中智集团携手亚信安全 打造立体化、智能化网络防御体系

如今，许多大型企业正在遭受前所未有的数据窃取攻击，全球 500 强企业大面积“沦陷”已经成为残酷的事实。在互联网威胁不断加剧的情况下，作为一家业务覆盖全球的超大规模企业，中国国际技术智力合作公司（简称中智，英文缩写 CIIC）的信息安全管理难度不断加大。为此，中智联手亚信安全，利用全球领先的云安全技术与创新产品全力打造立体化、智能化安全架构，形成主动有效的纵深防御体系。

网络威胁“无处不在” 大型企业成黑客重点目标

中智成立于 1987 年，是中央管理的国有重点骨干企业。作为中国人力资源市场的开拓者，中智主动适应全球知识经济时代新生产力的发展，在境内外设立 91 家分支机构，与 76 个国家和地区开展经济技术人才合作，业务广泛覆盖全外包、离岸化、投资服务、贸易服务等领域。随着企业规模的不断壮大以及业务系统的复杂化，中智越来越依赖“健康”的信息网络。

“中智的超大规模和所处业务领域的特殊性，大大提升了信息安全管理的难度。防御者是相对被动的，但必须向着主动防御进行转变，比如黑客可能只选取一种方式来进行网络攻击，但是我们必须掌握或考虑到各种各样的攻击防御方式。另外，为了确保数据安全 ,我们就不能选择分散的网络安全模式 ,因为如果不能整齐划一的去治理、部署、监控整个集团的信息化安全策略，必然会给黑客留下可乘之机，酿成数据泄露等严重后果。”作为中智信息安全体系的负责人曹赟希望集团信息安全战略落地能够步调一致。

曹赟针对数据泄露的担忧并非杞人忧天。资料显示，世界 500 强企业中超半数曾遭受过黑客攻击 ,中国 2011 年到 2014 年互联网公开的安全事故已导致 11.3 亿用户信息泄露 。而中智在人力资源领域耕耘多年，其高附加值的商业数据更易成为黑客攻击的目标。那么，中智以数据安全为核心的立体化架构又是如何建立起来的呢？

防御“间谍软件”立体化架构初步形成

这需要从十年之前，中智集团防御“间谍软件”攻击谈起。

曹赟表示，中智立体化的防御基础在十年之前就打下良好基础。他说：“中智的信息安全管理起步很早，而 2004 年与趋势科技中国，也就是现在的亚信安全展开合作，

则是一次重要的契机。当时，为了对抗间谍软件以及其它恶意威胁，我们必须全盘考虑，不仅需要统一部署防毒产品，更需要提升员工安全防护技能。而亚信安全为我们设计了多层架构的间谍软件防护解决方案，在网关与客户端、服务器上同时部署，并且还在所有安装亚信安全防毒墙网络版（OfficeScan）的客户端上提供了自动清除功能，员工并不需要手动处理病毒威胁。”

亚信安全防毒墙网络版（OfficeScan）领先的网络威胁防御能力和亚信安全防毒墙控管中心的统一管理，让中智的网络安全统一策略得以落实。在双方后续的合作中，中智陆续选择了亚信安全的防毒墙 Web 安全版（IWSS）、企业级邮件内容安全产品（IMSS）等，这为集团的业务创新和信息化应用提供了多层次的安全保障。

但是，间谍软件并未走远，反而被黑客加入翻新的攻击代码、采用更隐蔽的攻击手法，用于发动 APT（Advanced Persistent Threat）攻击。那么，新问题来了！亚信安全防毒墙网络版（OfficeScan）能够适应网络威胁的变化吗？亚信安全能够为中智提供防御 APT 攻击的解决方案吗？中智在采用虚拟化和云计算应用之后，安全管理能够为之提供充足保障吗？

再度联手 打造智能化网络防御平台

在亚信安全的协助下，中智采用的亚信安全防毒墙网络版（OfficeScan）不断加入“新鲜血液”，使其具备了更加智能的防御机能。另外，亚信安全还采用定制化智能防御(Custom Defense From Targeted Attacks)、深度威胁发现平台(Deep Discovery，DD)、专属咨询服务(TrendMicro Premium Support Program，PSP) ，协助用户达到了有效治理 APT 的目标。

首先，亚信安全防毒墙网络版（OfficeScan）经过十年间的不断升级，已经成为了企业终端安全的最佳解决方案。最新版本的亚信安全防毒墙网络版（OfficeScan）配合亚信安全防毒墙控管中心、云安全智能保护网络（Smart Protection Network），可以为中智集团所有终端用户有效拦截各类恶意代码攻击。另外，虚拟补丁、数据防泄漏、虚拟化安全、移动终端安全管理、Web 信誉评估等功能的加入，让用户进一步增强了防护能力。

其次，中智建立了全面的 APT 侦测体系。通过亚信安全深度威胁发现设备（TDA）可以与亚信安全其它网关、虚拟化、服务器以及终端安全防护产品整合，形成全覆盖的侦测平台，网络和应用的联动配合能够深入发现文档、URL、通信以及上网行为中藏匿的可疑对象。更进一步的是，中智的整体网络还能够与云安全智能保护网络（Smart Protection Network）形成实时威胁情报共享机制，了解全球发现的相同 C&C 恶意服务器或类似恶意软件的攻击，使得各个安全节点可以对 C&C 通讯和 APT 特征行为进行侦测和阻断。

最后，针对中智新建立的 BYOD、虚拟化和云存储，亚信安全提供了服务器深度安全防护系统（Deep Security）和企业安全云盘（SafeSync），在确保数据安全管理效果的同时，全面提升工作效率。例如：亚信安全企业安全云盘（SafeSync）在传输及文件存储过程中，采取了高安全性的加密设置，并在数据防泄密保护功能上实现了历史版本恢复和用户权限管理，能够防止因遗失、失窃、病毒或设备故障所造成的数据损失。

如今，在消除网络威胁、专注业务发展的情况下，中智的业务快速发展，在新兴服务领域拥有人才、资源、网络、规模、经验的巨大优势和影响力，成为了具有高度竞争力和领先性优势的全新创业组织。

“从有线环境下的 PC 走向移动终端和云应用，亚信安全已经是我们最可信赖的技术伙伴。十年间，我们一同经历了网络威胁的演化变迁，在产品、技术、服务等方面不断磨合、携手提升，进而形成了安全联动、立体化、智能化的防护体系。” 曹赟对亚信安全多年以来的护航服务表示十分满意。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com