CISCO
SECURE

CISCO The bridge to possible

中小企业网络安全：亚太地区企业为数字化防御做准备

2021 年 9 月

目录

前言

网络安全是数字化新常态之根基

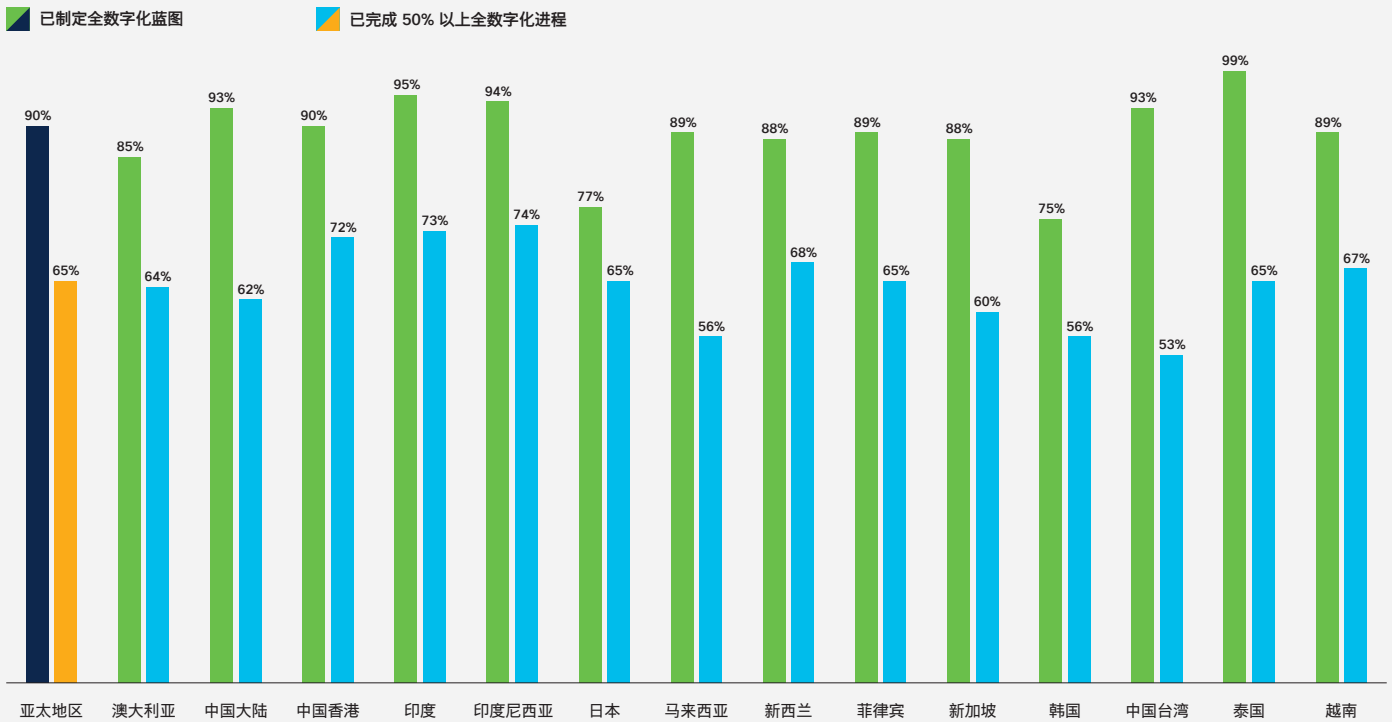
新冠肺炎疫情迫使各种规模的企业都需要投资于技术解决方案和培养相关能力。疫情伊始，很多企业为了生存而纷纷采用相关技术，期望即使整体经济因为封锁而陷入困境，他们依然能够维持运维，并继续为客户提供服务。与此同时，大多数员工开始采用远程工作模式。由于这些企业切身体验了技术带来的积极影响，而且现在各个国家/地区正在考虑逐步重新开放经济，因此各个组织都渴望充分利用技术，在新常态下蓬勃发展。

对整个亚太地区的中小企业 (SMB) 来说，尤其如此。我们委托开展了相关独立研究，以深入了解中小企业的技术趋势，特别是与网络安全相关的技术趋势。

研究发现，亚太地区 94% 的中小企业已采用某种技术形式。更令人鼓舞的是，绝大多数 (90%) 的中小企业制定了全数字化蓝图。在泰国和印度这种趋势尤为突出，99% 的泰国中小企业和 95% 的印度中小企业都制定了相应蓝图。不过，日本和韩国等成熟经济体的这一比例略低，分别有 77% 和 75% 的中小企业表示他们制定了全数字化蓝图或战略。

在实施方面，65% 的中小企业在全数字化转型之旅中进展顺利，已经部署了 50% 以上的全数字化计划。印度尼西亚、印度及中国香港特别行政区的中小企业已完成至少 50% 的全数字化转型进程。相比之下，中国台湾、马来西亚和韩国进展最为缓慢。

亚太地区各市场的中小企业全数字化进程



随着该地区中小企业的全数字化步伐加快，人们越来越关注网络安全，主要原因之一是不断加快的全数字化步伐导致中小企业向黑客和恶意攻击者暴露了更多的受攻击面。因此，我们一点也不奇怪，四分之三的中小企业表示，他们现如今比 12 个月前更加关注网络安全了。形势相当严峻。但令人鼓舞的是，这也表明中小企业对网络风险的意识有所提高。

他们的担心绝非杞人忧天。我们的研究表明，在过去一年里，亚太地区超过一半 (56%) 的中小企业曾遭遇网络安全事件，其中高达 85% 的中小企业遭受了恶意软件攻击，不幸成为网络犯罪的受害者。通过这些攻击，恶意攻击者开始染指宝贵的数据，从客户信息 (75%)、内部邮件 (62%)、员工数据 (61%)，到知识产权 (61%) 以及财务详细信息 (61%)，无所不及。

这对中小企业产生了切实的影响，62% 的受访者表示网络事件导致了他们的运维中断，61% 的受访者表示因此遭受了收入损失。

此外，57% 的受访者表示失去了客户的信任，而 66% 的受访者表示，网络安全事件对公司的声誉造成了负面影响。虽然声誉下降和信任削弱的程度无法量化，但却可能对任何企业造成灾难性后果。

从积极的方面来看，中小企业已经意识到他们面临的挑战。事实上，许多中小企业正在采取计划性更强的方法来应对这种挑战，通过战略性计划了解和改善自身的安全状态。我们的研究表明，81% 的中小企业在过去 12 个月内对潜在的网络安全事件进行了场景规划和/或模拟。大多数受访者 (81%) 制定了响应计划，而 82% 的受访者已准备好在需要时实施恢复计划。在接下来的安全成果研究报告中，我们将进行更深入的分析，衡量在此网络安全领域什么样的行动速度才能产生更积极的影响。

