浅析“云安全”技术

余娟娟
（同济大学，上海 200092）

摘 要：随着云计算的发展，云安全技术成为网络时代信息安全的最新体现。主要介绍了“云安全”的七大技术核心，分析云安全 3.0 体系的解决方案，探讨云安全系统建立的难点，并对云安全在国内外的应用现状进行比较。

关键词：云安全；云计算；虚拟；病毒

Analysis of Cloud Security Technology

YU Juan-juan
(Tongji University, Shanghai 200092,China)

Abstract: With the development of cloud computing, cloud security technology is becoming the latest exemplification in the era of network information security. This paper describes the cloud security of the seven core technology, analyzes cloud security 3.0 system solutions, investigates the difficulties in setting up cloud security system, and then compares the application status of cloud security at home and abroad.

Key words: cloud security ; cloud computing ; virtualization ; virus

1 引言

随着信息技术发展，近几年各种类型的云计算和云服务平台越来越多地出现在人们的视野中，比如邮件、搜索、地图、在线交易、社交网站等等。由于它们本身所具备的便利性、可扩充性、节约等各种优点，这些云计算和云服务正在越来越广泛地被人们所采用。

但与此同时，这些“云”也开始成为黑客或各种恶意组织和个人为某种利益而攻击的目标。比如利用大规模僵尸网络进行的拒绝服务攻击（DDoS）、利用操作系统或者应用服务协议漏洞进行的漏洞攻击，或者针对存放在“云”中的用户隐私信息的恶意攻击、窃取、非法利用等等，手段繁多。除此以外，组成“云”的各种系统和应用依然要面对在传统的单机或者内网环境中所面临的各种病毒、木马和其他恶意软件的威胁。

正是为了有效地保护构成云的各种应用、平台和环境以及用户存放于云端的各种敏感和隐私数据不受感染、攻击、窃取和非法利用等各种威胁的侵害，趋势科技推出了基于趋势科技云安全技术核心的全新的云安全 3.0 解决方案。

2“云计算”与“云安全”

2.1 云计算

“云计算”（Cloud Computing）是一种新兴的商业计算模型。它将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算力、存储空间和各种软件服务。这种资源池称为“云”。“云”是一些可以自我维护和管理的虚拟计算资源，通常为一些大型服务器集群，包括计算服务器、存储服务器、宽带资源等等。“云计算”将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。这使得应用提供者无需为繁琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

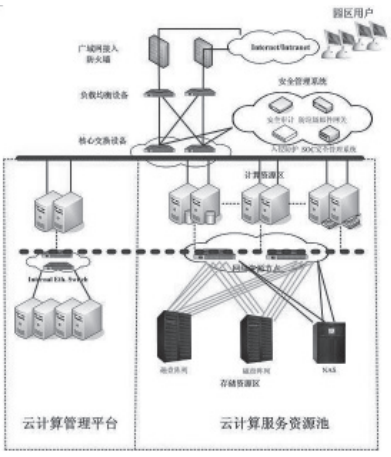

图 1“云计算”网络拓扑图

2.2 云安全

“云安全（Cloud Security）”紧随云计算之后出现。它是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，并发送到 Server 端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。未来杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，原有的特征库判别法显然已经过时。“云安全”技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。

“云安全”的策略构想是：整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。因为如此庞大的用户群，足以覆盖互联网的每个角落，只要某个网站被挂马或某个新木马病毒出现，就会立刻被截获。“云安全”的发展迅速，趋势、瑞星、卡巴斯基、MCAFEE、SYMANTEC、江民科技、PANDA、金山、360 安全卫士等都推出了“云安全”解决方案。

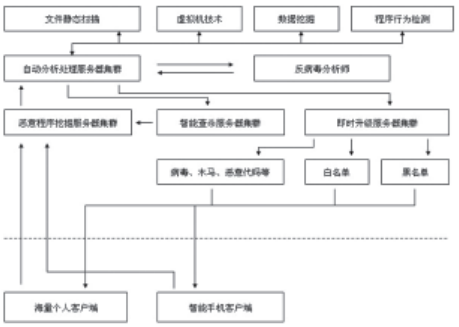

图 2“云安全”的立体结构防御体系图

3“云安全”的核心技术

从目前的安全厂商对于病毒、木马等安全风险的监测和查杀方式来看，“云安全”的总体思路与传统的安全逻辑的差别并不大，但二者的服务模式却截然不同。在“云”的另一端，拥有全世界最专业的团队来帮助用户处理和分析安全威胁，也有全世界最先进的数据中心来帮你保存病毒库。而且，“云安全”对用户端的设备要求降低了，使用起来也最方便。“云安全”为我们提供了足够广阔的视野，这些看似简单的内容，其中缺涵盖七大核心要素：

