

SITA

2018 航空运输业网络安全洞察






SITA

航空运输业网络安全洞察

2018年度航空运输业网络安全洞察报告是SITA展开的一项全球性调研，是针对航空运输业网络安全趋势进行的最综合研究。

报告针对2018年5月至7月的调查结果进行探讨，结论基于全球主要航空公司和机场的59位高级决策者的意见和建议，其中包括首席执行官、首席信息官、首席信息安全官、副总裁和IT及安全实践主管。



研究围绕航空运输业的网络安全现状展开。对投资趋势和投资重点、目前行业所面临的种种挑战、共同举措和技术趋势，以及行业特定风险和最佳实践进行了探讨。

2018年的调查结果对航空运输业的战略性方案和未来网络安全计划提供了清晰见解。



内容概要



网络开支和挑战



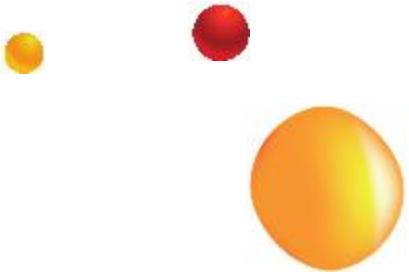
投资重点



焦点领域
和重大威胁



安全运营
中心 (SOC)



充分认识到网络安全的重要性，但现有挑战成为发展绊脚石



- 网络安全预算预计将增长，开支也将侧重于检测和预防。
- 风险上升有目共睹，但网络安全团队仍缺乏C级授权和定位。
- 缺乏资源、预算和技能是阻碍网络安全保护领域发展的主要障碍。

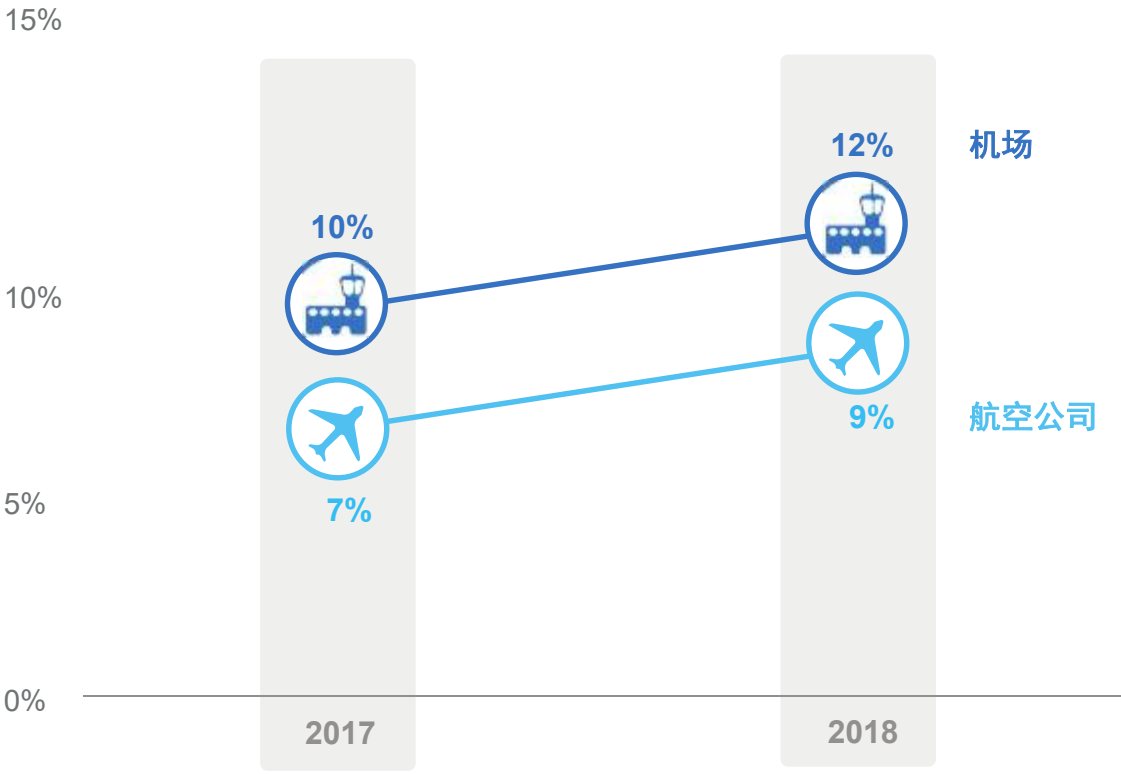
SITA建议

航空运输业利益相关者必须授权他们的网络安全团队并提供必要资源，以启动具体可行方案。



网络安全预算预计将增长，开支也将侧重于检测和预防

网络安全IT预算开支占比



分析

航空运输业网络安全开支水涨船高，与2017年相比，2018年水平更高。

航空运输业和其他行业的网络安全开支水平。平均而言，2017年各大航空公司的网络安全预算占其IT总预算的7%，而机场在该领域的投资达到10%。

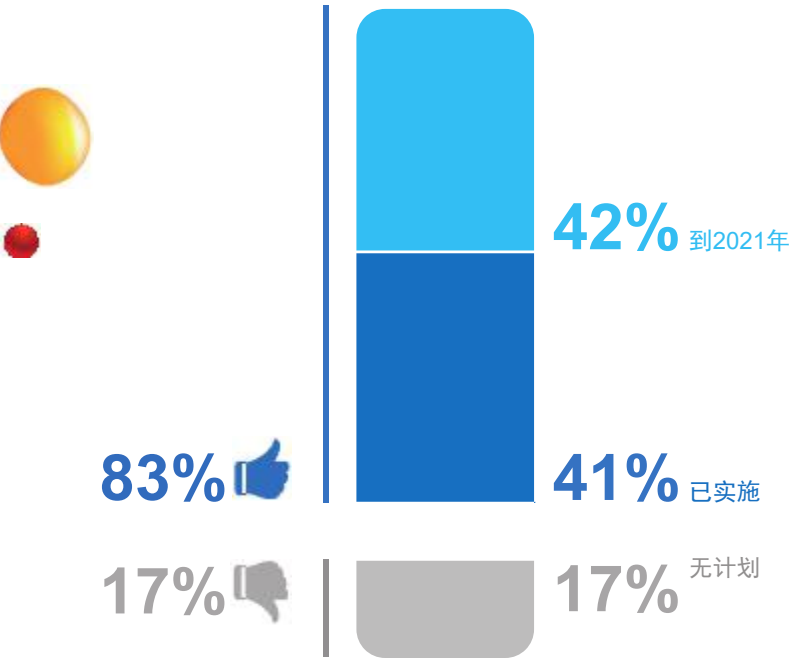
虽然网络安全投资尚不足够，但航空公司和机场2018年开支预计将分别增至9%和12%。反应出对数据保护及未经授权的系统访问的重视程度与日俱增。

