网康科技 NETENTSEC

智能协同 主动防御

云管端下一代网络安全架构

白皮书

北京网康科技有限公司

目录

摘要

- 网络攻击已经从早期的泛攻击演进为利用 0-day 漏洞、以获取重大经济/政治利益为目标、定向持续的高级攻击。

- 随着企业业务的云化、虚拟化、移动化，网络边界被拉伸、模糊甚至消失，传统的网络安全架构已不能适应 IT 架构的变化，无法应对新的高级威胁。

- 内部人员的误用、滥用或恶意行为，越来越成为安全事件频发的重要原因，内网不再是可信的安全区域，应加强内部人员网络行为的审计与监控。

- 现有网络安全防护体系基于 P2DR 模型，以网络边界为中心，以特征匹配为核心手段，重在防御，是静态、被动的安全模型，不能有效应对未知威胁。

- 云管端下一代网络安全架构基于 PDFP 模型，以异常检测、智能预测、协同联动为手段，强调对抗，是动态、主动的安全模型，能够有效应对未知威胁和 APT 攻击。

1、 不断失陷的网络安全

近年来，网络安全事件频发，危害逐渐升级。据 CNCERT《2014 年中国互联网网络安全态势报告》，2014 年通报的漏洞事件达 9068 起，比 2013 年增长 3 倍，其中“心脏滴血”和“破壳”漏洞，涉及基础应用与硬件设备，影响极为广泛严重；中国被控制的主机数量规模庞大，有 1081 万台僵尸主机被境外 4.2 万台服务器控制，针对互联网 DNS 服务、电商等大规模的 DDoS 攻击，与此不无关系。国际上，网络安全形势犹有过之，RSA 总裁 AmitYoran 认为 2014 年的网络安全是“Mega Breach”（Breach，失陷），而 2015 年的安全形势比 2014 年更糟，将是“Super Mega Breach”的一年。

回顾最近几年发生的影响巨大的网络安全事件：

2010.7

美国通过“震网”（Stuxnet）蠕虫病毒入侵伊朗核设施网络，利用 Windows 0-day 漏洞和离心机控制软件（SIMATIC WinCC）的 0-day 漏洞，改变浓缩铀离心机的运行速度，导致上千台离心机报废，伊朗核计划受到严重阻碍。

2013.12

纽约大型零售商 Target 受到网络攻击，7000 万消费者的身份信息以及 4000 万信用卡信息遭窃，黑市上以每卡 20-100 美元价格出售，全部损失超过 10 亿美元。Target 超市 CIO 与 CEO 先后引咎辞职。

2014.5

全球最大拍卖网站 eBay 官网发布通告，称因数据泄露呼吁其用户更新密码。eBay 事件是攻击者在对该公司员工进行成功鱼叉攻击后，利用员工的登录帐户进入未授权公司网络，最终导致注册用户数据泄露。

2015.2

黑客组织 Carbanak 在 2 年内连续攻击了俄、乌、白等 30 多个国家的金融机构，造成损失达 10 亿美元，引发俄罗斯银行业恐慌，有 2 家银行被迫放弃营业执照。

以上案例涉及金融、商业、国防等工业企业，展现了新型网络攻击的特点：利用系统的 0-day 漏洞，无法预先防御；目标明确，定向攻击；损失巨大，难以挽回。黑客攻击手段从传统的泛攻击演进为高级攻击，与技术的发展和黑色产业链的发展有着密切关系。一方面，云计算、大数据、移动互联网等新技术、新应用的普及应用，使得网络与信息面临更多的风险。另一方面，由于 0-day 漏洞潜在的巨大经济利益，黑色产业链逐渐形成并发展壮大，攻击目的从早期的技术炫耀转变为利益攫取，攻击者也从“独行侠”发展成为拥有强大经济与技术实力的集团组织。这使得应对未知威胁成为网络安全防护的常态。

