思科 AMP（高级恶意软件防护）让中欧国际工商学院的信息化之路更安全

内容摘要

在思科集成安全架构解决方案的帮助下，中欧国际工商学院有效抵御了各类恶意软件、尤其是勒索软件的攻击，最大程度地保证了学校的整体网络、数据安全，大量宝贵的数据免受侵袭，有效保障学院卓越声誉，使学院的信息化之路更安全。

客户简介

- 客户：中欧国际工商学院
- 行业：教育
- 总部：上海

在中欧国际工商学院内，智慧和思想的交流碰撞不断演绎。在这里，融汇中西、博学善教的全职教授们为中高层管理人员提供专业管理培训。伴随着知识传授、智慧碰撞的，则是这里“轻松随意”的学习环境。教授和学员们可以借助自己的电脑、PAD 甚至是智能手机，在学校内、外的任何地方，通过网络进行各种方式的授课学习。

这种“轻松随意”的学习环境表现，和教育行业所面临的严峻风险威胁形成强烈反差——教育行业每年面临恶意软件威胁不断增多，给很多高校数据造成了极大损失——数字化时代来临，无论是教授们的多年的课程资料，还是不同知识产权等研究成果等信息，无一不是通过数据的方式存在，数据对于高校来说，不仅意味着信息，它更代表着极为珍贵的“数字资产”。

面对复杂环境，中欧国际工商学院依靠一套行之有效的防御系统，有效抵御勒索软件入侵，大量珍贵数据资源和教学成果免受攻击，确保了数字化时代学校的教学秩序和教学效果，为其培养众多商界精英提供强有力保障，赢得大家的信任。

追求卓越，信任为基

中欧国际工商学院自1994年创建以来，一直秉承“认真、创新、追求卓越”的理念，致力于培养具有国际视野、积极承担社会责任的商业领袖。

追求卓著名声的基石来自信任。这种信任来自先进的教学理念和手段、国际化的视野和雄厚的人脉资源；也来自在数字化时代，为精英学员们所营造的安全、值得信任的网络环境。

业务挑战

- 中欧国际工商学院一直追求业务卓越和社会信任，需要在日益复杂和危险的互联网环境中保持全方位安全防御
- 传统教育行业安全防御架构简单、单点防御，无法抵御现代恶意软件无孔不入的威胁
- 传统的行业安全部署彼此分散，缺乏整体可视性和系统作业模式，容易遭受攻击并影响巨大
- 传统安全防御方式要求大量专业人员和专业设备，容易带来人力和IT投资上的巨大压力

解决方案

- 思科集成式架构安全解决方案
- AMP for Endpoints 面向终端的高级恶意软件防御
- 内嵌 AMP 服务的邮件安全网关
- 思科 TALOS 团队全球威胁情报实时防护

这种信任使得中欧国际工商学院在追求卓越之路上表现不凡。截止目前，学院已发展成为亚洲领先、世界一流的商学院，拥有遍布全国及世界各地的校友19000多位，并为逾10万人次的高层管理人员提供了管理培训。

拥有一个智能、安全的网络安全平台对于学院至关重要，它可以在越来越复杂多变的网络威胁背景下，更好地保障安全、管理安全，强化信任。

教育行业面临特洛伊木马屠城般新威胁

安全的环境对于当今的全数字化业务模式至关重要。然而目前教育行业多数采用只具备单点安全防护功能的传统解决方案，无法有效抵御现代恶意软件的威胁。

恶意软件能通过多个攻击媒介进入学校网络，很多学校网络不具备全面可视性来实现全面防御；高级恶意软件也会掩盖自身目的，增加检测难度。

传统方式，是在终端上堆叠更多的产品，以期获得可见性，以及应对那些绕过传统解决方案的威胁。但这增加了运营复杂性，防护效果乏善可陈——恶意软件就好像是“无孔不入”的“幽灵”一样，再也不按照“常理出牌”，导致教育行业防火墙边界为主的安全防御方式，被恶意软件轻松绕过，就犹如特洛伊木马屠城一般，对学校宝贵数据资产带来近毁灭性的影响打击。

