无惧复杂环境挑战 顺利实施数字化教学
——思科帮助上海纽约大学实现全方位威胁防护

内容摘要

在思科 AMP for Endpoints 面向终端的高级恶意软件防御、思科 Firepower 下一代防火墙、思科 TALOS 威胁情报分析以及其他安全产品的协作下，上海纽约大学在日益复杂的网络环境中，始终不必担心任何威胁侵扰，专注于教学创新。

客户简介

- 客户：上海纽约大学
- 行业：教育
- 总部：上海

作为美国纽约大学和华东师范大学合作成立的国际化大学。上海纽约大学从成立伊始，就为自己树立建立世界一流大学目标。

在纽约大学的全球版图中，位于中国的上海纽约大学与纽约大学阿布扎比分校、纽约大学纽约校区一样重要，共同组成纽约大学全球系统中的三个具有学位授予权的门户校园。

在教育方式上，上海纽约大学适应全球化趋势，所有课程用英语授课，课程设计体现了跨学科知识的融汇与传播，体现中美高等教育的发展趋势；同时学校也会安排学生在本科学习期间进行海外游学，努力培养跨文化环境中成长起来的国际化人才。

数字化教学亟需安全保障

上海纽约大学不但在师资力量上追求优秀，更在教学模式上期望“打破常规”，摆脱传统固化教学方法，采用更灵活新颖教学模式，让师生体验到现代化、智能化的教学体验，驱动教学改革。

学校选择的解决之道是数字化教学，让学校向数字化转型，采用各种先进数字化技术，让学校师生进行全新的、充满无限想象力的学习和生活体验，从而也成为整个上海、整个国内高校的标杆，给国内高校的数字化转型，提供意义深远的参考借鉴。

业务挑战

- 上海纽约大学要与纽约大学全球其他校区互联，进行网络互连的时候内部数据会产生泄露风险
- 学校需要对园区互联网边界、数据中心应用边界进行全方位防护，特别是在复杂网络环境下，学校将面临勒索软件以及更多的未知威胁侵扰，亟需做好相关安全防范
- 学校每天大量访客参观，无法对访客的网络访问行为，进行有效区别控制

解决方案

- 思科面向终端的高级恶意软件防御（AMP for Endpoints）
- 思科 Firepower2100系列下一代防火墙
- 思科 Firepower4100系列下一代防火墙
- 思科 ISE 解决方案

但实现数字化校园可不是那么简单，上海纽约大学必须要考虑转型中所遇到的一系列安全层面挑战。

首先，上海纽约大学要与纽约大学全球其他校区互联，进行网络互连的时候内部数据会产生泄露风险。

其次，学校需要对园区互联网边界、数据中心应用边界进行全方位防护，特别是在复杂网络环境下，学校将面临勒索软件以及更多的未知威胁侵扰，亟需做好相关安全防范。

最后，上海纽约大学知名度很高，每天会有的家长和其他访客，学校需要一套基于身份的网络访问控制方法，对这些访客和本校的教职员工进行区别控制。总之，现在互联网上威胁风险逐渐增多，特别是教育行业更是成为遭受恶意软件攻击的“重灾区”。特别是17年“永恒之蓝”等勒索软件对国内教育网攻击，导致有些高校的教学系统、甚至校园一卡通核心系统的瘫痪，严重影响那些高校的正常教学和日常生活。

上海纽约大学迫切需要一套有效的安全防范体系，让自身可以心无旁骛地建设数字化校园，避免网络安全成为影响自身教育创新的最大障碍。

解决方案

考虑到上海纽约大学的需求情况，思科为其部署了以威胁防御为中心集成式架构的安全防御体系。主要包括:

在网络边界阻止更多威胁-学校在互联网边界采用以威胁防御为中心的 Firepower 4100和 2100 系列的 NGFW 下一代防火墙，启用入侵防御检测和 AMP（高级恶意软件防护），通过 ASR 路由器和 DM VPN 与国外其他校区进行安全连接；快速发现和拦截恶意软件-在学校特别担心的恶意软件防护方面，配置了思科面向终端的高级恶意软件防御（AMP for Endpoints），专门针对零日威胁和恶意代码实时安全防护。

