

通过笔记本电脑、智能手机和平板电脑，一切都能一目了然？如果没有人读取这些信息呢……



工业安全的超级英雄

尽管现在可以实现远程访问和居家办公，但是如何应对远程劳动力的挑战，是一大难题——网络犯罪分子把大型工业和基础设施作为攻击目标，这并不是什么新鲜事。当部分员工不再在工厂场所的安全公司网络中工作时，IT 和 OT 安全变得至关重要，远程访问能保证其安全性吗？

文 / Will Stefan Roth

PROCESS-Tip

* 更多信息请扫描二维码：



chem.vogel.com.cn

* 反馈编码：A211118

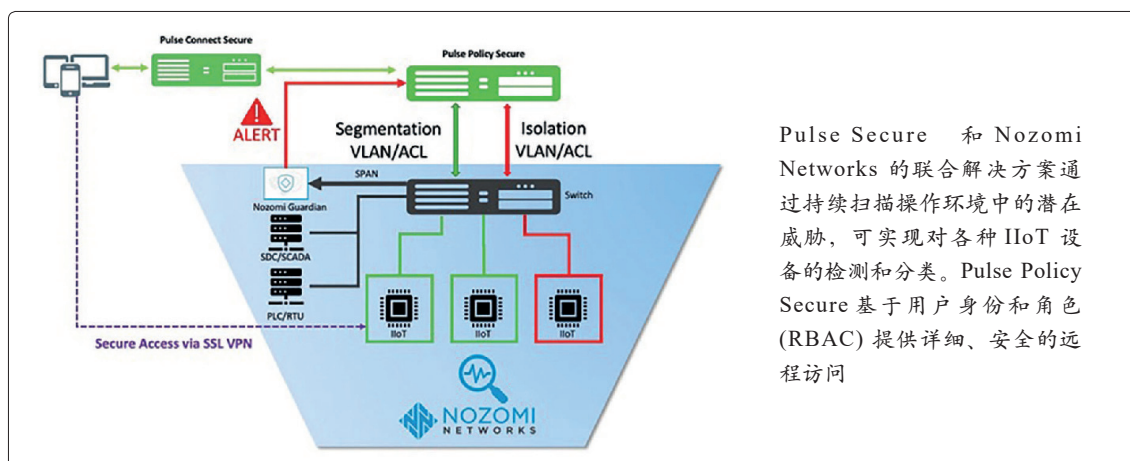
自从新冠病毒爆发以来，世界各地的公司都面临着各种挑战。许多公司的工作流程在将“办公室工作”转换为“远程访问”时遇到了问题，尽管“远程”现在已成为一个无

处不在的词：居家办公的员工比例从 10% 左右增加到 50% 以上。这不仅意味着工作程序和流程将发生重大变化，而且对企业的安全状况也有直接影响。安全专业人员面临的挑战是艰巨的：他们需要保护那些因为受新冠疫情影响而需要远程劳动人员的系统。因为许多员工会绕过从多年工作中发

展出来的安全系统，在没有保护的情况下使用邮件或 Zoom，或者禁用防病毒程序以访问被阻止的内容。这种情况可能会让网络安全专业人员无法处理，因为如果由于员工的疏忽或懒惰而没有使用安全系统，即使拥有最全面的保护系统也是徒劳。

目前许多公司通过取消线下

本文作者系 Nozomi Networks 公司销售总监。



会议和办公室集中办公、分班轮班和改变运营布局来保持社交距离，但是也有一些其他公司则试图通过完全的远程办公来保持运营。对于网络安全专业人员来说，这带来了许多挑战和风险。比如，如何可靠地实施或扩展安全的远程访问以及如何成功地监控一个与一个月前截然不同的网络环境，都是很大的问题。许多公司甚至在远程访问项目完成之前无法部署新的网络安全工具，这就使得问题变得更加复杂。他们必须先降低安全性，然后才能专注于监测。

可扩展计划

业的创新人员需要为以前未知的问题提出新的解决方案。为了提高远程员工的安全性，公司需要安全且易于使用的远程访问解决方案，在不妨碍员工工作的前提下以确保日常业务运行。这些周密的工具必须使网络安全团队能够通过 IT/IoT/OT/ICS 环境轻松保护任何类型的远程访问。这包括从 VPN 到浏览器中的无客户端远程桌面的所有内容，以及介于两者之间的一切。

当授予远程访问权限时，集成解决方案最好使用共享资产清单，以便对授予的权限做出更好的决策。以这种方式丰富起来的信息能够使远程访问的引入或扩展变得更加容易和安全。如此一

例如，Pulse Secure 和 Nozomi Networks 的联合解决方案通过持续扫描操作环境中的潜在威胁，可实现对各种 IIoT 设备的检测和分类。Pulse Policy Secure 基于用户身份和角色 (RBAC) 能够提供详细、安全的远程访问。

世界各地的 OT 安全专业人员的挑战是帮助他们的客户加强对新兴的新冠病毒相关的威胁和恶意软件的防御。因为许多网络犯罪分子正试图利用人们对新冠病毒的持续恐惧为自己谋取利益。为了实现这一目标，需要结合多种不同的措施来提高公司（尤其是制造业）的 IT 安全性。对员工进行相关安全培训，持续更新不断变化的威胁情况以及专门处理与新冠病毒相关的安全风险的社区工具，是顺应时代且强大的安全战略的基石。