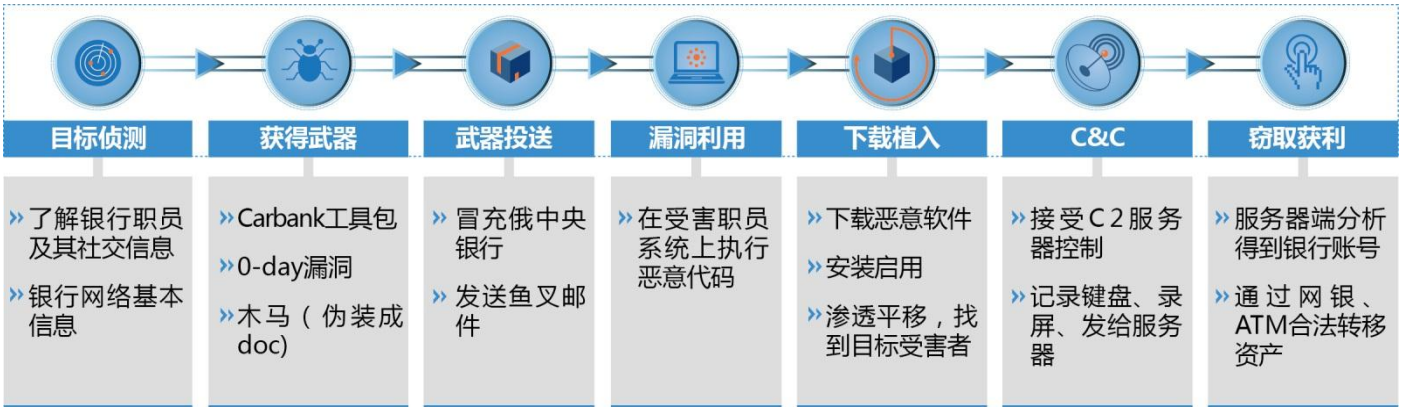
2、攻击者如何突破防御体系

为了保障信息资产的安全，大型组织都不惜重金投入，建立完善的防护体系，但攻击者为什么能够突破防御，频频“得手”？

以窃取客户信息资产为目标的网络攻击，通常是利用未知威胁实施的定向 APT 攻击，由多个阶段组成。我们可以从 Cyber Kill Chain （简称 CKC）模型解释完整的攻击过程。CKC 模型由 Lockheed Martin 公司提出，认为网络边界并非安全攻防的唯一重心，边界突破既不意味着攻击一方取得了胜利，更不意味着防守一方受到了损失。由于窃取信息资产才是网络攻击的核心，因此安全防御体系应该针对“敌人”的意图与行为进行部署，而不是只“看守好”既有边界。该模型把攻击过程分为 7 个步骤：

- ✓ **Reconnaissance（目标侦测）**
- ✓ **Weaponization（获得武器）**
- ✓ **Delivery（武器投送）**
- ✓ **Exploitation（漏洞利用）**
- ✓ **Installation（下载植入）**
- ✓ **C&C（命令控制）**
- ✓ **Actions on Objectives（窃取信息）**

攻击者只有完成所有步骤才认为攻击成功，因此在每个步骤都存在攻防对抗，都存在防守反制的机会。下面以俄罗斯银行大劫案为例，具体分析攻击的过程与特点，可以把 CKC 模型的 7 个步骤合并为 3 个阶段。



Carbanak CKC 攻击过程

- **第一阶段——感染传播**

黑客一开始会伪装成俄罗斯联邦中央银行，向目标金融机构的普通职员发送电子邮件（鱼叉攻击），诱使他们打开一个包含恶意软件的附件（为避免收件人生疑，附件为 doc 格式）。收件人打开附件后，自动执行漏洞利用代码（0-day 漏洞），电脑被植入木马，失陷。然后黑客以此为跳板进行渗透平移，在内网大量传播扫描，直到找到并攻陷掌握银行交易权限的高级管理人员，“初战告捷”。

- **第二阶段——获取情报**

突破管理人员的电脑后，黑客会进一步植入特种木马程序，记录键盘敲击信息，并每隔 20 秒钟截屏，源源不断传送到远端的控制服务器（C&C）。服务器端有专人分析，得到合法账号、密码、以及系统操作流程。

