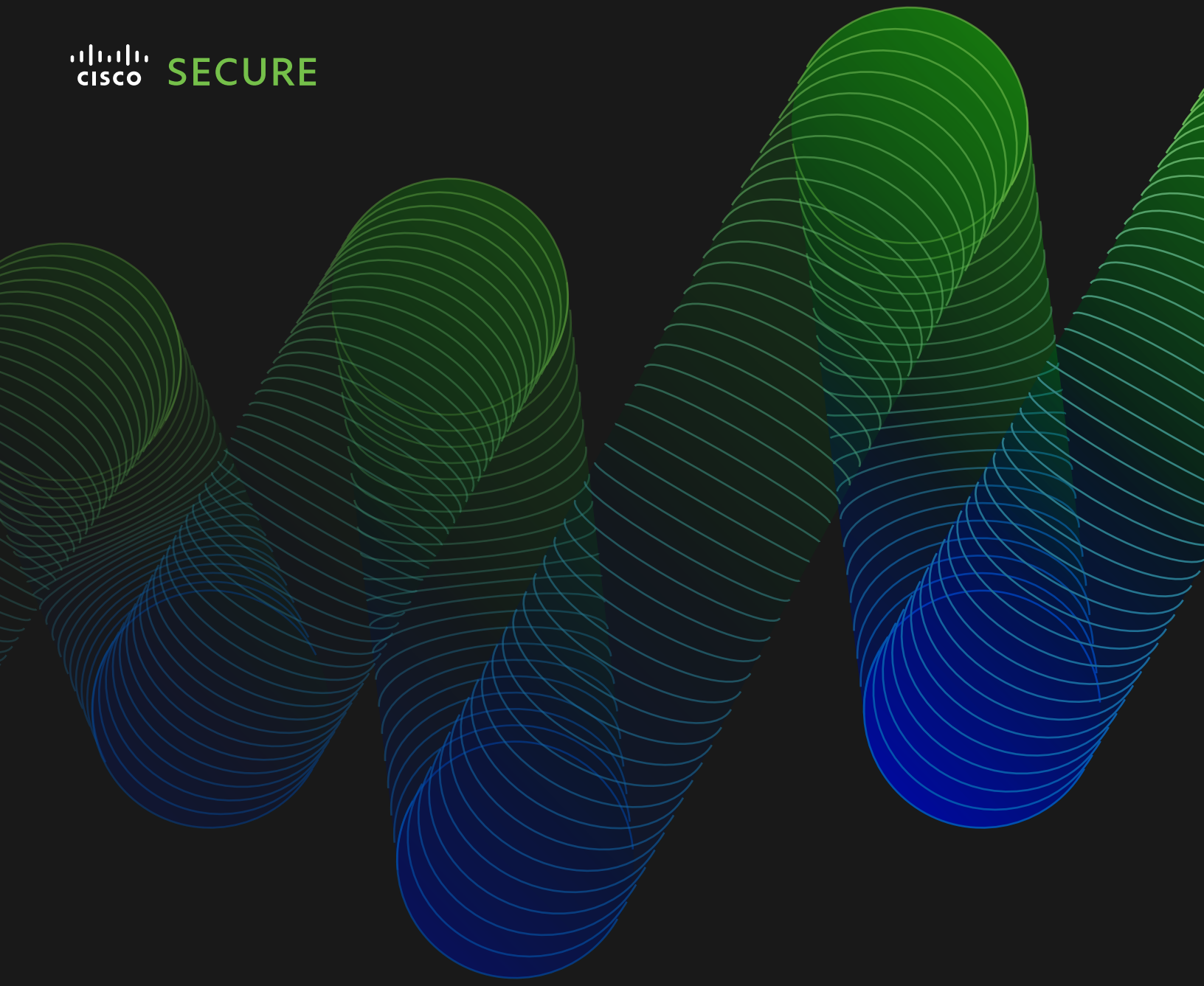
cisco SECURE



亚太地区安全弹性现状

《安全成果报告》第 3 卷的研究成果

cisco The bridge to possible

评估安全弹性

什么是安全弹性？为何安全弹性至关重要？ 组织如何显著提高安全弹性？这些都是我们在最近发布的《安全成果报告》第 3 卷中试图回答的问题。该报告分析了向全球 4700 多名安全主管及专业人员收集的数据 。本文旨在重点分析在亚太地区工作的 1400 多名受访者给出的答复。