我们希望本报告能够针对亚太地区中小企业面临的网络安全挑战提供有益洞察。该地区的中小企业正在准备迎接未来的混合工作模式，支持员工在办公室办公和远程办公之间自由切换，这为解决网络安全问题额外增加了一层复杂性。我们希望阅读本报告的所有人员都可以受益于其中提供的实用建议，使网络做好迎接挑战的准备并努力提高网络弹性。

随着世界数字化程度日益提高，网络安全的重要性愈发突出，所有中小企业都应该投入时间和资源来管控和克服其网络面临的安全障碍，打造高弹性、适应未来需求的企业网络，最终推动企业取得成功。

Kerry Singleton
思科亚太、日本及大中华区
网络安全业务总经理

Michiko Kamata
思科亚太、日本及大中华区
中小企业发展办公室主管

Bidhan Roy
思科亚太、日本及大中华区
商业企业和中端市场总经理

引言

我们对亚太地区超过 3700 家中小企业中负责网络安全的业务和 IT 主管开展了一项调查，本报告阐述并分析了各项调查结果。该调查开展于 2021 年 4 月至 7 月期间。

本报告旨在更深入地了解该地区中小企业面临的不断变化的网络安全挑战，以及中小企业领导者如何准备应对网络安全挑战，并提出改进建议。

调查涵盖亚太地区 14 个市场：澳大利亚、中国大陆、中国香港、印度、印度尼西亚、日本、马来西亚、新西兰、菲律宾、新加坡、韩国、泰国、中国台湾及越南。

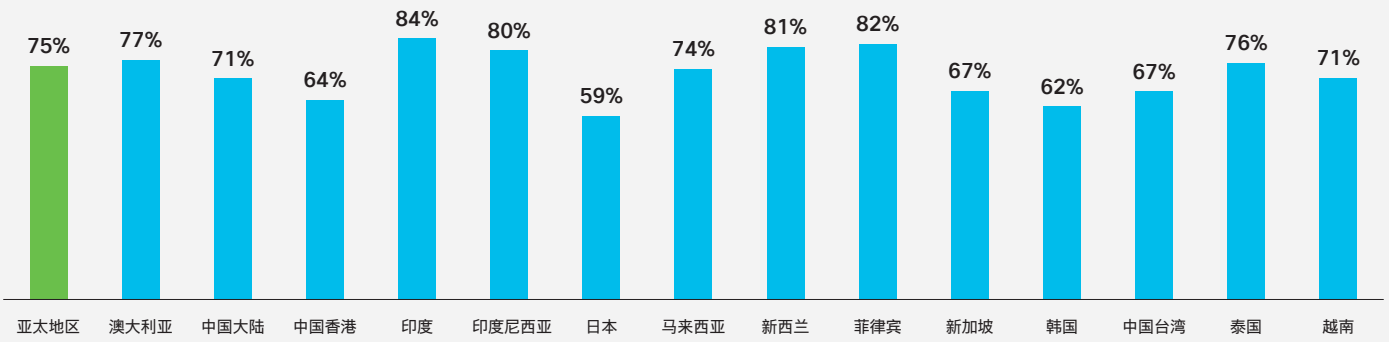
接受调查的中小企业来自众多行业，包括商业服务、建造、教育、工程、设计与建筑、金融服务、食品和饮料、医疗、制造、媒体与通信、自然资源、个人护理服务、专业服务、房地产、零售、技术服务、旅行、交通及批发。

面对威胁，担忧安全

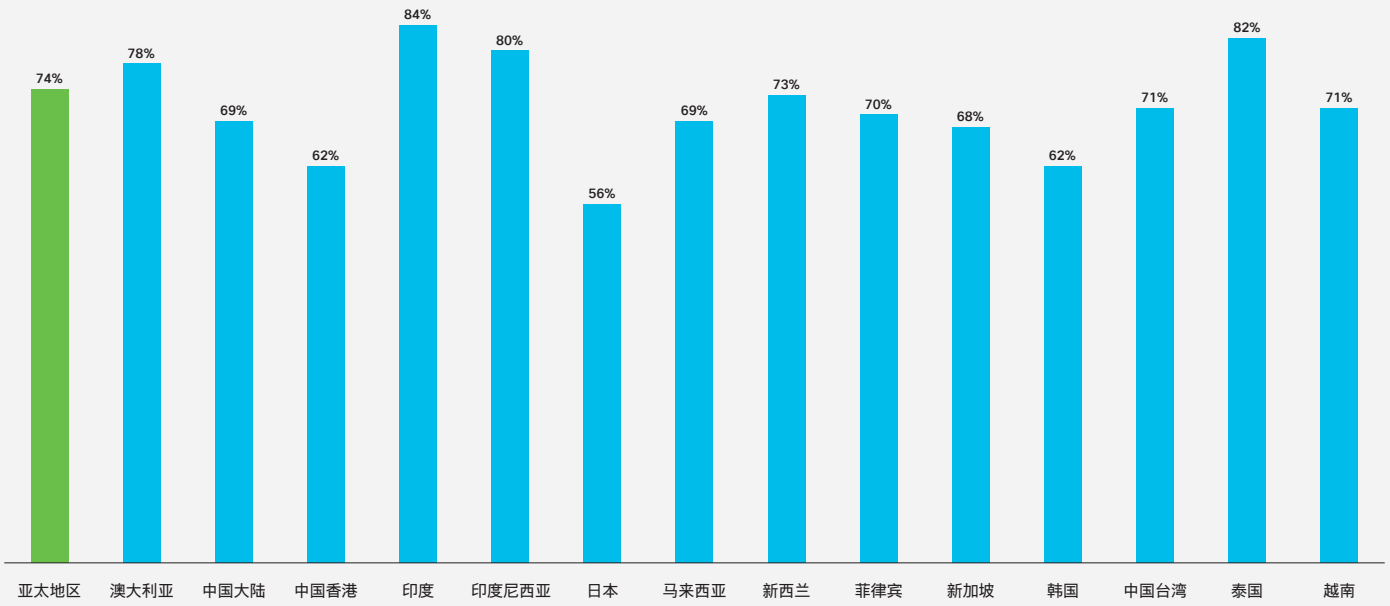
随着商业环境快速发展，网络威胁局势在过去一年里也发生了显著变化。这使得整个亚太地区的中小企业对网络安全风险更加忧心忡忡。该地区四分之三 (75%) 的中小企业表示，他们现在比 12 个月前更担心网络安全，其中担忧程度最高的市场是印度 (84%)、菲律宾 (82%)、新西兰 (81%)、印度尼西亚 (80%) 及澳大利亚 (77%)。