3.1 Web 信誉服务

借助全信誉数据库，“云安全”可以按照恶意软件行为分析所发现的网站页面、历史位置变化和可疑活动迹象等因素来指定信誉分数，从而追踪网页的可信度。然后将通过该技术继续扫描网站并防止用户访问被感染的网站。为了提高准确性、降低误报率，安全厂商还为网站的特定网页或链接指定了信誉分值，而不是对整个网站进行分类或拦截，因为通常合法网站只有一部分受到攻击，而信誉可以随时间而不断变化。

通过信誉分值的比对，就可以知道某个网站潜在的风险级别。当用户访问具有潜在风险的网站时，就可以及时获得系统提醒或阻止，从而帮助用户快速地确认目标网站的安全性。通过 Web 信誉服务，可以防范恶意程序源头。由于对零日攻击的防范是基于网站的可信程度而不是真正的内容，因此能有效预防恶意软件的初始下载，用户进入网络前就能够获得防护能力。

3.2 电子邮件信誉服务

电子邮件信誉服务，按照已知垃圾邮件来源的信誉数据库检查 IP 地址，同时利用可以实时评估电子邮件发送者信誉的动态服务对 IP 地址进行验证。信誉评分通过对 IP 地址的“行为”、“活动范围”以及以前的历史进行不断地分析而加以细化。按照发送者的 IP 地址，恶意电子邮件在云中即被拦截，从而防止僵尸或僵尸网络等 Web 威胁到达网络或用户的计算机。

3.3 文件信誉服务

文件信誉服务技术，它可以检查位于端点、服务器或网关处的每个文件的信誉。检查的依据包括已知的良性文件清单和已知的恶性文件清单，即现在所谓的防病毒特征码。高性能的内容分发网络和

本地缓冲服务器将确保在检查过程中使延迟时间降到最低。由于恶意信息被保存在云中，因此可以立即到达网络中的所有用户。而且，和占用端点空间的传统防病毒特征码文件下载相比，这种方法降低了端点内存和系统消耗。

3.4 行为关联分析技术

通过行为分析的“相关性技术”可以把威胁活动综合联系起来，确定其是否属于恶意行为。Web威胁的单一活动似乎没有什么害处，但是如果同时进行多项活动，那么就可能会导致恶意结果。因此需要按照启发式观点来判断是否实际存在威胁，可以检查潜在威胁不同组件之间的相互关系。通过把威胁的不同部分关联起来并不断更新其威胁数据库，即能够实时做出响应，针对电子邮件和Web威胁提供及时、自动的保护。

3.5 自动反馈机制

“云安全”的另一个重要组件就是自动反馈机制，以双向更新流方式在威胁研究中心和技术人员之间实现不间断通信。通过检查单个客户的路由信誉来确定各种新型威胁。例如：趋势科技的全球自动反馈机制的功能很像现在很多社区采用的“邻里监督”方式，实现实时探测和及时的“共同智能”保护，将有助于确立全面的最新威胁指数。单个客户常规信誉检查发现的每种新威胁都会自动更新趋势科技位于全球各地的所有威胁数据库，防止以后的客户遇到已经发现的威胁。

由于威胁资料将按照通信源的信誉而非具体的通信内容收集，因此不存在延迟的问题，而客户的个人或商业信息的私密性也得到了保护。

3.6 威胁信息汇总

安全公司综合应用各种技术和数据收集方式——包括“蜜罐”、网络爬行器、客户和合作伙伴内容提交、反馈回路。通过“云安全”中的恶意软件数据库、服务和支持中心对威胁数据进行分析。过7×24小时的全天候威胁监控和攻击防御，以探测、预防并清除攻击。

3.7 白名单技术

作为一种核心技术，白名单与黑名单（病毒特征码技术实际上采用的是黑名单技术思路）并无多大区别，区别仅在于规模不同。AVTest.org的近期恶意样本（Bad Files，坏文件）包括了约1200万种不同的样本。即使近期该数量显著增加，但坏文件的数量也仍然少于好文件（Good Files）。商业白名单的样本超过1亿，有些人预计这一数字高达5亿。因此要逐一追踪现在全球存在的所有好文件无疑是一项巨大的工作，可能无法由一个公司独立完成。

