安全专家指出，中小企业都更倾向于向攻击者支付赎金，以便快速恢复正常运营。他们根本无力承担停机和无法访问关键数据（包括客户数据）所带来的损失。（见图 3。）

图 3` 中型企业最关心的安全问题[5]



来源：思科 2018 年安全能力基准研究

中小企业不可忽视的其他威胁

尽管勒索软件让人担忧，但思科安全专家认为这一威胁会逐渐衰退，因为更多的攻击者在将重心转向非法挖掘加密货币（简称“挖矿”）。这种活动极具吸引力，理由有三：利润丰厚、收入无法追踪、攻击者无需过于担心其行为可能引发的刑事责任。（例如，不会出现由于勒索软件锁定医院的系统和关键数据而使患者无法获得危重护理的风险。）攻击者还可以通过各种方法（包括基于邮件的垃圾邮件活动和漏洞攻击工具包）传播挖掘软件（“挖矿程序”）。[3]

3 “勒索软件日渐式微？恶意加密货币挖矿软件成为攻击者牟利百万的新宠”，2018 年 1 月31 日：https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html。

思科威胁研究人员指出，恶意攻击者现在采用全新的非法加密挖掘业务模式，“不再通过引诱受害者打开邮件附件或运行恶意脚本，从而劫持其系统并索取赎金，来对受害者实施攻击。现在，[他们] 会想方设法利用受感染系统的资源。”[4] 中小企业会无意中助长非法加密挖掘行为，除非他们拥有在加密货币挖掘活动发生之初就能准确检测的适当技术，否则就只有在系统性能变慢后才会意识到自己遭遇了入侵。

0.5% 的内部威胁：这个比例绝对太高？

随着受访者企业将更多数据和流程迁往云端，他们必须采取措施管理另一种潜在威胁：恶意内部人员。如果没有工具可以检测可疑活动（例如下载敏感客户信息），这些企业将面临从企业云系统中丢失知识产权、敏感财务数据和客户数据的风险。

思科威胁研究人员近期执行了一项调查，重点研究这一风险：他们使用机器学习对 34 个国家/地区的 15 万名云服务用户进行分析，调查从 2017 年 1 月至 6 月间的数据泄露趋势。在一个半月中，研究人员发现有 0.5% 的用户执行了可疑下载行为。0.5% 很可怕吗？换句话说，这表示一家 400 人的公司内就有两名员工可能构成内部威胁。这个比例绝对太高。具体而言，这些用户总共可从企业云系统下载超过 390 万份文档。这意味着在一个半月内，每名可疑用户可下载 5200 份文档。[5]

思科 2018 年安全能力基准研究

本特别报告选用思科 2018 年安全能力基准研究的数据结果。来自 26 个国家/地区的 3600 多名受访者参与了此项研究调查。如需深入了解各种规模的组织当前采用的安全实践，以及与思科以往调查结果的比较情况，请下载《思科 2018 年度网络安全报告》，该报告可从以下网址获取：https://www.cisco.com/c/en/us/products/security/security-reports.html。

4 同上。
5 有关详细信息，请参阅《思科 2018 年度网络安全报告》的“内部威胁：利用云端”部分，该报告可从以下网址获取：https://www.cisco.com/c/en/us/products/security/security-reports.html。

挑战

为有效防御上述威胁，就需要统筹协调 IT 资源。这些资源通常是指可由企业召集起来以共同阻止攻击的人员、流程和技术。

但是，小型企业要通过适当方式协调这些资源，深入洞察威胁，并在攻击造成损害前及时阻止或缓解，在这一方面，他们面临的挑战更甚于大型企业。长期缺乏安全人才对企业的影响在小型企业中体现更为明显。

SMB 安全技术趋势

今后，小型企业切实需要寻求通过新型工具阻止威胁，化解威胁自身组织的网络安全挑战。

基准研究的受访者表示，如果拥有相应的员工资源，他们更有可能采取以下措施：

- 升级终端安全解决方案，实现更完善的高级恶意软件保护/终端检测与响应 (EDR)。受访者中做此回复的人数最多，达到 19%。
- 考虑采用更好的 Web 应用安全解决方案来防御 Web 攻击 (18%)
- 部署入侵防御，这仍被视作一项阻止网络攻击和漏洞攻击企图的重要技术。(17%)。（请参见图 5。）