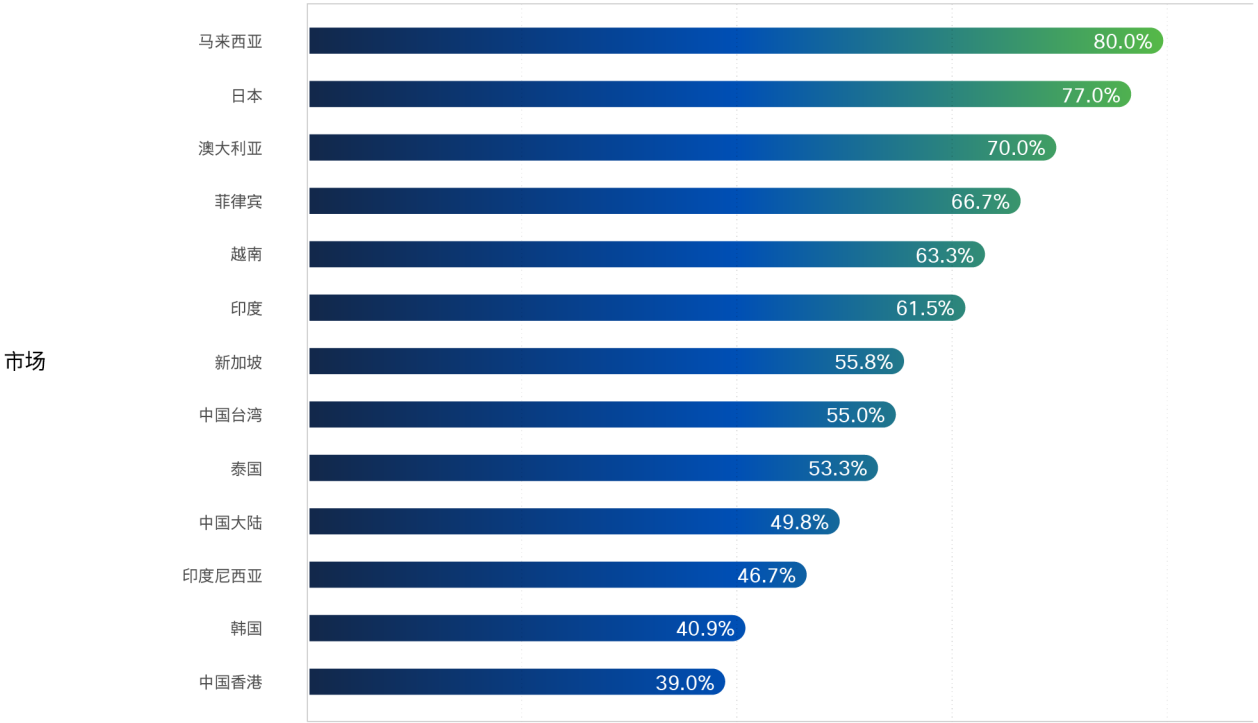
高管是否关注和重视弹性？

是的! 我们向受访者询问了其高管对安全弹性的关注程度和重视程度。受访者的答复清楚地表明, 97% 的亚太地区高管认为安全弹性非常重要, 而这一统计数据在整个地区差异不大。

网络事件是否会影响弹性？

全球 62% 的组织 (58% 位于亚太地区) 报告经历过危及业务运营的重大安全事件, 而且大多数此类事件都发生在近几年内。 在整个亚太地区, 影响安全弹性的事件的发生率差异很大。报告的事件频率最低的是香港 (39% 的组织) , 最高的是马来西亚 (80% 的组织) , 其他市场则以一定的间隔落在这两个极值之间。

图 1: 报告的影响弹性的安全事件发生率

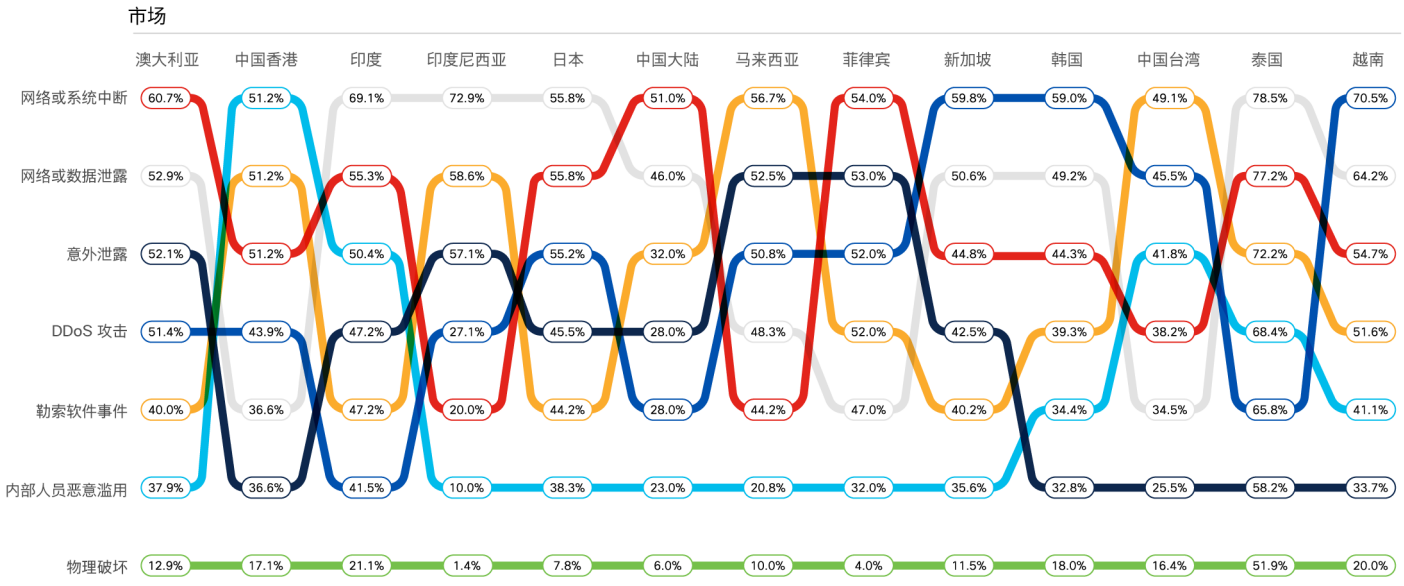


来源：思科安全成果报告

哪些类型的网络事件会影响弹性？

我们还邀请受访者详述所经历的影响弹性的事件类型。下图根据每个市场中报告安全事件的组织百分比对常见事件类型进行了排名。例如，DDoS 攻击在新加坡 (60%) 和韩国 (59%) 最常见，但在印度 (37%) 排名倒数第二。涉及物理破坏的事件在所有市场中都是最不常见的。

