360互联网安全中心

互联网时代的企业安全发展趋势

第 1 期

2 2020 年预防将失效：通过普遍监控和集体情报保护信息

11 中国企业安全现状分析

23 企业安全解决方案

28 关于 360 互联网安全中心

专题调研报告，调研机构：

Gartner

来自 Gartner 文件：

2020 年预防将失效：通过普遍监控和集体情报保护信息

有针对性的高级攻击将使以预防为中心的战略过时。2020 年，我们需要向以信息为中心和以人为中心的安全战略转变，再结合内部普遍监控和安全情报分享，才能确保企业安全。

重大挑战

- 信息安全无法再预防有针对性的高级攻击。
- IT 部门将无法掌控用户使用的大多数用户设备或服务。
- 在预防攻击方面投入的信息安全支出过多，而在安全监控和响应能力方面的投入不足。
- 如果不对关于威胁和攻击者的情报进行集体共享，单个企业将无法进行自我防卫。

建议

- 立即启动一个项目，以了解企业中哪些部门负责创建、移动、转换、存储和存档敏感信息。利用所了解到的情况将投资按优先顺序进行排序。
- 构建普遍监控。为未来五年逐年加强监控而编制预算，增强监控技术的深度和广度。
- 在事故响应能力方面进行投资。设定一个流程来快速了解已检测到的违规行为的范围及影响，并为该流程配备员工。
- 向安全解决方案提供商提供大量企业的大致情况，使之了解威胁和攻击者的情况。

战略规划设想

到 2020 年，60% 的企业信息安全预算将分配到快速检测和响应方法方面（2013 年不足 10%）。

到 2018 年，80% 的终端保护平台将包含用户活动监控和入侵取证功能（2013 年不足 5%）。

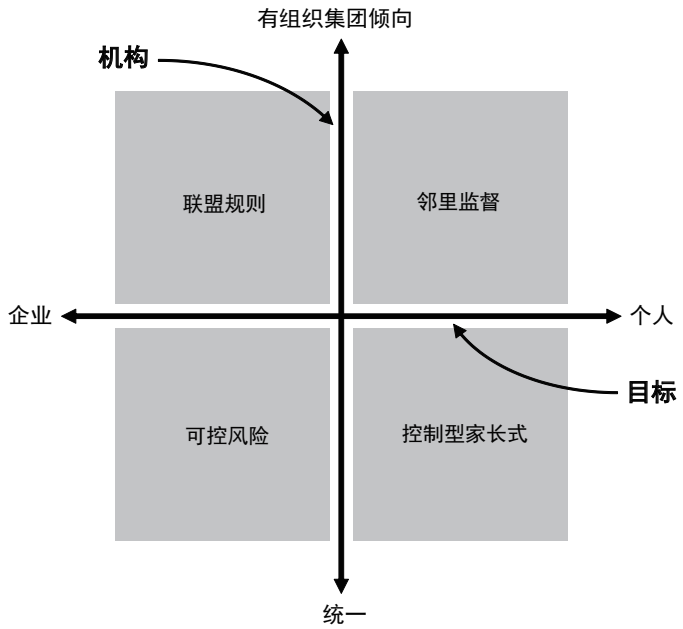
简介

2020 年，企业的外部威胁会产生多种可能的情景，这取决于攻击者直接针对的是企业资产还是个人。这种差异会因为对这些攻击做出的响应而进一步扩大 — 无论其是协调统一的机构还是分散的、有组织集团倾向的机构（参见图 1，“2020 年安全和风险管理情景规划”、“在未来情景中优化安全控制的四大战略”、“有控制地释放个人数据”以及“加大业务持续性管理力度，以应对‘联盟规则’情景”）。

不过，各种情景中都存在以下三大主要趋势：

- **持续性危害。**有针对性的高级攻击将会继续增加，它们会绕开传统的保护机制，在更长的时期内始终不被发现。因此，在所有情景中，必须假设系统和个人都会受到危害。
- **出于财务目的的攻击。**大多数情况下，针对企业和个人的有针对性的高级攻击都在试图盗取敏感信息 — 客户信息、信用卡数据、商业机密、配方、流程、计划、价格和类似知识产权。在某些情况下，其目标是通过进入关键系统或者使业务流程中断来给目标企业造成经济损失。
- **IT 部门将失去控制权。**IT 部门越来越无法直接掌控用户所使用的用户设备或服务，这限制了 IT 部门实施“侵犯性”控制手段的能力。消费化和“携带个人桌面”程序以及基于云的服务的使用量的增大趋势共同创造了一种计算环境，在这种环境中，IT 部门将失去对所使用的消费设备和服务的控制。

图 1. 2020 年 Gartner 安全情景

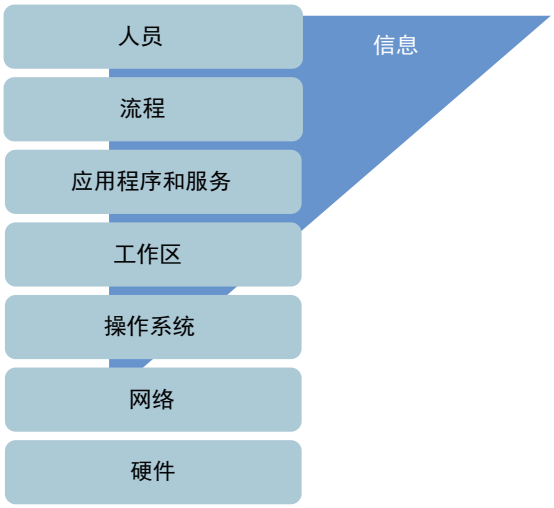


信息来源：Gartner（2013 年 5 月）

总之，这些大趋势将在信息安全组织、流程和战略方面引发多方面的转变（我们将在此研究报告中讨论这些转变）：

- 在 IT 堆栈结构中，将安全保护提升到保护信息（而非保护系统）的高度
- 从以控制为中心的模式向以人为中心的模式转变
- 使流程和开支朝着持续监控和普遍监控的目标转变
- 朝着利用集体情报和信誉服务的目标进行转变

图 2. 典型的 IT 堆栈



信息来源：Gartner（2013 年 5 月）

分析

向以信息为中心的安全战略转变

考虑典型的 IT 堆栈（参见图 2）。

2020 年，企业 IT 部门将不再掌控设备，在使用基于云的服务时，它们可能会也可能不会控制最终用户使用的网络、服务器、操作系统和应用程序。2020 年，IT 部门可以真正直