组织在考虑采用新技术时面临一项挑战，即确定产品之间可以如何相互协作以保护企业。我们不应低估联合多个控制台以响应威胁或安全事件的管理负担。

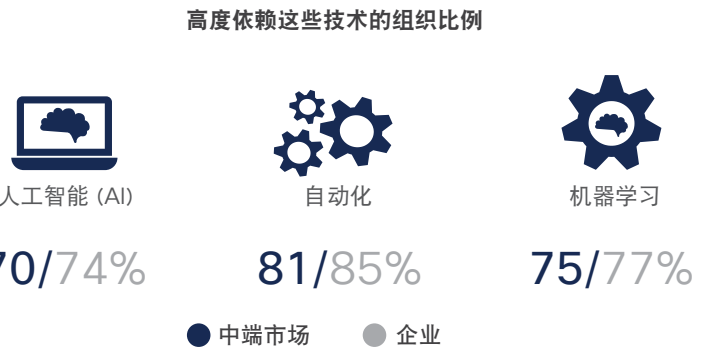
“很多人认为选择多个供应商就是绝佳途径，可以实现更好的保护”，思科合作伙伴 Liberty Technology（位于佐治亚州格里芬）的首席执行官 Ben M. Johnson 表示，“但现实却事与愿违，更难管理、成本更高、整体安全效力下降。”

机器学习：安全助手还是炒作？

机器学习是最近的热门话题，我们都有所耳闻。结果显示，中型企业对可以有效检测攻击的行为分析解决方案的依赖并不亚于大型企业。但对于使用机器学习和自动化技术的解决方案，中型企业的依赖程度略微低于员工人数超过 1000 人的组织（图 4）。

与单独购买产品进行“机器学习”相比，将机器学习用作已部署产品的额外检测功能可以更充分发挥其效力。这样，团队既可利用机器学习的优势快速检测异常和威胁，又无需承担更多负担。

图 4 中型企业对自动化和 AI 工具的依赖较小



来源：思科 2018 年安全能力基准研究

移动中端市场

企业还认识到，他们的安全方法必须满足现代工作环境的需求，特别是向移动商务转型和采用移动设备。56% 的受访者表示，他们认为保护移动设备免受网络攻击非常或极度困难。

中端市场和云

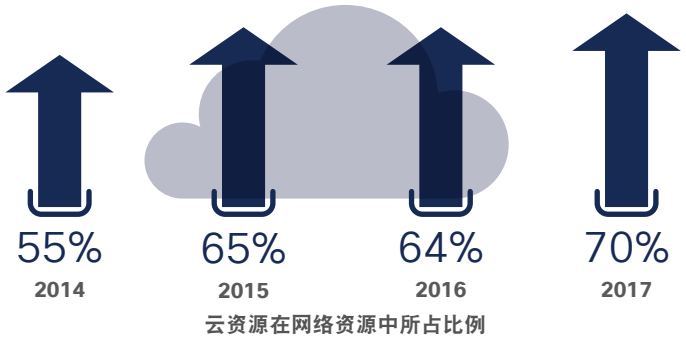
意识到自身面临的安全挑战后，许多受访者开始转向云端，希望在无需增加人员或使现有资源疲于应付的情况下，增强防御。问题是，将安全部署迁移到云端的战略是否能有效抵御攻击。此外，企业不能仅仅通过将数据迁移到云端来摆脱安全责任：他们还需要了解云供应商实施的安全控制措施，以及云端的潜在漏洞可能对本地资源造成的影响。

根据思科研究，中型企业采用云服务的趋势明显上升。2014 年，55% 的企业表示他们以云的形式托管了部分网络，到 2017 年，这一数据已经增加到 70%（图 5）。

很多受访者认为，云有助于弥补自身的防御缺陷，还能解决一些基础设施的缺点和人员能力不足的问题。事实上，根据思科研究，中型企业在云端托管网络的首要原因是，他们相信云端的数据安全性更高 (68%)；其次是，企业缺乏足够的内部 IT 员工 (49%)。（请参见图 6。）