越来越多的中小企业意识到，严重的安全事件可能对其业务造成重大影响，这在一定程度上加重了他们对于安全问题的担忧。四分之三 (74%) 接受调查的中小企业负责人表示，重大网络事件甚至可能会导致其组织瓦解。

现在比 12 个月前更担心网络安全的中小企业百分比



相信严重网络安全事件可能导致企业终止运维的中小企业百分比

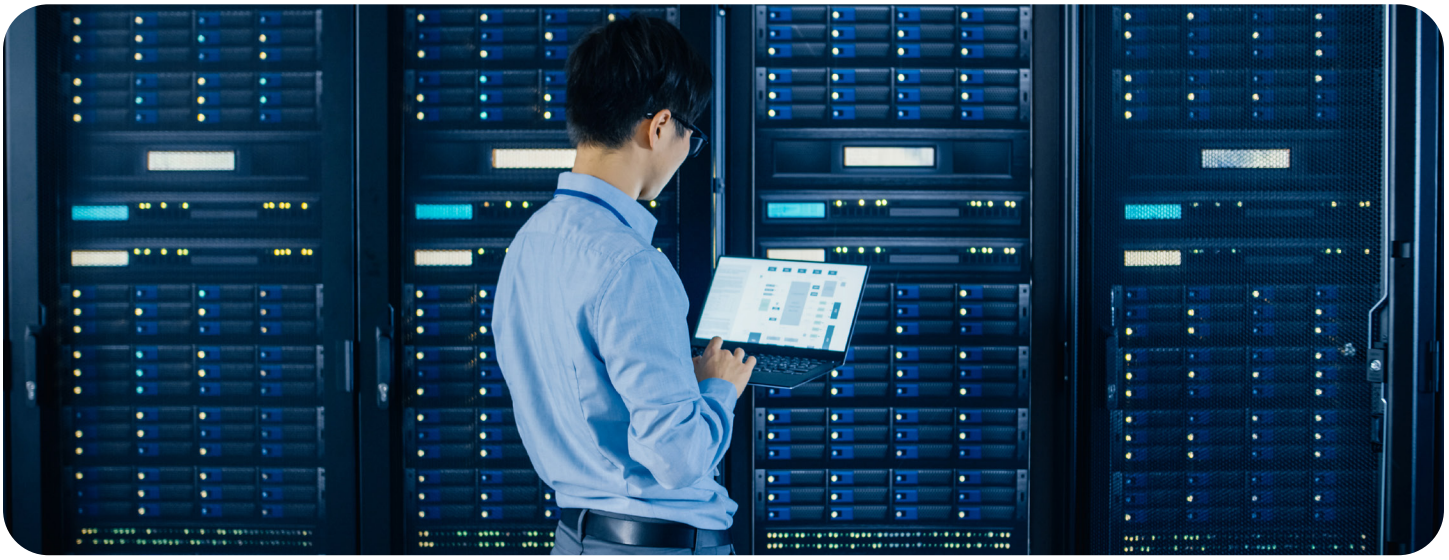


中小企业也越来越清醒地意识到最大威胁来自何处。本调查的一大发现是，亚太地区的中小企业将网络钓鱼攻击视为首要威胁，43% 的受访者将它排在第一位。网络钓鱼攻击是指黑客伪装成可信赖的实体，试图诱使用户打开黑客向其发送的特定数字通信内容，例如邮件、超链接或即时消息。虽然这种攻击策略早已存在，但由于其简单性和有效性，它仍然很受黑客欢迎。

与此同时，商业环境瞬息万变，在疫情的影响下，中小企业的运维方式发生了巨大的变化。最明显的变化是，很多企业转为远程工作模式，大量员工需要从外部网络连接到公司内部网络访问信息。许多员工还会使用个人设备来进行这些连接和访问。中小企业在调查中强调，不安全的笔记本电脑（20%，排名第一）、恶意攻击者的有针对性攻击（19%，排名第一）和个人设备（12%，排名第一）是其整体安全面对的主要威胁。

您认为以下哪一项对您的组织构成头号网络攻击风险？

暴露在外，遭遇攻击

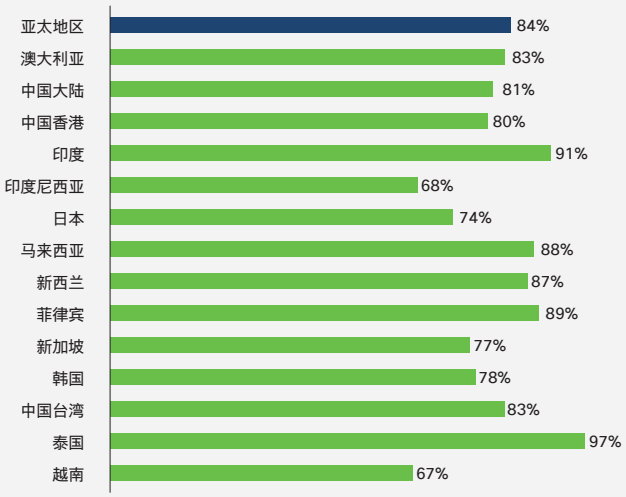


中小企业有充分理由担忧。亚太地区超过五分之四 (84%) 的中小企业感觉面临网络安全威胁，其中三分之一的中小企业感觉威胁尤为严峻。主要原因之一是许多中小企业经历过网络安全事件。我们的研究表明，56% 的亚太地区中小企业在过去 12 个月内曾遭遇过网络安全事件。

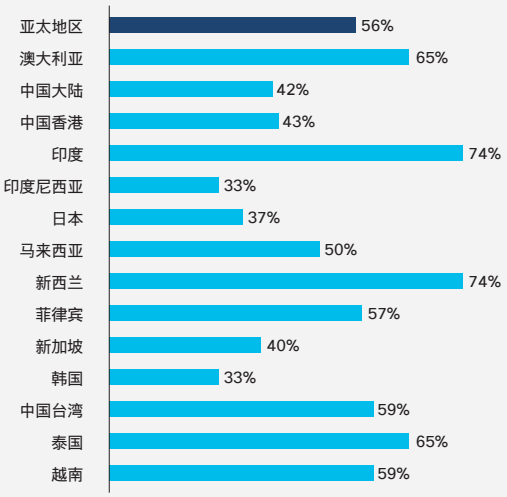
不过各个地区的数字有所不同，印度和新西兰有 74% 的中小企业经历过安全事件，而印度尼西亚和韩国只有 33%，日本有 37% 的中小企业称曾被攻击。