- **第三阶段——转账获利**

黑客得到合法账号后，通过正常的操作流程，避开银行的异常监控系统，将资金通过转账、信用卡、ATM 机等多种方式顺利转走。

3、传统网络安全防护体系无法应对新的安全威胁

传统网络安全理论基于 2 个核心模型：边界安全模型，P2DR 防御模型。

- **边界安全模型**

把网络划分为多个安全域，如内网、外网，认为内网是可信任的，风险来自边界之外，只要在边界做好防护就可以高枕无忧，这是今天在网络出口部署防火墙、IPS 等网关设备的主要依据。但随着组织业务的云化、虚拟化、移动化以及向合作伙伴开放，传统的网络边界被拉伸、模糊甚至消失，边界设备已无法防御新的风险；此外，大量事实表明，内部人员（包括外包业务合作伙伴的人员）的误用、滥用或恶意行为，是安全事件频发的重要原因，内网不再是可信的安全区域。传统的安全边界模型，过于简单、静态，已不适应 IT 架构的快速变化。

- **P2DR 防御模型**

P2DR 首先对信息系统的风险进行全面评估，然后制定相应的防护策略，包括：在关键风险点部署访问控制设备（防火墙，IPS，认证授权等），修复系统漏洞，正确配置系统，定期升级维护，教育用户正确使用系统。检测是响应和加强防护的依据，通过检测网络流量和行为，与预设策略进行匹配，如果触发防护策略，则认为发生了网络攻击，响应系统就执行预设动作阻止攻击，并进行报警和恢复处理。

P2DR 以策略为核心的防御模型，包括 4 个环节

- ✓ **策略（Policy）**
- ✓ **防护（Protection）**
- ✓ **检测（Detection）**
- ✓ **响应（Response）**

在 P2DR 模型中，所有的防护、检测和响应都是依据策略实施的，因此策略是模型的核心，其完备性至关重要。它假设信息资产面临的风险是可以充分评估预知的，然而这种假设在 0-day 攻击和 APT 攻击面前完全失效，未知威胁可以轻松绕过防护体系。即使特征库和策略不断升级，也赶不上攻击特征的变化速度。

传统安全产品，如终端杀毒、防火墙、IPS、Web 安全，都是基于已知特征和预设规则展开工作的，其理论依据是边界安全与 P2DR 防护模型，这是一种静态的、被动的、防御思维的安全模型。由于网络边界的变迁、未知威胁的爆发、来自内部人员的威胁，使得传统安全模型跟不上 IT 架构的变化，已无法应对新的安全威胁。

4、云管端下一代安全架构

4.1 PDFP 安全模型

针对 0-day 漏洞、特种木马和 APT 等高级威胁，网康科技提出了 PDFP 安全模型，该模型对于安全环境的理解与传统 P2DR 有很多不同，认为：

- **IT 信息系统永远存在未知的威胁，无法通过评估获得充分认知；**
- **防御系统无法确保阻止黑客攻击，网络、设备、应用一定会失陷（breach）；**
- **当前网络事实上已经失陷，只是损害状态不为我们感知；**
- **内网与外网一样不安全，内部人员误用、滥用或恶意的行为每天都在发生；**

PDFP 安全模型图

PDFP 是以预测为核心的安全模型，包括 4 个环节

- ✓ **检测（Detection）**
- ✓ **取证（Forensic）**
- ✓ **防御（Prevention）**
- ✓ **预测（Prediction）**

检测（Detection）

既然信息系统已经失陷，那么安全应当从检测开始。这里的检测与传统检测（特征库匹配）不同，指的是异常行为的检测，通过检测用户、应用、流量等行为模型有无偏离常规基线，判断是否发生了绕过防御策略的入侵行为。检测的目标不是阻止入侵，而是触发告警，以便分析取证和调整策略，减少损失。

取证（Forensic）

检测到入侵行为后，需要进行调查取证，了解有哪些系统遭受攻击，有无信息遭窃，入侵发生在何时，利用了未知威胁还是未打补丁的已知漏洞，目前处于 CKC 攻击链的哪个阶段，攻击者动机是什么，是个人行为还是有组织支持？了解的信息越详细，越有利于调整防御策略，以免未来发生相同入侵。

防御（Prevention）

通过部署防护策略、安全产品以及管理流程以防御网络攻击，提高攻击者的难度，在攻击者试图进入网络时进行阻止。通常的防御策略包括：在网络边界部署防火墙、IPS 设备，在应用服务器前端部署 WAF 以及审计设备，在所有终端设备安装杀毒与管控软件。有时还要设置蜜罐，以增加攻击成本、延缓入侵进度，也是防御的一种手段。

