中国的安全形势：向集成化解决方案迈进

在中国，许多雄心勃勃的企业正在日益壮大。对这些企业来说，保持安全运营可以获得竞争上的优势。但是，中国的很多企业目前都围绕单点解决方案构建安全基础设施，这在很大程度上是因为此类解决方案只需要数额较小的短期投资。然而，这种碎片化的方案无法为企业提供真正可靠的安全保护。

与全世界的很多企业一样，中国企业也担心勒索软件等各种威胁对正常运营造成的影响。要遏制这些威胁，企业必须寻求可以更全面地应对日常安全威胁的集成解决方案：

- 企业需要考虑端到端平台所能带来的价值。单点解决方案的成本似乎较低，但维护碎片化的基础设施可能会带来更高的长期成本。而且，这种安全方法有可能存在安全缺口，攻击者能轻易地侵入网络。
- 通过将安全解决方案融入运营流程，并使其与公司目标保持一致，企业可以获得竞争优势。不仅如此，这也有助于为实施互联商业模型（例如制造业的中国制造业 2025 规划或金融服务业的无网点银行业务）做好更充分的准备。

主要研究结果

在本文中，思科专家使用《思科安全能力基准研究》中的数据分析了中国的 IT 安全能力。[1]在分析中，我们发现中国企业对安全基础设施的重视程度有待提高。尤其值得注意的是，中国的企业应该通过系统集成，提供更加全面的端到端网络保护：

- 投资端到端解决方案的一个理由是，企业可能很难将碎片化的解决方案集成到一起，构建全面的统一安全平台。50% 的大公司和 42% 的中小型公司（SMB）认为，与旧版系统的兼容性问题是采用安全流程和安全技术的一大障碍。30% 的大公司和 43% 的中小型公司认为，预算限制是主要障碍。
- 2015 年，85% 的企业表示他们遵循了标准化信息安全规范（如 ISO 27001 或 NIST 800-53）。2014 年，这一数字为 71%。在中国，这一比例如此之高，是因为公司必须满足某些标准。但是，这些认证其实仅仅是一个开端。获得这些认证并不代表公司就一定安全。真正的安全需要持续的努力。

理解集成安全解决方案的价值

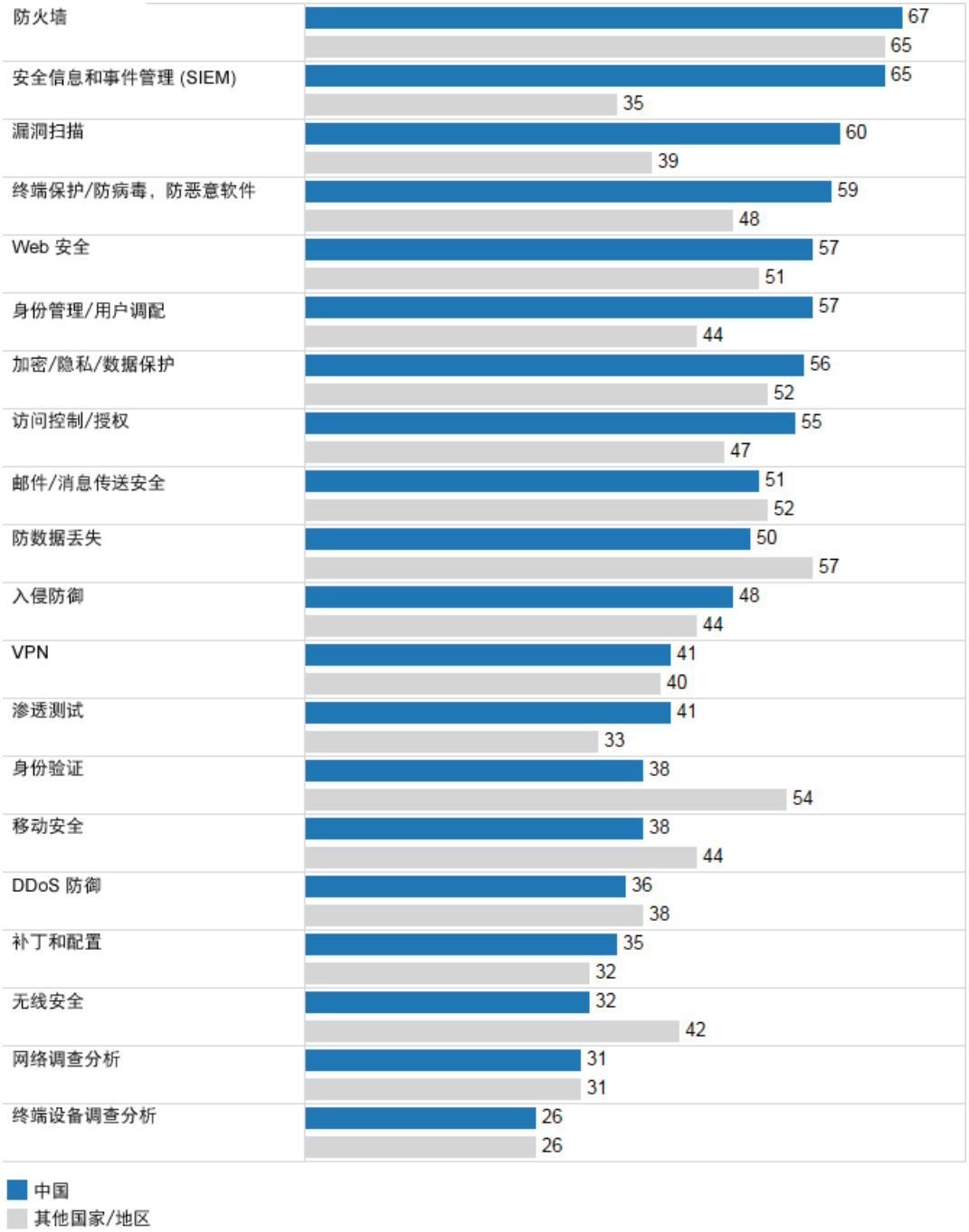
对很多中国公司而言，购买安全解决方案最重要的考虑因素可能是成本负担。在中国竞争激烈的安全解决方案市场中，低成本无疑是一项优势，因为这符合企业精简预算的目标。但是，公司在规划安全投资时，应综合考虑到短期和长期成本。