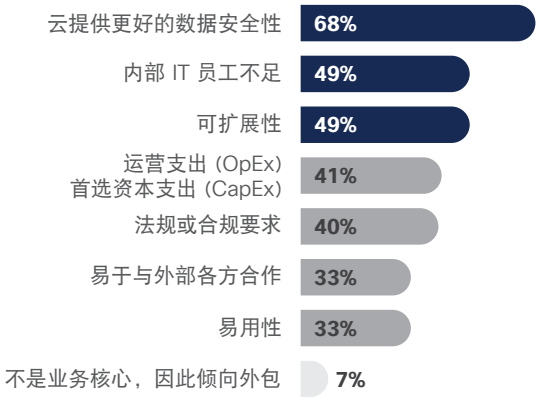
中型企业选择云端的另一个原因是它具有可扩展性，可以减少企业对内部资源的依赖，而且可以灵活地转向运营支出而非资本支出（图 6）。

图 5 中型企业的云采用率稳步上升



来源：思科 2018 年安全能力基准研究

图 6 云服务凭借安全性和高效赢得中型企业青睐



来源：思科 2018 年安全能力基准研究

人员：发掘人才，增强安全性

好消息是，基准研究表明 92% 的中型企业有高管负责安全工作。（请参见图 7。）

如果有足够的人员资源，中型企业愿意添置更多的安全工具，例如高级终端保护或 Web 应用防火墙。

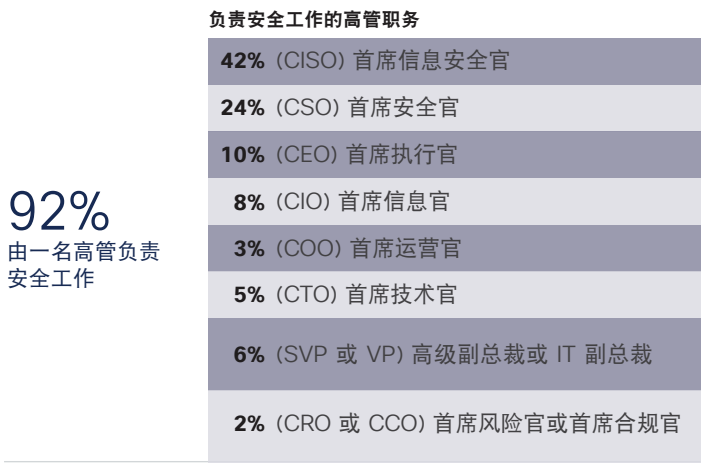
中型企业与大型企业有一个共同之处，即：IT 人员短缺削弱了加强防御的能力。根据思科的研究结果，企业内部根本没有足够的人员来管理可提高安全性的工具。

因此，许多中小企业寻求外包人才援助，提高自身对威胁的了解、节省成本，同时更快地应对攻击。需要获得客观的洞察力是中型企业将安全工作外包的最主要原因（图 8），其次是成本效益和及时响应安全事件的需求。

外包援助不失为帮助企业充分利用有限资源的好办法。但是，如果这些公司认为外包供应商或云合作伙伴能够提供内部缺乏的所有能力，那就情况不妙了。

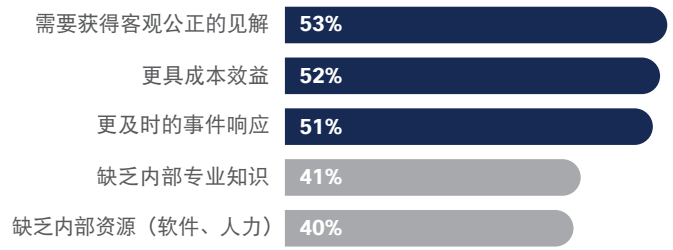
思科合作伙伴 NuWave Technology Partners（位于密歇根州卡拉马祖）的首席执行官 Chad Paalman 发现，许多中小企业并不清楚自己的外包安全服务供应商能够具备多大（或者多小）的分析和监视能力。