此外，近一半的受访者表示，他们在疫情期间遇到的网络安全事件有所增加，其中印度 (70%) 和新西兰 (61%) 增长最多，其次是菲律宾 (53%)、越南 (53%) 和澳大利亚 (50%)。

感觉受到网络安全威胁的中小企业百分比



在过去 12 个月内遭遇网络安全事件的中小企业百分比

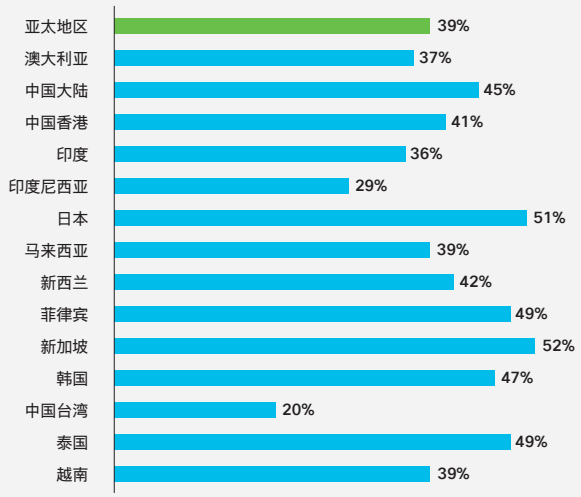


在遭受网络安全事件的受访者中，三分之一 (33%) 认为，企业没有采用网络安全解决方案是首要原因。不过，有更多的中小企业 (39%) 认为，首要因素是他们现有的网络安全解决方案不足以检测和防御攻击。这凸显出一个事实：要建立一个强大稳定的安全环境，拥有合适的技术至关重要。*思科安全成果研究报告*也深入探讨了中小企业领域的安全问题，同样有此重大发现。

经历过网络安全事件的中小企业承受了攻击者尝试渗透其系统的各种不同方式。其中恶意软件攻击影响了 85% 的中小企业，位居榜首。

随着计算机、平板电脑和智能手机等设备的采用率及使用率不断提高，攻击者越来越广泛地尝试在这些系统上部署恶意软件。恶意软件攻击者对中小企业的攻击尤为密集，试图中断、破坏或获得对目标设备的未授权访问。

认为“网络安全解决方案不足以检测到威胁或防御攻击”是首要因素，从而导致网络安全事件发生的中小企业百分比



攻击者对中小企业的兴趣可归结于几个关键原因。首先，黑客社区普遍认为，与大型组织相比，中小企业在网络安全方面相对薄弱，这使其成为有吸引力的目标。其次，中小企业与大型企业的合作也日益紧密多元。黑客们希望，如果他们能够渗透到特定的中小企业的网络中，就可以利用它作为跳板，然后入侵正在与之协作或进行数字交易和数字通信的大型公司的网络中。

根据受访者的说法，网络钓鱼攻击仅次于恶意软件攻击，70% 的受访者表示他们曾遭受网络钓鱼攻击。受访者报告的其他主要攻击形式包括 DNS 隧道 (68%)、服务阻断 (64%)、SQL 注入 (62%)、中间人攻击 (61%) 及零日漏洞攻击 (60%)。