例如，公司可能倾向于从多家供应商购买单点解决方案，然后选择功能最好、成本最低的产品来满足不同方面的安全要求。但是，这种方法会使基础设施碎片化，从长期来看，这反而需要付出更高的成本和大量的时间进行管理。此外，碎片化的安全环境可能会存在缺口，不仅让攻击者有机可乘，而且会导致额外的成本。综合各方考虑，投资购买集成安全架构是值得的，这比购买大量单点解决方案更高效、更简单。

安全工具在中国的使用率很高，这也可以用中国企业偏好单点解决方案来解释。如同其他国家/地区的企业一样，中国的企业至少会采用加密和防火墙等安全防御措施（见图 1）。事实上，中国的企业在很多工具的使用上比例更高：在接受调查的中国企业中，有 65% 使用安全信息和事件管理 (SIEM) 系统；而在其他国家/地区的企业中，这一比例只有 35%。同样，60% 的中国企业使用漏洞扫描工具，而这一数字在其他国家/地区只有 39%。

[1] 有关这项研究以及此系列其他白皮书的详情，请参阅本文档的最后几页。

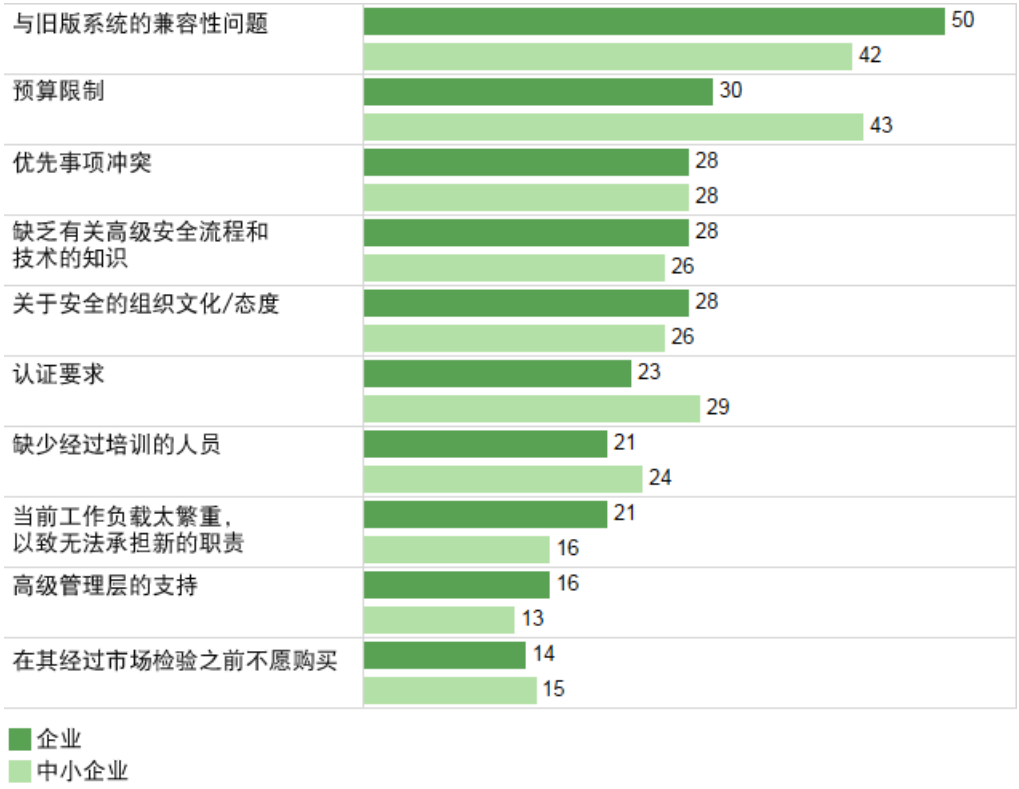
图 1. 中国的企业和其他国家/地区的企业对各种威胁防御工具的使用情况（单位：百分比）