73%的受访者将监管合规和数据隐私监管视为首要任务。过去三年，这一直被认为安全投资的重要驱动因素。未来数年，安全开支预计将转向检测和响应。

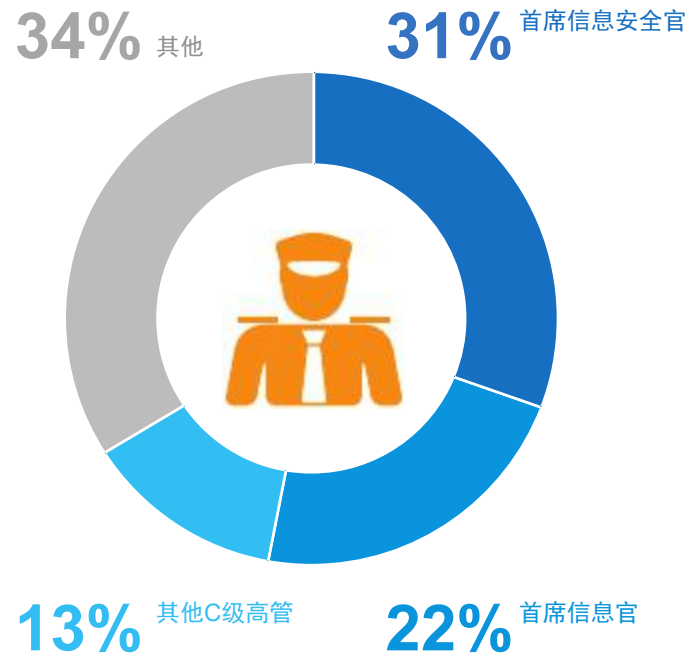


风险上升有目共睹，但网络安全团队仍缺乏C级授权和定位

将网络安全纳入其全球风险范畴，以改善风险管理的组织占比



对组织信息安全负责的职位



分析

网络安全风险与日俱增——安全管理者已就此达成共识。设立首席信息安全官（CISO）这一职务对可视性和有效实施至关重要。

2/3（66%）的受访航空运输业组织将信息安全事宜全权委派给“首席管理层”，反应出对行业网络安全的重视程度与日俱增。

目前，41%的受访者已将网络安全纳入全球风险范畴，而另有42%的受访者计划到2021年，将网络风险纳入其关注事项。进一步表明航空运输业网络安全风险上升。

然而，只有31%的受访组织专门设立了CISO，该职务对C级安全团队授权和定位至关重要。



缺乏资源、预算和技能是阻碍网络安全保护领域发展的主要障碍

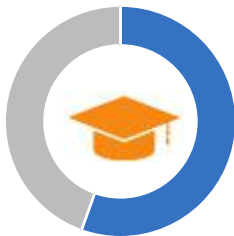
在组织内实施网络安全的挑战



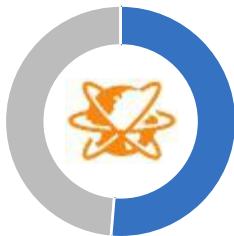
78%
有限资源



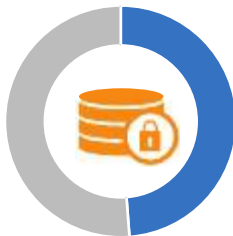
70%
有限预算



56%
员工培训



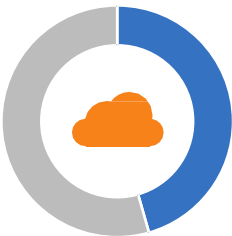
51%
网络和IT资产可视性



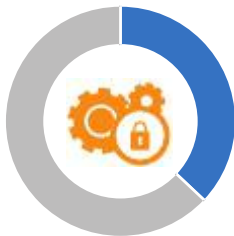
49%
数据保护



47%
员工招聘和保留



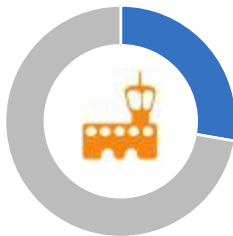
46%
云使用情况
(已批准/未经批准)



38%
巩固运营技术 (ICS, SCADA)



34%
高级管理层的支持



28%
巩固办事处

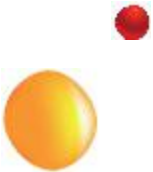
分析

在应对网络安全事宜时，航空运输业面临着与其他行业类似的挑战：缺乏资源、预算和技能。

航空运输业已超前意识到并构建了防范网络威胁所必需的坚实基础。

然而，高管们也意识到，他们需要更进一步，才能让网络安全水平更上一层楼。

在试图改善网络安全保护时，航空公司面临着巨大困难。最大的障碍是缺乏资源，78%的组织受此困扰。缺乏足够的网络安全预算使这一情况雪上加霜——这也是70%的组织面临的问题。高管们面临的重大挑战包括：保留和招聘专业技术员工（47%）和员工培训能力（56%）。行业需要利用外部专业知识来补充内部资源。