图 2：影响弹性的安全事件类型

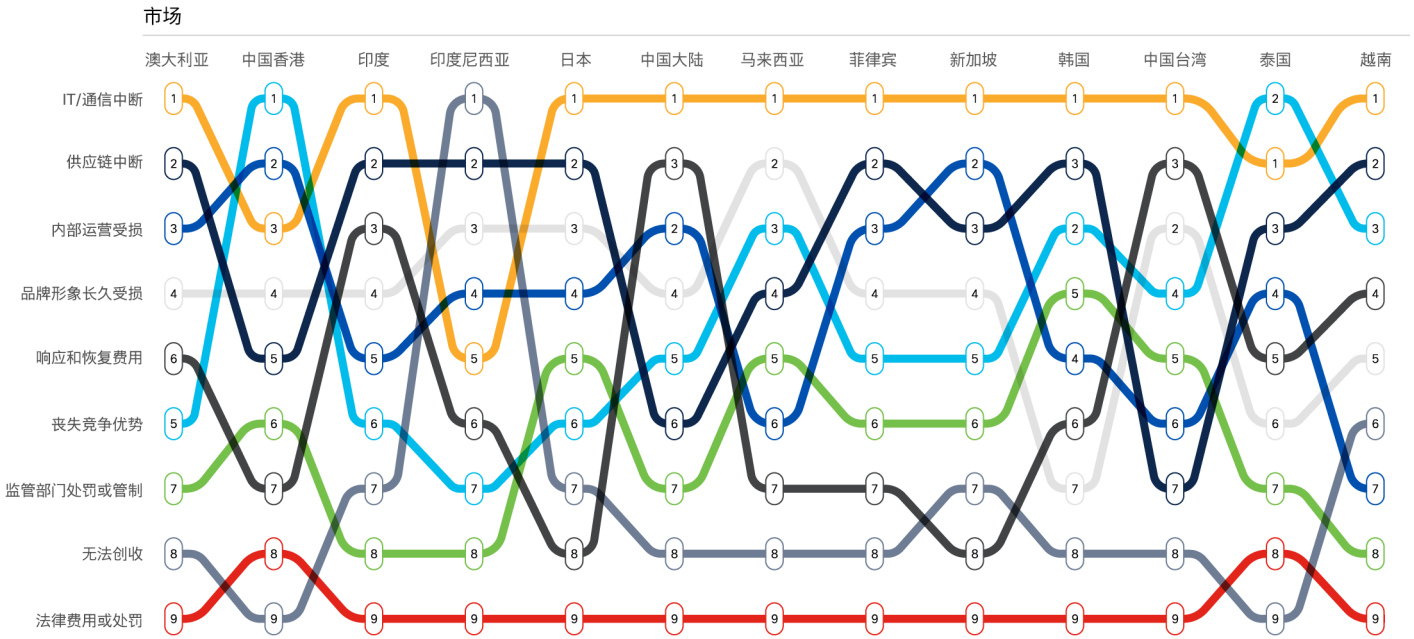


来源：思科安全成果报告

事件会对业务造成怎样的影响？

我们向受访者询问了这些重大安全事件对其组织产生了怎样的影响。下图根据每个亚太市场中报告经历过安全事件的组织百分比对影响类型的排名进行了比较。例如，在大部分市场中，IT 中断是最常见的影响类型，而法律费用或处罚通常排在最后。事件过后无法创收在印度尼西亚排名第 1，在中国香港和泰国则变为了第 9。

图 3：安全事件造成的弹性影响类型



来源：思科安全成果报告

可能造成不同市场之间安全事件发生率、类型和影响存在差异的原因包括：监管和合规压力、地缘政治因素、流行的业务模式、事件检测能力和安全计划成熟度等方面的差异。

“在保护资产之旅中，许多组织都在初始策略创建和实例化方面遇到了困难。如果没有适当地遏制安全事件，恶意软件或其他威胁可能会在整个组织的网络中肆意传播，通过横向移动引起广泛感染。

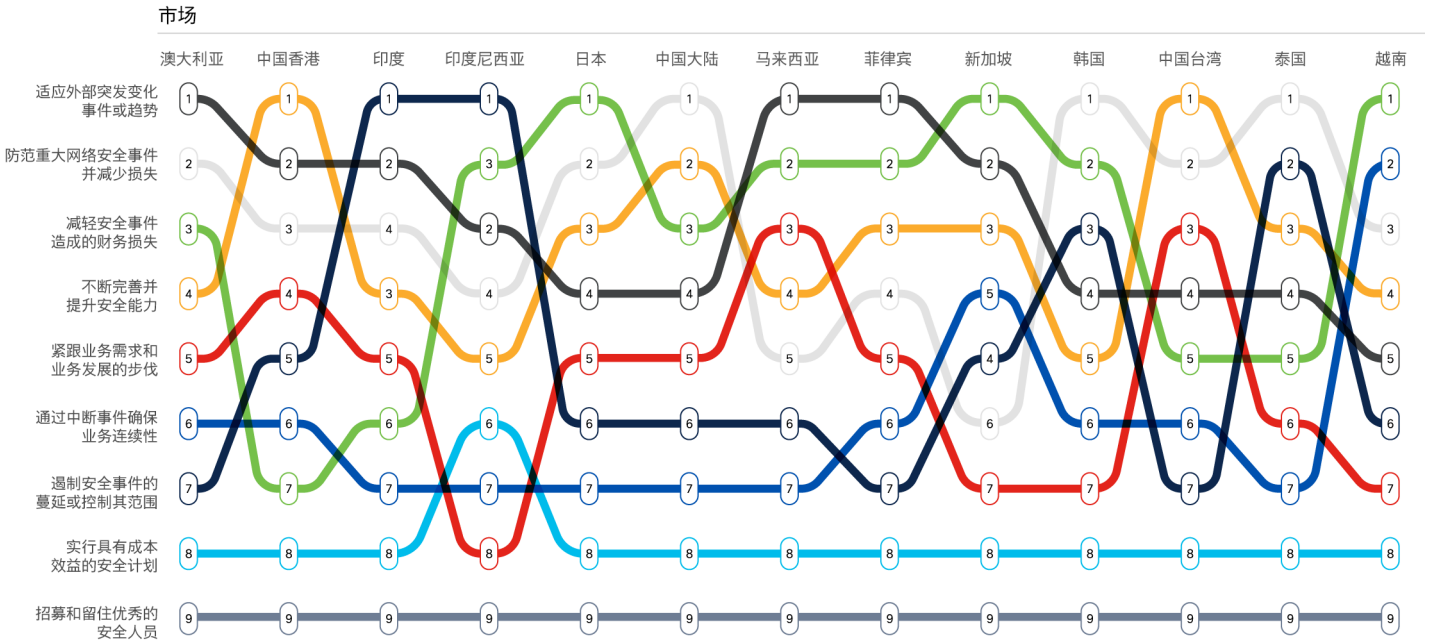
缺乏安全事件遏制措施还会导致难以识别和隔离感染源，这样可能会延长解决问题所需的时间，甚至使组织陷入服务器完全中断的境地，即本文中提到的“IT/通信中断”和“内部运营受损”。