广泛使用各种安全工具固然很好，但构建融合基础设施是更好的选择。中国的企业应开始寻求集成安全解决方案，而不是购买大量不能交互操作且很难管理的技术。虽然集成解决方案的初期成本较高，但是此类系统更有可能预防安全漏洞，而且从长期来看所需的维护和管理成本可能更少。

从企业对集成的担忧便可以看出碎片化的方案对安全的影响：50% 的大公司和 42% 的中小型公司表示，与旧版系统的兼容性问题是采用安全流程和安全技术的一大障碍（见图 2）。30% 的大公司和 43% 的中小型公司表示，预算限制是主要障碍。

图 2. 对采用安全解决方案时存在多种障碍表示认同的大公司和中小型公司的比例

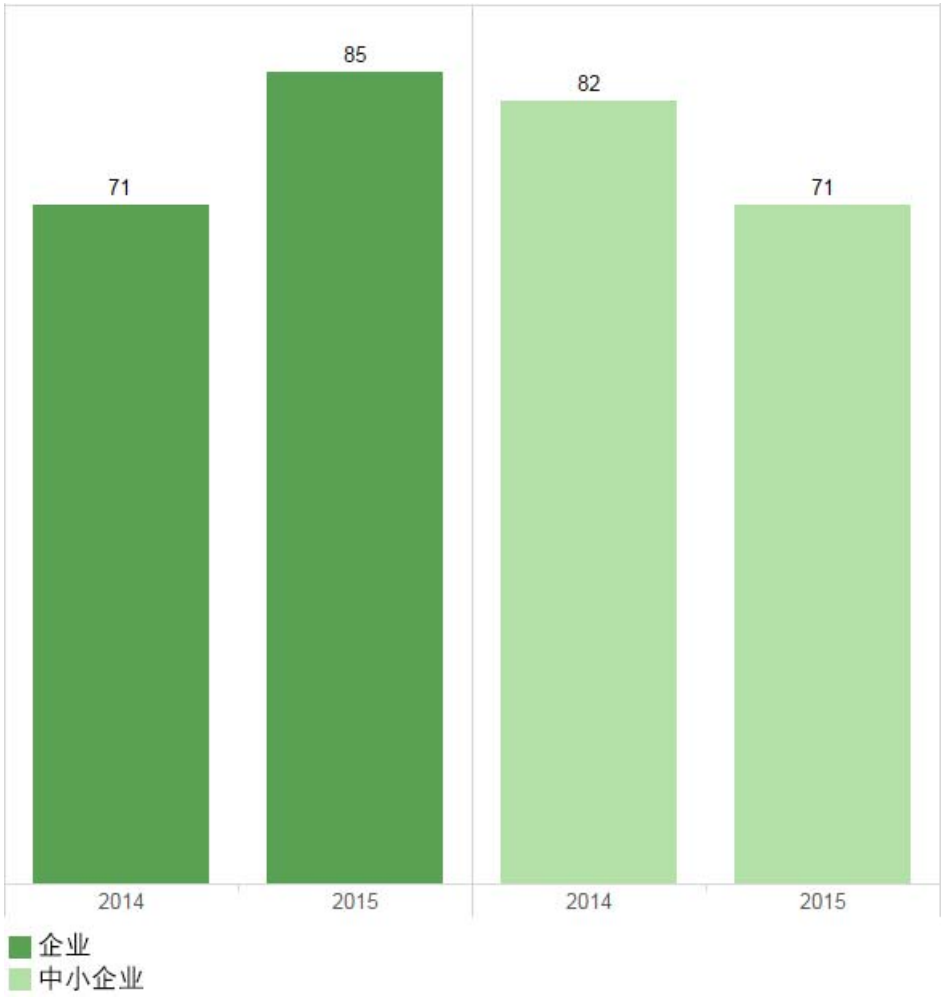


即使企业已经满足安全标准，也仍需要关注自己的安全状况

许多中国的企业（例如产品销售企业）必须取得国家公安部的认证。此外，企业也可以选择遵守其他标准，如 ISO（国际标准化组织）标准。遵守此类标准不仅能满足国家要求，而且可以对国际贸易合作伙伴产生更大的吸引力。