大多数航空公司和机场已部署核心保障措施，并准备向下一级别推进



- 安全基础已部署，旨在实现持续改善。
- 员工意识被视为防范网络风险的重中之重。
- 构建良好基础是各网络安全领域的首要任务。

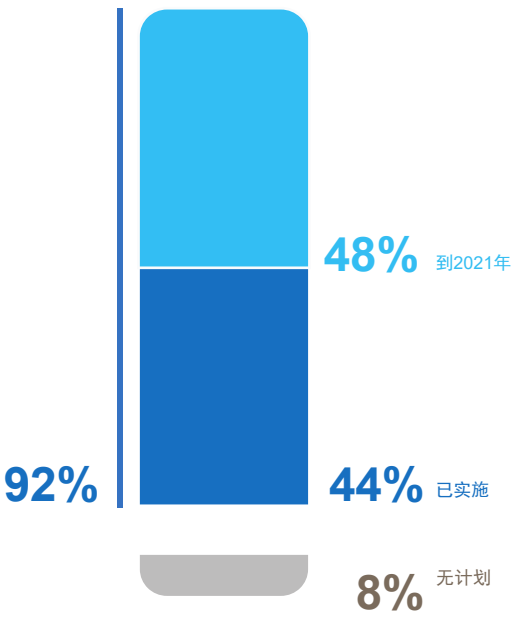
SITA建议

为提高组织的网络安全成熟度，制定明确的、与组织业务目标和IT环境一致的长期网络安全战略至关重要。

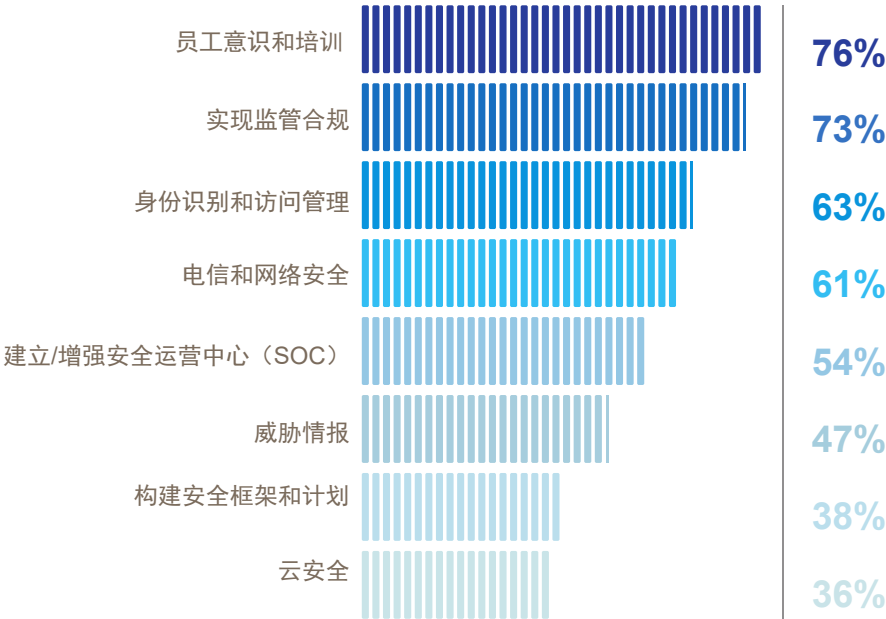


安全基础已部署，旨在实现持续改善

制定正式信息安全战略的组织占比



网络安全举措投资重点



分析

行业领导者开始引入防御网络攻击所需的核心构建模块。

目前，将近一半（44%）的受访者制定了正式信息安全战略。到2021年，几乎所有的受访组织将部署正式网络战略。

目前，投资重点包括：“员工意识和培训”（76%）、“实现监管合规”（73%）和“身份识别和访问管理”（63%）。

过去三年，监管合规和数据隐私法规推动了安全开支的增长。最新的一个案例是，2018年，《通用数据保护条例》（GDPR）在欧洲生效。这些法规推动着开支的增长，特别是数据安全工具开支，如身份识别和访问管理技术。