图 7 有高管负责安全工作的中型企业



来源：思科 2018 年安全能力基准研究

图 8 中型企业通过外包服务来解决内部资源不足的问题



来源：思科 2018 年安全能力基准研究

“许多企业领导并不了解自己的网络。他们认为只要有防火墙，就会御敌于门外，没人能够进入他们的网络。他们还认为，如果将安全工作外包给托管服务提供商 (MSP)，就会获得日志监视，或认为其服务中包含入侵检测。”

NuWave Technology Partners 首席执行官，Chad Paalman

实质上，中小企业依赖外包合作伙伴提供以下服务：

- 外包建议与咨询服务 (57%)、
- 事件响应 (54 %)、
- 安全监视 (51%)。

但是，他们可能不会将威胁情报等工作外包出去 (39%)。（请参见图 9。）

好消息是，中型企业似乎会预留部分有限资源来了解和应对威胁，例如支持威胁情报和事件响应。

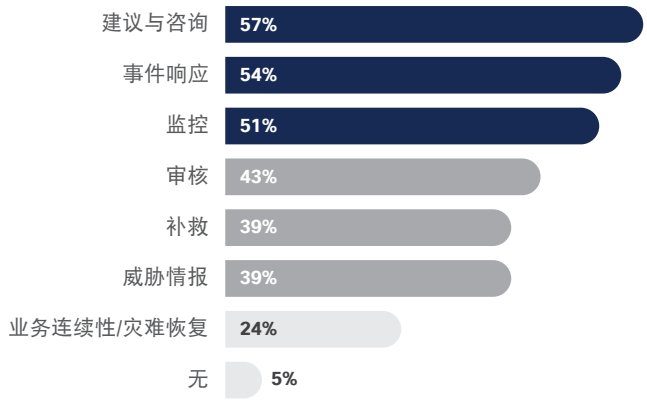
流程：定期检查以管理安全性

全面、定期的安全流程（例如，控制高价值资产、审查安全实践）可帮助企业识别安全防御中的薄弱环节。可能由于中小企业的人员不足，此类流程在这些企业中并不普及。

例如，根据《思科 2018 年安全能力基准研究，与大型组织相比，中型企业更少采取以下流程：定期审查安全实践、采用相应工具来检查安全效力或定期调查安全事件（图 10）。

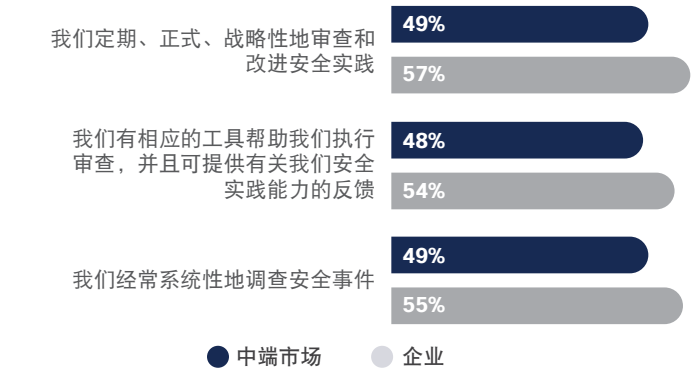
从积极方面来看，91% 的中型企业表示他们至少每年进行一次演习，测试自身的事件响应计划。但是，由于企业对云服务和外包服务合作伙伴的依赖，现在的问题是，此类事件响应计划是否足以抵挡日益复杂的攻击者。

图 9 中型企业获得建议与咨询访问以及事件响应能力



来源：思科 2018 年安全能力基准研究

图 10 中型企业更少使用运营流程



来源：思科 2018 年安全能力基准研究

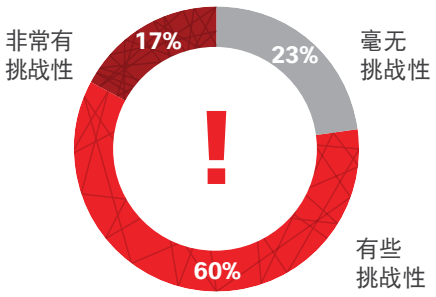
连接人员、流程和技术：协调挑战

如果中小企业在防御系统中添加更多安全产品和供应商，同时将 IT 资源转向管理这些产品，是否就能提高他们的安全管理效力？情况可能正好相反，至少在了解并协调安全警报方面会如此。

