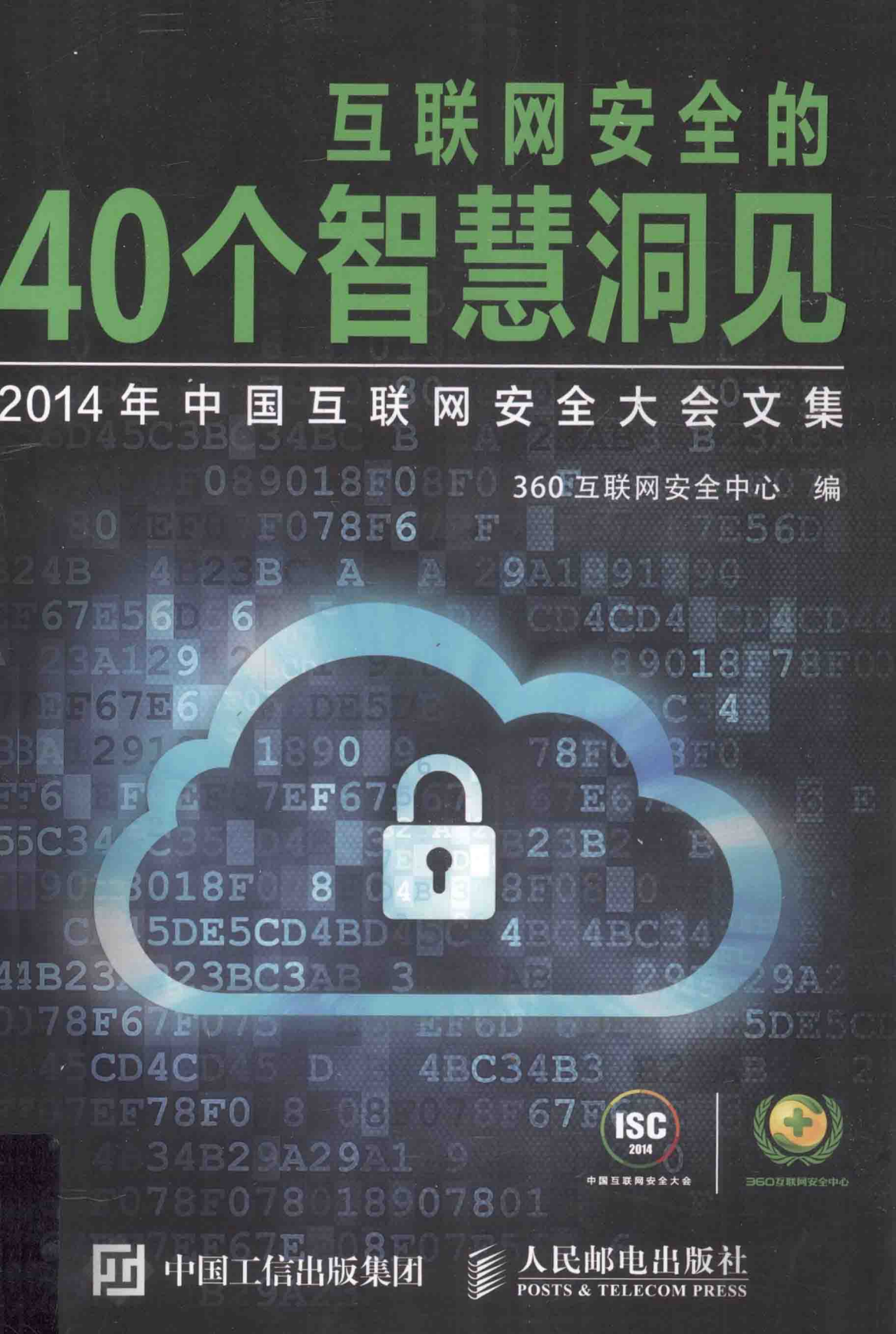
互联网安全的40个智慧洞见

2014年中国互联网安全大会文集

360互联网安全中心 编



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

互联网安全的40个智慧洞见

——2014年中国互联网安全大会文集

360互联网安全中心　编

人民邮电出版社
北　京

图书在版编目（CIP）数据

互联网安全的40个智慧洞见 : 2014年中国互联网安全大会文集 / 360互联网安全中心编. -- 北京 : 人民邮电出版社, 2015.2
ISBN 978-7-115-38401-0