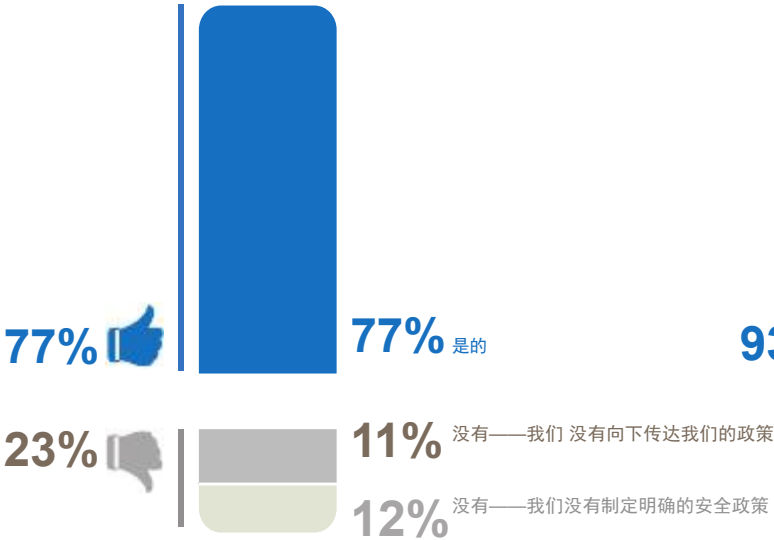




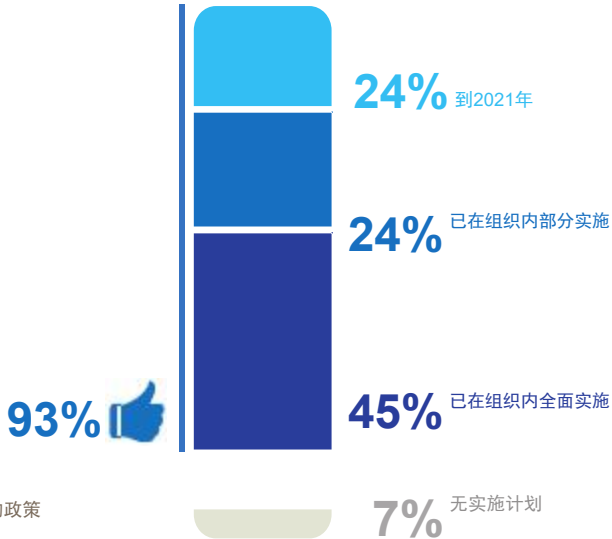
员工意识被视为防范网络风险的重中之重



向员工传达战略政策的受访者占比



针对员工部署正式网络安全培训计划的受访者占比



分析

员工是航班抵御网络攻击最薄弱的环节，也是经常被强调的首要话题。航空运输业的安全专家也认同员工应成为风险防范的重中之重。

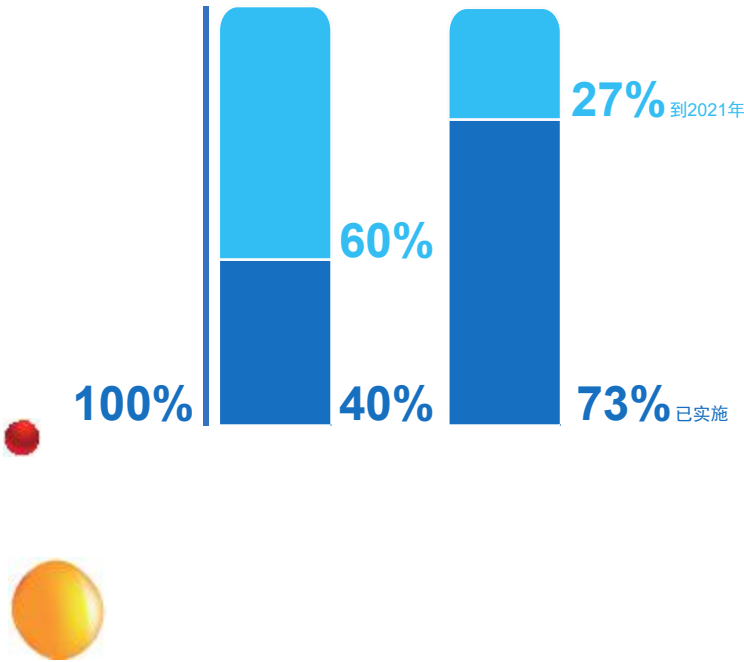
SITA的航空运输业网络安全洞察报告显示，“员工意识和培训”是网络安全的首要任务（76%）。

随着勒索软件和网络钓鱼成为风险防范议程的重中之重，众多组织已将员工视为网络安全最佳实践的重点。超过四分之三（77%）的航空组织向员工传达了安全政策，而69%的组织已部署正式培训计划。

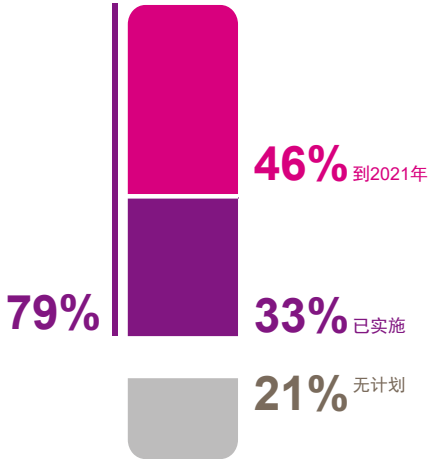


构建良好基础是各网络安全领域的首要任务

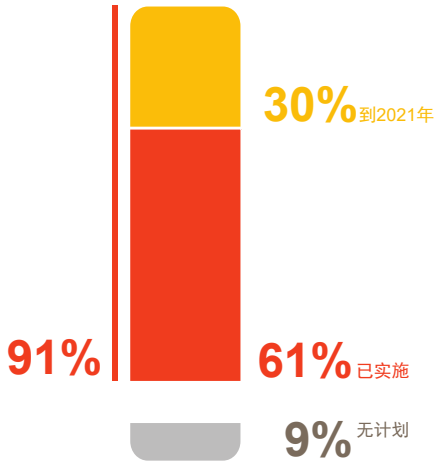
评估
保留关键业务流程清单的组织占比 保留关键基础设施/应用程序清单的组织占比



检测
具备安全运营中心的组织占比



响应
具备明确网络安全事件处理流程的组织占比



分析

保护您的组织意味着具备评估、检测并适当响应风险和违规行为的能力。

令人欣慰的是，目前，绝大多数受访组织正开展正式的风险评估（93%）。33%的受访组织设立了安全运营中心来监控他们的IT环境，另有46%的受访组织计划到2021年完成这项工作。如发生违规行为，近2/3的受访组织具备明确的事件处理流程。

然而，虽然目前已有73%的受访组织保留了关键基础设施清单，但仅有40%的受访组织针对关键业务流程保留了清单。表明如今许多组织的业务流程和IT系统之间都缺乏联系。将业务流程和IT系统连为一体可使组织根据其潜在财务或运营影响，来管理网络安全。



领先的网络安全驱动因素正在从合规转变为主动保护，重点是检测外部威胁和防止中断



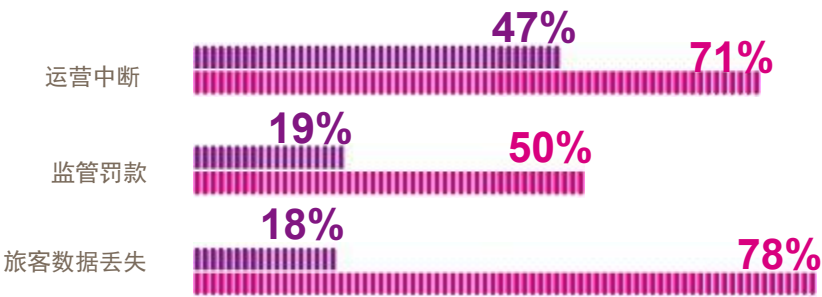
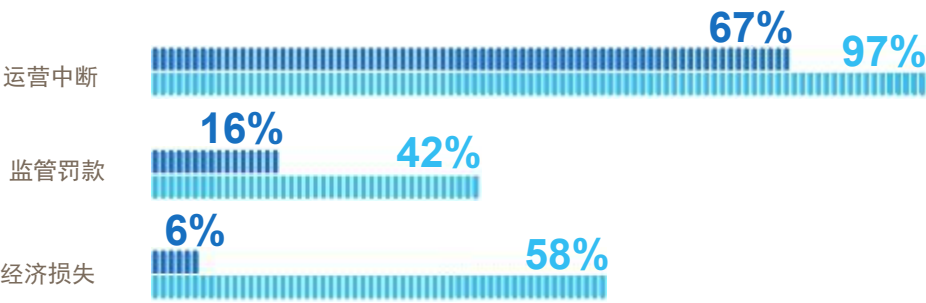
- 航空运输业的首要任务——利益相关者：避免运营中断、数据丢失和监管罚款。
- 航空运输业是各种网络威胁的首要目标。外部威胁仍然是关注重点。
- 今天，保护核心网络已成焦点，下一步是保护相关企业。

