下一代网络安全解决方案

摘　要

随着网络的泛化和无边界化，传统的安全理论模型和安全体系已经不能适应新的威胁产生的态势，面对网络安全问题越来越严峻的事实，需要新的安全体系来解决新的安全问题。

随着网络的泛化和无边界化，网络安全问题会越来越严峻。单就恶意代码一项，就呈现出爆炸增长的趋势。目前全球已经有 50亿恶意样本，每天还将以300万种的速度产生。如果把恶意代码问题看作天灾的话，那么现代网络同时还面临着“人祸”。“棱镜门”事件揭露了网络数据被监听的事实，暴露出国家安全、网络安全形势严峻。无论数据被恶意代码破坏，还是被黑客监听，最终都使得安全问题回归到了安全体系如何建设这样一个根本命题。

1 安全现状

地下黑色产业链的发展，使得制作黑客工具、控制用户终端、盗取用户信息、滥用互联网资源、攻击受害系统等行为形成产业化，并快速壮大，对互联网安全造成严峻挑战。

新型安全攻击方式增长迅猛，传统技术难以应对。利用0Day进行攻击案例迅速增长，而APT攻击方式向更加多维化的方向发展，综合运用各类攻击手段的能力、复杂度继续提升。

网络

IP化、IPv6、云、物联网的智能化发展趋势，产生了更为复杂的安全问题。

运营商网络往往规模庞大，安全脆弱点多，安全体系建设难以达到更好的效果，在这样的网络结构下，运营商骨干网、短信系统长期受到攻击，获取用户信息，难以发现，国家安全部门发现运营商重要系统中被植入特种木马的事例也逐渐增多，在这种安全趋势下，新的安全威胁对旧的安全体系发起了挑战。

2 基于 P2DR安全模型的早期安全防护体系

早期的安全体系建设就是基于 P2DR模型，包括

4个主要部分：策略、防护、检测和响应。

1

策略（Policy）：根据风险分析产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。

2

防护（Protection）：通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

1

检测（Detection）：是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。

2

响应（Response）：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

该安全体系的好处是基于风险评估理论，将安全看做一个动态的整体。通过策略与响应来使得安全问题形成闭环，但是该安全体系并没有对安全威胁的本质进行分析，是安全体系的初级阶段的产物。

基于该安全体系，产生了一些如防火墙、入侵检测等初期的安全产品。

3 基于木桶原理的近期安全防护体系

随着安全威胁的不断发展和对安全理解的不断加深，人们开始对安全本质进行思考，出现了基于木桶原理的安全防护体系。

木桶原理简单的说就是整个系统的安全系数取决于最弱一环，即短板理论，因此整个安全体系的建设就是寻找整个网络的所有安全边界，然后将这些安全边界进行防护，避免安全短板的出现。

安全领域近

10年的时间都是靠边界思想来指导安全体系建设，用网关防护类产品确定网络入口的安全边界，用网络版防病毒确定终端的安全边界，用系统加固系统确定

服务器的安全边界，用 STANDARDIZATION
风险管理制度确定人的安全边界。

传统的安全防护思想就是基于木桶理论为用户构建一个完整的线式防御体系，但是攻击却是点式的，任何一点被攻陷，整个安全体系就会崩溃，因此基于目前的理论基础，安全体系建设本身就是一个花费大量力气，但成效却不好的举措。这会使安全的成本变得极其昂贵。

4 基于大数据安全的下一代安全防护体系

基于木桶理论的安全体系属于被动的威胁防御思想。事实上，真正有效的安全体系是基于主动的威胁发现思想，主动出击，主动感知威胁。

不管威胁如何演变，威胁总是遵循图 1模型。

即不管网络的安全风险点有多少个，威胁入侵只有两条路径，一条是从外网向内网的威胁入侵路径，一条是从内网向外网的威胁扩散路径。从外网向内网威胁入侵的最经典事件是黑客攻击和
APT攻击，而从内网向外网威胁扩散的最经典事件是
U盘病毒。从理论上看，只要对这两条关键威胁路径进行监测和管控，就能遏制威胁产生的态势，以最小的安全成本解决企业的安全问题。