接控制的还剩下什么？答案是信息本身。在大多数情况下，信息必须成为信息安全战略的焦点。

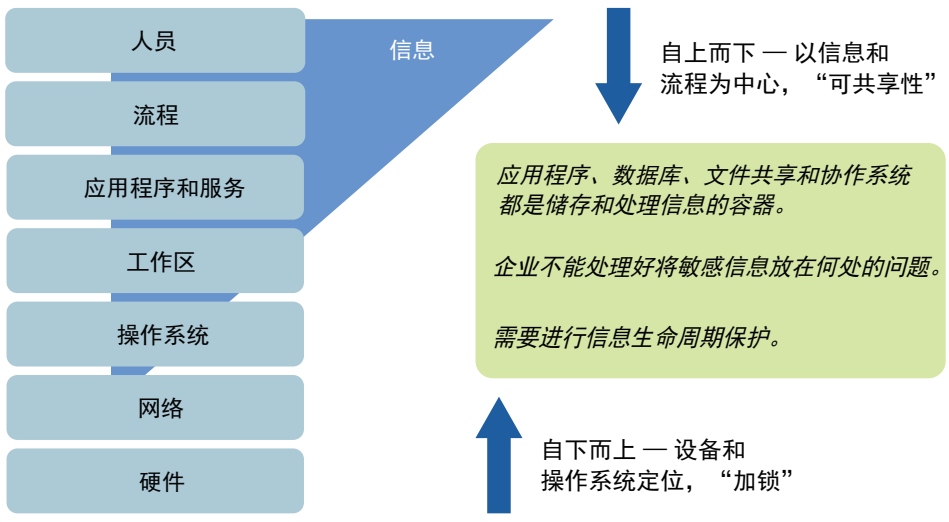
这是一种朝向信息安全的基础的回归，因为信息安全的目标始终是保护信息的机密性、完整性、真实性、可用性和实用性，以及保护对信息的访问。[1] 对于许多企业来说，对设备、应用程序和服务器的控制和加锁是达到目的的一种手段。为了实现保护信息的目标，我们利用设备所有权，通过加锁和控制来保护信息。但是，这会把加锁、所有权和控制等同于信息安全，将手段与最终目标混为一谈。所有权和严格控制代表着信任。在未来，当 IT 部门越来越无法掌控或控制技术的使用或发送时，人们就需要使用新的信任模型了。信息安全战略需要从自下而上的设备和以网络为中心的战略，转变为自上而下的以信息为中心的战略，且该战略注重信息本身（参见图 3）。

根据实际发生的情景是四种情景中的哪一种，攻击者将更改他们攻击信息的目标和方式（参见图 4）。无论如何，从保护用于保存和传输信息的媒介（例如，网络基础设施和终端）到保护数据和信息本身的转变的需要，将是所有情景中最重要的转变。

如果攻击者把企业系统作为目标，信息安全战略将需要关注那些用于访问、处理和存储信息的企业系统。具体来说，这包括增加在应用程序安全方面的投资，例如，应用程序安全扫描仪、应用程序安全防火墙、数据库审核和保护、文件共享监控和保护以及企业内容管理系统的保护（包括诸如 Microsoft 的 SharePoint 之类的平台）。基于云的服务中的企业信息可以通过加密技术来保护，也可以通过使用云入口安全代理（请参阅“云入口安全代理越来越重要”）的令牌化进行保护，或者使用专为信息保护和云加密网关设计的特定平台（请参阅“2012 年云安全的技术成熟度曲线”）进行保护。在这些情景中，我们的保护工作集中在图 5 的左半部分。

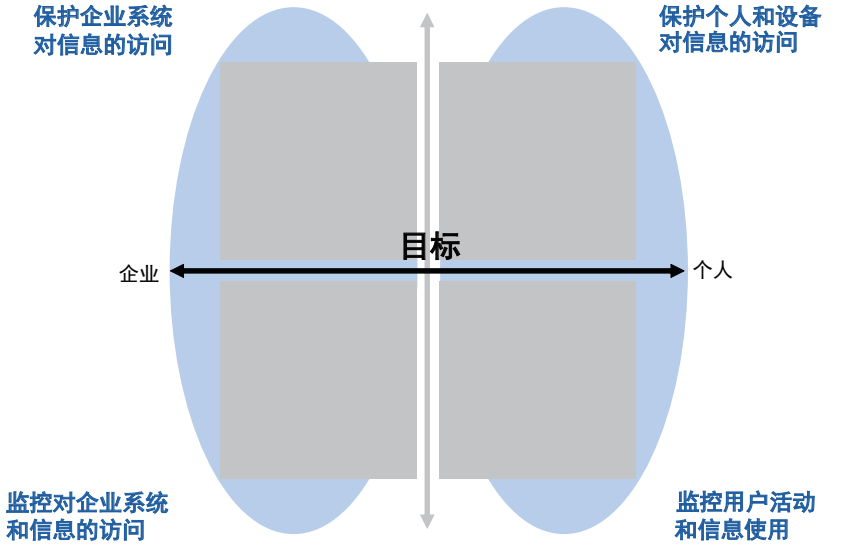
如果攻击者以个人为目标，信息安全战略将需要更加关注消费方面，即保护最终用户设备上的信息（无论是企业拥有的信息还是个人拥有的信息）。有一种简单而笨拙的方法会