SITA建议
提高网络安全成熟度的关键先决条件是，明确最关键业务因素及其相关威胁等级。



航空运输业的首要任务——利益相关者：避免运营中断、数据丢失和监管罚款

受访者将网络安全风险视为重点防范事项



■ 排名第一
■ 排名前三

分析

通过保护机场和航空公司运营流程确保业务连续性已成航空运输业的重点考虑事项。

57%的航空公司和机场行业管理者的首要任务仍是保护运营系统和流程免受网络攻击，以确保业务连续性。

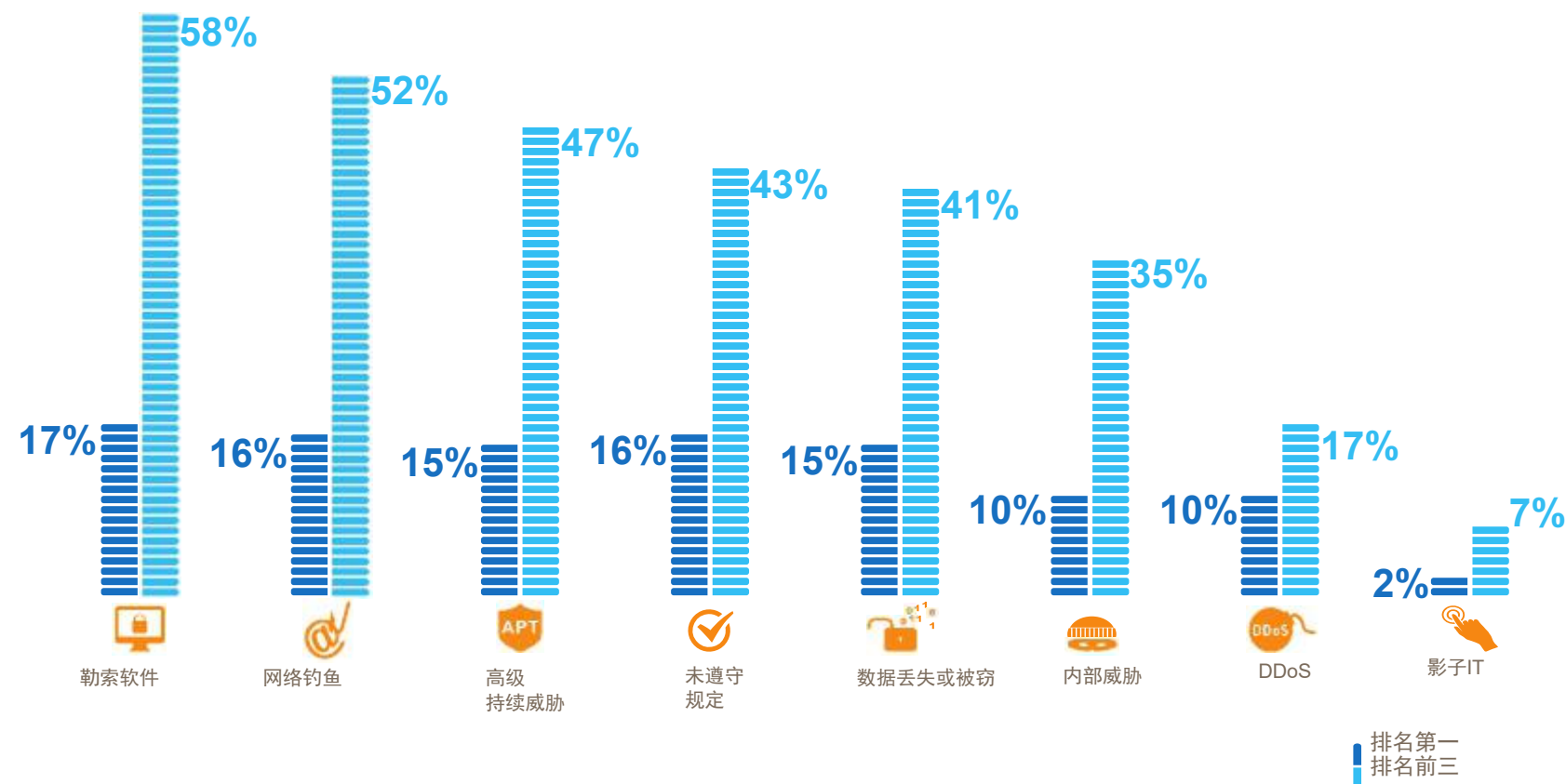
对于机场而言，中断是它们最担心的问题。航空公司（71%）依然视运营中断为重中之重，但它们的高管（78%）对旅客数据保护和财务损失也同样重视。