保护员工随时随地接入网络-在网络接入认证方面，遵循纽约大学全球标准，部署网络接入认证整体解决方案。思科 ISE 解决方案用于访客和供应商的无线接入与访问控制；思科 Access Register 解决方案用于学校内部员工接入认证，结合网络端设备，利用 VRF 实现访客流量与学校内部人员流量隔离；在核心、边界路由器上部署 ACL，进行严格访问控制。

客户收益:

- AMP for Endpoints 提供了针对学校所有师生、所有终端设备的深度可视性和安全防御
- 上海纽约大学再也不用担心任何威胁出现，在思科全球 Talos 安全情报团队的帮助下，任何新威胁都能短时间内被甄别、发现
- 上海纽约大学可以针对访客和供应商等不同用户，进行不同等级、不同权限的身份验证以及访问控制授权

“思科 AMP for Endpoints 和其他思科设备的深度融合，让上海纽约大学的安全防御进入到一个新的阶段。这个以威胁防御为中心的安全体系，让我们充满信心，脚踏实地去进行教育方面的创新研究，让教师和学生群体更安心地在数字化校园中畅游知识海洋、享受校园生活。”

——上海纽约大学CIO 常潘

学校收益

思科为上海纽约大学所部署的安全解决方案，已经在学校开始部署运行，其不凡的表现，以威胁为中心的先进安全架构理念，是学校在使用其他安全解决方案时所无法感受的。

学校全面防范终端恶意威胁

特别是在对恶意威胁的防御方面，AMP for Network 与 AMP for Endpoints 的部署，一方面借助思科 TALOS 基于云的庞大情报规模，可以更快地发现并阻止一切安全威胁——思科 TALOS 团队每天分析超过150万个恶意软件样本和数万亿字节数据，确保了 AMP for Network 和 AMP for Endpoints 能够保持最新的威胁防御策略，确保上海纽约大学得到实时和有效的安全防护。

AMP for Endpoints 提供了针对学校所有师生（无论是教授还是学生或后勤工作人员）、所有终端设备（无论是教授办工作上的电脑，还是学生宿舍的笔记本、甚至是每个人使用的苹果或安卓手机）的深度可视性，只要上面的文件表现出“恶意行为”，就会被立即发现，并被 AMP for Endpoints 立刻“追本溯源”，显示该恶意软件一段时间以来的所有行动——从哪里来？都感染过哪些终端？现在正在执行什么活动？这些均通过可视化呈现，并能快速地在所有受到影响终端上自动隔离感染文件，立即修复。

安全深度可视，及时发现全新威胁

在学校网络边界，部署了思科 Firepower4100 和 2100下一代防火墙，提供了涵盖入侵检测和恶意代码检测的全面防护功能，保证了对来自外部的威胁连接与对外的可疑连接进行智能威胁监控，实现了全局可视化。

特别需要强调的是，思科 Firepower 4100 和 2100 下一代防火墙具备全面的威胁可视性，网络中所有用户、移动终端、客户端应用程序、操作系统、虚拟机通讯、漏洞信息、威胁信息、URL 等信息都可以通过图形化的形式显示。

灵活验证及控制授权，实现安全可控的网络访问

通过部署思科 ISE 身份认证引擎，上海纽约大学可以针对不同用户，进行不同等级、不同权限的身份验证以及访问控制授权。

这样，只有那些经过授权的设备，才能获得网络访问权限。让上海纽约大学印象深刻的是，思科 ISE 可以帮助学校进行设备发现和分析，特别是每天有大量访客和供应商的情况下，那些以前只能认为是“未知”的设备，会很容易被迅速发现、识别，并获得足够安全更新。

未来计划

思科整体安全解决方案的表现，让学校对于安全防范充满了希望。正如上海纽约大学 CIO 常潘所言：“上海纽约大学所部署的全面集成的、以威胁防御为中心的安全体系，让学校的安全防御进入到一个新的阶段。让我们充满信心，脚踏实地去进行教育方面的创新研究，让教师和学生群体更安心地在数字化校园中畅游知识海洋、享受校园生活。”

正如学校不断增长的师生力量、以及品牌名气一样，上海纽约大学在未来，也会进一步巩固自身的安全防御能力，以应对日益增加的复杂恶意攻击，给师生创造一个更安全的数字化校园环境。