图 3. 自上而下的以信息为中心的安全模式



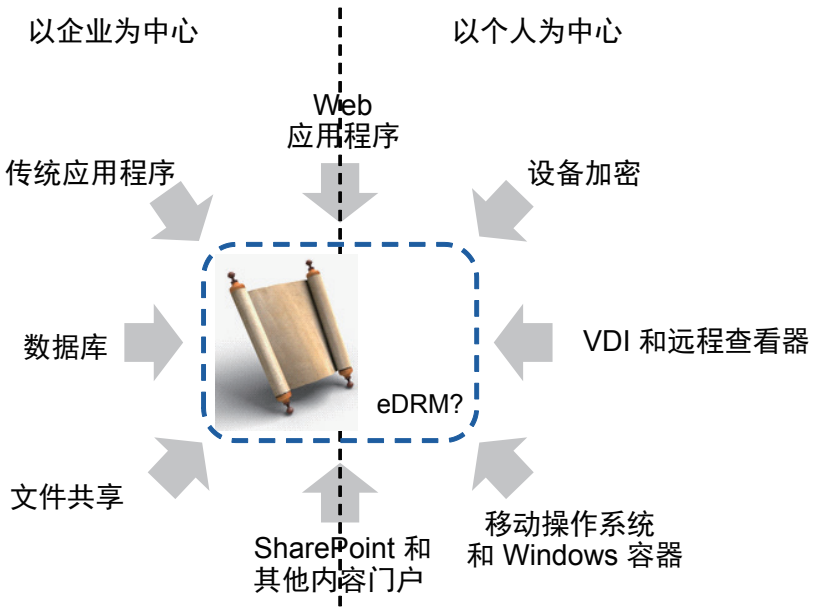
信息来源：Gartner（2013 年 5 月）

图 4. 信息安全战略的不同重点



信息来源：Gartner（2013 年 5 月）

图 5. 以企业为中心的信息保护模式与以个人为中心的信息保护模式比较



信息来源：Gartner（2013 年 5 月）

加密整个设备以防设备丢失或被盗，但是这种方法对有针对性的高级攻击毫无作用，因为这种高级攻击进行的是基于凭据的访问。

另一种方法是将企业内部的信息以及处理信息的应用程序保存在一个中央位置，使用托管虚拟桌面 (HVD)/ 虚拟桌面基础设施或类似的技术，向最终用户远程呈现信息。同样，使用远程查看器应用程序也可以获得相同的最终结果，无需传输整个桌面，只需查看文档（请参阅“如何控制文件同步服务并防止企业数据泄露”）。

如果允许将企业信息存储在本地设备上，则针对移动和非移动系统，将出现用于特定于应用程序和独立于应用程序进行控制的解决方案（请参阅“用于企业数据管理和安全的移动应用程序容器的技术概述”）。此时，将使用加密技术单独保存潜在的敏感企业信息，以实现逻辑隔离，这将使删除数据就像废除密钥一样简单。

建议

- 从传统的方法转变为开始使用信息生命周期方法，通过确定在企业用户和系统中创建、操作、转换、存储和存档敏感信息的位置，来保护信息。
- 假设到 2020 年大多数设备和服务都将不受信任，从信息层级开始设计保护措施，一路向上兼顾各层级，直至消费系统或服务。
- 不要对所有应用程序和系统采用相同的保护级别。根据应用程序和系统保存的信息的敏感性和关键性以及这些应用程序和系统所支持的业务流程的重要性，确定相关保护工作的投资的优先次序。
- 对于敏感信息存储在非企业设备上的情景，要探索使用 (HVD) 或远程查看器来直接控制信息，或使用新出现的控制解决方案来保护信息。

从以控制为中心的安全模式转变为以人为中心的安全模式

到 2020 年，针对信息安全的传统的技术性方法（以控制为中心）将被淘汰。2013 年，这种方法就已经越来越难以维持下去了。最大的难题是：这种方法试图使信息免受由合理访问信息的人员造成的蓄意损害或意外损害，同时又设法最大限度地减小对效率和灵活性产生的消极影响。IT 交付模式的多样性和复杂性以及数据量的剧增，使针对安全问题的传统方法站不住脚。以人为中心的安全模式 (PCS) 创建了一种现代、高效、侵犯性小且成本较为低廉的安全模式，可以替代传统的“加锁”模式。

PCS 是一种针对信息安全的战略方法，强调个人的责任和信任，不再强调限制性和预防性的安全控制。PCS 以一套主要原则和个人的权利及相关责任为基础。PCS 的前提是员工拥有一定的权利，但这些权利是与特定责任相连的。这些权利和责任建立在以下理念的基础之上：如果个人没有履行自己的责任或者其行为方式没有尊重其同事和企业的利益相关者的权利，那么这些个人将受到处罚。

这种权利和责任的紧密结合在员工之间创造了一种集体的互相依赖性，利用了公司内的现有社交资本。PCS 原则侧重于运用检测性及反应性控制以及透明的预防性控制，而不侧重于运用侵扰性的预防性控制。同时该原则还假设个人拥有适当的知识来了解其权利、责任和相关决策。

在情景规划象限中，只要目标是个人，就适合运用 PCS 原则。在控制型家长式情景中，企业负责为 PCS 设定相关的文化背景。在邻里监督情景中，许多文化背景和基本原则都是由个人（及其组织）所在的社区提供的。

最佳做法 / 建议

- 研究针对信息安全的更加以人为中心的方法背后的概念和原则，并考虑在安全战略中采用这些概念和原则中的一些或全部。

- 认为需要转变为使用 PCS 方法的组织必须：
  - 认真规划一项有效的文化变革计划。
  - 确保工作场所协议是灵活的并且完全合法。
  - 确保他们的 PCS 方法仍然符合其必须恪守的标准。

将安全计划重点转向快速检测和响应

到 2020 年，企业系统将处于一种遭受持续性危害的状态。它们将无法防止有针对性的高级攻击在系统中立足。遗憾的是，到目前为止，人们错误地试图预防所有攻击，因而将大多数的企业信息安全支出集中用在了预防上。随着形势的发展，尽管人们仍然需要运用预防措施（例如，企业防火墙、入侵防御系统和终端反恶意软件系统），但这些预防技术的有效性将下降，这些技术在信息安全预算中所占的百分比也将下降。此外，上文所述的向 PCS 的转移暗示着从预防性控制向检测性控制转移。我们相信大多数的信息安全支出都将转变为支持快速检测和响应能力，这些能力随后会与保护系统相连，以阻止攻击的进一步扩展。

在缺少基于签名的机制的情况下，要解决如何识别攻击这个看似无法解决的问题，一种措施就是实施普遍监控，识别与正常行为不同的有实际意义的特别行为，从而推测恶意目的。如果您假设系统会遭受有针对性的高级威胁，则在信息安全方面的努力就需要转变为详细、广泛且可感知背景情况的监控，以检测这些威胁。[2] 然而，当转向以信息为中心的安全战略时，我们的监控重点将因情景而异（参见图 3）。

对于攻击的重点是企业系统的情景，我们对监控、检测和响应的重视将处于企业级别，具体来说就是，采用与信息保护大致相同的方法（监控对应用程序、数据库、文件系统和内容管理系统的访问）来监控企业对应用程序和信息的访问。

可以对用户访问模式进行衡量和分析来判断是否存在隐含恶意目的的异常行为，比如，可以分析访问的频率、下载信息的数量、访问信息的类型和背景信息（例如，发送请求时间是在一天当中的什么时间，或者发出请求的设备是什么类型的设备）等。除了特定于领域的监控解决方案（例如，数据库审核和保护）之外，业界还涌现出了身份和访问情报解决方案，这些解决方案也能分析上述模式。即使在通过云使用信息和服务的情况下，云入口安全代理（例如，Skyhigh Networks）也可以针对云服务访问进行同样的衡量和异常检测。

