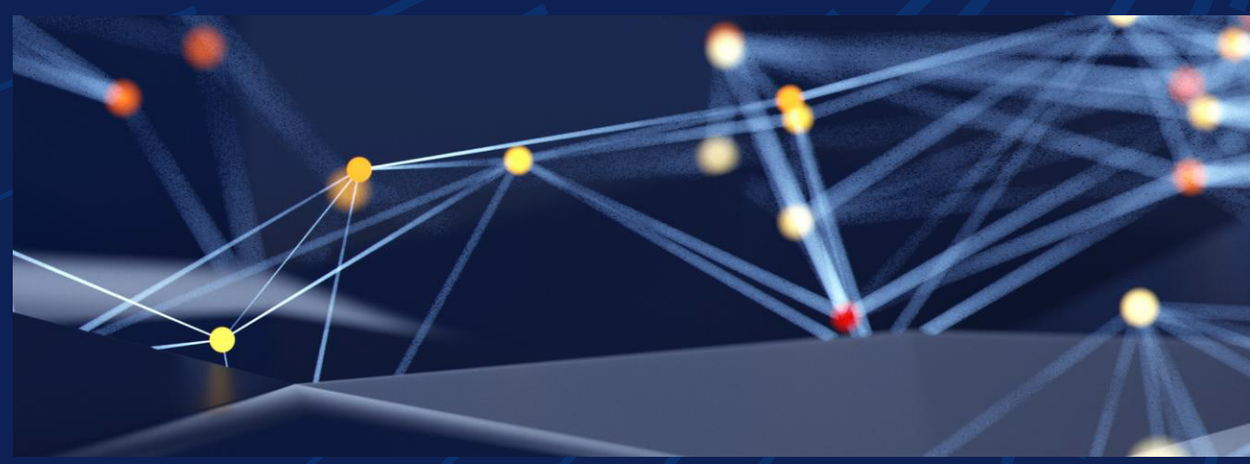
网络安全的未来：

适应数字新时代



网络安全专业人员通常专注于防范攻击和制定恢复计划，但整体安全环境却在不断变化。因此，为未来做好准备至关重要。

从长远来看，三个领域尤为突出 – 后量子密码学、监管环境的变化以及新兴威胁。组织应立即采取行动，在解决方案可用时就着手规划部署。

后量子密码学的黎明

量子计算蕴含着转型行业的前景，其惊人的计算能力可以解决经典计算机无法企及的难题。然而，这种功能可能会使当前的加密方法过时。RSA 和 ECC 等支撑当今安全通信的算法，可能被足够先进的量子计算机在数秒内破解。这种迫在眉睫的威胁加剧了后量子密码学转型的紧迫性。

后量子密码学 (PQC) 致力于开发在量子计算时代仍能保持安全的加密算法。为了应对这一潜在风险，美国国家标准与技术研究院 (NIST) 已经采取行动，正在领导推动抗量子算法的标准化工作。

对企业而言，为这一转型做好准备已势在必行。尽早采用 PQC 解决方案将确保在攻击者获得量子计算能力时数据仍能保持安全。

网络安全副总裁兼戴尔业务部门安全官 Bobbie Stempfley 指出，组织应着重关注两个关键领域，从而启动这一过程：

识别和清点当前使用的所有加密模型。
考虑传输中数据，而不仅仅是静态数据。考虑密钥管理、代码签名、设备标识、安全访问和遥测。创建全面的清单，然后制定路线图。

了解供应商的准备情况。
鉴于现代企业可能拥有数千家供应商，必须警惕其可能带来的风险。确保这些供应商同样在为变革做准备。

除了这些起点，还需要开展风险评估以识别易受攻击的系统，考虑实施混合加密模型以在过渡期间保持正常运行，并与已经在探索量子安全解决方案的供应商协作，但请记住，不会有一家单独的供应商或技术可以提供全包式解决方案。

全球化世界中的监管变革

另一个塑造网络安全未来的关键驱动因素是不断变化的监管环境。当今法规已远超合规范畴，正逐渐成为在数据驱动的互联世界中强化问责、推动技术升级和保护公民的核心框架。然而，这些法规快速迭代且地域差异显著，进一步加剧了合规复杂性。

值得注意的是，这些法规不仅是违规处罚工具，更是优化网络安全实践的催化剂。一旦企业主动将政策与监管要求保持一致，将能开启更高层次的信任度和运营效率。为此，企业应建立能够灵活适应法律变化的治理框架，定期进行合规审计，并投资培训员工按照最新标准处理敏感信息。

安全高管在筹备合规工作时，必须确保其内容可被理解且已被理解。安全从业者常使用专业术语沟通，却难以引起客户、监管机构及其他利益相关者的共鸣。安全专业人员有责任确保信息传达清晰，而非让听众自行解读。

> 将后量子密码学转型想象成搬运一栋装满家具的房子。任务将非常复杂，关键挑战在于确保在整个过程中做到毫发无损。”

Bobbie Stempfley
Dell Technologies 网络安全和业务部门安全官副总裁

威胁（和防御）环境的演变

AI 正在革新商业领域，提高生产力，并发掘人类潜能的新机遇。从网络安全的角度来看，AI 既有利于恶意行为者，也有利于防御者：

恶意使用：AI 正催生更复杂的攻击手段，例如高度逼真的鱼叉式网络钓鱼和深度伪造。

防御使用：AI 通过以下方式帮助防御者：

- 快速处理大量安全数据。
- 更有效地确定威胁的优先级。
- 增强检测和响应能力。

然而，安全工具将持续升级 – 通过自然语言处理技术，安全专业人员可以更直接地与系统交互，并且系统可以主动采取网络安全纠正措施。

组织应当双管齐下：既要充分利用这些功能，又要确保培训等防御机制持续更新。培训是防止员工沦为复杂攻击受害者的最佳手段。

迈向无密码化

密码不再是身份和访问管理的最安全方法。

基于密码的传统系统存在重大漏洞，使其越来越无法满足现代网络安全需求。密码容易遭受凭据填充、网络钓鱼和暴力尝试等攻击的威胁，往往会使组织暴露于不必要的风险中。此外，用户的不良行为（如重复使用密码或设置简单密码）会加剧这些漏洞。

无密码身份验证方法（包括生物识别、数字证书和硬件令牌）通过消除所有与密码相关的威胁类别，提供了更强大、更安全的替代方案。迁移到无密码系统意味着身份和访问管理的关键演变，能够使安全措施与日益复杂的网络威胁保持同步。

采用无密码技术还可带来诸多好处，包括减少攻击面、通过更快速的无缝登录改善用户体验，以及通过减少密码相关的事件降低 IT 成本。先进方法的应用可确保增强安全态势，并帮助组织满足监管标准合规要求。向无密码系统过渡不仅是一种趋势，更是为个人和组织构建更安全、更高效的数字生态系统的必要步骤。

结论

网络安全正步入一个由量子计算、法规演变和日益复杂的威胁共同塑造的变革时代。为了保持领先地位，组织必须采用后量子密码学、AI 驱动防御和无密码身份验证等创新技术。通过优先考虑准备情况、协作能力和战略投资，企业可以构建更安全、更具弹性的数字环境。采取行动，正当其时。

戴尔产品和解决方案，可以助您一臂之力

精选戴尔解决方案	说明
网络安全咨询服务	专家指导，可帮助您针对不断变化的威胁环境（包括当前和新出现的威胁）进行规划。
vCISO	虚拟首席信息安全官及网络安全专家，可协助识别和管理风险，并指导战略决策。

了解如何应对当今一些主要的网络安全挑战：**dell.com/cybersecuritymonth**