作为一种核心技术，现在的白名单主要被用于降低误报率。例如，黑名单中也许存在着实际上并无恶意的特征码。因此防病毒特征数据库将会按照内部或商用白名单进行定期检查，趋势科技和熊猫目前也是定期执行这项工作。因此，作为避免误报率的一种措施，白名单实际上已经被包括在了Smart Protection Network中。

4 “云安全”3.0体系

“云安全”3.0解决方案为：通过先进的网络层主动深度威胁防护技术与虚拟补丁技术从网络层去阻断和防范针对漏洞的攻击，为各种物理服务器、虚拟机、操作系统、服务系统和应用程序漏洞提供统一的先于零时差攻击的即时防护，为企业防范各种由于没有相应补丁或者不能及时实施补丁而产生的安全风险，从而在使企业在免受各种攻击和威胁危害的同时，有效地降低了安全管理和实施的成本和风险。

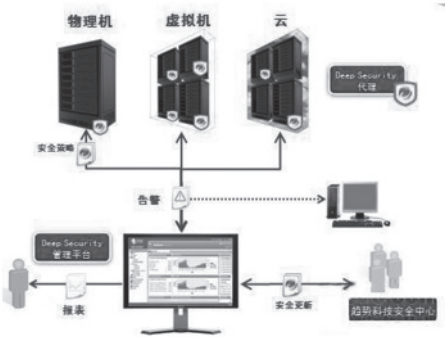

图3 趋势科技“云安全”3.0体系

“云安全”3.0 系统，从单纯的利用云技术来保护互联网安全，转变为对“云”本身进行安全保护，用“云中防护盾”和“云中保险箱”保护整个“云计算”链条。

图 4“云安全”3.0 保护“云计算”链条

趋势科技从早期使用“云计算”来提高防护效果，到保护“云计算”本身，其“云安全”3.0 体系是在云环境下，为企业至关重要的信息平台与数据资产两个核心要素提供安全防护：一方面用“云的防护盾”技术来保障“云”平台本身的高可用性，使得各种企业数据中心／应用系统或者云环境免受病毒、攻击、系统漏洞等威胁侵害；另一方面，通过“云中保险箱”技术来保护用户存放于云端的隐私和关键数据不被非法窃取和利用。这两个方面独立但又相辅相成。

4.1 云的防护盾

通过整合防火墙、入侵防护、应用服务保护、系统完整性保护、虚拟补丁、防恶意软件等重要功能，并和虚拟环境（VMware，Ctrix，Hyper-V 等）动态集成，从而全面的保护从单台物理服务器或虚拟服务器构成的简单系统，到企业的服务器集群、数据中心或者各种应用服务系统（如 Web，数据库，邮件服务器等），到由多系统、多平台、多应用、物理虚拟混合环境所构成的各种云应用／云服务平台。

在研究“云安全”3.0 相关技术和产品时，趋势科技与虚拟化厂商 VMWare 合作推出了 Deep Security，这一集成“云的防护盾”技术的服务器和应用程序保护软件，能使物理的、虚拟的以及“云计算”环境拥有自我防御能力。无论是以软件、虚拟应用或是混合式的方式实施，Deep Security 可以减少系统资源消耗、简化管理及加强虚拟机的透明安全性。

4.2 云中保险箱

趋势科技的云中保险箱功能也与其类似，可将需要保护的数据伪装起来。它通过先进的趋势科技云中密钥管理机制，对企业存放于云端的数据进行加密保护，使得企业可以随时随地安全地使用云平台存放或者交换数据。使用趋势科技云中保险箱服务的企业，将不会被任何云服务供应商所绑定，可以很自由地对数据进行迁移，不需要担心他们的数据在传输过程中被窃取，并拥有数据存取的惟一权限。

目前在欧美已经有一些机构和企业已经开始使用“云安全”3.0 解决方案带来的服务，包括美国花旗银行和英国电信等等。“云安全”3.0 解决方案正在保护他们着“云计算”数据中心，并在出现可部署的补丁之前为他们的关键服务提供主动的安全防护。