Ⅰ. ①互… Ⅱ. ①3… Ⅲ. ①互联网络－安全技术－文集 Ⅳ. ①TP393.408-53

中国版本图书馆CIP数据核字(2015)第021679号

内 容 提 要

本书内容全面覆盖 Web 安全、移动安全、企业安全、电子取证、云与数据、软件安全、APT 等热点安全领域，还涉及国家网络空间战略、新兴威胁、工控安全、互联网安全、信息安全立法等新兴安全领域。

◆ 编　　360 互联网安全中心
责任编辑　李　静
执行编辑　徐明静
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京瑞禾彩色印刷有限公司印刷

◆ 开本：690×970　1/16
印张：29　　2015 年 2 月第 1 版
字数：314 千字　　2015 年 2 月北京第 1 次印刷

定价：88.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

序

互联网安全技术的颠覆之路

齐向东

360 公司总裁

过去十年间，安全技术经历了一场深刻的变革。传统的、基于特征码识别的单体软件杀毒技术逐步退出了历史舞台，取而代之的是以云计算为基础的现代互联网安全技术。所谓互联网安全技术，顾名思义，就是“互联网 + 安全技术”。它是在传统安全技术的基础之上，进行大量地深化与创新，并同互联网领域的新兴技术，包括云计算、大数据和人工智能等进行结合的产物。

有趣的是，引领这场安全技术革命的并不是传统意义上的专业安全厂商，而是以 360 为代表的一批新兴的现代互联网企业。互联网技术与互联网思维的运用，不仅彻底颠覆了传统安全产业的商业模式，同时也彻底颠覆了传统安全产品的技术模式。

一、互联网的普及推动传统安全技术向互联网安全技术转移

互联网安全技术是互联网普及的必然产物。不过事实上，互联网的普及，首先带来的并不是安全技术的演进，而是安全形势的急剧恶化。主要表现在以下几个方面。

1. 恶意程序数量呈指数增长

随着游戏产业、网络社交和电子商务的迅速崛起，制作木马病毒的经济价值主线显现了出来。于是木马病毒的制作也开始从少数黑客的炫技全面转向了产业化、规模化的生产。到了2006年前后，每天新增的木马病毒样本数量就已经过万，而到了2013～2014年，平均每天新增的木马病毒样本数甚至达到了百万个以上的规模。

2. 恶意威胁快速传播与进化

互联网飞速发展的时代，恶意软件与恶意攻击也在不断快速进化。借助互联网快速通畅的通讯渠道，恶意软件可以随着互联网网站、互联网应用在全球范围内快速传播。同时，这些恶意威胁可以借助互联网通道快速变化并及时生效，甚至可以实时同攻击者交互产生变化和进化，快速对抗安全软件。安全厂商和用户面对的恶意威胁迅速从“已知”变为“未知”。

3. 海量攻击的威胁

借助互联网的便捷性和联网设备的爆发式增长，恶意威胁也呈现爆发式的增长趋势。利用广泛部署的互联网网站系统、操作系统或应用程序的弱点或漏洞，恶意攻击者可以在极短的时间内感染或入侵全球数以

百万计的设备，并操纵这些设备实施大规模攻击行为，或者借助这些设备谋取巨额利益。

4. 网络设备互通、定向攻击与高级持久性威胁

由于互联网的便利与互联互通的特性，即使是存储和处理了极其敏感和重要的企业、政府、金融甚至军事信息的内部网络和用户，也无法避免同互联网直接或间接地进行接触。个人电子设备，尤其是移动电子设备的普及更加速了这种接触的深度和广度，将企业和政府机构的封闭内部网络，实质上同开放的全球互联网连接起来。这就给瞄准这些信息的商业电子间谍行动或国家级电子间谍行动提供了有力的突破口。

这些电子间谍组织背后往往拥有巨额资金和极其优秀的攻击人才等资源支持。他们编写极其复杂的恶意软件，花费数月甚至数年时间，使用最新的网络、软件甚至硬件的安全漏洞，针对特定用户或特定设备进行攻击，以便渗透政府或企业的内部网络并获取敏感机密信息。这种高级的恶意威胁常常是由多种极其隐秘和未知的软件漏洞利用、高级恶意软件、高级恶意攻击技术等复杂组合而成。

互联网的普及使安全威胁的形式、数量和攻击手段等都发生了巨大的变化。这也就迫使我们必须在传统安全技术方法的基础上，认真思考如何用互联网的方法来解决互联网的安全问题。