定义

服务阻断攻击：试图关闭机器或网络，使其目标用户（通常针对的是银行、媒体公司或政府机构的 Web 服务器）无法访问

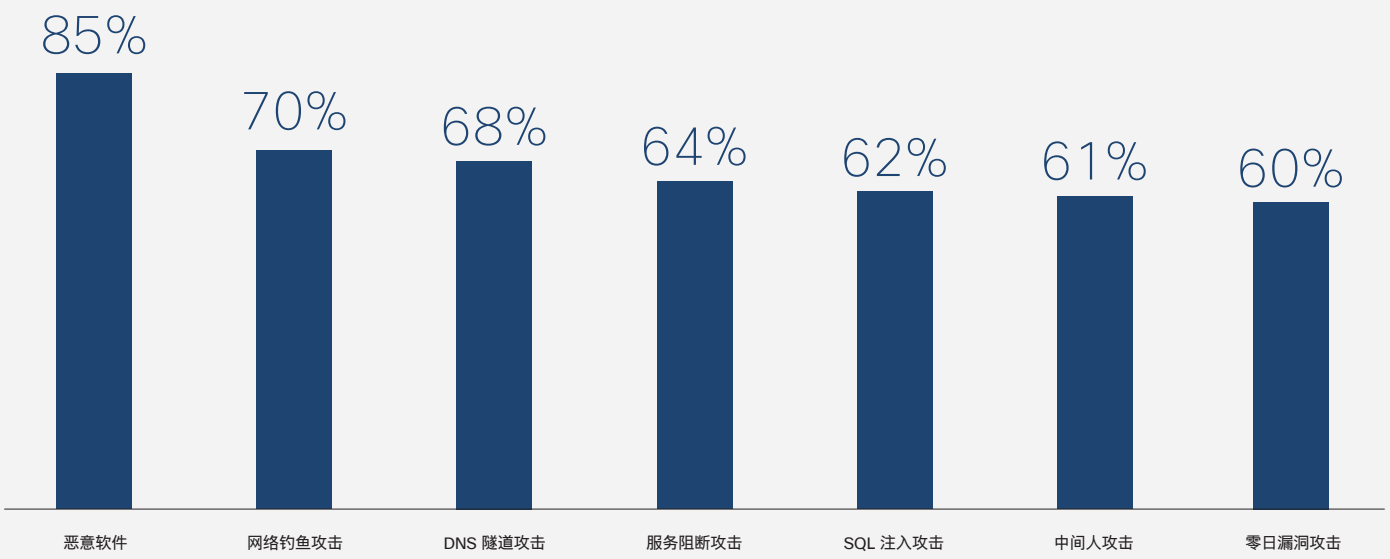
DNS 隧道：把其他程序或协议的编码数据封装到 DNS 查询和响应中

SQL 注入：用于攻击数据驱动的应用，在这些应用中，将恶意 SQL 语句插入到输入字段中并执行（例如将数据库内容转储给攻击者）

中间人攻击：攻击者将自己置于用户与应用之间的对话中，假装进行正常的信息交换，真正目的是窃取个人信息

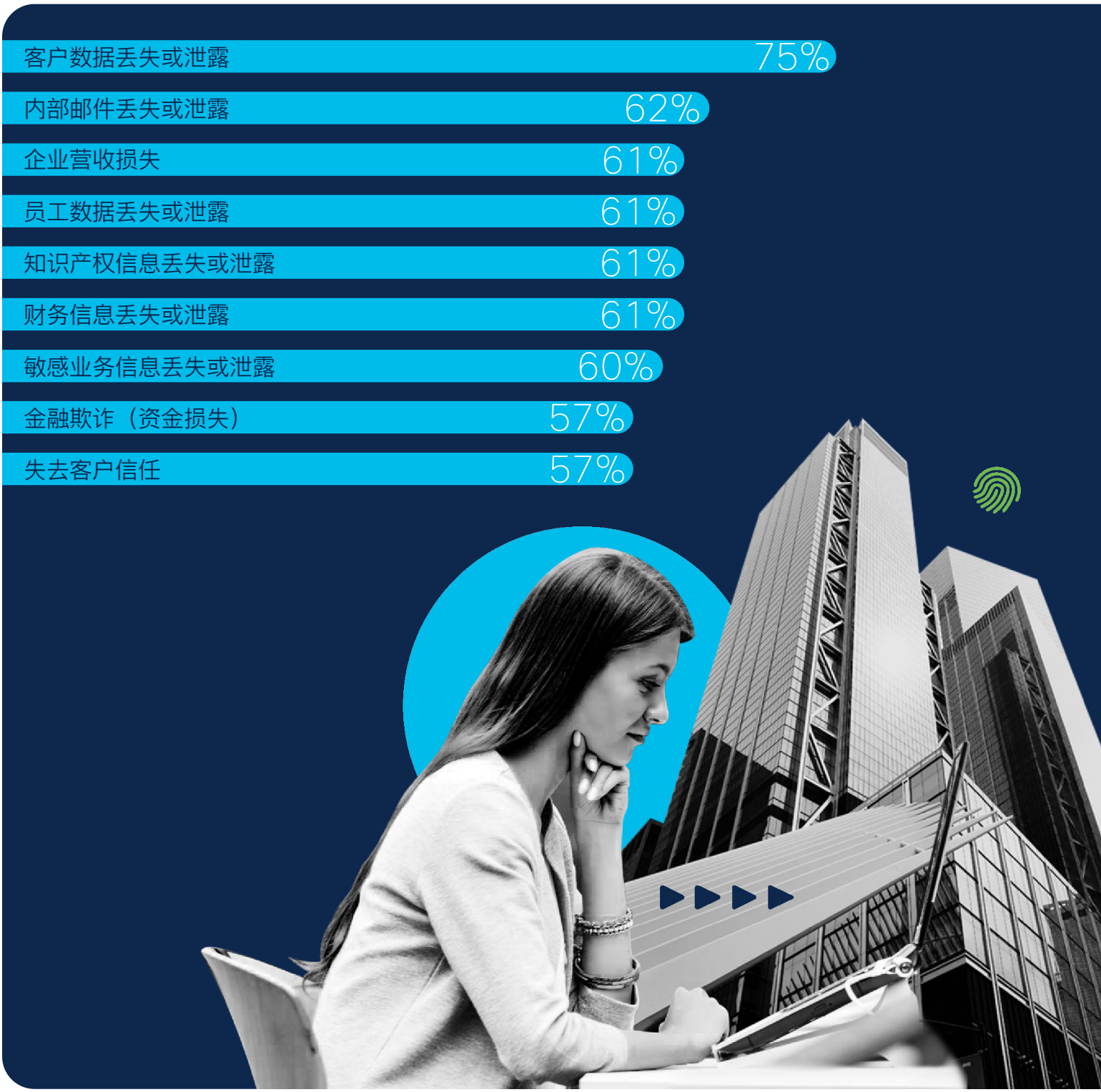
零日漏洞攻击：针对最近发现的软件漏洞发起的攻击，旨在窃取数据或造成损害

过去 12 个月亚太地区中小企业遭遇的网络攻击类型



损失惨重，难以数计

曾被攻击过的大多数中小企业都遭受了某种程度的损失。在经历过网络攻击的中小企业中，高达 75% 的企业表示，这导致了客户数据的丢失。在遭受攻击的中小企业中，60% 表示事件对企业营收造成负面影响。



业务中断，每秒必争

网络安全就像一种赔率游戏。在现实中，恶意攻击者占据了上风，赢面向他们倾斜。他们不断攻击目标，寻找机会。受到攻击的中小企业需要赢得每一次胜利才不至于功亏一篑，而攻击者只需打破一次防御就可以取胜。

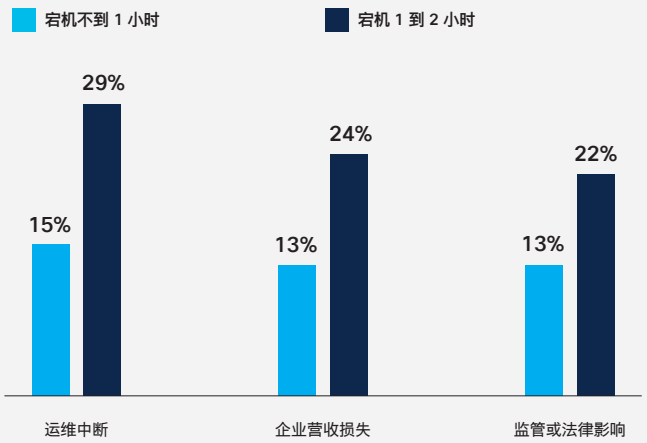
此外，企业确实需要一些时间来探测和调查威胁，以及在受攻击后进行修复。这通常为恶意攻击者提供了先发制人的机会，以致造成损失。

中小企业目前面临的挑战是，在这个高度互联、全数字化优先的世界里，企业必须即时满足客户的需要。这意味着企业在面对网络安全事件时，几乎没有中断运维的任何余地。他们需要能够快速检测、调查、阻止或修复任何网络安全问题。

研究强调，亚太地区 15% 的中小企业表示，不到 1 小时的宕机就会导致运维中断，而 29% 的中小企业表示，宕机时间在 1 到 2 小时之间会导致同样的情况。量化这种影响的结果是，13% 的受访者表示宕机时间少于 1 小时会严重影响企业营收，而 24% 的受访者表示 1 到 2 小时的宕机时间可能会造成同样的收入损失。

最能说明问题的是，10% 的中小企业表示宕机一天将导致其组织关闭。

宕机时间长度造成影响升级*



* 有关这些指标的市场细分数据，请参阅附录 A 中的图表

与此同时，随着国家/地区开始引入和实施网络安全指南和法规，网络安全事件导致的宕机也会带来法律影响。这一趋势已经开始出现，有 13% 的中小企业表示宕机时间少于 1 小时会对他们产生法律影响，而 22% 的中小企业表示，宕机时间在 1 至 2 小时之间可能会造成同样的后果。

