企业应考虑的重要网络升级

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The Top Network Upgrades You Should Consider Today		
原文作者	约翰·爱德华兹（John Edwards）	**原文发布日期**	2021 年 9 月 21 日
作者简介	约翰·爱德华兹是一位科技记者。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/networking/top-network-upgrades-you-should-consider-today		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	随着 2021 年进入最后一个季度，企业的网络负责人应考虑进行下述五项网络升级：（1）增强网络安全性；（2）改进云管理；（3）加强网络智能；（4）增强网络弹性恢复能力；（5）增强网络适应性。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

企业应考虑的重要网络升级

约翰·爱德华兹

2021 年 9 月 21 日

要想跟上不断发展的网络技术，企业需要持续不断地努力。幸运的是，重大技术进步和新的安全威胁往往会间歇性地出现，这让网络管理员得以在两次网络升级之间喘口气。

随着 2021 年进入最后一个季度，企业的网络负责人应考虑进行下述五项网络升级。

（1）增强网络安全性

随着勒索软件攻击和网络漏洞的增加，网络安全已成为企业的重中之重。Sungard Availability Services 全球解决方案工程部门的解决方案架构师马修·帕森斯（Matthew Parsons）指出，企业的网络管理员应考虑进行网络升级，包括升级入侵检测系统（IDS）和入侵防护系统（IPS），以增强企业网络的安全性。帕森斯还建议网络管理员升级安全信息和事件管理（SIEM）和日志收集系统，强化 Web 应用程序防火墙，以及改进端点保护、加密、漏洞扫描和渗透测试。“安全漏洞可能会给企业带来数百万美元的损失，并对其品牌/声誉产生负面影响。安全的网络有助于防止和减轻此类漏洞。”他说。

帕森斯发现，在规划网络升级时，IT 经理面临的最大挑战是预算和人员。企业高管通常将网络安全视为不必要的成本，因此可能不愿提供必要的资金。“这些高管需要接受培训，以了解网络安全是企业安全的关键组成部分，在网络安全方面的投资会为企业节省更多的资金。”

企业缺乏 IT 专家也会导致安全升级的延迟。“企业的全天候安全运营中心（SOC）通常缺乏正确管理事件和登录所需的技能”，帕森斯说，“即使企业有必要的技术，在培训现有 IT 人员和/或雇用新的安全分析师上也面临着挑战，这两者都会增加安全解决方案的成本。”

（2）改进云管理

网络设备提供商 Extreme Networks 的首席信息官约翰·阿贝尔（John Abel）表示，除了增强网络安全之外，企业还应投资于云管理系统，这是一项很重要的升级。

阿贝尔指出，在过去的一年里，云已经成为一种必不可少的工具，它使企业能够无缝地管理分布式办公——基于云的协同工具兴起就说明了这一点。他说，许多前瞻性的企业已经开始采用基于云的网络管理，来精简对日益复杂的分布式环境的监管，将其云战略提升到了一个新的水平。

阿贝尔发现，许多员工可能会无限期地居家办公，因此企业需要一种云策略来无缝管理和保护分散的网络。他补充说，升级到云网络还能消除企业每三到四年更新一次网络设备所需的大量成本。“使用云解决方案，企业只需每年付一次订阅费用，网络提供商就会负责其设备的定期更新。这样一来，企业就不会存在过时的设备，能够提高安全性。”

（3）加强网络智能

随着网络的日益复杂，强有力的网络管理成为企业的当务之急。物联网产品和服务提供商 Digi International 高级技术总监哈拉尔·雷默特（Harald Remmert）表示，随着员工的日益分散和 IT 人员不断缩减，以人工智能和机器学习形式出现的网络智能，已成为保持网络平稳运行的关键。“这种智能需要集中化，以提供跨多个设备和位置的单点命令、控制和可见性。这种智能还要完全实现自动化，以便在没有 IT 人员参与的情况下执行关键任务。”他指出。

（4）增强网络弹性恢复能力

大多数企业网络都处于不断变化的状态——新设备不断上线，而旧设备日益变得不合规。“再加上人为因素，企业网络一直存在出现故障的可能性。”雷默特说，“关键是建立一个具有弹性恢复能力的网络，该网络可以持续运行、自我修复、进行故障转移，并保持客户和应用程序的连接。”他说。

（5）增强网络适应性

新冠疫情几乎在一夜之间改变了网络世界——拓扑、技术和数据模式迅速出现变化。现在，企业应清楚地认识到这一事实并升级其网络基础设施。无论企业的底层连接技术是什么（光纤、MPLS，还是 4G/5G），无缝、灵活的互操作都是优先事项。雷默特指出，较新的技术通常能够更容易、更快速地部署，“有助于企业创建更安全、智能、弹性和适应性的网络”。

结论

为确保网络基础设施具有弹性恢复能力，帕森斯建议企业管理人员对其网络基础设施进行漏洞/风险评估。他还建议企业执行业务影响分析（BIA），以揭示现有漏洞，并了解每个安全漏洞可能会给企业带来多少损失。“这将有助于获得领导层的预算批准。”帕森斯说。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com