– Timothy Snow，
思科，亚太地区首席信息安全官顾问兼架构师

哪些弹性成果优先级最高？

主要报告提出了与安全弹性相关的 9 个核心目标或成果。我们向受访者询问了在这 9 项成果中其组织认为哪项最重要，亚太地区市场的排名如下。在几乎所有市场中，实行具有成本效益的安全计划和招募/留住优秀的安全人员优先级都是最低的。然而，其他成果之间存在相当大的差异。例如，减轻安全事件造成的财务损失在日本和新加坡优先级最高，但在中国香港和印度优先级则分别排在第 7 位和第 6 位。

图 4：安全弹性成果优先级排名

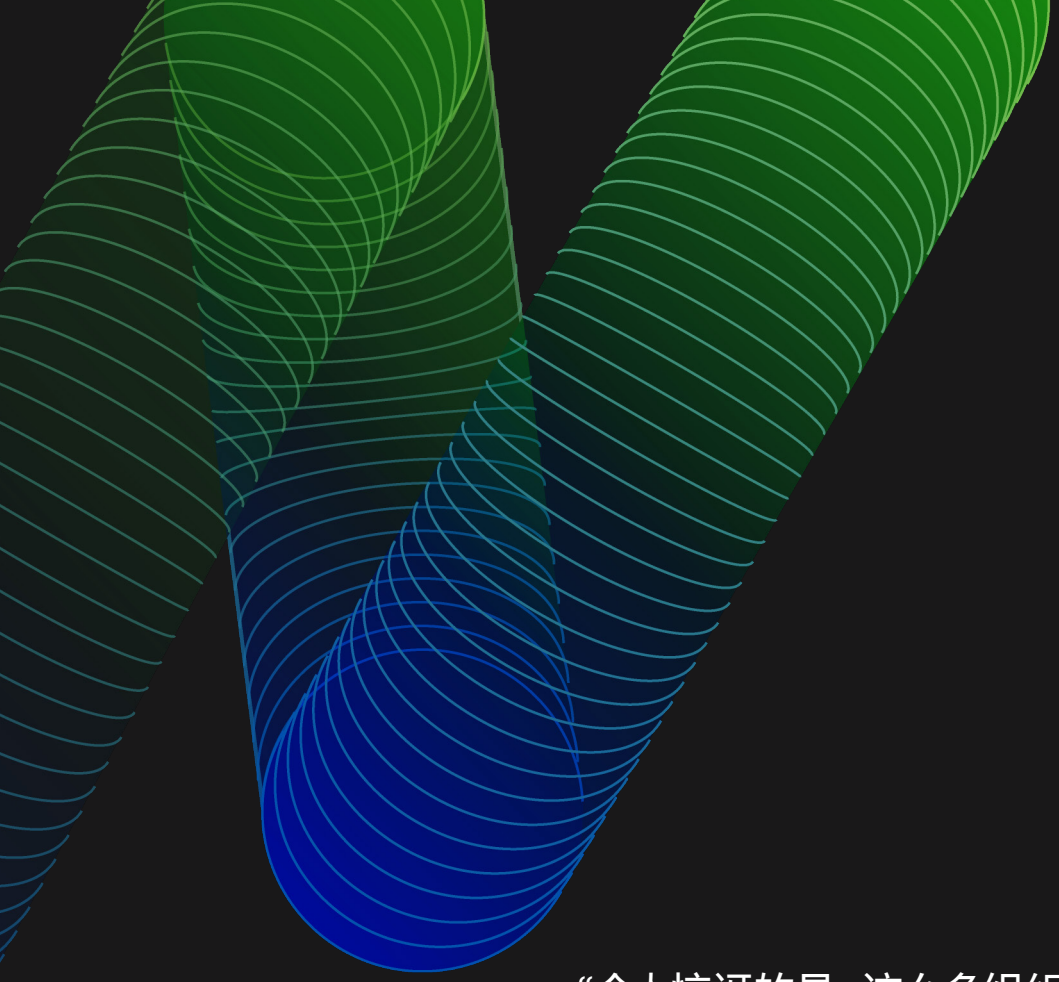


来源：思科安全成果报告

客户聚焦

聆听 Kasikorn Bank and Business-Technology Group (KBTG) 首席信息安全官 Chatchawat Asawarakwong 讲述这家金融服务组织如何利用 Cisco CX 为其数字化转型之旅保驾护航。观看视频。

为了保护其 2.5 万名用户，澳大利亚最大的国内和国际航空公司 Quantas 部署了 Cisco SASE 以减少混合办公面临的阻碍，提高员工满意度。阅读案例研究。