面临如此重大后果，却只有 15% 的受访者表示他们可以在 1 小时内检测到网络威胁。这足以说明，保障网络安全对中小企业而言是一个巨大挑战。在一小时内可以完成修复的企业数量甚至更低，仅有 10%。

检测和修复安全事件所需时间分段百分比

	亚太地区	澳大利亚	中国大陆	中国香港	印度	印度尼西亚	日本	马来西亚	新西兰	菲律宾	新加坡	韩国	中国台湾	泰国	越南
检测网络事件平均时长															
1 小时内	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
1 到 2 小时	30%	28%	36%	28%	34%	31%	18%	32%	28%	28%	16%	34%	16%	33%	33%
事后修复平均时长															
1 小时内	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
1 到 2 小时	23%	20%	31%	26%	23%	27%	13%	21%	17%	22%	21%	18%	21%	26%	24%

鉴于反应迟缓对企业的影响，对事件做出快速反应变得至关重要。

中小企业不仅必须努力应对网络安全事件造成的企业营收损失，还要关注这些事件对整体收入的影响。在过去 12 个月内经历过网络事件的中小企业中，有超过一半 (51%) 表示，安全问题给企业造成的损失超过 50 万美元，而 13% 的中小企业表示损失超过 100 万美元。

事实上，被攻击过的大多数企业都遭受了经济损失。总体而言，83% 的受访者表示事件成本超过 10 万美元。

除此之外，还有无形的成本。在过去一年遭受网络攻击的企业中，57% 的受访者表示事件导致失去客户信任，而 66% 的受访者表示这会对企业声誉造成负面影响。虽然声誉下降和信任削弱的程度无法量化，但却可能对任何企业造成灾难性后果。

过去 12 个月内网络事件的财务影响（美元）

	亚太地区	澳大利亚	中国大陆	中国香港	印度	印度尼西亚	日本	马来西亚	新西兰	菲律宾	新加坡	韩国	中国台湾	泰国	越南
50 万美元或以上	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
100 万美元或以上	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

有备无患，加强安全

尽管亚太地区的中小企业忧心忡忡，并已经明显受到了网络安全事件的影响，但他们并没有就此放弃，而是准备正面迎战。他们从规划和培训入手，81% 的受访者表示已完成情境规划和/或模拟。

切合实际的情境规划和模拟可以帮助中小企业抢在攻击者之前发现网络安全环境中的薄弱环节，因此成为网络安全准备工作中的一项关键工作。已经开展了安全模拟演习的中小企业中，有 85% 表示他们发现了网络防御中的薄弱环节或问题。

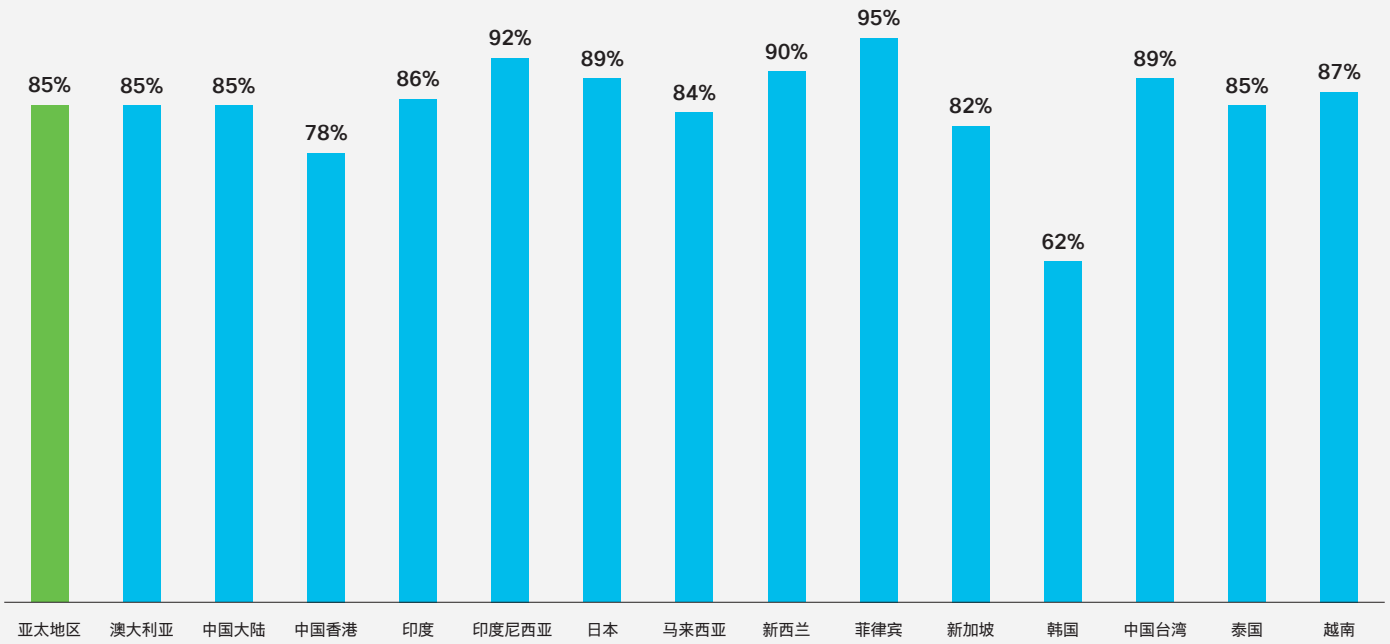
在发现了安全漏洞的组织中，95% 表示，这些演习揭示了一个关键问题：他们没有适当的技术解决方案来检测网络攻击或威胁。同样数量的受访者发现他们拥有过于庞杂的技术而难以集成；相比之下，96% 的受访者发现他们没有适当的技术解决方案来阻挡攻击。

很大一部分受访者认为他们组织的网络攻击响应流程不明确 (94%)。同时，95% 的受访者表示，虽然他们拥有适当的技术，但他们没有掌握适当技能的足够员工来利用这些技术解决问题。

令人鼓舞的是，大约有一半的中小企业能够在两周内解决他们在情境规划中发现的差距或问题。唯一例外是那些发现了问题但却没有适当技术来检测攻击或威胁的中小企业，他们大多需要更长的时间来解决这些问题。

虽然亚太地区的中小企业正在采取正确的步骤和计划以增强网络安全的恢复能力，然而他们在其他领域仍有不少工作要完成。排在首位的工作是教育所有利益相关者。近五分之一 (17%) 的受访者表示，他们的主管对当地网络安全法律和法规了解有限。这种认知差距在新西兰 (30%)、中国香港 (29%)、日本 (28%) 及韩国 (27%) 显著上升。