二、传统安全技术的局限性加剧了互联网安全技术的颠覆

传统的安全技术大部分发展和成熟于互联网时代之前，包括传统的

反病毒软件、防火墙、IDS/IPS 等安全技术与产品，都是基于对已知恶意软件或恶意攻击的特征识别。它们往往对未知的恶意威胁缺乏防护和发现响应能力。而由于传统安全产品大部分依赖“样本捕获→样本分析→样本采样→定时更新”特征库这样一套流程来更新对恶意软件或恶意攻击的识别能力。在应对快速传播、变化或爆发的恶意攻击时，面临时间差问题。对于快速变化的爆发式大规模攻击，往往传统安全厂商还没来得及推送防护升级，攻击者已经感染了数以百万计的用户。对于未知或高级的攻击，传统安全厂商则往往需要经历数年之久才能意识到恶意攻击或恶意软件的存在。

下面就来具体分析一下传统安全软件的局限性。

1. 依赖单机能力，病毒特征库臃肿且更新不及时

由于传统杀毒软件在工作过程中基本不需要联网工作，它们几乎是完全孤立的在每个用户的电脑上运行。因此，其查杀能力完全取决于单体软件本身的能力以及用户计算机的运算能力。这就要求客户端软件必须不断的更新病毒特征库，从而使病毒特征库越来越臃肿庞大，甚至是无限的膨胀，不仅吃掉了大量的磁盘空间，同时也使电脑的运行速度越来越慢。

不过，即便是电脑上存储空间足够，病毒特征库可以无限增大，传统的杀毒软件仍然无法解决病毒特征库更新不及时的问题。传统杀毒软件一般的跟新周期是一个月、一周或一天。但当每天都有几十万上百万的新的恶意程序样本出现时，即使选择最短的更新周期，每天都更新一次病毒特征库，而且聪明的杀毒引擎能够识别90%以上的未知木马，那么，

每天也至少仍然几百几千个，甚至几个万病毒是完全无法查杀和防御的。

2. 无法解决海量样本的收集问题

对于传统杀毒软件来说，最让研发人员头痛的一件事就是木马病毒样本的收集问题。传统安全公司主要采用人工采集、蜜罐技术以及复杂的客户端上报机制等方法来收集木马病毒。但实际上，木马病毒通常情况下攻击的都是用户终端，恰好落入安全厂商的样本搜集空间的概率非常有限。当木马病毒样本量以每天几万个，甚至上百万个的规模快速增长时，传统的样本收集方法就更显得效率低下。所以，当安全厂商收集到某个新的木马病毒样本时，这个样本可能已经感染了很多的用户。安全厂商无法保证在木马病毒发动攻击的第一时间捕获样本。

3. 无法填补样本分析的人力投入

基于病毒特征码识别技术的传统杀毒方法，往往要求开发者对每一个病毒的特征都有深入和透彻地了解，而这一过程通常需要有人来参与。所以，传统杀毒厂商通常都必须建立庞大的恶意病毒分析团队，一线安全厂商甚至需要建立拥有数千名病毒分析师的病毒分析团队。如此巨大的人力成本和管理成本的消耗，不可避免的使得杀毒产业变成了一个高投入、低产出的产业，严重的制约了产业整体的做大做强。而且，在互联网时代木马病毒数量成几何基数增长的情况下，病毒分析人员的数量根本不可能无限地增长。

4. 一旦引擎被破解病毒就可以免杀

完全基于单机计算的特征识别技术还有一个致命的弱点，就是攻击者一旦掌握了杀毒引擎的检测方式，就可以非常轻易地对安全软件的检

测进行规避，这种方法现在也被业界称为“免杀技术”。而一旦某款病毒对某个杀毒软件实现了免杀，所有安装该杀毒软件的电脑就都成款了病毒的活靶子。

三、云计算是互联网安全技术的基石

从 2007 年开始，360 开始深入研究云安全产品。当时，还很少有安全厂商针对云安全技术做深入地探索，更不用说将云安全作为整套安全体系的基础。而 360 则领先于时代，看到了互联网时代恶意攻击和威胁飞速变化的趋势，凭借着互联网公司具备的强大的海量数据处理和分析挖掘能力，选择了基于云安全的安全路线。

直到今天，很多业内人士甚至专业的安全厂商仍然认为云安全 / 云查杀不过是将海量的黑白名单散列存储到云端上进行查询。即使在全球范围，也仅有极少数的安全厂商能够真正地理解云计算结合安全技术背后的意义。