对于专门以个人为目标的情景，监控和检测功能将以身份和角色为中心，理想情况下会扩展至设备本身，直接在终端执行详细的用户活动监控。此前，已经有多个监控和入侵取证工具在提供这些功能，包括 Mandiant、Bit9、RSA（EMC 的安全部门）、HBGary、Cyvera 和 Guidance Software。未来三年内，我们期望最主要的终端保护平台 (EPP) 提供商能够改进他们的平台，以提供相似的功能。通过详细监控用户系统上运行的应用程序以及用户与内容、可执行文件和企业系统之间进行的交互活动，企业便能够“像数码录像机录像一样”监视所发生的一切情况。即使在无法避免的违规事件中，企业也可以通过查询这些数据来了解其他哪些用户被当作攻击目标，哪些系统可能会遭受危害，以及哪些信息会被泄露。

在这两种情况中，使用背景信息对于基于行为和基于异常的方法的成功至关重要，这些方法可以减少错误率（例如，添加设备、位置和身份识别等），然后将这些内容与监控行为联系起来，从而提高结果的准确度。

建议

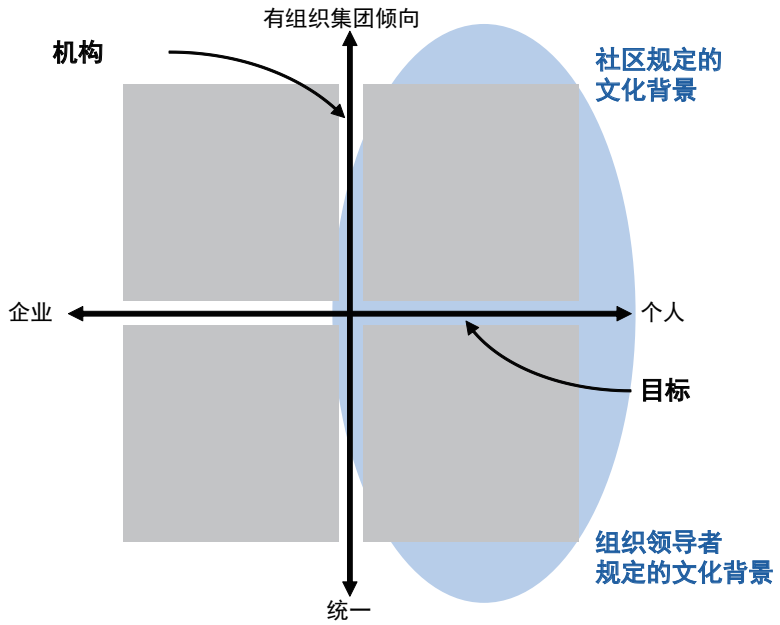
- 首先将监控工作的重点放在企业最重要的信息资产（一般是财务数据库和客户数据库）上，然后再扩展到其他敏感的存储库。
- 分析对信息的监控以提高发现结果的准确性时，使用补充的背景信息。
- 实施企业终端监控 — 理想情况下，这是通过要求终端保护供应商提供详细的登录和审核信息（作为其 EPP 解决方案的不可或缺的部分）来实现的，无需购买第三方解决方案。
- 针对未来五年内信息安全监控方面日益增加的数万亿字节范围的数据存储需求进行规划（请参阅“信息安全将成为很大的数据分析问题”）。
- 不要在网络和终端安全方面投入过多的资金，将省下来的资源用到监控和检测计划方面。针对以保护为重点的元素选择聚合安全平台（下一代防火墙 /IPS），为中小企业选择统一威胁管理（请参阅“中端市场背景：‘2013 年 IT 安全预算和人员规划’”）和 EPP。

企业集体的、以社区为基础的安全情报服务

到 2020 年，在有针对性的高级攻击造成持续危害的情况下，需要组织分享安全情报，以便更好地了解是哪些地方遭受了危害以及是如何遭受危害的。在所有情景中，无法单独对抗这些攻击的企业将转而与其他组织分享自己的安全情报，以便更好地了解攻击者的工具、技术和目标。与内部监控一样，情报范围的扩大为改进安全决策提供了更多的数据和更多的背景情况。企业参与共享其情报的方式会因情景而异（参见图 6），但是在所有情景下都需要共享信息。

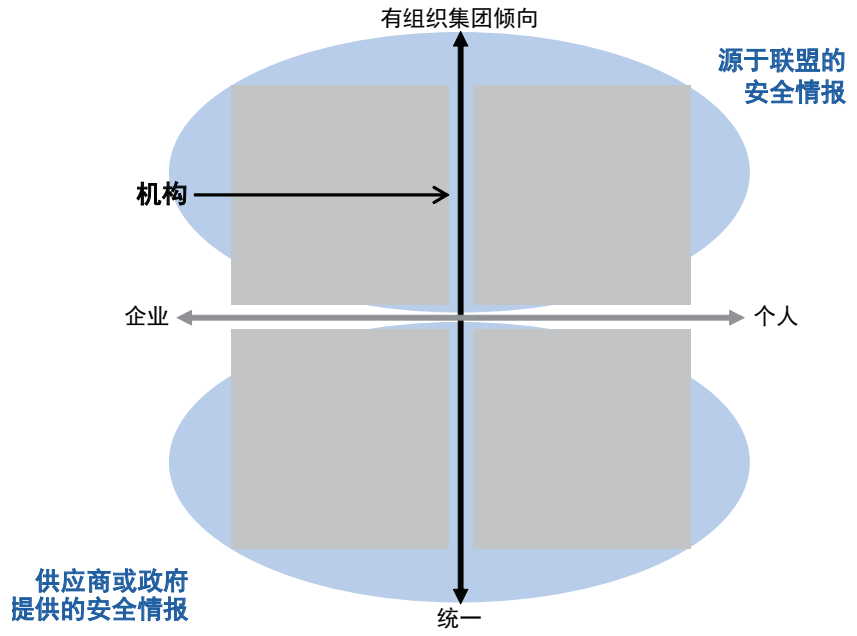
当机构是一个统一的整体时，我们期望让集中管理的强大实体（供应商和政府）成为集

图 6. 各种情景在集体情报方面的差异



信息来源：Gartner（2013 年 5 月）

图 7. 各种情景在情报服务方面的差异



信息来源：Gartner（2013 年 5 月）

体安全情报的主要来源。企业将与集中管理的实体分享他们所了解和监控的情况，以便使自己和在同一个强大的生态系统中生存的其他企业都能受益。

即使是有组织集团倾向的、分散的机构，也会共享情报，这种共享一般会通过同一行业中的企业联盟来实现。例如，金融服务信息共享和分析中心 (FS-ISAC) 在安全情报以及供应商（例如，Red Sky Alliance 和 Threat Connect）最新产品方面进行的共享。[3]