在网络安全情境规划和/或模拟中发现网络防御存在弱点的中小企业百分比



调整投资，物尽其用

中小企业还要确保通过投资支持其安全防备计划。实际上，研究表明亚太地区的网络安全投资水平普遍很高。

该地区三分之二 (63%) 的中小企业平均将至少 4% 的年收入用于网络安全，其中 30% 的中小企业的网络安全支出至少为 6%，9% 的中小企业的网络安全支出超过 10%。

实际上，自疫情开始以来，亚太地区大约有四分之三的中小企业增加了对网络安全的投资，大约有五分之二的中小企业增加了 5% 以上的投资。

值得一提的是，企业增加的支出已经在关键领域平均分配，这表明企业强烈需要采用多层面的综合解决方案来构建强大的网络安全环境。

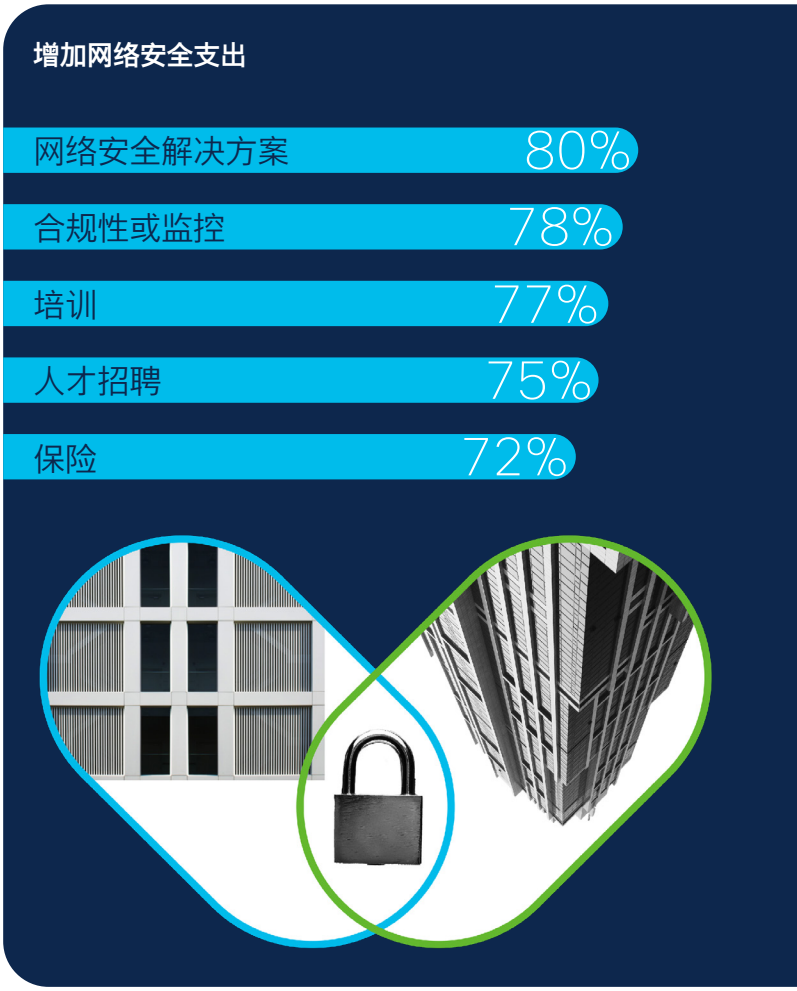
平均每年在网络安全上的支出百分比

	亚太地区	澳大利亚	中国大陆	中国香港	印度	印度尼西亚	日本	马来西亚	新西兰	菲律宾	新加坡	韩国	中国台湾	泰国	越南
无	1%	1%	0%	2%	1%	1%	8%	0%	0%	1%	2%	3%	0%	1%	0%
低于 1%	8%	11%	4%	7%	6%	5%	18%	13%	17%	7%	9%	15%	13%	6%	2%
1-3%	27%	27%	30%	38%	20%	14%	33%	28%	26%	32%	29%	37%	42%	19%	18%
4-5%	33%	34%	45%	40%	30%	37%	29%	23%	24%	32%	36%	28%	24%	32%	53%
6-10%	21%	15%	15%	9%	30%	34%	9%	24%	21%	14%	17%	15%	17%	27%	16%
超过 10%	9%	11%	6%	3%	13%	9%	3%	12%	11%	15%	7%	2%	4%	15%	11%

挑战仍然存在。中小企业表示提高网络安全恢复能力的主要障碍是：与不断发展的技术和安全要求保持同步 (77%)、追踪不断发展的网络威胁 (76%)、让员工积极参与并负起责任 (75%)、行业过于复杂 (75%)，以及难以招聘到合适人才 (73%)。

如右图所示，为建立正确的网络安全环境，亚太地区中小企业朝着正确方向迈出了一步，开始在解决方案、合规性、人才和培训等领域加大投资。

中小企业着眼于整体防范这一事实，最能够说明他们对网络安全的认知日益成熟。但是，即使中小企业努力在解决方案、人才及培训等方面进行投资，他们还是发现自己处于被攻击的位置。行业性质决定了中小企业是恶意攻击者的重点目标。随着人们越来越了解网络事件对企业的潜在影响，特别是面对持续增加的法律影响，中小企业正在将网络安全保险作为一项关键领域加以投资。这可以为他们提供一种保障，缓解任何此类安全事件对其企业产生的财务影响。



在提高网络弹性方面存在以下障碍的中小企业百分比

	亚太地区	澳大利亚	中国大陆	中国香港	印度	印度尼西亚	日本	马来西亚	新西兰	菲律宾	新加坡	韩国	中国台湾	泰国	越南
与不断发展的技术和安全要求保持同步	77%	82%	63%	73%	87%	53%	69%	84%	83%	89%	79%	75%	72%	71%	80%
努力追踪不断变化的网络威胁	76%	80%	59%	71%	87%	50%	66%	87%	81%	88%	82%	74%	74%	77%	81%
让员工积极参与并承担责任	75%	76%	61%	65%	86%	55%	70%	81%	82%	81%	75%	67%	68%	73%	81%
行业过于复杂	75%	77%	61%	63%	85%	57%	65%	80%	87%	82%	82%	69%	65%	74%	79%