因此，中国的企业应确保所采用的安全工具和流程满足或超过此类标准的要求。目前，采用此类标准的企业越来越多：2015 年，85% 的大公司表示他们遵守 ISO 27001 或 NIST 800-53 等标准化信息安全规范；而在 2014 年，这一数字为 71%（见图 3）。但是，中小型公司采用此类标准的比例稍有下降。2014 年，表示遵守标准化信息安全规范的中小型公司为 82%，但这一数字在 2015 年降低到 71%。

图 3. 2014 年和 2015 年遵守标准化信息安全政策的中国大公司和中小型公司的比例



就中国的企业而言，需要注意的一点是合规不等同于安全。换言之，仅仅是采用安全标准并满足政府规定，并不一定能维持网络安全。

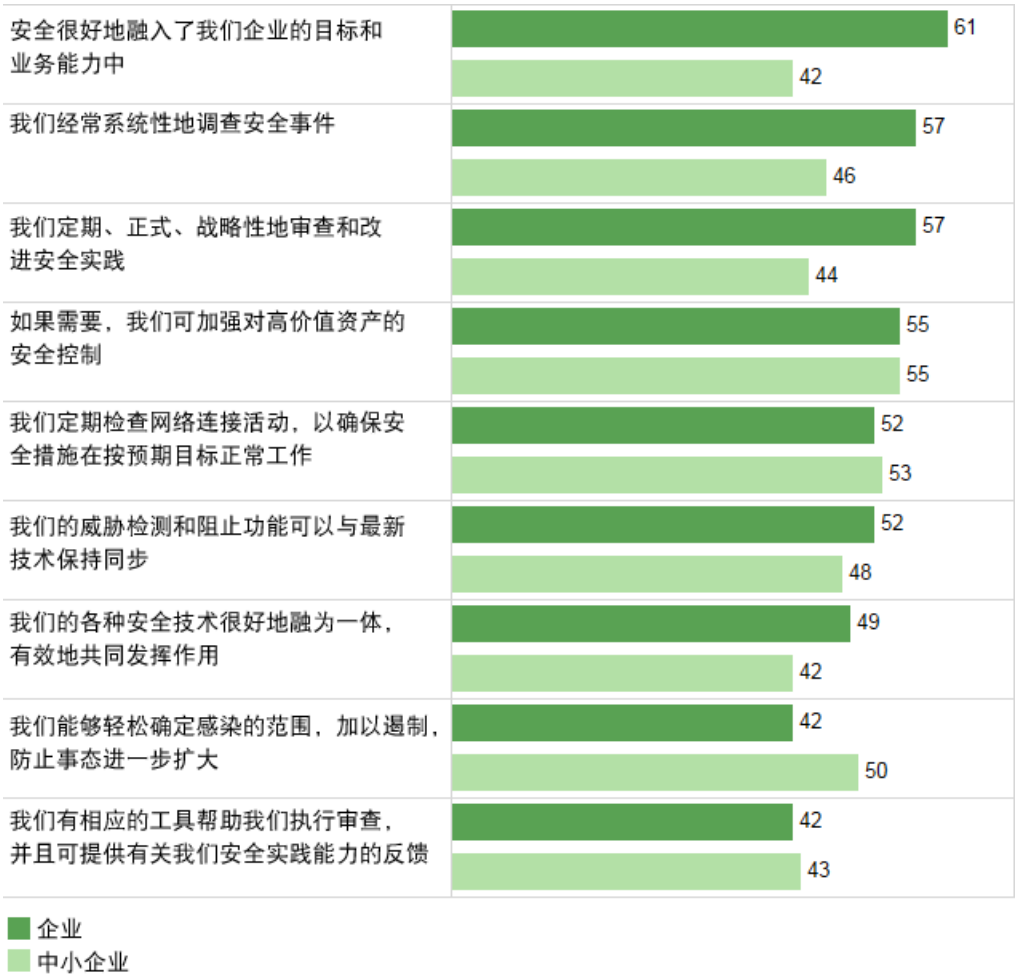
大多数中国企业已经采用正式的安全策略。此举帮助他们改善了安全状况，而且在贸易关系中加强了自己的品牌。84% 的大公司和 85% 的中小型公司表示他们制定了正式的书面安全政策，并且会定期审查。