集体安全情报服务的三种类型非常重要：信誉服务、威胁情报和攻击者情报。

- **信誉服务：**在 IT 无法掌控或控制使用或交付元素的情况下，云和以社区为基础的信誉服务会填满“灰色地带”，为能够替代“所有权等同于信任”模式的新的信任模式奠定基础。到 2020 年，企业将需要应对各种类型的未知实体 — 设备、内容、应用程序、身份、域名、URL 等等。信誉服务会帮助组织回答一个问题：“我是否足够信任此实体，以在当前环境中执行所要求的操作？”这些类型的服务主要用于支持在线个人银行服务，在这些服务中，设备也是不受掌控的、是未知的、可能受到潜在感染并且无法操纵所使用的浏览器。出于相同的原因，类似的模式也将用于企业 IT 部门。

- **威胁情报服务：**在未来情景中，目标是企业，企业威胁情报服务将是一项重要的资产。在这种服务中，共享的情报包括企业的哪些漏洞会成为攻击的目标，以及攻击者会采取何种攻击方式（参见图 7）。这些服务倾向于以威胁为中心，能够使企业识别并弥补被攻击者发现的漏洞。示例包括 Symantec Cyvelliance、IBM、Secunia 和其他公司（请参阅“如何选择安全威胁情报服务”）。Imperva 最近推出了 ThreatRadar，

这是一种以社区为基础的威胁共享和情报服务。此外，该公司还推出了由社区驱动的独立威胁情报功能。

- **攻击者情报服务：**对于目标是个人的情形，被攻击者发现的漏洞一般都在最终用户自身上。由于给最终用户打补丁是一项难度更大的工作，因此这种情景将演变为共享有关攻击者的具体情报（与威胁相比）（参见图 7），例如，攻击者在侦察期间采取的攻击方式和具体的行为模式。此前，供应商（例如，CrowdStrike、Mandiant、Mykonos 技术公司（由 Juniper 收购）和 ThreatMetrix）已经提供了有关攻击者情报服务的最新示例，例如，Mykonos 服务（现在重新命名为 Spotlight Secure），其 Web 安全解决方案可以不依赖攻击者攻击时所在的位置或使用的设备辨别出攻击者，并将此作为一种基于云的攻击者情报服务。[5]

最佳做法 / 建议

- 使用外部威胁来源和攻击者情报增强您的安全技术和流程，以便更好地了解您的企业是否遭受了攻击以及在遭受攻击时更好地了解这一情况。
- 优先选择那些可以提供安全威胁情报和安全攻击者情报的供应商，因为这两种类型的情报都是必需的。
- 参加特定行业的新兴共享集体，共享信息安全情报。

注释

[1] 信息安全是指为了保护打印、电子或其他任何形式的机密、私人和敏感信息或数据，使其免遭未经授权者访问、使用、滥用、泄露、破坏、修改或毁坏，而设计并实施的流程和方法（请参阅 www.sans.org/information_security.ph）。

信息安全（有时简称 InfoSec）是指保护信息使其免遭未经授权者访问、使用、泄露、破坏、修改、阅读、检查、记录或毁坏的措施。这是一个通用于各种数据的术语，无论数据采用何种形式（例如，电子形式或物理形式）。

[2] 背景情况感知监控 — 示例包括位置、一天当中的具体时间、设备信誉、IP 地址信誉和 URL 信誉（请参阅“未来的信息安全模式是背景情况感知和适应模式”）。

[3] https://www.fsisac.com/sites/default/files/Repository%20Conceptual%20Overview%2022Mar2013.pdf

[4] Titan 是由社区驱动的新兴威胁情报功能的一个示例。Titan 是一种用于恶意软件分析和威胁情报的自动化框架。

[5] http://juniper.mwnewsroom.com/press-releases/JUNIPER-NETWORKS-ANNOUNCES-NEXT-GENERATION-SECURIT-nyse-jnpr-989255

信息来源：Gartner Research, G00252476, Neil MacDonald, 30 May 2013

中国企业安全现状分析

1. 企业内部信息安全

信息技术对于企业是提高生产和管理效率的工具，但同时也成了攻击者的武器。

目前，在中国工商行政管理总局注册的企业有 1100 万家，随着社会信息化进程的加速，信息化技术在这些企业运营过程中的作用越来越重要，而企业信息化进程中所暴露的安全问题也越来越受到社会的关注。

敏感信息泄露、重要数据被破坏、业务系统被非法控制、商业信誉遭恶意言论攻击，这些利用信息化系统实施的攻击行为，轻则损害企业的经济利益，重则造成重大的社会影响，甚至危及国家安全。

1.1. 企业面临的安全问题

对于拥有大量商业机密并且对信息安全保护要求较高的企业来说，仅仅使用个人版安全软件确实存在一定程度的安全隐患。

目前，U 盘是黑客对企业用户发动攻击的常用媒介。由于很多企业都会对内网系统进行隔离保护：有的是在网络层隔离，有的则干脆进行物理隔离。对于这种与世隔绝的网络，U 盘就成为了一个很好的木马载体。除了 U 盘病毒外，针对办公软件发动攻击的宏病毒和利用局域网系统传播的 ARP 病毒，也是对企业用户威胁较大的病毒。

某些企业简单地通过内外网的隔离来进行安全防护，却可能导致其内网用户的电脑系统无法在第一时间安装漏洞补丁，安全软件也不能实现及时有效的安全更新，客观上反而使内网系统处于一种更加不安全的状态，一旦遭遇木马病毒的入侵，就可能造成严重的系统破坏。

与个人电脑安全不同，企业安全属于一种集体安全问题。一般来说，联入内网系统的电脑中，只要有一台电脑被黑客攻破，那么就有可能造成内网安全体系的崩溃和商业机密的泄漏。也就是说，安全性最差的一台电脑实际上就决定了整个企业内网系统的安全级别，这就是企业安全问题中的“木桶效应”。

1) 缺乏统一管理容易形成木桶效应

如前所述，安全性最差的一台电脑实际上就决定了内网系统的整体安全级别。而对于使用个人版安全软件的企业来说，很难掌握员工的电脑安全水平，也很难对企业内网安全状况进行全面的了解和监控。安全维护只能依赖于员工个人的职业技能和安全素养。另外，一旦有员工电脑被感染或是企业内网被入侵，网络管理员也很难及时地发现和解决问题。

而使用管理功能较强的企业版软件，终端的安全状况都会汇总到一个控制中心，网络的管理员可以通过管理平台掌控全网的安全状况，为企业内部终端进行统一的查杀病毒、修复漏洞和产品更新等操作，还可以为每个终端配置正确的安全策略，并能在出现问题时及时收到报警通知，从而有效地避免木桶效应的影响。

