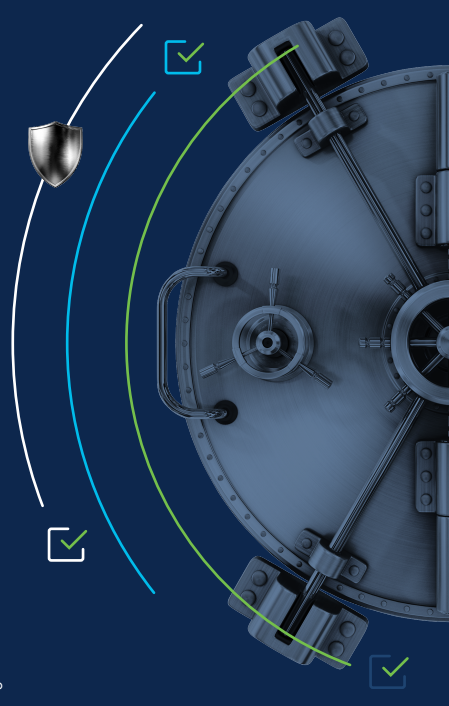
CISCO
SECURE

数据为证：左右网络安全成败的五项关键举措



网络安全挑战从未走远。每一天，我们的世界都变得更加紧密相连，也更加错综复杂。而对于网络安全团队而言，更复杂的局面就意味着更沉重的责任。

好在，企业可以通过一些具体措施改善网络安全。在《安全成果研究报告（第二卷）》中，我们汇集了来自 27 个国家/地区超过 5100 位安全和 IT 从业者的数据。从这些数据中，我们归纳出了五项能有效促进网络安全计划成功的关键举措：

更新技术

平均而言，组织使用的 39% 的安全技术已经过时。

不要等到问题来临才被动地评估使用的技术，当下就应着手制定更加主动的技术更新战略。

> 将近 40% 的组织都用着过时的安全技术，安全欠债问题非常严重。另一方面，那些采用现代化整合式云架构的组织已通过积极主动的技术战略，实现了高水平的技术更新。问题和解决方案一目了然！”
>
> Richard Archdeacon，思科首席信息安全官顾问

充分集成，提升可视性

超过 77% 的组织宁愿购买现成的集成解决方案，也不愿自行构建。

幸好随着基于云的解决方案日益盛行，实现强大的集成变得空前简单，使安全团队能更全面广泛地洞察系统。

> 相比于任何其他安全举措或控制措施，充分集成的现代化 IT 更有助于整个计划的成功。”
>
> Helen Patton，思科首席信息安全官顾问

扩充团队

安全人员配置比例最高的组织，其威胁检测和事件响应的能力比其他组织高 20%。

没有余力扩充团队？不妨考虑提高现有员工的技能水平和熟练程度，培训永远不失为一项明智的投资。

> 为您的安全运维团队选择技术最娴熟的人员，而不是仅仅关注人数。自动化可以帮助您弥合新进员工与资深员工之间的差距，获得同样出色的成果。”
>
> Wendy Nather，思科首席信息安全官顾问委员会主管

巧借威胁情报，助力智慧办公

采用威胁情报的组织，其威胁检测和响应能力是其他组织的 2 倍。

无论您是否打算发展团队，都要利用一切可以利用的情报工具来缩小差距。让工作更智慧，成果更出色。

> 一旦企业把精兵强将、高效流程和前沿技术合而为一，就能掌握高超的威胁检测和响应能力，如果再加上可靠的威胁情报，就更完美了。
>
> Dave Lewis，思科首席信息安全官顾问

有的放矢，不破不立

实践混沌工程的公司改善业务连续性的可能性是其他公司的 2 倍。

有目的地定期实施 IT 中断有助于组织为应对真正的威胁做好准备。践行混沌工程，从容清杂去乱。

> 定期进行各种测试的组织，在紧急情况下保持正常运维的可能性是其他组织的 2.5 倍。推行混沌工程可以进一步强化这一优势。”
>
> Wolfgang Goerlich，思科首席信息安全官顾问

践行这些有数据支持的举措，有助您成功增强网络安全态势。然而，这并非我们的一面之词。您可以立即查看完整报告，从调查成果的所有支撑数据中一探究竟。

获取报告

CISCO The bridge to possible