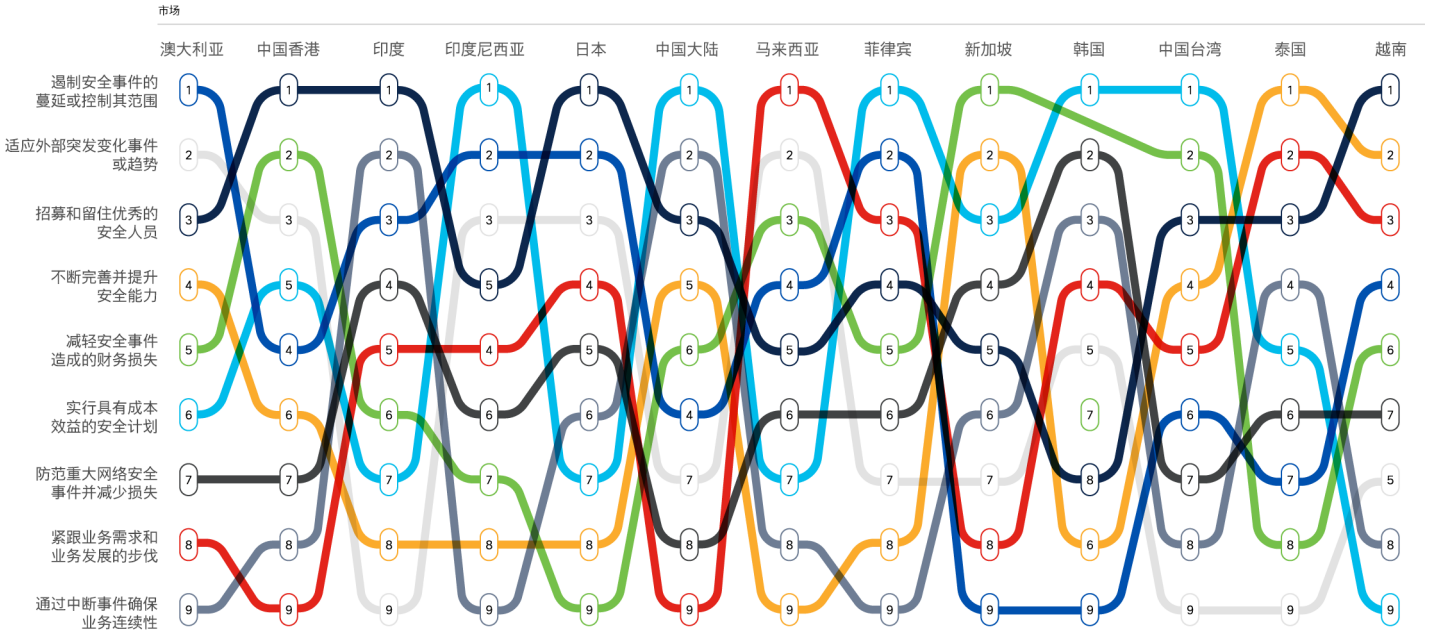
“令人惊讶的是，这么多组织竟然将‘招募和留住安全人才’的优先级排得这么低，因为我们看到很多组织在采用新技术方面举步维艰，就是因为他们没有专业人才，他们现有的团队已经捉襟见肘。这种情况在中小型组织中更为普遍，但即使是大型企业也存在人才流失的问题。这直接影响了采用新技术拓展并保护业务的成效。”

– Timothy Snow，
思科，亚太地区首席信息安全官顾问兼架构师

哪些弹性成果最难以实现？

我们还请受访者评估了其组织在实现每项弹性成果方面的实际成效。下图显示了与每项成果关联的相对挑战性排名，以及排名在整个亚太地区的变化轨迹。每个市场应对不同挑战的情况各异，很有意思。例如，对于澳大利亚的组织，遏制安全事件的蔓延或控制其范围是最大的挑战，但对于新加坡和韩国的组织，这是最小的挑战。马来西亚的公司在确保安全计划紧跟业务需求方面遇到的挑战最大，但中国香港和中国大陆的公司则认为此项是最小的弹性挑战。