1. 云查杀是对传统安全技术杀防能力的一次解放

传统反病毒软件针对恶意软件的检测方法，是捕获样本，分析样本，之后针对恶意样本提取采样的特征数据后，利用匹配或启发式匹配的技术进行样本识别。在攻击者对匹配方式不了解的情况下，这种技术针对未知样本具备一定的检测能力。如果攻击者一旦掌握了被检测的方式，例如利用黑盒方式快速定位特征码位置，甚至逆向分析安全软件的检测特征，就可以非常轻易地对安全软件的检测进行规避，即业界俗称的

“免杀”。

云查杀是360利用云安全技术从传统安全技术中解放出来的第一个武器。云查杀在传统特征查杀的基础上，结合云计算和大数据分析，进行了创新和改进。客户端收集本地样本在各个维度上的信息，包括样本和系统的关系信息、样本散列、数据特征等，发送到云端进行鉴定识别。这样一来，云端可以结合更多、更丰富的信息进行识别和判断，拥有比传统特征码更具优势的识别条件。鉴定流程的云端化和鉴定信息的丰富化极大地提高了攻击者发现针对样本识别方式的难度和门槛。攻击者难以快速定位安全软件的检测方式，就无法快速进行免杀和变形。

同时，这些计算和识别任务完全在云端完成，也避免了传统杀毒软件将病毒数据库存储在用户计算机上所消耗的性能和存储成本。

最后，云端可以随时根据威胁的趋势变化、客户端的软件环境和情况进行数据挖掘，实时发现、动态调整和快速适应。无论是快速爆发的大规模攻击威胁，还是针对特定用户的定向攻击，又或者是可能的误报情况，都可以第一时间发现并进行处理，解决了传统反病毒技术的时间差问题。

表面上看来，360的云查杀是收集样本信息并返回样本处理策略。实际上，云端有复杂的自动化处理和鉴定、追踪流程，最终将这些分析结果转化为实时处理的防御交由客户端处理。也就是说，除了用户遇到的未知样本的在后台的自动化分类、分析，对样本进行扫描、虚拟运行和行为分析外，云端系统还会综合这些分析获得的信息，进行实时分析、实时判定并将处理结果。

在360的云安全不仅是运用云计算技术的查杀技术，更是整个安全体系的基石。利用云端强大的计算、存储和实时分析能力，我们尝试将每一项传统安全都进行深入的改造和创新，使其能够同云端紧密结合，通过云计算将其强大的威力释放出来。这也是360在实施互联网安全技术发展的指导思想和方向。

经过最近数年来的安全技术和攻防对抗技术的发展，云安全技术是现代安全技术的基础，这已经成为新一代安全厂商的共识。云安全技术以及将云同传统安全技术结合的技术能力，将成为现代安全产品实质的准入门槛。不具备云安全能力，就无法适应现代恶意软件和恶意威胁的对抗环境。

2. 人工智能安全是对传统安全技术人工成本的一次解放

在对抗恶意软件的发现→分析→处理三大流程中，云安全打通了发现和处理两个部分。但是，剩下的“恶意软件分析”过程仍然是整套流程中的一个相当严重的瓶颈，因为传统意义上，这个过程一直强烈依赖“人”的参与。

在传统的安全技术范畴内，恶意软件的分析必须要由人来参与才来完成。传统的安全厂商针对恶意软件样本需要建立庞大的病毒分析团队。通常，一线安全厂商需要建立拥有数千名病毒分析师的病毒分析团队。这不仅消耗了大量的人力和管理成本，而且在互联网时代日益扩大的恶意软件规模和不断加快的变形速度情况下，病毒分析人力却无法无限增长。

事实上，传统安全厂商一直面临着这样的矛盾：一方面，为了分析

更多更新更复杂的恶意软件，厂商不得不投入更大的分析人力；另一方面，新增的分析人员仍然无法满足处理大量新增恶意样本的需求。厂商面临着要么牺牲分析质量，出现大量漏报或误报，要么出现恶意软件的处理速度大大落后于恶意软件的传播速度的两难局面。

要将恶意软件分析人员从分析流程的流水线上解放出来，就需要将恶意软件分析的经验与自动化技术相结合，实现高速、无瓶颈的恶意软件分析。

作为一家开展搜索引擎业务的互联网公司，360 拥有大量国内顶级的人工智能和机器学习领域的技术专家。在这些技术专家的启发与建议下，使用基于人工智能技术来实现机器学习恶意软件分析技术，并最终实现自动分析的方法，就自然进入了 360 的视野。借助人工智能技术，我们可以让软件对恶意软件分析人员的分析结果进行机器学习，并使得软件“懂得”如何高速且自动地分析和鉴定恶意软件。经过数年的努力，在 2010 年，360 推出了使用人工智能机器学习的方式，自动化地分析和鉴定恶意软件的 QVM 技术，并将其应用到本地防御与扫描引擎中。