预测（Prediction）

由于无法针对未知威胁预设策略，因此需要动态地检测网络异常、取证分析，了解攻击的动态，依据 CKC 模型对后续攻击进行预测，预测结果将成为调整防御策略的重要依据。预测所需数据源除了企业组织自身的安全策略、防护日志，还应该包括外部的威胁情报、同行业的安全策略、黑客攻击动态，以更准确地预测可能的网络攻击，实时调整应用发布和防御策略。预测分析依赖检测、取证作为输入，同时引入了外部智能，预测的有效性得到进一步提升，而有效的预测可以增强检测、取证分析和防御效果，可见，预测能力成为应对未知威胁的核心能力。

PDFP 不再依赖特征匹配比对，而是动态监测全网异常行为，把攻击、漏洞、人员、行为、应用、内容等日志信息实时汇集起来进行全局分析，快速判定攻击，进行攻击溯源，在 CKC 的每个阶段主动反制防御。可见这是动态的、主动的、具有对抗型思维的网络安全模型。

4.2 云管端下一代网络安全架构

云管端下一代网络安全架构，是网康科技遵循 PDFP 模型，率先践行的应对高级威胁的网络安全架构。

“端”——指终端设备

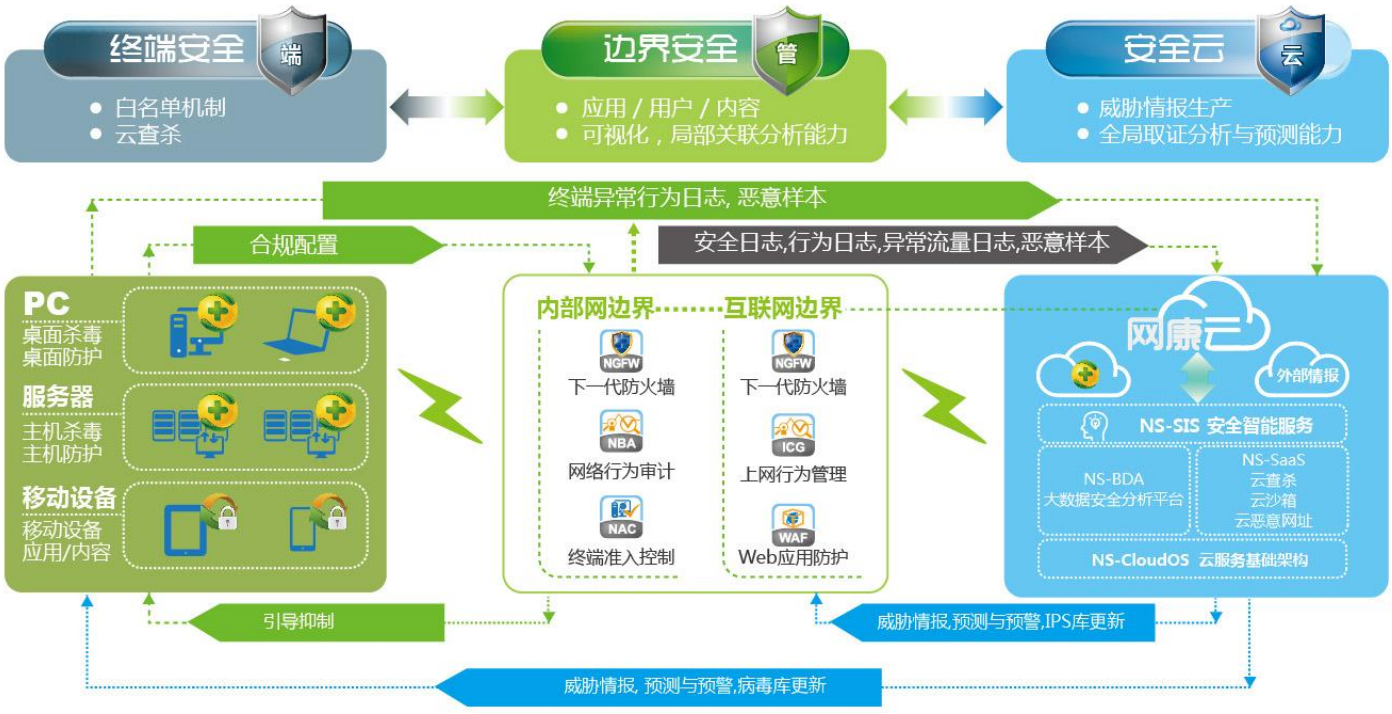
包括 PC、服务器、智能移动终端，是距离应用系统和数据最近的设备，是重要的风险引入点，需要部署杀毒和管控策略（360 天擎，天机）；