“监管罚款”的风险分别被50%的航空公司和42%的机场视为优先考虑事项。随着全球监管生态系统日趋成熟，关注该领域的组织或将增加。



航空运输业是各种网络威胁的首要目标。外部威胁仍然是关注重点

安全风险被视为亟需解决的重中之重



分析

业界一致认为，航空运输业面临的所有网络威胁都同等重要。

与其他行业相同，勒索软件（58%）、网络钓鱼（52%）和高级持续威胁（47%）是航空运输业的常见风险。

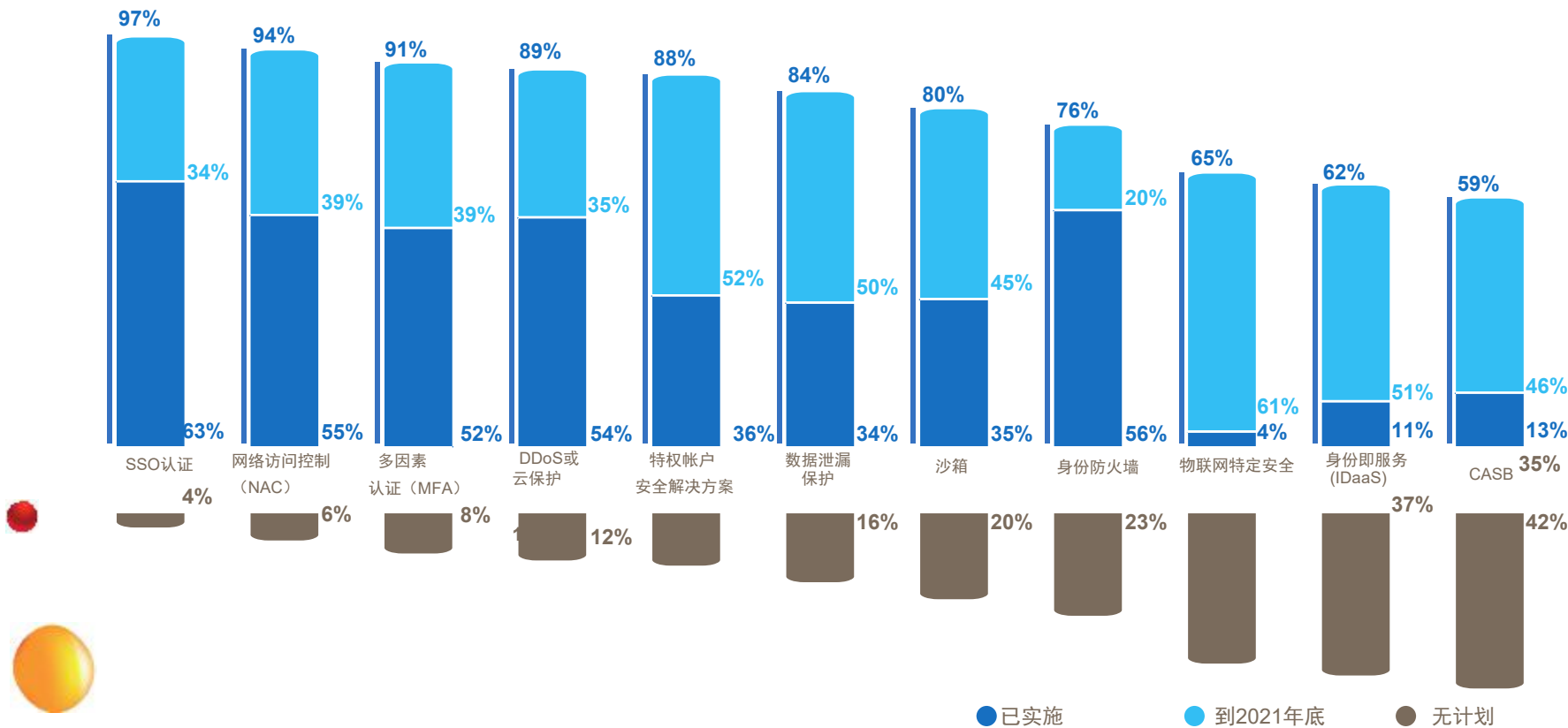
今天，人们更多关注来自外部参与者的威胁，只有10%的受访者视防范内部威胁为当今首要任务。未来，该领域将受到更多关注，因为据分析师报告称，超过1/4的网络攻击涉及内部人员。

SITA预计，需在未来密切关注“影子IT”——目前仅有7%的组织将此视为重点考虑事项。影子IT，特别是员工对第三方云解决方案的采纳在其他行业已成显著趋势。它能提高生产力，但也会暴露一些漏洞，因此需谨慎管理。