5“云安全”系统的难点

建立“云安全”系统并使之正常运行，需要解决四大难点：

（1）需要海量的客户端（“云安全”探针）。只有拥有海量的客户端，才能对互联网上出现的恶意程序，危险网站有最灵敏的感知能力。一般而言，安全厂商的产品使用率越高，反映应当越快，最终应当能够实现无论哪个网民中毒、访问挂马网页，都能在第一时间做出反应。

（2）需要专业的反病毒技术和经验。发现的恶意程序被探测到，应当在尽量短的时间内被分析，这需要安全厂商具有过硬的技术，否则容易造成样本的堆积，使“云安全”的快速探测的结果大打折扣。

（3）需要大量的资金和技术投入。“云安全”系统在服务器、带宽等硬件需要极大的投入，同时要求安全厂商应当具有相应的顶尖技术团队、持续的研究花费。

（4）可以是开放的系统，允许合作伙伴的加入。“云安全”可以是个开放性的系统，其“探针”应当与其他软件相兼容，即使用户使用不同的杀毒软件，也可以享受“云安全”系统带来的成果。

6 国内外“云安全“的应用及比较

现在各个杀毒软件厂商都在应用“云安全”技术，其中最具代表性的是趋势科技和瑞星。

6.1 以趋势科技为代表的国外“云安全”

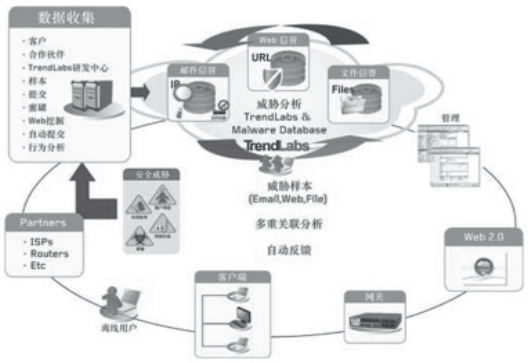

图 5 趋势科技“云安全”架构体系

趋势科技的“云安全 Secure Cloud”主要用于企业级产品当中，强调的是对复合式攻击的拦截和轻客户端策略，最终目的是让威胁在到达用户计算机或公司网络之前就对其予以拦截。

目前的病毒常常包含多个组件，而不是依靠单一的病毒体。对于用户来说，单一的组件可能不具备什么威胁，看似是无害的。但是多个组件组合在一起就形成了一个符合式的攻击。而趋势的“云安全”正是解决这一问题，在各个组成部分上进行检查，最终判断威胁。

其次，是轻客户端策略。在趋势官方的举例中，提到当用户收到一封含有网络链接的恶意电子邮件时，先会在邮件信誉服务数据库中检查其发送源地址，然后会在 Web 信誉服务数据库中检查邮件中的链接，然后会将网页的组件和重定向网页进行分析，提取 IP 地址并且添加到交互式威胁数据库中。

可以看出，趋势的“云安全”可以概括为基于互联网数据库的轻客户端程序，也就是构架一个庞大的黑白名单服务器群，用于客户端的查询。在趋势的“云安全”概念中，趋势的服务器组成一个大“云”。因此，趋势“云安全”必须建立在大量服务器基础上。

诺顿网络安全特警 2009 中的 Norton Insight 中使用的“云安全”策略与趋势技术类似，它是通过软件中的 Norton Insight 模块，连接到互联网中的服务器，自动对用户计算机上的进程文件进行识别，安全的即标记为可信文件。这种认证是一次性的，以后监控和病毒查杀时就可以无需扫描这些已知文件，从而加快扫描的速度。简单点说就是建立一个白名单库，其主要是对外来威胁进行组合、判断、拦截。诺顿实际上是将趋势的黑白名单缩减成一个白名单库。

趋势“云安全”存在的缺陷是，无法对已经存在在本地计算机上的未知威胁进行感知。从趋势的“云安全”概念中可以看到，其主要是对外来威胁进行组合、判断、拦截。一旦有未知病毒或威胁通过其他渠道入侵到用户的计算机当中，趋势是无法对已经在本机的安全威胁有效感知的。

6.2 以瑞星为代表的国内“云安全”