体系化遏制威胁，避免头疼医头脚疼医脚

传统的安全解决方案，耗费太多时间在检测威胁上，在勒索软件已经攻击时，才有所发觉，匆忙应对，但为时已晚（整个业界平均需要花费100多天的时间，才能检测出环境中存在的威胁）。

传统的行业安全部署彼此分散，缺乏整体可视性和系统作业模式，无法感知被恶意软件所“感染”的真实情况，难以实现彻底修复——“头疼医头脚疼医脚”的防御方式，导致教育行业在恶意软件威胁面前迅速败下阵来。最典型当属2017年爆发的两次大规模勒索软件事件，众多国内外高校纷纷中招，几乎没有任何的抵抗就被勒索软件长驱直入。

集成式架构安全方案
构建智能安全的网络平台

对于中欧国际工商学院而言，一个坚实可靠的安全防御平台，可以降低业务风险，赢得学员和外界对学院的信任，同时还能帮助学院的数字化转型提供强大网络安全基础，让学院更有信心来实施能够加强创新与增长的数字化技术。

客户收益:

- 中欧国际工商学院建立集成式架构、全方位的安全防御阵线，涵盖了从网络边界到终端安全的全面防御，特别是阻断了勒索软件的主要入侵渠道，有效遏制恶意软件的威胁。
- 在 AMP for Endpoints 帮助下，恶意软件“无处遁形”，快速发现，快速打击，确保学院内部的安全网络环境和数据信息保护
- 思科 AMP for Endpoints 独特的 SAAS 部署模式，让中欧国际工商学院彻底去掉相关硬件和维护技术人员投入负担，真正做到“轻装上阵”
- 在未来，中欧国际工商学院将会把思科 ISE 身份认证服务引擎、下一代防火墙、网络可视与安全分析、AMP for Endpoints 完美集成，彼此信息共享深层联动，自动快速隔离潜在威胁，全面保护中欧国际工商学院数据资产

“思科集成式架构安全方案给我们留下深刻印象，特别是 AMP for Endpoints 帮助我们实现了面对威胁的全面可视性，并让我们以自动化方式，实时阻止恶意软件对所有类型终端的威胁。真正帮我们实现全面有效安全。”

——中欧国际工商学院CIO 薛东明

思科与中欧国际工商学院深入合作，为其部署了集成架构安全方案，实现了从网络到终端一体化高级恶意软件防护，其中的组件包括思科面向终端的高级恶意软件防御（AMP for Endpoints），全面防御各类恶意软件攻击，例如勒索软件的威胁；邮件安全网关支持集成 AMP（高级恶意软件防护），实现恶意软件威胁信息的共享和全面可视化。在思科 TALOS 团队的全球威胁情报实时防护的帮助下，中欧国际工商学院做到对任何恶意软件的威胁都能做到快速感知、自动定位、追溯，快速遏制，这一切都基于全面可视化实现，保障了学院的数字资产安全，强化学员们的信任感。

全面、持续性威胁防御,有效阻止更多威胁

面对恶意软件无孔不入的威胁环境，中欧国际工商学院建立集成式架构、全方位的安全防御阵线，涵盖了从网络边界到终端安全的全面防御，并且还借助内嵌了 AMP 服务的邮件网关，阻断了恶意软件，特别是勒索软件的主要入侵渠道。这种全面性的防御体系，帮助中欧国际工商学院建立了一个“密不透风”的安全网络，有效遏制更多恶意软件的威胁。

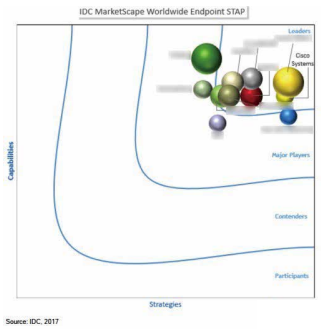
其中特别值得注意的是集成式架构中的 AMP for Endpoints 面向终端的高级恶意软件防御，采用了思科以威胁为中心的安全架构，可充分利用云的庞大规模与强大性能，支持中欧国际工商学院更快速地发现并阻止更多威胁——这得益于思科 Talos 团队每天分析超过150万个恶意软件样本和数万亿字节数据，并将情报自动推送给 AMP for Endpoints 以及其它思科安全产品，确保中欧国际工商学院得到全天候保护。