图 5：实现安全弹性成果的难度排名



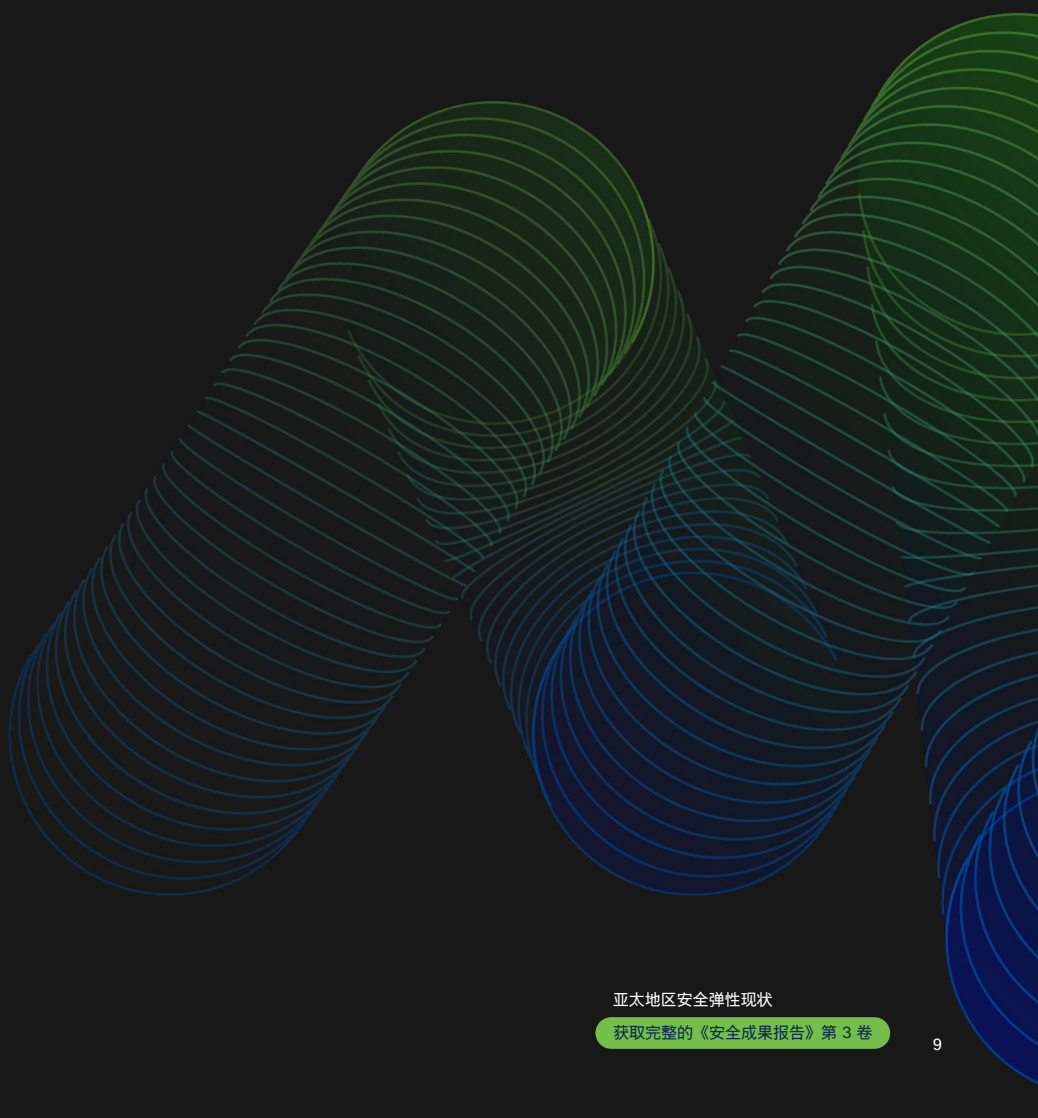
来源：思科安全成果报告

利用安全弹性适应和克服挑战

无缝集成的安全堆栈可以降低实际产品成本，并减少用于部署、管理和维护的资源。从云优先解决方案到托管服务，Cisco Secure 可以让您的安全团队专注于更关键的业务计划。详细了解如何构建安全弹性，同时降低风险和成本：
阅读电子书

“亚太地区非常注重成本，其中有几个市场将‘实行具有成本效益的安全计划’排在首位。成本效益不仅体现在产品或服务的购买方面，更体现在技术的安装、许可、培训和维护上。这还可以反映出该地区在构建全面的安全架构方面困难重重。正如上一期《安全成果报告》(第 2 卷) 中所述，安全人员配备比例与更敏捷的威胁响应之间存在直接关联，与那些安全人员配备比例较低的组织相比，比例更高的组织具有更强的响应能力。”

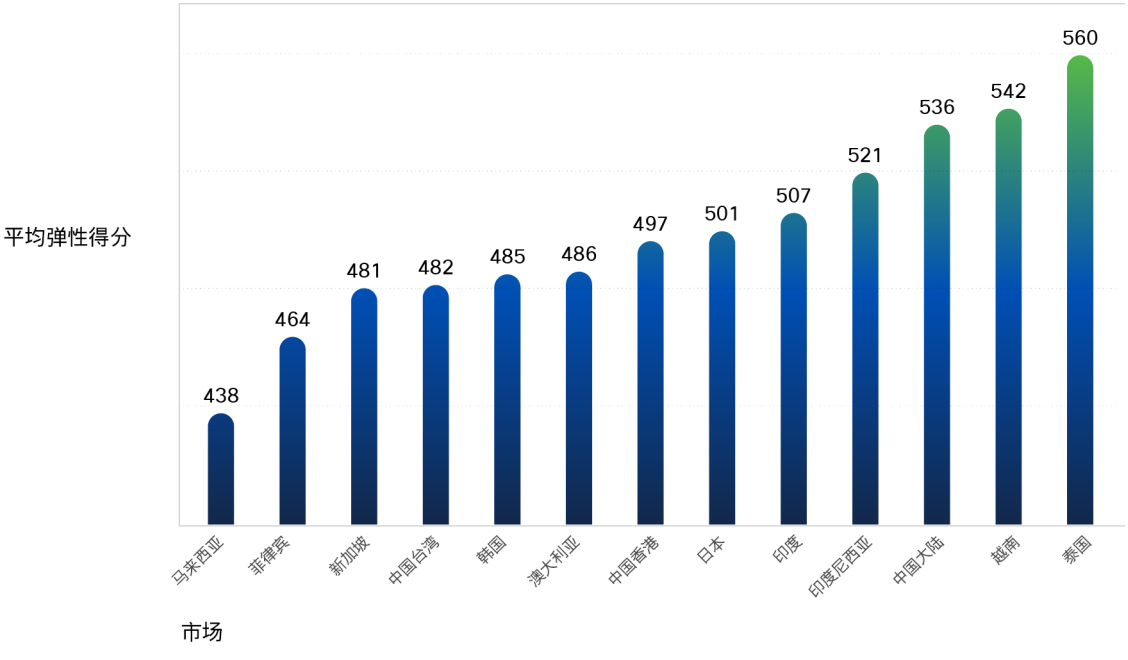
– Timothy Snow，
思科，亚太地区首席信息安全官顾问兼架构师



我们能否衡量整体安全弹性？

我们根据每个组织在 9 项成果中的成绩，汇总了其安全弹性得分。 按照全球平均值为 500 分，对这些得分进行了标准化处理。总体而言，在亚太地区的 13 个市场中，有 6 个市场的表现超过全球平均值。马来西亚组织的平均安全弹性得分最低 (438)，泰国组织的平均安全弹性得分最高 (560)。

图 6：各市场中组织的平均安全弹性得分



来源：思科安全成果报告

提高安全弹性

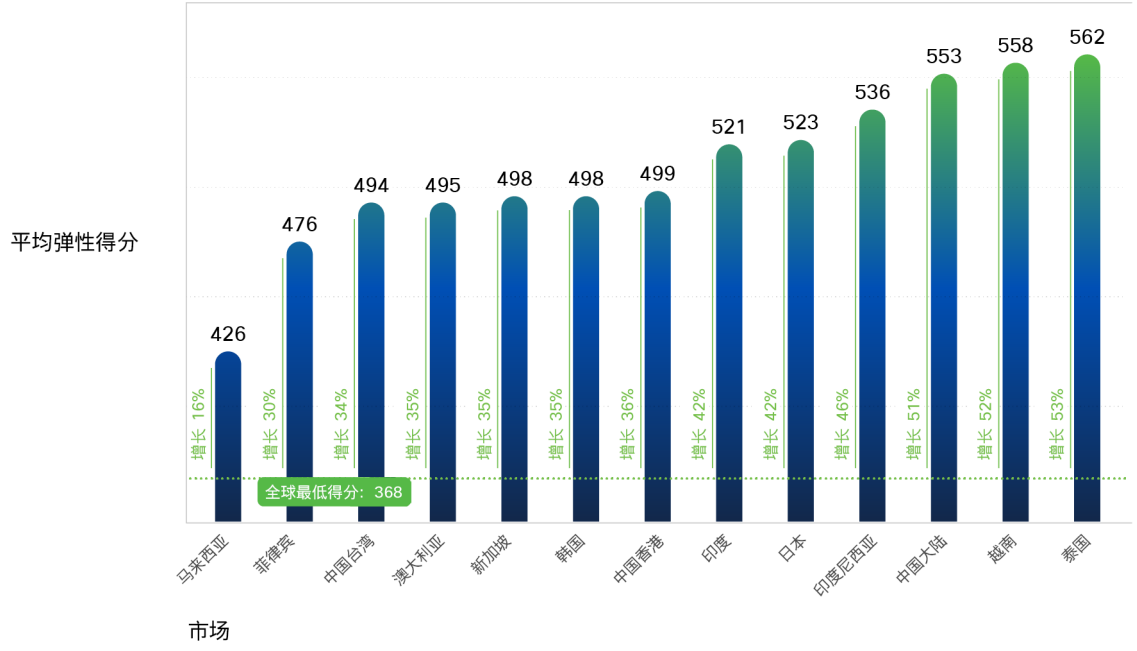
根据亚太地区各组织在 9 项成果方面的整体安全弹性得分，我们分析了许多因素，从而确定了可以显著提高这些成果的 7 大因素。现在，我们来看一下与亚太地区几个特定因素相关的整体安全弹性得分的潜在提高幅度。