事实上，早在十年前，国外安全公司赛门铁克就尝试过使用初级的人工智能技术实现恶意软件识别，但效果不佳。而几乎与 360 同时，在 2010 年左右，另一家国外安全公司小红伞也在利用机器学习技术实现恶意软件识别与分析方面进行了一些理论探索。但这些探索和尝试都没有能够最终转化为可以大规模应用于商业产品的可靠技术。

人工智能技术本身并非高不可攀，但如何教会机器准确地利用人类的经验，确保在误报和漏报之间实现平衡，是基于人工智能技术的恶意

软件识别能否成功的关键，也是这些探索和尝试的最大难点，而帮助我们突破这一难点关键的正是云安全技术为我们积累的海量样本，以及我们通过大数据的方法对海量样本的分析和处理。

最终，借助人工智能技术，通过海量云端数据训练锻造的 QVM 引擎不仅针对恶意软件的检出能力远远超过绝大多数其他安全产品，在误报比率上也比传统安全软件低了数倍，真正实现了高速、精准识别的目标。目前，QVM 引擎的开发已经到了第三代，并被部署到了云端的自动分析系统上，这就代替了绝大多数需要人工分析的工作。

QVM 引擎最终打通了恶意软件处理的最后一道过程的瓶颈，将互联网安全技术带入一个新的境界。

3. 云智能主防是未知威胁的最大克星

在恶意软件的识别和鉴定进入新的高度后，360 还在继续思考如何能够更快、更好地为用户防御恶意软件和恶意攻击的威胁。我们希望不仅仅能够快速识别和查杀恶意软件和恶意软件的未知变种，还能够在第一时间防御即使是完全未知的恶意程序。这个高难度的要求就需要运用行为识别、主动防御这个传统安全技术。

基于行为识别的恶意软件识别和阻断在传统安全厂商和传统安全产品中运用已有二十年左右的历史，但是纵观历史传统安全产品的主动防御，防护能力效果并不出色。这是因为要实现完备、有效的主动防御系统，就必须对操作系统几乎所有的内部机理都有深入的研究和理解。仅仅这一点，绝大多数传统安全厂商就远远无法做到。大多数传统的主动防御产品对恶意软件的基本行为的完备性识别都存在很大问题。即使是已经

能够识别的行为，在细节处理中也存在很多由于对系统机制理解不足而造成的漏洞和问题。恶意软件作者只要稍微转换思路，就可以轻易绕过这些防御产品。

传统安全产品中的主动防御无法成功的另外一个重要的原因是难以平衡的误报和报警。要实现完备的恶意软件行为识别，就需要针对大量程序行为做监视和拦截。这样带来的问题是：一旦监视和拦截的策略过于严格，就容易产生误报，导致过多的报警干扰，甚至导致正常软件无法工作和运行。反之，如果放松规则，就会带来大量漏报。

360吸引了大量对操作系统内部机制有着深入理解的技术专家，因此，他们在传统的主动防御技术基础上进行了大量的深化和创新。同时，和人工智能、云查杀一样，360的云安全再次在智能主动防御领域发挥了巨大的威力，成为了360的主动防御体系最终能够在普通用户的系统上成功大规模运用的关键。

我们之所以将360的云主防称为360云智能主防，这其中的智能体现在3个方面。

（1）云端海量的自动化行为分析、识别和拦截

360云主防不依赖本地或固定的安全策略，而是实时同云端进行交互。云端则会结合行为识别数据库和后台海量白名单，对用户系统上的程序行为进行分类和识别，依靠云端复杂的实时分析和决策机制，以及庞大的文件与行为白名单系统来发现恶意软件，以及决定最终的处理策略。

（2）智能而稳定强大的本地行为识别系统

有别于常规的行为防御产品，360凭借对操作系统内部机理和攻防技

术的深入了解，强化了行为防御的识别和处理能力，极大减少了恶意攻击程序绕过行为识别的可能。同时，360 云智能主防会借助一些新颖的内核技术，准确定位及归类，更有效地“理解”恶意软件的行为。最后，我们通过成熟的防御拦截技术实现了高效而稳定的防御系统，不会出现传统主动防御类软件常见的影响系统稳定性和性能的问题。