追本溯源，威胁无处可遁

AMP for Endpoints 还能提供对学院内部所有终端上的可执行文件以及其他文件进行深入可视性。无论是教授，还是学员，无论是使用运行 Windows 或者 Mac OS的笔记本电脑，还是安卓手机或苹果手机，只要上面任何文件表现出恶意行为，AMP for endpoints 都会立刻“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。

这种恶意软件入侵到威胁发现之间的时间越长，组织所遭受的安全影响和损失就会越大。中欧国际工商学院通过采用思科的先进技术，不断加快威胁发现的检测速度，将平均威胁检测时间缩短到3.5个小时(行业平均时间为100-200天)，让威胁无处可遁，快速“围剿歼灭”。

在2017年 IDC Marketscape 的终端安全报告中，思科终端安全防护产品-面向终端的 AMP 被评为行业的“领导者”，



IDC Marketscape 终端安全报告

“轻装”上阵，简约 IT 释放更强 IT 价值

数字化时代，IT开始驱动额外的创新。中欧国际工商学院也不断塑造安全可信IT环境，驱动业务变革。同时也借助虚拟化技术发展，精华而简约学院的IT资源，“轻装”上阵，但又不简单，充分适应IT新技术趋势下的新业务发展模式，提供敏捷部署和足够的灵活度，支撑学院创新多变的业务开发和发展需求，释放更强能量的IT价值。

思科 AMP for Endpoints 独特的 SAAS 部署模式，一切分析均在云端进行，教授和学员们设备性能不会受到任何影响，中欧国际工商学院彻底去掉相关硬件和维护技术人员投入负担，真正做到“轻装上阵”。

思科 AMP 高级恶意软件防护这种存在的形态，导致它可以无处不在、无时不在，可以存在于终端上，也可以存在于下一代防火墙、分支路由器等网络边缘，还能出现在邮件网关和 Web 安全等设备中，有效阻断恶意软件中最具代表性的勒索软件的入侵主要通道。

借助思科集成式架构安全解决方案，中欧国际工商学院获得深度可视性，借助图形化界面轻松而高效地实现恶意软件的预防、发现和修复，实现IT简约性，极大简化运维的压力。

现在，思科集成式架构安全方案在中欧国际工商学院部署完毕，其卓越的表现给中欧国际工商学院留下深刻印象。“思科集成式架构安全方案给我们留下深刻印象，特别是 AMP for Endpoints 帮助我们实现了面对威胁的全面可视性，并让我们以自动化方式，实时阻止恶意软件对所有类型终端的威胁。真正帮我们实现全面有效安全。”中欧国际工商学院CIO 薛东明

未来的计划

“道高一尺魔高一丈”，在数字化转型时代，安全与恶意威胁永远处于胶着的缠斗之中。面对日益复杂的网络威胁环境，以及恶意软件越来越狡诈、善于伪装（例如隐藏在加密流量中或者通过社交媒体进入），中欧国际工商学院对于未来的安全发展，亦有清晰规划。

中欧国际工商学院未来计划引入思科的网络可视与安全分析方案，实现更全面可视，可以在无需解密情况下，使用网络分析方法快速识别出隐藏在加密流量中的恶意软件。同时把整个网络中所有设备，都变成为“安全探针”，借助大数据分析方法，机器学习进一步提高威胁感知能力。

同时，中欧国际工商学院已经部署了思科 ISE 身份认证服务引擎，解决了不同设备在接入网络时候身份识别与策略分配，它可以和下一代防火墙、网络可视与安全分析、AMP for Endpoints 完美集成，彼此信息共享深层联动，自动快速隔离潜在威胁，全面保护中欧国际工商学院数据资产，将思科安全架构的集成式特点表现得更加淋漓尽致。

了解思科高级恶意软件防护方案（AMP），请扫描二维码

致电: 4006 680 680

如需了解思科公司的更多信息，请浏览 http://www.cisco.com.cn