2) 内部软件或网址易遭安全软件误报

很多企业都会使用一些内部专用的软件。由于这些软件并未公开发行，也没有接受过安全公司的检测，并且某些敏感的操作可能和病毒木马比较接近，因此很有可能被安全软件误判为恶意软件。也有一些企业需要用一些远程控制软件管理网络或者终端，某些远程控制软件甚至与木马功能类似，因此也很有可能被个人版安全软件当做木马病毒或可疑程序予以禁止或删除。

另外，某些企业，包括某些大型国企，为了使用方便，经常会用自己内网专有的 DNS，

将本来不是自己企业注册的域名重定向到企业内部的办公系统。而相同的域名在公共互联网上可能也会同时存在，只是普通用户与企业内网用户的 DNS 解析结果不同而已。如果公网上相同域名的网站恰好是钓鱼网站或挂马网站，那么当企业内网用户请求访问该域名时，就有可能被个人版安全软件拦截，从而形成误报。

3) 每台电脑独立升级占用企业上网带宽

每台电脑独立升级占用企业上网带宽。个人版安全软件一般都是各自独立进行升级、打补丁等操作。而对于企业用户来说，如果每个员工电脑都要独立地联网升级，就会占用大量的网络带宽，影响正常的上网速度。这对于那些租用固定网络带宽，同时员工数量又比较多的企业来说，影响尤为明显。

而使用企业版安全软件，则可以通过控制中心端的缓存数据，进行二次分发，给内网用户统一升级、统一打补丁，从而在最大程度上减少升级、打补丁等联网操作对企业网络带宽的占用。

4) 办公电脑混用

在办公电脑安装与工作无关的个人应用，将办公的业务数据、企业的保密数据与个人应用数据之间无隔离同盘存储是目前各个企业网络管理、应用管理、安全管理所面临的一个重要问题。

在办公电脑上任意安装个人软件将带来非常严重的安全隐患，大量来源不明、随意下载的应用软件自身安全漏洞频出，为攻击者留下大量低成本的可乘之机，更严重的是，很多未经验证和鉴别的应用软件本身就含有木马、病毒等恶意代码。这些被植入恶意代码的主机很可能成为发起 DDoS 攻击的僵尸主机，甚至成为进一步渗透企业内网，完成 APT 攻击的重要跳板。

5) 漏洞修复滞后

补丁的下载与漏洞修复最关键的是及时性、全面性，否则稍有延迟、稍有遗漏就有可能使得内网安全功亏一篑。

目前对于国内的大部分企业（既包括中小型企业，也包括大型企业）来说，全面统一监控终端漏洞状况的监控系统并未建立；统一管理终端补丁，对终端进行统一补丁分发与安装的控制系统并未建立；有效避免外连升级服务器导致出口堵塞的专用企业补丁分发系统并未建立。在这种情况下对于国内的大多数企业来说，及时更新补丁，全面修复漏洞还不具备基础，企业内网安全仍将由于漏洞修复的不及时、不全面而存在于大量的威胁之中。

6) 终端安全缺失

终端安全防范是信息安全领域出现最早的一种安全防范形式，其中，终端杀毒软件作为最主要的终端安全防范措施已经有近 30 年的历史，发展到现在，以终端杀毒软件为核心的终端安全防护措施已成为构建企业安全防护体系不可缺少的重要组成部分。

根据 360 互联网安全中心 2012 年的抽样调查统计，国内企业普遍存在用免费的个人版安全软件代替企业版安全软件的情况。在接受调查企业中，国有大中型企业使用企业版安全软件的比例较高，达到 78%；而中小企业的情况则让人担忧。配备企业版安全软件的比例不足 5%，约 94% 的中小企业仅为员工电脑安装个人版安全软件，还有 1% 左右的企业根本不使用任何安全软件。

7) Wifi 缺乏管理

目前国内使用 Wifi 的企业非常普遍，特别是中小型企业，甚至已经取消了传统有线网络，完全依靠 Wifi 进行办公，而这些广泛采用 Wifi 信号的企业基本上都没有有效的 Wifi 管理措施，完全在无管理、无防护的状态下使用 Wifi 来办公和提供业务服务，这已经成了国内企业，特别是中小企业必须面对和解决的现实安全问题。

私建无线热点，很可能因为没有专业的安全配置，在原有经过严密规划过的纵深安全防御体系上打开了一个非法接入的网络入口，使得入侵者可以毫不费力地绕过所有边界安全防护产品和措施直接进入到企业内部核心网络实施攻击。这对于企业的网络安全体系来说，毫无疑问是非常致命的。

另外一方面，伪造的无线热点成为钓鱼和欺骗的工具，随意接入 Wifi 热点，如公众场合：机场、宾馆、咖啡厅、商场等，对于很多企业的员工在使用移动设备（如笔记本）在接入到企业提供的 Wifi AP 接入时，存在着被伪造的热点钓鱼欺骗和劫持的危险。

8) 移动终端接入

随着近两年移动互联技术的迅速发展，移动互联网不仅仅渗透到了我们生活的方方面面，而且还将渗透到我们的工作当中，Bring your own device（BYOD）正在成为一种趋势，但同时也带来了安全问题。BYOD 使得个人和工作任务在同一设备上混合。联系人名单、电子邮件、数据文件、应用程序和访问互联网可能面临挑战。理想的情况下，用户希望他们的个人资料和活动与工作分开。在个人时间访问个人照片、短信、电话，上网浏览需要个人隐私保护，而工作时间内完成的文件、档案，使用企业数据的应用程序和互联网浏览需要符合企业政策。

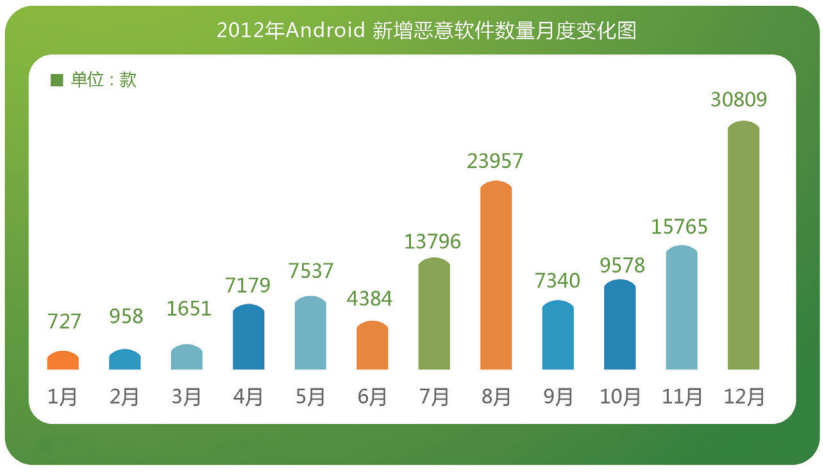
目前国内外大部分企业还没有一套完整的解决方案来应对 BYOD 带来的安全威胁，面对 IT 应用环境的改变，如何确保企业信息资产的安全，同时又享受 BYOD 带来的便捷，这成为企业安全管理的一个难点。