如今，大多数中小企业都意识到，随着他们构建更加复杂的产品和供应商环境，自身的责任也在加大。例如，77% 的中型企业发现从众多解决方案中协调安全警报有些困难或非常困难（图 11）。

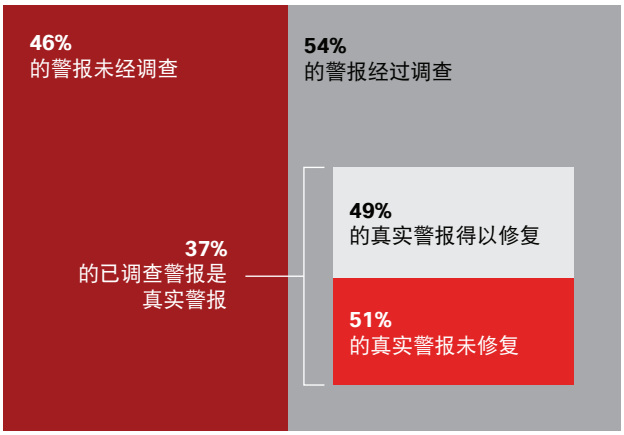
基准研究发现，当企业试图分析这些警报时，人员、流程和技术共同构成的挑战可能导致很多警报被忽视（图 12）：

图 11 中型企业更少使用运营流程



来源：思科 2018 年安全能力基准研究

图 12 未经调查或补救的安全警报的百分比



来源：思科 2018 年安全能力基准研究

对未来的建议

技术

当组织考虑采用新工具时，最好能避免增加供应商队伍，避免生成更多警报。

为此，就应当考虑，产品是否具备开放性？它们在共享数据和威胁情报时如何与其他产品集成？是否集成了管理控制台？

如果供应商表示，他们的产品可与其他产品协同工作，则还应考虑他们的产品是能开箱即用，还是需要买家执行大量 API 工作？

尽管炒作不断，但是机器学习的确在安全领域占有一席之地。不过，我们应该将机器学习用作已部署产品的额外检测功能，而不能将其作为来自其他供应商的单独产品，否则就会增加额外的产品管理负担。

人员和流程

简单说来，就是要制定战略，以改善网络安全。根据商业领袖资源中心 - Vistage Research Center 的数据，只有 38% 的中小企业制定了有效的网络风险战略。[6]

您的计划中是否包括让最终用户接受适当培训？您的保单是否涵盖网络攻击导致的业务损失？如何制定业务持续性和危机通信计划，从而实现更快速的恢复并帮助防止声誉受损。

此外，IT 领导者必须明确说明业务管理层需要了解的安全攻击相关信息：

- 安全攻击对组织有何影响
- 安全团队采取哪些措施来遏制和调查威胁。恢复正常运营需要多长时间。[7]

“通过采用一系列可协同工作的安全平台和工具，而不是拼凑可能彼此冲突的各种安全产品，可以提升安全效力并简化管理。”

Ben M. Johnson，Liberty Technology 首席执行官

“中小企业应该评估这些风险并在漏洞发生前制定响应计划，而不是亡羊补牢。”

Chad Paalman，NuWave Technology Partners

6 《中小企业面临的网络威胁及其解决方案》，Vistage Research Center，2018 年。与思科和国家中端市场调研中心 (NCMN) 联合编制。您可以从下列地址访问思科软件顾问：https://www. vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 《思科 2017 年年中网络安全报告》：https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf。13 同上。

结论

最终建议是，对于中小企业，要改进网络安全，就要认识到渐变胜不变。简而言之，在安全方法方面，不能因为追求“完美”而错失“变好”的机会。和所有其他事物一样，没有百分百完美的安全方法。

中小企业还必须清楚，并不存在能够解决所有网络安全挑战的“万全之策”。他们面临的威胁形式复杂多变。受攻击面始终在不断变化扩展。相应地，安全技术和战略也应持续演进。

要详细了解思科以威胁为中心的安全方法，请访问 cisco.com/go/security。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

发布时间：2018 年 7 月

© 2018 思科和/或其附属公司。版权所有。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问以下网址：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

Adobe、Acrobat 和 Flash 是 Adobe Systems Incorporated 在美国和/或其他国家/地区的已注册商标或商标。