需要更注重将安全解决方案融入运营流程

中国的企业如果只选择单点解决方案而不考虑长期影响，可能会妨碍安全计划的实施。也有一些企业可能只是为了满足合规要求而制定安全计划，并错误地认为这足以保护他们的企业。这些企业应重新考虑自己的安全策略，并且要关注结果：在所有可能的攻击阶段对网络进行防御。

要做到这一点，中国的公司应注重将安全解决方案融入运营流程，并采用更有效的工具。这些措施所能达到的效果，将远远超过单纯采用单点解决方案，而不制定总体计划来决定如何将这些解决方案融入一个集成安全架构。在中国，只有 61% 的大公司和 42% 的中小型公司认为安全已高度融入他们的企业目标和业务能力中（见图 4）。此外，只有 42% 的大公司和 43% 的中小型公司认为自己拥有可供审查的工具，并对安全能力提供了反馈。

图 4. 对其安全运营流的各项陈述表示同意的中国大公司和中小型公司的比例



结论：扩大对集成安全架构的投资

中国企业即将迎来一个前所未有的互联时代。以号召升级国家制造业基础设施的"中国制造 2025"规划为例，在各种类似计划的带动下，基于物联网的系统将得到越来越多的采用。此外，诸如"无网点银行"等其他计划将扩大技术的影响范围，使过去未连接到网络的人群也能享受网络的便利。但是，广泛的连接也将带来风险，例如使网络暴露在威胁之下。要在这样一个时代生存和发展，中国的企业必须对自己的安全需求进行长远思考：既要考虑自己的目标和成果，又要考虑如何利用安全优势促进业务上的成功。

中国的安全专业人员应树立以下意识：

- 改变对安全解决方案的看法，从短期思维转变为长期思维，了解如何从集成解决方案的优势（更有效的安全保护和更少的 IT 管理负担）中获得价值。
- 寻求更全面的解决方案，以便能够在遭受攻击前、攻击中和攻击后为整个扩展网络提供安全保护。转为使用以威胁为中心的方法，从而降低复杂性和分散性，并提高可视性与可控性。

- 提高解决方案兼容性，以确保不会因为集成上的难题而延误增强安全性。

了解详情

如需了解有关最新威胁的详细信息，请访问 http://www.cisco.com/cn/mcr2016 获取《思科 2016 年年中网络安全报告》。要了解思科综合性的先进威胁防范产品和解决方案组合，请访问 http://www.cisco.com/cn/security。

关于思科 2015 年安全功能基准研究

思科 2015 年安全功能基准研究从三个方面对防御者进行评估：资源、功能和完善程度。此研究涵盖了 12 个国家/地区多种行业的企业。我们总共对 2400 多名安全专业人员进行了调查，这些人员包括首席信息安全官 (CISO) 和安全运营 (SecOps) 经理。接受调查的专业人员分别来自下列国家/地区：澳大利亚、巴西、中国、法国、德国、印度、意大利、日本、墨西哥、俄罗斯、英国和美国。选择这些国家/地区进行调查是以经济重要性和地理多样性为依据的。

要了解内容更丰富的《思科安全功能基准研究》中的研究结果，请获取《思科 2016 年年度安全报告》，网址为 http://www.cisco.com/cn/asr2016。

关于此系列

思科的行业和国家/地区专家小组对《思科 2015 年安全功能基准研究》进行了分析。他们就 10 个国家/地区以及 4 个行业（金融服务、医疗、电信和交通运输）的安全形势提出了针对性的见解。此系列白皮书重点说明了组织在网络安全领域面临的安全形势和挑战。该过程有助于在具体情景下理解此项研究的结果，并将重点放在我们分析的每个国家/地区和行业的相关主题上。

关于思科

思科致力于构建集成化、自动化、开放、简单易用且真正有效的安全解决方案。凭借无与伦比的网络实力以及业界最全面、最雄厚的技术和人才力量，思科提供极高的可视性和响应速度，可检测出更多威胁并更快地进行补救。通过借助思科安全解决方案的力量，公司将能够安全地利用新的全数字化商机。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
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。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。