9) 安全制度落实

完善的安全体系建设需要有产品作基础、有技术作保障、有服务作配合、有制度作管理。只有产品、技术、服务、制度协调配合，多管齐下，才能有效保障企业内网的安全。

安全问题不只是技术问题，究其根本，安全问题是人与人、人与组织围绕着利益的对抗行为，因此安全问题具有诸多的不确定因素，如：攻击技术的不确定性、攻击途径的不确定性、鉴定结论的不确定性，安全说到底是要解决人（包括攻击者、被攻击者）的问题，

图 1



信息来源：360 互联网安全中心 (2013 年 1 月)

而不是解决技术本身的问题，这使得安全防御工作、安全体系构建工作必须综合考虑方案、技术、产品、人、制度等多方面因素，才能实施有效的防御措施。

1.2. 企业移动信息安全

1) 手机恶意软件款数激增，同比增长达1907%

2012 年，360 互联网安全中心新增手机恶意软件样本 174977 款，同比 2011 年增长 1907%，感染人次 71664334 人次，同比 2011 年增长 160%。

其中，Android 平台以新增样本 123681 款，占全部新增样本数量的 71%，感染量达 51746864 人次，占恶意软件感染总次数的 78%，成为手机恶意软件的主要感染平台。2012 年 12 月，其更以单月新增 30809 款达到历史新高。

2) 系统漏洞频发，涉及数百款机型

2012 年中，更多手机恶意软件还开始利用手机平台中存在的系统漏洞来进行攻击，如 2012 年 10 月，三星 Galaxy 系列手机被曝存在拨号指令漏洞，可被利用使用户误格手机；

三星、魅族、小米等手机的芯片组被曝存在内核驱动漏洞，直接涉及如 Galasy S3、Note2 等数百款主流机型。

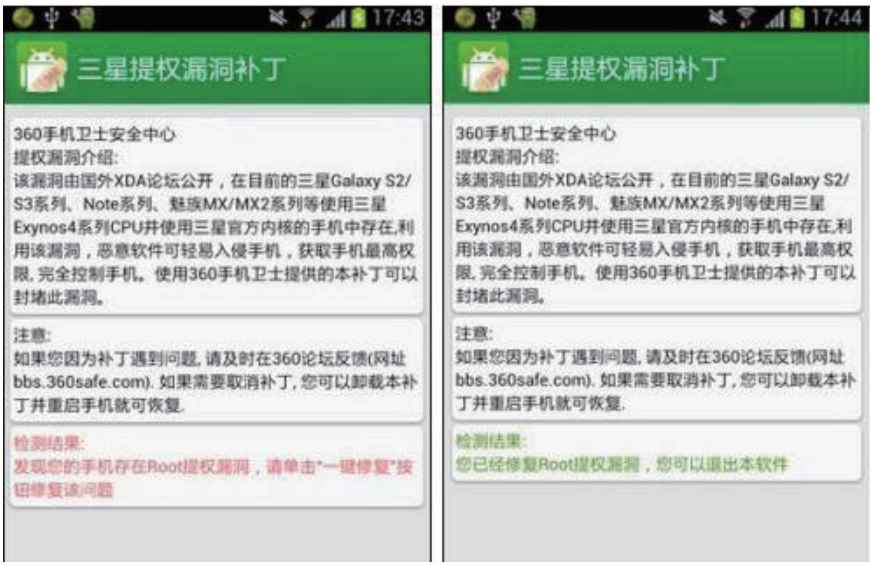
一系列安全漏洞的出现，也使得手机终端厂商开始愈发重视设备安全问题，如在一系列漏洞出现之后，终端厂商和芯片厂商都在第一时间做出了快速响应，升级系统版本、提供修复补丁等解决方案等。

3) 隐私安全危机濒临爆发临界点

2012 年中，在智能手机用户持续增长的同时，隐私安全问题也愈发引人关注，大量因手机丢失导致隐私泄漏的案例和多款手机 APP 应用被曝存在后台收集用户通讯录、手机短信、监听通话内容甚至录音的行为，使得隐私安全问题已经濒临大规模爆发的临界点，任其发展后果将十分严重。

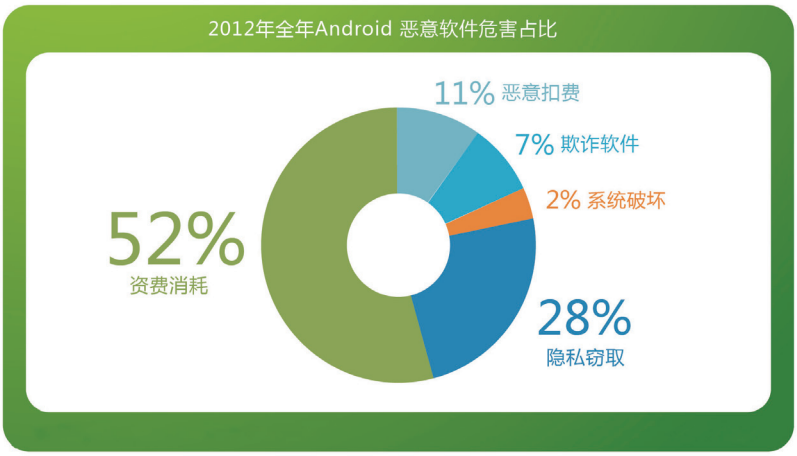
例如，2012 年中，360 手机卫士相继查杀如专门盗取短信、IMEI(手机串号)、Google 账号等隐私信息的 DroidDreamLight 系列手机恶意软件，可窃听通话、盗取短信内容的 X 卧

图 2



信息来源：360 互联网安全中心 (2013 年 1 月)

图 3



信息来源：360 互联网安全中心 (2013 年 1 月)