（3）云端海量的行为数据挖掘体系

在建立了云端海量的实时全局行为数据库后，云端可以对数据进行多维度的挖掘和分析。云端分析系统可以针对恶意软件、恶意威胁进行趋势分析，还可以对恶意攻击甚至漏洞攻击进行提前发现和预警。

借助对操作系统内部机制的深入理解和云安全的力量，我们实现了这套高强度、高智能、高稳定和高易用的主动防御系统，并将其大规模应用到用户系统中，为第一时间快速发现和拦截未知的恶意软件、漏洞攻击和恶意攻击发挥了巨大的作用。

2014 年初，为了应对微软停止对 Windows XP 进行更新给中国用户带来的影响，我们在云智能主防体系下，开发出一套专门针对 XP 系统进行漏洞防护的安全产品 360XP 盾甲。XP 盾甲通过 4 项核心的安全防护策略：系统沙箱、系统加固、应用加固和热补丁，可以在操作系统存在安全漏洞的情况，对系统实现有效的防护。特别值得肯定的是，在目前已经完成的国内外所有针对 XP 系统的安全防护测评中，360XP 盾甲的测评成绩始终名列全球第一，并且迄今为止，还从未在测评中被攻破。360 XP 盾甲的出现，也标志着国产的民用安全软件已经走在了世界的前列。

四、白名单是互联网安全技术的翅膀

传统安全技术采用的是鉴黑不鉴白的杀毒方法。但这种方式存在一个明显的效率问题。因为任何用户遭遇木马病毒的攻击都是一种偶发事件，而绝大多数情况下运行的其实都是正常程序。如果任何一个程序运行起来时都要被当作未知程序检查一遍安全性，那么实际上就是把绝大部分的时间成本用于了对正常程序的检测，这也是传统杀毒软件安装以后，电脑卡、慢的一个重要原因。

而同样的效率问题，在云安全技术体系下仍然存在。如果云端只能识别恶意程序，却无法识别普通的正常程序的话，那么可能客户端 90% 以上的云查询结果都会是安全性未知。为了解决云查询的效率问题，360 的安全工程师们就开始构想：除了黑名单之外，我们是否可以通过建立一个足够全面的可信程序的白名单机制，将所有正常软件都加入这个白名单，之后采用“非白即黑”的方法来杀毒呢？这种思想当时一经提出，就被很多传统杀毒厂商嘲笑为一种“没有任何技术含量”的杀毒技术。

的确，就 PC 端的复杂度来说，白名单杀毒机制肯定要比传统的基于特征识别的杀毒引擎简单得多。但是，一个关键的问题是：互联网上每天出现的新软件至少有成千上万种。如果不能保证白名单样本足够全，足够大，更新速度足够快，就会形成大量的误报，就不能真正有效的提高云查杀的效率。赛门铁克、趋势科技等也都曾经尝试过使用白名单的

技术方法，但就是由于他们都无法解决白名单的样本收集问题，所以始终都没能使相关技术达到商用的程度。

那么，360 是如何解决白名单更新问题的呢？事实上，360 原本是一家做搜索引擎的互联网公司。进入安全领域后，360 很快的就开始使用蜘蛛爬虫来监控全球绝大多数软件下载分发站点和软件厂商的官网。这套系统能够在数秒内发现和响应新出现的软件。目前，360 已经维护了世界上规模最大的白名单系统，白名单中的样本数量已经达到了数亿个的规模，而且每天仍然在进行快速的更新。所以，使用 360 的安全软件进行防护，即便完全使用非白即黑的杀毒方法，也能实现极低的误报率，绝大多数普通用户甚至完全感觉不到误报的存在。

白名单机制一旦建立起来以后，我们就会发现，在某些对安全性要求非常苛刻的条件下，非白即黑的杀毒方法实际上是唯一完全可靠的杀毒方式。将白名单与云查杀、云主防、云人工智能相结合，就形成了 360 一整套互联网安全技术体系。

五、互联网安全技术颠覆之路的几点启示

互联网安全公司为什么能够创造颠覆性的互联网安全技术，其中有一些启示值得我们思考。

1. 互联网公司广阔的平台能够聚拢顶尖的安全人才

互联网公司拥有更广阔的平台和客户群，可以吸引大量高级安全技术人才参与安全技术研发，为互联网安全公司在传统安全技术上的深化