目前，保护核心网络已成焦点，下一步是保护相关企业

已实施或计划实施IT安全技术的受访者占比



分析

到2021年实施的最常见技术将用于保护核心网络的边缘，而物联网（IoT）安全、数据泄漏保护和云访问代理（CASB）将成为下一个技术部署趋势。

大多数受访者已经实施了SSO认证（63%）、网络访问控制（55%）和多因素认证（52%），大多数航空公司将到2021年底实施所有这些保护技术。

如今，CASB、物联网安全和身份即服务等技术的部署受到限制。随着数字化转型的发展和团队迈向保护相关企业，未来三年，将加大对这些技术的部署。



未来三年，二分之一的组织将实施“安全运营中心”，旨在强化保护



- 航空运输业的直接目标：实施“安全运营中心 (SOC)”。
- 在扩展至应用程序层之前，SOC的实施将强调基础设施层。

SITA建议

安全运营中心服务是必要且复杂的项目。为了确保更快的投资回报率，分阶段实施至关重要，应在扩展至不太关键的领域前，从业务关键点着手。

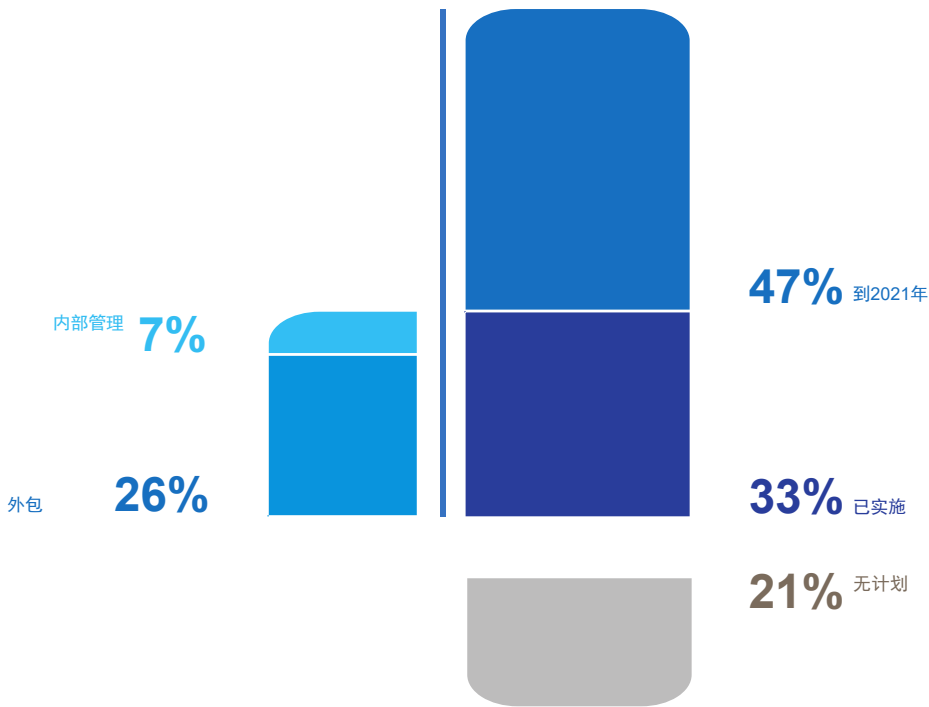


航空运输业的直接目标：实施“安全运营中心 (SOC)”

这来自我们的网络程序库吗？
徽标是旧版本==>删除？



已实施或计划实施安全运营中心的组织占比



分析

通过安全运营中心 (SOC) 进行主动监控是主动网络安全的核心主题。令人鼓舞的是，大多数受访者均制定了快速实施此类服务的计划，以便快速检测入侵。

SOC通常是安全管理人员在构建其网络防御能力时审视的第一个部分。目前只有33%的受访组织实施了SOC，但另有47%的受访者将到2021年，计划进行此类投资。

这一调查结果也强调指出安全外包的重要趋势，目前，80%的SOC由外部供应商运营。外包SOC服务解决了许多关键挑战，特别是内部资源和技能的缺乏，被列为实施网络安全战略的首要挑战。



在扩展至应用程序层之前，SOC的实施将强调基础设施层

分析

目前，大多数航空运输行业组织都在通过安全运营中心监控基础设施，但鉴于所需条件的限制，他们均未进入应用程序层。

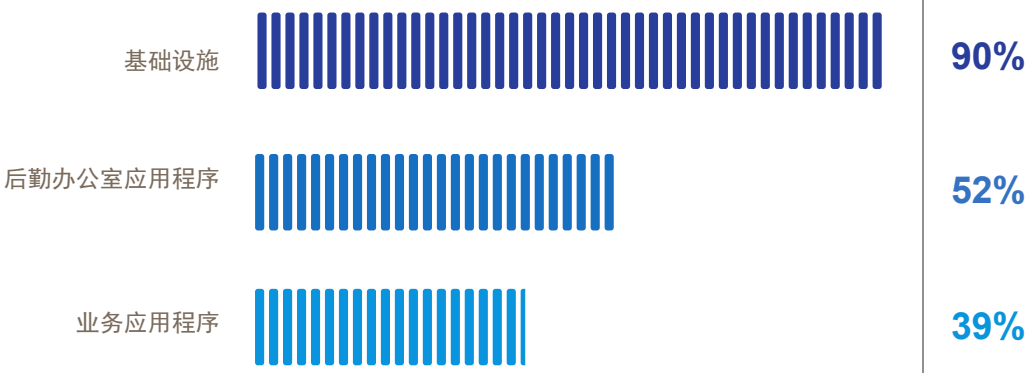
90%的受访者通过SOC监控网络和基础设施，仅有52%的受访者监控后勤办公室应用程序，39%的受访者监控业务应用程序。

鉴于现有知识和最佳实践，保护基础设施的速度更快。评估和监控关键应用程序，特别是定制业务应用程序，比监控基础架构层更复杂。

通过SOC监控业务应用程序需要深入理解应用程序的行为方式以及需监控哪些交互来探测入侵。对于那些涉及深层应用程序知识的SOC而言，往往需要付出更多努力。



当前通过安全运营中心 (SOC) 监控





调查报告总结



充分认识到网络安全的重要性，但现有挑战成为发展绊脚石

风险日益增加，这一点有目共睹，必须开展更多工作，来提高董事会或高级管理层对网络安全的重视。网络安全开支逐年增加并与其他行业保持一致。然而，缺乏资源、预算紧张和技能缺失仍然是阻碍航空运输业网络安全保护发展的主要障碍。



领先的网络安全驱动因素正在从合规转变为主动保护，重点是检测外部威胁和防止中断

航空运输业利益相关方的首要任务是，通过保护核心网络免受外部威胁来规避运营中断。CASB、物联网安全和身份即服务等技术将在未来三年内大幅实施，因为航空运输业的数字化转型将取得进展，保护扩展网络已成关注焦点。



大多数航空公司和机场已部署核心保障措施，并准备向下一级别推进

今天最常见的开支优先事项是“员工意识和培训”，实现“监管合规”和“身份识别和访问管理”。更强大的安全基础正在部署当中，旨在实现持续改善。在业务流程和IT系统之间建立更强大的纽带是实现基于影响的保护的关键。



未来三年，二分之一的组织将实施“安全运营中心”，旨在强化保护

航空运输业的当务之急是实施“安全运营中心（SOC）”。SOC通常是安全管理人员在构建网络防御能力时审视的第一个部分。如今，只有33%的受访组织实施了SOC，但另有47%的组织计划到2021年进行此类投资。目前，绝大多数的实施都强调基础设施层，然后再扩展至应用程序层。