而基于大数据安全的云 +端
+边界的安全模型，能够很好地解决这一安全问题。

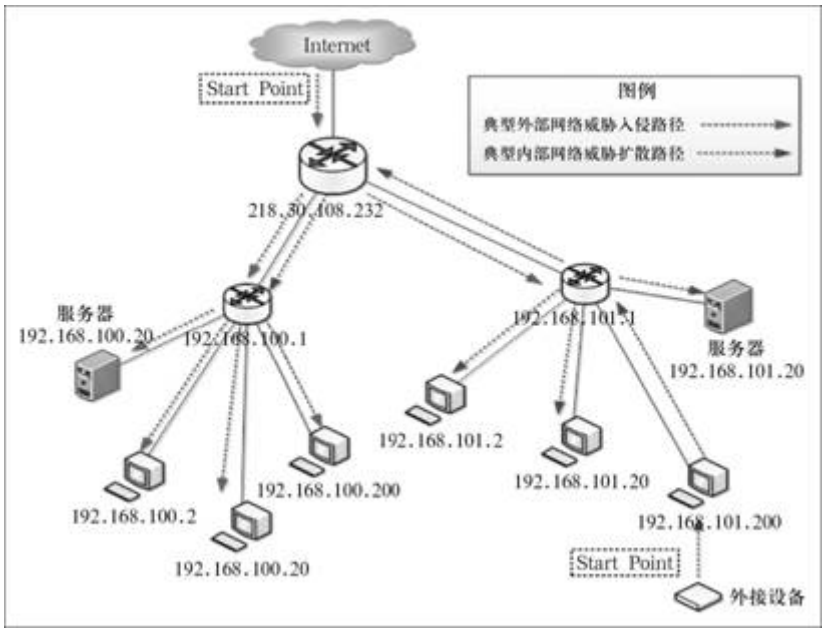

图1 威胁入侵模型

安全模型如图 2所示。

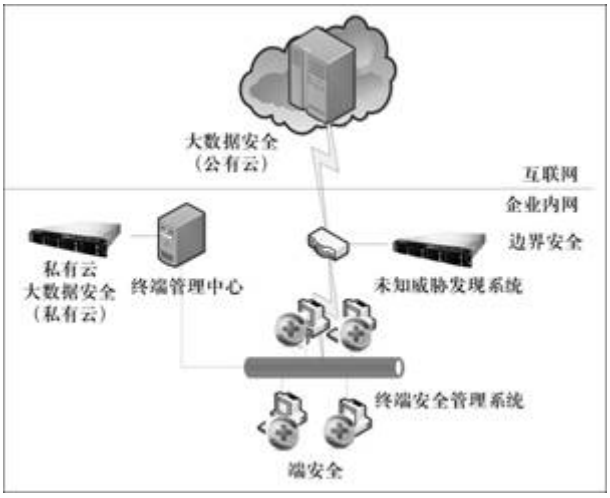

图2 云+端+边界安全模型

云 +端

+边界的安全防御体系，是为了适应新的威胁的下一代的智能防御体系，整个体系包括大数据安全、边界安全和端安全 3个关键部分。

大数据安全是指基于大数据技术构建的安全威胁捕获和分析平台。分为公有云和私有云两部分。在互联网环境下，使用公有云，对于隔离网环境，则使用私有云。边界安全是指基于大数据安全技术的未知威胁发现技术。端安全是指基于大数据安全技术的终端的安全管理与防护系统。

大数据安全就是我们常说的云安全体系，一般的云安全模型如图 3所示。

基于终端的木马感知云，将大量的可疑样本收集到

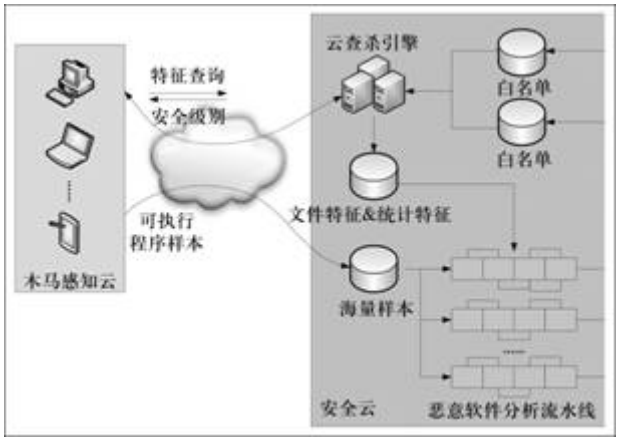

图3 大数据安全分析模型

安全云中，首先进行海量样本分拣，然后将分拣后的样本放入恶意软件分析流水线，最终将分析后的样本进行黑白名单的分类，然后将产生的大数据安全数据提供给云查杀引擎使用。由于该系统是一个生态的自循环系统，因此可以在最短的时间内发现世界上新产生的威胁，将这些威胁分析整理，用于边界防护和端防护。能够对企业网络进行很好安全防御。

5 总结

运营商的网络规模庞大，结构复杂，如果采用传统的基于木桶理论的边界防护的安全体系，无疑是一件不可完成的任务。而基于大数据安全的下一代安全防护体系，则能够利用有限的成本迅速发现新的威胁，有效地解决网络的安全问题