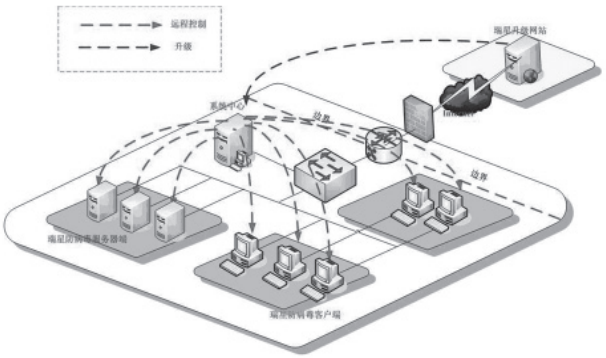

图 6 瑞星“云安全”架构体系

瑞星“云安全”官方给出的定义：通过网状的大量客户端对网络中软件行为的异常监测，截获互

联网中的木马、恶意程序的最新信息，然后推送到服务器端进行自动分析和处理，然后再把病毒和木马的解决方案分发到每一个客户端。

通过各个客户端对用户计算机进行扫描，然后提取可能是病毒的文件上报，经过瑞星的处理后，升级杀毒软件或卡卡再推送给用户。

瑞星的“云安全”的实质是一个样本收集处理机制。实现瑞星“云安全”需要有大量的客户端（卡卡安全助手），才能组成真正意义上的云，另外需要有对病毒的快速分析处理能力。在瑞星“云安全”里，由于客户端才是云的组成部分，所以不需要架设那么多服务器。

瑞星的“云安全”特点是能够感知用户计算机上已经存在的未知病毒，但瑞星是否有能力真正的达到“云安全”设想的目标，就需要用时间去检验了。

与瑞星“云安全”类似理念的产品也比较多，比如 Eset 的 ThreatSense.Net、卡巴斯基 2009 的卡巴斯基网络安全体系以及赛门铁克的 Norton Community Watch 等等。这种模式需要大量的客户端。

瑞星的“云安全”也有自己致命的缺陷，它虽然能感知用户计算机上已经存在的未知病毒，但却不具备在未知病毒入侵计算机前对其进行拦截的能力，可以说是“事后诸葛”。

6.3 国内外“云安全”的比较

通过以上分析，趋势和瑞星都提出了“云安全”概念，但二者并不相同。趋势的“云安全”强调阻止外来威胁，需要大量的服务器（厂商）；瑞星的“云安全”则强调对用户计算机上已经存在的未知威胁进行感知，需要有大量的客户端（用户）。瑞星的“云安全”和趋势的“云安全”讲述的并不是同一个概念。趋势“云安全”中的“云”是趋势的服务器群，而瑞星的“云”则是大量用户。在瑞星的“云安全”当中，瑞星的服务器反倒成了一个 Client 端。

国外的“云安全”中的“云”是通过服务器群，而国内的“云”则是大量用户，每个用户的电脑都变成了服务器群中的一份子，对电脑配置的要求高。它们分别代表了两大阵营，许多厂商也都在迅速跟进。但两者目前都存在缺陷，趋势忽略了对本机未知威胁的感知、收集，而瑞星则只能被动防守，不能在未知威胁进入到电脑前进行拦截。理想的“云安全”应将两者应该结合起来，即能对目前通过挂马、优盘等渠道进入计算机的未知威胁进行拦截，也要对通过其他渠道（手段）已经进入到用户计算机中的未知威胁进行感知。

7 结束语

“云安全”充分利用了网络的力量，即时搜集病毒库，使得广大网友可以随时共享“云安全”带来的完美保障。未来的“云安全”使用杀毒软件可以查杀一切难以处理的病毒，让用户彻底的安全，每个客户都有个性化的病毒库、各种设置规则等。它将运行在手机、MID、智能电视甚至联网的冰箱上，其客户端只有极小的体积，运行完全感觉不出来。未来“云安全”将具有企业级的病毒防御能力，否则如果“云安全”遭到破坏的时候，对于网络的毁灭性也是巨大的。

参考文献：

[1] 刘鹏．云计算发展现状[DB/OL]. [2009-04-03]. http://www.cnw.com.cn/server-cloud/htm2009/20090403_171367.shtml.

[2] 方杰．浅谈云安全．信息系统工程，2009-08-08.

[3] 杨新民．关于云安全的分析．信息安全与通信保密，2009年9月．

[4] Assessing the Security Risks of Cloud Computing. Jay Heiser and Mark Nicolett. 3 June 2008.

作者简介：**余娟娟**（1982-），女，同济大学软件工程硕士在读，助理工程师，主要研究方向：软件工程。

收稿日期：2011-7-29.