

案例研究

# 澳大利亚国立大学凭借零信任建设安全校园



Gigamon 帮助我们摆脱了打地鼠式查找和追踪每个漏洞的局面，转向了更具战略性的网络安全方法。它为我们提供了建立网络弹性、减少攻击面以及使威胁行为者更难影响我们的环境所需的数据。

**SUTHAGAR SEEVARATNAM**

澳大利亚国立大学首席信息安全官

## 挑战

- 为零信任网络架构奠定正确的基础
- 保护混合云环境
- 改善网络安全态势，保护学生、教职员工和大学数据

## 解决方案

- GigaVUE® Cloud Suite
- GigaVUE HC 系列
- GigaVUE-FM
- GigaSMART®

## 客户获益

- 实现了对 60 个站点的设备、网络和流量的深度可见性
- 为零信任环境奠定了坚实的基础
- 易于部署，并提供企业范围内的可见性

## 关于客户

澳大利亚国立大学 (ANU) 是一所世界一流大学。澳大利亚国立大学位于澳大利亚首都堪培拉，拥有 4500 名学术和专业人员，为约 10000 名本科生和 11000 名研究生提供服务。截至 2018 年，该校共有七个学术学院，获捐赠资金达 18 亿美元。Suthagar Seevaratnam 是该大学的首席信息安全官，他担任这一职位已有三年。

## 业务挑战

该大学在 2018 年经历了一次数据泄露事件，Seevaratnam 和他的团队追查到这很可能是一封网络钓鱼电子邮件所造成的。这次攻击为团队敲响了警钟，他们需要改善大学的安全态势。NTT Data 发布的 2020 年全球情报威胁报告显示，教育机构是受攻击最严重的部门之一。报告显示，2019 年，教育部门遭受的攻击占所有攻击的 38%，仅次于政府部门。Seevaratnam 认识到网络攻击呈上升趋势，并采取积极措施加强学校的安全战略。

Seevaratnam 特别关注勒索软件和数据泄露相结合的攻击。他知道，仅仅关注一种类型的攻击是不够的。随着网络攻击的日益复杂化，大学 IT 基础设施也越来越复杂，Seevaratnam 认为零信任方法是最佳的方案。

## 解决方案

在考察了多家供应商之后，Seevaratnam 选择 Gigamon 作为核心平台之一，将大学的网络架构引向零信任战略方向。在大多数大学典型的混合环境下，此举是理所应当的。零信任的基本原则是“永不信任，始终验证”，这适用于网络以及用户和设备。Gigamon 使组织能够缩小设备、网络和流量中的可见性差距，从而更好地检测隐藏的和新出现的威胁。这种对澳大利亚国立大学网络、本地和云端所有动态数据的深度可观测性，使该大学能够增强其弹性并抵御攻击。

该大学在 2 个数据中心和 60 多个站点部署了 350 多台 Gigamon 设备，覆盖了澳大利亚国立大学阿克顿校区和澳大利亚各地的许多其他地点。该大学还部署了虚拟网络终端接入点 (TAP)，以提供对超过 26 台 VMware ESXi 主机的可见性。GigaSMART 通过更深入的情报扩展了这些功能，提高了对应用程序流量的可见性。内置传感器将 NetFlow 和应用程序 Metadata 元数据属性从 GigaSMART 传输到威胁搜寻的解决方案，从而提供有关学校如何使用应用程序的更多见解。

Gigamon 使该大学能够缩小可见性差距，并跟踪任何设备、网络和流量类型的活动，包括东西向流量。将来自 GigaSMART 的详细数据输入资产发现和网络安全自动化工具，以便对网络上的每个连接设备进行识别、细分并强制合规。该组合解决方案发现了大量暴露在互联网上的潜在易受攻击设备，包括物联网 (IoT) 设备、医疗 IoT 设备和使用停产 (EOL) 操作系统的设备。大学环境在不断变化和发展，因此澳大利亚国立大学与 Gigamon 合作，派一名工程师全职驻扎在现场，以优化和扩大 Gigamon 为澳大利亚国立大学提供的可见性。

Gigamon 还与领先的网络分析解决方案 ExtraHop 集成。这有助于安全团队建立性能指标基准，确保他们正在进行的数字化转型尽可能取得成功。

## 获益

Seevaratnam 表示：“Gigamon 帮助我们摆脱了打地鼠式查找和追踪每个漏洞的局面，转向了更具战略性的网络安全方法。它为我们提供了建立网络弹性、减少攻击面以及使威胁行为者更难影响我们的环境所需的数据。”

Gigamon 为该大学提供了强化网络安全态势所需的深度可见性和高保真对手检测。该集成解决方案为澳大利亚国立大学实施零信任方法奠定了坚实的基础，在网络架构方面实现了真正的范式转变。通过这种现代安全堆栈实现遥测，澳大利亚国立大学现在拥有了防止未来事故和保护其基础设施所需的工具。

## 关于 Gigamon

Gigamon 可以提供一个深度可观测性管道，该管道可以利用切实可行的网络级情报来增强可观测性工具的能力。这种强大的组合使 IT 组织能够确保安全性和合规性治理，加快分析性能瓶颈的根本原因，并降低与管理混合云和多云 IT 基础架构相关的运营开销。结果：许多现代企业充分实现了云技术所蕴含的转型潜力。Gigamon 为全球 4000 多家客户提供服务，包括 80% 以上的“财富 100 强”企业、10 家最大移动网络提供商中的 9 家，以及全球数百个政府和教育机构。要了解更多信息，请访问 [gigamon.com](https://gigamon.com)。

**Gigamon®**

全球总部

3300 Olcott Street, Santa Clara, CA 95054 USA

+1 (408) 831-4000 | [gigamon.com](https://gigamon.com)

© 2022-2023 Gigamon。保留所有权利。Gigamon 和 Gigamon 徽标是 Gigamon 在美国和/或其他国家的商标。Gigamon 商标请参见 [gigamon.com/legal-trademarks.html](https://gigamon.com/legal-trademarks.html)。所有其他商标是其各自所有者的商标。Gigamon 保留更改、修改、转让或以其他方式修订此出版物的权利，恕不另行通知。