“管”——可理解为泛化的网络边界

除了部署对外的防御设备（下一代防火墙，上网行为管理，WAF 等），还应在内网部署行为审计设备，加强内部人员违规行为监控；

“云”——网康云

除了提供云沙箱、云查杀、云信誉评估等基础服务外，还针对终端和边界设备上传的异常日志进行全局关联分析、异常行为建模分析，使溯源取证与风险预测可视化。



云管端下一代网络安全架构图

云管端联动是下一代网络安全架构区别于传统安全架构的核心能力，三个环节彼此依赖，协同防御。

- 终端设备遇到未识别的灰度文件时，通过云查杀获得分析结果，第一时间更新本地防护策略；
- 终端设备无论访问内网资源还是互联网，都需要与边界设备联动，进行严格的准入准出控制；
- 边界设备（无论是对外防御设备，还是内网审计设备）实时把安全日志、异常行为日志、灰度 URL 样本、异常流量日志上传至云端；
- 网康云除了提供实时云信誉查询服务，还利用外部威胁情报、终端和边界设备的异常日志，进行大数据分析，做出攻击预测报警，实现云管端智能协同、主动防御。

4.3 下一代网络安全架构的 5 项关键能力

为了应对未知威胁和高级威胁，下一代网络安全架构需要从应用和内容层面深入理解网络的变化，从全局视角分析各种异常网络行为之间的关系。我们认为以下 5 项是下一代网络安全架构的关键能力。

● 情境感知（context-aware）能力

指利用各种辅助网络信息分析安全状态，以做出更准确的安全决定。情境信息通常指传统网络流量元组（IP、端口、协议）之外的环境信息与操作信息，它更能刻画攻击者的行为和动机。安全产品必须能够识别用户、应用、内容，并根据时间、地点、频率等信息进行模型分析，比如，在一个普通的网络环境，连续几天检测到夜间 2 点开始有主机连接国外 URL，则很可能是发生了泄密行为。因此，情境信息有助于识别那些绕过传统安全防护设备的网络攻击，在不产生误报的情况下，判断网络行为是否偏离了常规基线。

● 威胁情报利用能力

威胁情报之所以备受关注和认可，在于它通过信誉机制（Reputation）提供了准确度很高的威胁信息，比如：恶意的 IP，URL，DNS，文件等。有些威胁情报服务还提供攻击过程的说明，攻击的目标是什么，以及建议企业如何防御。威胁情报是第三方专业安全机构提供的高级服务，对于企业组织防护最新的已确认的网络攻击很有帮助。一个典型的应用：威胁情报提供了 Command & Control 服务器的 IP 地址，防火墙对于与该 IP 发生的任何连接可直接阻断。

● 内部人员行为审计能力

越来越多的企业组织认识到内控的必要性，但采取的措施限于数据库审计、终端设备管控、以及 SIEM 安全日志分析。这些措施的重点放在了业务自身的安全分析，却忽略了对人的管理，事实上内网安全风险主要是由于人员

的误用、滥用或恶意行为导致的。PDFP 安全模型认为内网不再可信，甚至是零信任（zero-trust）网络，要求对内网人员进行认证识别、行为审计、基线行为建模、异常行为识别报警，降低由于人员行为不当导致的安全隐患。