确立高管支持

从整体来看，对于高管支持不力的组织，其安全弹性得分比获得高管大力支持的组织低 39%。我们主要报告的数据中提供了一些关于如何获得这种支持的线索。在这里，我们感兴趣的是，亚太地区的市场是否表现出类似的效应。

下图显示了各市场中安全计划获得高管有力支持的组织的平均安全弹性得分（蓝条）。这些长条一侧的增长百分比衡量的是，相对于缺乏高管支持的组织而言，整体的潜在提高幅度。例如，从中可以看出，马来西亚的组织确实受益于高管的大力支持（平均安全弹性得分增长 16%），但相比 39% 的全球平均值，这一增长幅度并不那么显著。但是，在泰国，当组织获得高管大力支持时，平均安全弹性得分增长幅度相对更大，达到了 +53%。

图 7：高管支持对安全弹性的潜在影响



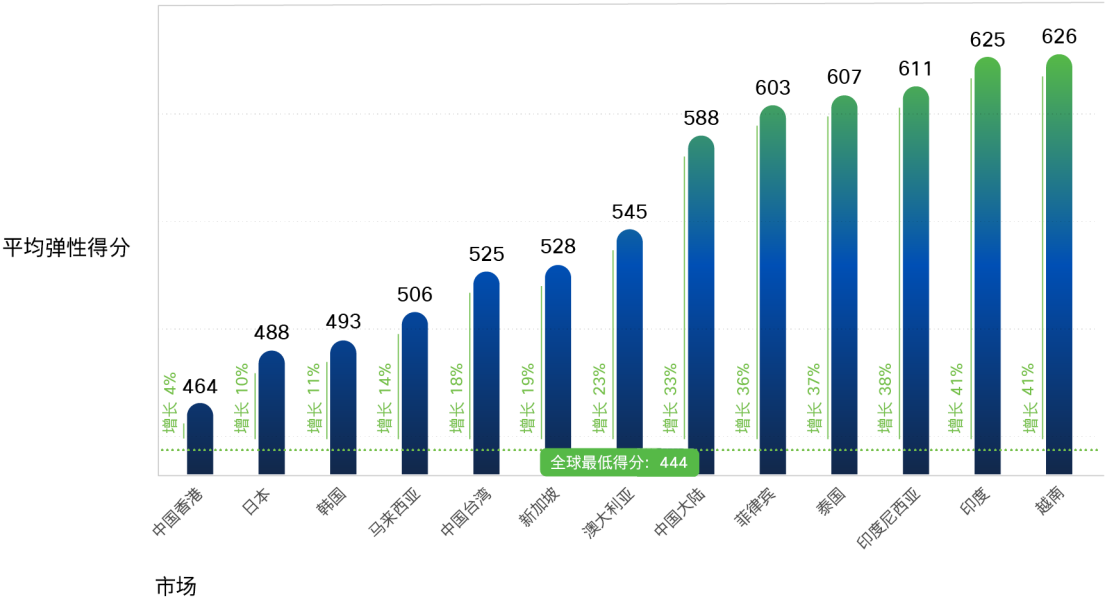
来源：思科安全成果报告

最大限度地提高零信任采用率

主要报告表明，尚未开始实施零信任原则的组织与已充分实施此类原则的组织（后者实施了 MFA、持续验证以及包含自适应策略、广泛监控和用户工作流程协调的微分段）之间，平均安全弹性得分差异达到了 30%。

在大多数情况下，亚太地区市场表现出了与零信任相关的相似弹性得分增长状况。充分实施零信任原则后，香港公司的安全弹性增长幅度 (+4%) 与全球平均水平相比要低得多，而越南公司则高得多 (+41%)。