中小企业：五种习惯保安全

本报告揭示了中小企业在应对不断变化的网络安全形势时面临的常见挑战。这一节将介绍各种规模的中小企业可借鉴的五种改善其网络安全环境的好习惯。

1 **沟通交流大有益处：**网络安全环境在不断发展，因此中小企业需要紧跟最新变化，随时了解网络威胁及其给组织带来的潜在影响。高层负责人和所有利益相关者之间应该定期频繁进行沟通，以确保将网络威胁应对方案纳入业务规划。我们的调查表明，具备充分能力应对网络安全事件的中小企业经常沟通安全问题。超过 90% 的受访者每周讨论安全问题和风险，而超过三分之二 (68%) 的受访者每天讨论。面对威胁，组织不力的中小企业讨论网络安全问题的频率较低，大约三分之一 (31%) 的中小企业讨论问题的频率低于每月一次。

2 **简单至上：**处理网络安全的传统方法是购买单点安全产品和解决方案，以解决当时的特定问题。但是，这导致许多中小企业在基础设施中堆积了大量的产品和解决方案。在许多情况下，这些产品和解决方案无法集成，从而在网络安全事件发生之际导致复杂操作及不必要的延迟。要想加快处理攻击的速度及得到有效成果，必须评估网络安全解决方案中的各部分如何协同工作，这一步不可或缺。中小企业需要利用单一集成的平台连接各种各样的产品和解决方案，以获得对整个安全基础设施的清晰可视性，并且确保系统在实际环境中面对真实考验时，可以无缝协同工作。

3 **有备才无患：**确保中小企业为现实网络世界做好准备的一个方法，是在一个更可控的环境中模拟各种问题和结果。这可以帮助中小企业真正了解任何漏洞可能存在的地方，并为他们提供解决这些漏洞的机会，从而为真实世界的情境做好准备。事实上，我们的研究发现，准备更充分的中小企业有一个共同特征，那就是超过 98% 的中小企业在过去 12 个月内进行了情境规划或模拟。几乎所有这些中小企业 (高达 96%)制定了恢复计划，以确保他们在遭遇攻击后能够尽可能快速高效地重新启动业务。相比之下，在缺少有效规划的中小企业中，超过一半 (58%) 没有实施情景规划，而且近三分之二 (63%) 的企业没有恢复计划。

4 **培训再培训：**我们必须了解的是，在中小企业可以部署的所有技术和解决方案中，员工往往是最薄弱的环节。正因为如此，我们可以看到尽管行业不断在进步，但网络钓鱼攻击（诱使人们点击发送给他们的数字通信中的链接）仍然是头号威胁。中小企业应该保证每位员工都了解网络安全的基本知识，以及自己在维护企业安全方面可以发挥的作用，无论其工作角色是什么。

我们在这方面的研究数据令人震惊。在管理网络安全形势方面未雨绸缪的中小企业中，96% 同意或强烈同意员工对网络安全有总体了解，95% 的受访者了解潜在攻击的严重性及其自身的职责。相比之下，准备不足的公司对员工的信任度较低，只有 15% 认为员工了解网络安全。

5 **同心协力，其利断金：**要想在网络安全方面取得全面成功，与合适的技术伙伴合作是关键所在。中小企业应牢记一些原则。首先，合作伙伴应该能够为他们的整个业务提供端到端保护。在大多数情况下，这需要将不同的产品和解决方案集成到单一平台上，以实现整个基础设施的简化性和可视性。其次，随着中小企业踏上全数字化之旅，他们的业务将最终实现增长，运维也将同步扩展。但是无论规模大小，中小企业选择与之合作的技术伙伴应该有能力保障其运维安全。最后，合作伙伴应该为中小企业提供技术部署的不同使用模式。

关于本研究

3748 名受访者 涵盖 14 个市场

市场

- 澳大利亚
- 中国大陆
- 中国香港
- 印度
- 印度尼西亚
- 日本
- 马来西亚
- 新西兰
- 菲律宾
- 新加坡
- 韩国
- 中国台湾
- 泰国
- 越南

受众

负责网络安全的 IT 和业务主管

这些组织包括:

- 小型（1 至 249 名员工）
- 中型（250 至 999 名员工）

行业

- 广告或市场研究
- 业务服务（例如会计、咨询）
- 建筑
- 教育
- 工程、设计或建筑
- 金融服务
- 医疗
- 制造
- 媒体和通信
- 自然资源（例如石油、采矿及森林）
- 个人护理服务
- 专业服务
- 房地产
- 餐饮服务
- 零售
- 技术服务
- 运输
- 旅行服务
- 批发
- 其他

附录 A

由于宕机时间延长而导致影响升级

	亚太地区	澳大利亚	中国大陆	中国香港	印度	印度尼西亚	日本	马来西亚	新西兰	菲律宾	新加坡	韩国	中国台湾	泰国	越南
在组织运维受到严重影响之前的宕机时长															
1 小时内	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
1 到 2 小时	29%	25%	28%	21%	32%	35%	18%	32%	39%	28%	23%	29%	28%	31%	30%
在企业营收受到严重影响之前的宕机时长															
1 小时内	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
1 到 2 小时	24%	20%	26%	21%	24%	27%	17%	23%	19%	27%	20%	19%	34%	28%	20%
在企业面临监管或法律影响之前的宕机时长															
1 小时内	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
1 到 2 小时	22%	19%	24%	18%	24%	32%	15%	23%	20%	19%	24%	21%	25%	22%	17%

关于 Cisco Secure

思科长期以来一直是网络行业领导者，在此过程中构建了一个开放的集成式网络安全解决方案组合。我们认为，各项安全解决方案应该像一个团队一样协同合作。它们应该作为一个协同的单位去发现问题并做出响应。在这种情况下，安全系统性和效力才能得以提升。作为全球最大的 IT 基础设施和网络服务提供商，以及全球最大的 B2B 网络安全企业，多年来我们一直深受客户的信赖。

Cisco Secure 秉持不断优化、简化的安全原则。我们提供以客户为中心的精简安全方法，可确保各产品不仅易于部署、易于管理、易于使用，而且可以协同工作。我们深知，客户及其相关人员是我们产品和服务的核心，他们希望消除复杂性和干扰，获得可靠的安全解决方案，注重最终成果。这就要求我们做到简化而不过于简单。我们的云原生平台在这方面实现了巨大飞跃。

利用 Cisco SecureX 平台，我们可以为安全行业提供可靠的安全解决方案，确保您在当下和未来免受威胁困扰。我们提供全球最全面、集成度最高的网络安全平台，帮助财富 100 强公司防御当前和未来的各种威胁。如需详细了解我们如何简化体验，促进您取得成功并提供面向未来的安全保护，请访问 cisco.com/go/secure。

思科安全成果研究

如需深入了解，请阅读面向中小企业 (SMB) 的 2021 年安全成果研究，并访问我们的专用页面，了解更多 Cisco Secure 思想领导力内容。

美洲总部
思科系统公司
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 Amsterdam
荷兰阿姆斯特丹

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


CISCO