- **全网智能协同能力**

一次成功的网络攻击涵盖边界突破、终端感染、渗透平移、服务器漏洞利用等多个步骤，各个步骤彼此依赖，相互配合。大型组织通常部署了多种网络安全产品，以保护服务器、终端、网络边界，然而这些设备/系统基本是孤立运行的，不了解攻击行为与其它防御点的关系，无法从全局理解正在发生的安全事件，无法形成协同效应。孤岛防御容易被绕过，因此需要对终端和边界设备赋予智能，使他们能够同步信息，互相配合，以应对不断变化的 IT 架构和复杂的网络风险。

- **大数据安全分析能力**

攻击者除了突破多道防线，还需要足够“耐心”才能取得成功，复杂的攻击可能长达数月甚至几年。因此对攻击行为进行跨时空分析，才能看清整个攻击链条。目前 SOC 或 SIEM 系统能够收集各种安全日志，进行基本的统计分析，但还远不能解决安全事件的可视性和可溯源性问题。主要原因在于数据来源不够广泛，没有引入外部威胁情报；数据粒度不够精细，缺乏必要的情境数据；时间跨度不够长久，没有跨年度的完整日志；分析方法过于简单，无法洞察攻击过程，更不能进行预测。面对未知威胁，只有采用云计算和大数据分析技术，才能从根本上解决数据来源广泛性、数据充分性、分析模型有效性的问题。其中建模分析尤为重要，数据不经有效的分析就永远是数据，甚至是垃圾数据。除了传统的统计、聚类、贝叶斯分析外，前沿厂商都在尝试全局关联分析、启发式机器学习等分析模型。

4.4 云管端安全架构的价值

相比传统以边界防护为核心、相互孤立的网络安全体系，云管端下一代网络架构具有明显的优势。

- ✓ 赋予了终端设备和边界设备应有的智能，不再依赖本地静态特征库/策略库，可以实时感知网络威胁的状态并做出调整，防御能力大幅提升。
- ✓ 云管端联动机制，使得网络安全具备了全局可见性，防御方式也从孤岛模式演进为协同模式，从而能够有效防御已知威胁和未知威胁。
- ✓ 网络安全始终都是大型组织投入的重点，云管端架构使买“安全感”真正变成了买“安全”，实现价值落地，提高了网络安全投资回报率。

任何事务发展都有内在的延续逻辑，而非断崖式替代，分享以下 3 个观点。

- ✓ 以边界防护为中心的安全体系存在固有缺陷，但并非毫无价值，它们能够很好地应对已知威胁，并发挥着重要作用。但企业组织应该用动态、主动的思维方法重新审视面临的威胁态势，并调整安全投入的重点。
- ✓ 云管端架构不是万能良药，不能期待解决所有的安全问题。安全问题永远是人与人之间的智力对抗，道高一尺，魔高一丈，安全的主动权掌握在攻击者一方，下一代网络安全架构提供了主动对抗的手段。
- ✓ 安全问题极为复杂，云管端模型预测攻击的准确度不可能百分之百，需要安全专家介入，结合实际业务特点进行分析判断，以减少误报。

5、关于网康科技

北京网康科技有限公司（以下简称网康科技）成立于 2004 年，总部位于北京，是中国上网行为管理理念的缔造者和下一代网络安全管理的引领者。网康科技拥有员工近千人，建立了遍及全国的销售与服务网络。产品线涵盖网络安全、应用安全、网络管理及优化，形成了完整的网络安全解决方案，并在业内率先发布云管端下一代网络安全架构与方案，实现云管端智能协同、主动防御，有效应对未知威胁及 APT 攻击。网康的产品和方案广泛应用于政府、金融、能源、教育、通信、企业等众多行业，客户数量超过 20000 家。

网康科技是业界最具技术创新和产品研发实力的企业之一，拥有一流的互联网内容研究实验室和网络安全攻防团队，并缔造了“全球最大的中文网页分类数据库”和“中国最大的网络应用协议库”。

网康科技承担了国家工业和信息化部技术改造项目、国家发展和改革委员会信息安全专项、下一代互联网专项、北京市发改委工程实验室技术创新能力建设项目、北京市科学技术委员会高新技术成果转化等项目，并被评为“国家级高新技术企业”，“北京市知识产权局专利试点单位”。网康科技还入选德勤“亚太区高技术、高成长企业 500 强”，并荣获“福布斯 2014 非上市潜力企业 100 强”，“中关村 2014 高成长企业 TOP100”等荣誉。