图 8：采用零信任原则对安全弹性的潜在影响



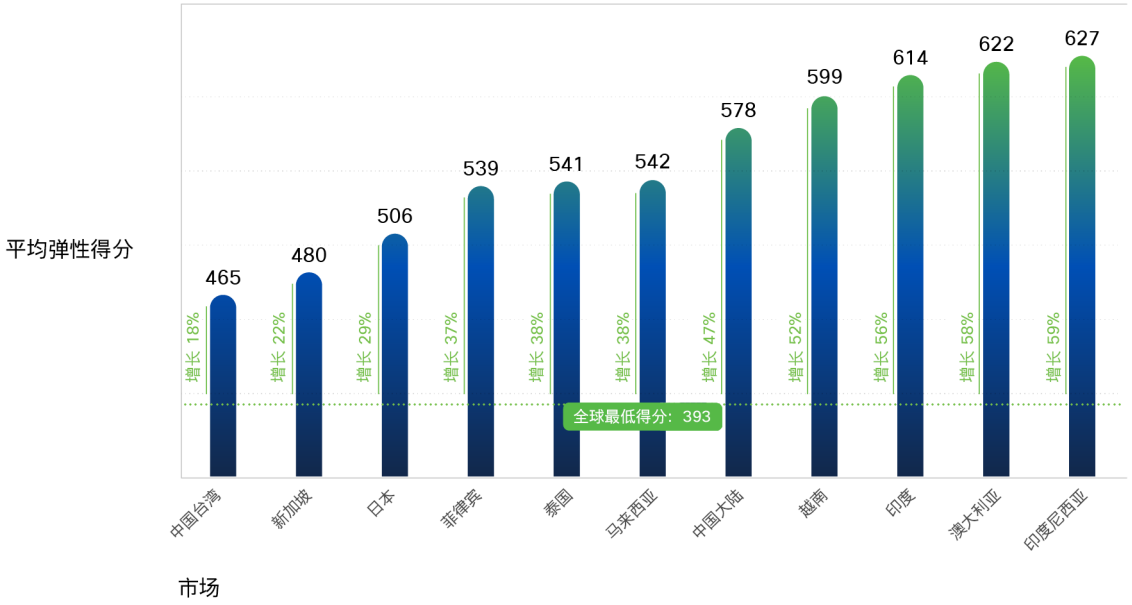
来源：思科安全成果报告

扩展检测和响应能力

现代网络威胁的传播媒介多种多样 。因此，在这些媒介上部署多个观测点对于网络防御非常有利。扩展检测和响应 (XDR) 解决方案的核心价值主张就是提供跨网络、云、终端和应用的数据可视性，同时应用分析和自动化功能来检测、分析、搜索当前和未来的威胁并采取补救措施。

我们的数据表明，XDR 实现了所主张的价值。充分实施 XDR 的组织的整体弹性得分比没有 XDR 能力的组织高 45%。根据下图，亚太地区主要市场的平均增长在高于 (中国、越南、印度、澳大利亚、印度尼西亚) 和低于 (中国台湾、新加坡、日本、菲律宾、泰国) 该基准的两侧相对均匀分布。

图 9：采用 XDR 对安全弹性的潜在影响



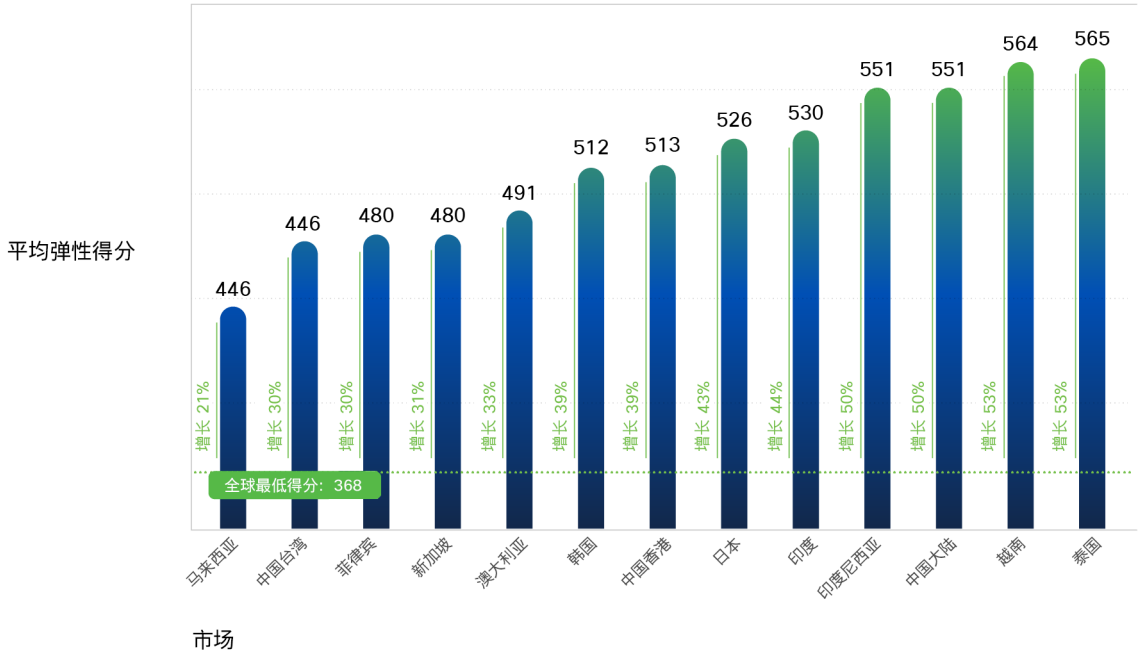
来源：思科安全成果报告

将安全扩展至边缘

由于混合办公快速发展（包括移动办公、设备激增以及应用广泛分布于多个云提供商中），保护这种分散化的广泛互联面临着越来越大的挑战。安全访问服务边缘 (SASE) 提供了一种策略，可将网络和安全融合到云服务中，简化运维，在面对不断变化的业务需求时保持弹性。此外，最新的《安全成果报告》有力地证明了 SASE 确实卓有成效。

从世界范围来看，未实施 SASE 与已完善地实施 SASE 的组织之间平均弹性得分差异达到 27%（点击此处可查看 SASE 包括哪些内容）。亚太地区除了一个市场（马来西亚）以外，所有市场中公司的弹性得分增长幅度都比尚未开始部署 SASE 的公司的基准更高，泰国则高达 +53%。

图 10：采用 SASE 对安全弹性的潜在影响



来源：思科安全成果报告

结论

尽管亚太地区不同国家和市场对于我们所提出的问题的答复存在一定差异，但也有一些值得探究的共同之处。整个地区的高管普遍认为安全弹性非常重要。那么，在组织内部可以采取哪些举措来解决有关安全弹性的问题？数据已经清楚地表明，增强 XDR 能力、加强对零信任原则的采用和充分实施 SASE 是实现更高弹性的关键。当然，优化其中每一个方面都要经历一个过程，需要 IT 和安全运营团队共同进行规划和协作。

详情请访问：

要深入了解团队如何协作才能实现其弹性目标，请下载完整的《安全成果报告》第 3 卷：打造安全弹性。

CISCO
SECURE

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

发布日期：2023 年 3 月

The bridge to possible