方法论

调查

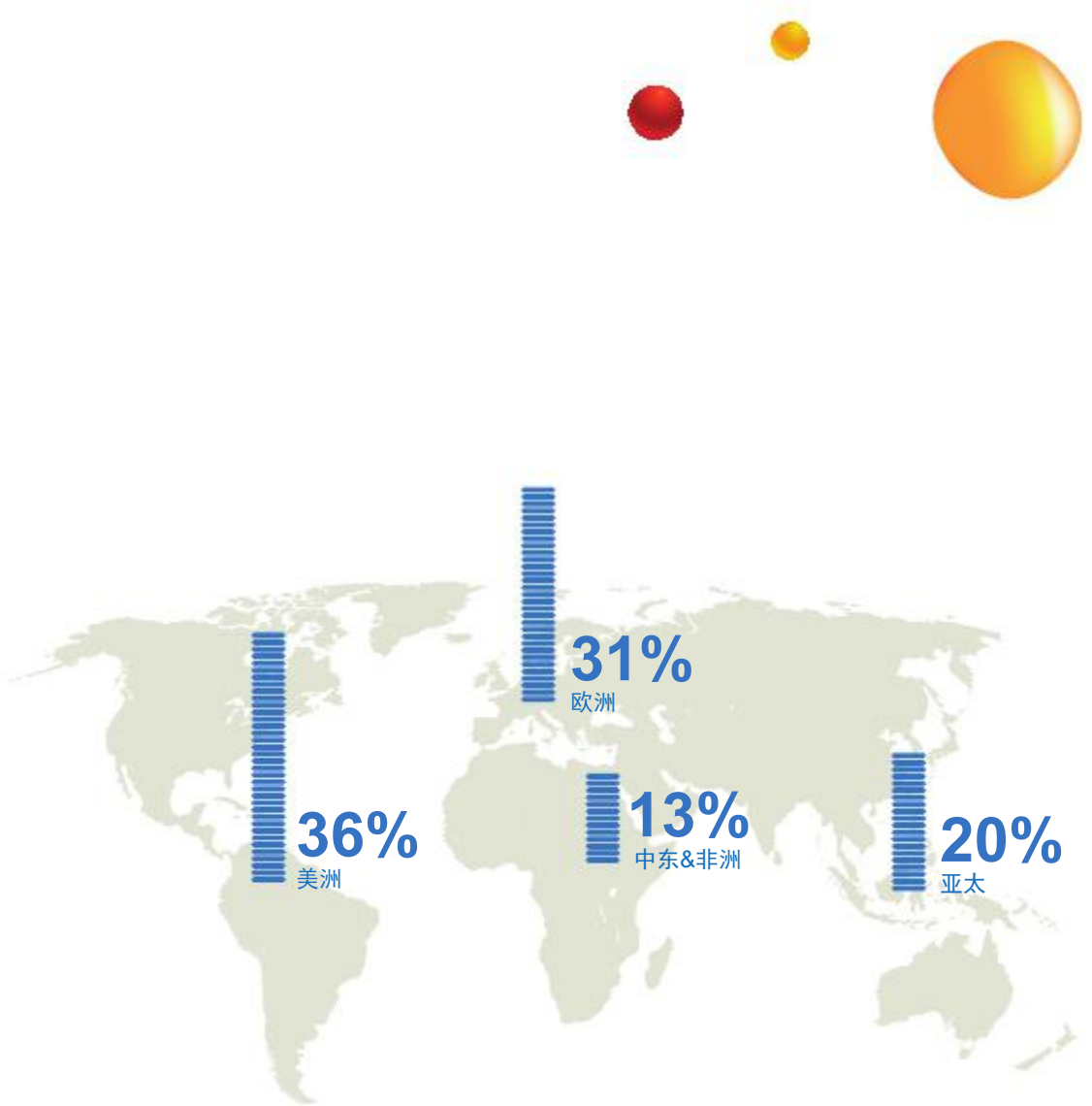
2018年度航空运输业网络安全洞察报告是SITA展开的一项全球性调研，是针对航空运输业网络安全趋势进行的最综合研究。报告针对2018年5月至7月的调查结果进行探讨，结论基于全球主要航空公司和机场的59位高级决策者的意见和建议，其中包括首席执行官、首席信息官、首席信息安全官、副总裁和IT及安全实践主管。

研究

独立市场研究机构Circle Research接受委托，代表SITA开展研究。该研究严格保密，结果将以汇总形式呈现。所有源数据均为机密信息，个人反馈结果不会透露给任一研究利益相关方。

加权

本调查根据受访者年均客运量统计使用了加权系统，以确保结论是与全球客运量相关的代表性样本，并可补偿受访组年度波动。



SITA 一览

便捷旅行每一步。SITA运用技术为各航空公司、机场、飞行和边境管控带来革新。

- SITA愿景：“便捷旅行每一步”。
- 从旅行前，值机和行李托运，到登机、安检和机上联网服务——通过先进的信息和通信技术，我们打造轻松简便的端到端旅程。
- 我们与200多个国家和地区的约400名航空运输业成员和2,800位客户合作。全球几乎所有航空公司和机场都与SITA有业务往来。
- 我们的客户包括航空公司、机场、全球分销系统和政府。
- SITA是航空业忠实的IT通信合作伙伴，它100%隶属于航空业，可有效应对行业需求和问题。
- 我们与航空运输业客户、行业机构和合作伙伴共同创新和发展。通过SITA董事会和理事会——由世界各地的航空运输业成员构成，我们的投资组合和战略方向整个获得行业的有力推动。
- 我们通过世界上最广泛的通信网络提供服务，它是将全球航空运输业连为一体的一笔宝贵资产。
- 我们的客户服务团队由遍布全球的2,000多名优秀员工组成；为打造最卓越客户服务，我们投入巨资，旨在为服务提供全天候本地和全球支持。
- 正如我们的行李报告一样，我们针对航空公司、机场和旅客开展的年度航空运输业和旅客IT趋势调查在业内享誉盛名。
- 2017年，我们的合并收入为16亿美元。
- 更多详情，敬请访问 www.sita.aero



如需垂询，请致电或发送电子邮件至SITA

北美

+1 770 850 4500

info.amer@sita.aero

亚太

+65 6545 3711

info.apac@sita.aero

欧洲

+41 22 747 6000

info.euro@sita.aero

中东、印度 & 非洲

+9611 637300

info.meia@sita.aero