对信息安全产业未来的三点思考 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/64/2021_2022__E5_AF_B9_E4_BF_A1_E6_81_AF_E5_c40_64821.htm 火花1 ： 安全产品走向融合 在网络通信界的巨头们热烈讨论网络融合美妙前景的同时，网络安全界已经用行动去品尝各种安全技术融合的滋味。但如果我们比较一下两种融合趋势就会发现他们之间有很大差异。 网络通信的融合的源动力来自新技术的创新，而这种融合的方向是多种业务在一个平台上的承载。而信息安全界的融合源动力来自网络攻击手段的融合。而融合的方向是以安全技术的融合对抗攻击手段的融合。可以说信息安全界的融合是让愈演愈烈的网络攻击逼出来的虽然这听起来有点以彼之道还彼之身的味道，但事实确实如此。以网络病毒为例从去年的尼姆达到今年的振荡波，冲击波，还有最近的QQ尾巴，我们可以看出在现在的网络攻击手段中，既包括病毒攻击，也包括隐通道、拒绝服务攻击，还可能包括口令攻击、路由攻击、中继攻击等多种攻击模式。双拳难敌四手，众多攻击手段让传统上各自为战的安全产品破绽百出。 IDS不是用来对付网络蠕虫的，防病毒软件不会理睬网络上拒绝服务攻击，防火墙对病毒攻击和隐藏在合法服务下木马后门鞭长莫及。用户不是技术专家，当安全问题出现时，他们不会追究到底是摆在这边的防火墙还是放在那边的IDS谁失职，他们会责问安全提供商：我掏了一大堆钱，为什么我的网络老出问题，你们安全产品到底灵不灵？ 入侵检测技术侧重监测、监控和预警领域，而防火墙和IPS能在访问控制领域发挥长处，防病毒软件，安全认证分属于不同的安全领域的安全产

品,可惜用户并不是讨论某一种安全技术乃至某一个安全产品与其他技术和产品哪个更安全，其实不如探讨如何将各种安全产品整合成一个安全体系让这些安全产品有效地协同工作更为务实。 我们可以看到现在各大安全产品制造商的产品线已经在尝试将不同的技术融合在一起：以侧重于检测的入侵检测技术和侧重于访问控制的防火墙技术两种技术协同和融合起来一直是信息安全研究的前沿课题。而防火墙和防病毒的融合已经在防毒墙这一产品中得到体现。所以只有将不同安全侧重点的安全技术有效的融合起来，安全产品的性价比才能更高，才能在日益激烈的信息安全市场上有优异的表现。 一个木桶能装多少水不但要看木桶最短的那块模板的长度，也要看木板之间的紧密程度。这个模型应用在信息安全领域就是：一个企业网络的信息安全不但依赖单个安全产品自身的性能也依赖于各个安全产品之间的协作。众多安全产品之间的关系不是简单堆砌，而是相互协作，将不同安全防范领域的安全产品融合成一个无缝的安全体系。 来自天融信的余海波介绍说：这种融合趋势不仅仅是安全技术，也席卷了安全体系和架构。网络安全产品已不能再仅仅是个安全设备，还必须是个高性能的网络设备。 思科自防御网络的体系框架把安全的基因融合到路由器、交换机、终端、防火墙 VPN IDS产品中，并采用了集成化管理软件。从终端方面的网络准备控制（NAC），到交换机上的防火墙、入侵检测、流量分析与监控、内容过滤形成全面的网络安全防御体系。这个安全防御体系代表了安全和网络融合成一体的整体安全解决方案也成为网络安全领域的共识和发展方向。 火花2： 安全厂商之间不仅仅是竞争关系 说到竞争，在信息安全市场上，安

全厂商们之间不仅仅是激烈的竞争，他们还有合作。合作不仅仅是不同领域的安全产品之间的必须有良好的兼容性，这个技术问题对于前来座谈的厂商不是什么大问题，真正的问题来自于厂商之间在市场竞争中的合作。来自瑞星公司的市场部副总经理马刚谈到了价格竞争，讲了一个真实案例，在一次采购招标中，一家小的安全产品服务商为了能拿到一个单子，用低于盗版的价格硬是将瑞星还有另外两家国内知名安全厂商挤出局，马刚说：“ 当我听到他的报价，一个单机版5元！那就没什么可说的了。5元一个软件，别说是软件开发成本，服务提供成本，就是我的服务人员来你这里提供及时的上门服务的车票钱都不够！ ”这种严重的恶意压低产品价格只能是阻碍，而不是促进信息安全业的健康发展。非理智的低价竞争恐怕受损失不仅是厂商自己，用户最终也会为这个非理智低价承担相应的损失。而刚才那个案例的用户就是折腾了两个星期后又把上面3家安全产品提供商请回来重新竞标，原因当然也勿须多说，从这个案例我们可以看出信息安全这个产业需要每一个参与游戏者都自觉遵守一定的游戏规则，而其中一条重要的规则就是不参与低价竞争。需要指出的是现阶段的信息安全产业环境和网络通信界的产业环境有一个重要的不同：那就是竞争过度。网络通信界天天有人喊打破垄断，鼓励竞争，只有竞争可以让垄断者出让一部分剩余让消费者享受，可是在信息安全产业内是恰恰相反，竞争的不止是有点过头，而是千军万马过独木桥，十几家厂商为一个单子互开低价，而且是一边骂别人瞎搞拆台，一边给用户开出0折扣的支票，让客户自己去填价格！这种恶性竞争不但影响安全制造商，安全服务提供商自己的健康成长，而

且超低价产品和超廉价服务只是一个短期行为，长期下去会滋生劣质产品、劣质服务，这反而不利于信息安全市场的成长。所以安全厂商之间不仅仅是刺刀见红的竞争关系，而且每一个想在信息安全产业做久做大的企业都必须建立一种战略合作，通过这种合作去建立一种行业秩序，这种行业秩序同国家的宏观产业政策互相呼应才能营造出一种良好的市场环境，促进信息安全市场健康发展。显然信息安全市场的健康发展的受益者是信息安全市场的每一个参与者，不仅是产品和服务的提供者，还有产品和服务的接受者。我想信息安全界自律公约的出台就说明这种合作的必要性已经被各大信息安全相关厂商意识到了。