底系列间谍软件最新变种等，其可通过巧妙伪装植入用户手机，获取录音、联网等权限后盗取用户隐私，行踪隐蔽，让用户很难察觉。

4) 非越狱 Iphone 也存在 iOS 安全危机

2012 年中，此前被认为因相对封闭，而安全系数较高的 iOS 平台中也开始出现一系列安全问题，如在同年 8 月，法国黑客发现的 iOS 短信漏洞可将诈骗短信伪装成合法的身份，诱骗用户接收、点击其中的短信链接等，由于这一漏洞在非越狱手机中也同样存在，更使用户极易落入短信欺诈陷阱之中。

同时，随着大量用户开始购买和同时使用多台 iOS 设备，如 iPhone、iPad、Mac 等，在信息同步过程中也开始出现一系列安全问题，如一旦黑客成功破译 Apple ID 账号，可导致用户的 iMessage 信息、安装的应用列表、以及 iCloud 数据被轻易同步到另外的 iOS 设备上，直接盗取隐私信息等。

1.3. 企业安全的重磅杀手：APT

对于中国大型支柱性企业来说，外部威胁不断升级，来自已经军事化到了牙齿的网络对手的攻击，防御之难甚至无法想象，伊朗核电站的震网事件历历在目，继二战末期推出原子弹之后，美国又在网络信息战中推出了核武器级别的网络攻击工具：APT

APT（高级持续性威胁）作为一种新的攻击形式俨然在全球信息安全领域掀起了新一轮网络安全军备竞赛。

反复渗透、巧妙植入、长期潜伏、精确打击是 APT 攻击的典型特点。

通过先进的攻击手段，精确地选择攻击目标进行持续性的攻击，攻击成功率接近惊人的 100%，到目前为止，国际上已公布的典型 APT 攻击的防御均以失败告终。高价值商业机密信息、高价值国民经济数据、高价值军工设计图纸等等事关国计民生的机密信息早已成为国外谍报组织重点渗透的目标，通过网络攻击手段获取这些数据已经在传统的保密战场之外开辟了一块难度更大的新型保密战场，国有大型支柱性企业的网络安全系统建设是我们在这场战争中生存下来的重要保障。

事实证明，传统安全防护设备、防护思路在 APT 攻击面前已经不堪一击，防护 APT 攻击需要采用更先进的技术、更先进的产品、更严格的管理。

传统的安全防御设备大多数依赖于云、信誉评价（ERT）和病毒签名等，他们的优势在于面对已知威胁的检测稳定可靠。但同时这种

技术体系的缺陷也非常明显，就是构架于信誉评价、已有特征、签名技术思路之上的检测体系对于那些未知的攻击、未知的漏洞、未知的病毒木马完全失效，而 APT 攻击之所被称为网络信息战中的核武器，就是因为 APT 攻击采用的都是 0day 漏洞、未知木马、未知攻击手法，在这种情况下，突破传统安全防护设备的检测就变得非常简单。

另一方面，现有安全防护体系是一套纵深防御的立体防御体系，其构建思路是对各种可能进入到企业内网、接触到核心资产的网络路径进行穷举、演绎，然后在这些可能的路径上层层设卡，部署设备。而已经发生的 APT 攻击已经说明，攻击者完全可以通过思路创新结合技术创新，不走寻常路，找到一条新的，没有被穷举、演绎过的渗透途径，甚至可以不是网络途径，绕开所有的检测设备关卡，直接进入到内网，接触到核心资产。我们对震网事件进行复盘的时候就慨叹于美军和以色列采用极具创新的“U 盘摆渡”的技术思路，这些都说明，企业要做到 APT 的有效防御，必须抛开常规的技术、抛开常规的安全产品、抛开常规的防御思路，尽可能寻找理论上能够保障核心资产运行安全的防御思路。经过实践证明，奇虎 360 的内网安全防护体系和思路在 APT 防御方面走在了中国企业内网安全 APT 防范的前列。

APT 攻击相比普通病毒攻击有如下不同（参见图 4）：

国家互联网应急中心报告显示，2012 年，我国境内至少有 4.1 万主机感染了具有 APT 木马特征的程序，对国家和企业数据安全造成严重威胁。

在 2013 年，有国家背景的个人或有组织的团体将继续使用网络战术，企图损害或破坏其目标信息或资金的安全。我们将看到网络威胁的力量相当于武力的威胁，国家 / 组织甚至个人团体会使用网络攻击，显示自己的“实力”。

APT 攻击案例：

伊朗的核设施拥有一个物理隔离、高度防护的网络，但是在 APT 攻击下，核设施参数被修改，核进程被推迟几年。

攻击者对伊朗核设施进行了为期数月甚至更长时间的潜心准备，搜集应用程序与业务流程中的安全隐患，定位关键信息的存储位置与通信方式，在这个 APT 攻击中，名为 Stuxnet 的计算机蠕虫病毒使用 USB 移动介质作为跳板，

图 4

项 目	APT攻击	普通病毒攻击
是否有目标	明确的攻击目标	大面积扩展僵尸网络
目标用户	定向的机构和公司	用户个人凭据（银行卡号）
攻击频率	频繁	一次性
攻击途径	多种0Day 精心构造的RAT 各种后门程序	各种常见攻击工具 构造恶意URL 全功能的木马软件
检测难度	通常存在较长时间的样本空白，检测率低于10%	成活时间短，容易被捕获，检测率超过95%

信息来源：360 互联网安全中心 (2013 年 1 月）

植入了木马文件（伪造有效的数字签名），成功绕过安全产品的检测。利用 Windows 和西门子系统漏洞，成功入侵离心机的控制系统，修改了离心机参数，干扰其正常运行，但控制系统却显示一切正常。在 2011 年 2 月的攻击中，伊朗纳坦兹铀浓缩基地至少有 1/5 的离心机因感染该病毒而被迫关闭。

面对可能遭受的信息泄露或被利用做攻击的发起方，企业需要安装专业的企业级防护软件，采取有效措施避免。

2. 企业外部信息安全

2.1. 企业网站安全问题趋势分析

随着电子信息化的高度普及，越来越多的企业开始建立自己的企业官方网站，通过企业网站对外发布信息，以及进行相关产品发布宣传等。企业网站已经成为企业对外的一面镜子，折射出企业自身的形象。但是这面镜子在来自互联网的攻击面前却十分脆弱，很多企业由于自身官网被黑客入侵导致蒙受巨额经济损失，并严重影响了企业自身形象，造成用户流失等一系列恶意影响。

1) 网站漏洞遭受攻击方式：

根据 360 网站安全检测平台的抽样统计显示，75.6% 的国内网站存在高危安全漏洞，而 39.6% 的网站存在大量高危安全漏洞。黑客可以利用这些漏洞入侵网站系统，夺取最高权限，篡改网页内容，窃取数据库信息。

目前已知的各类高危网站漏洞大约有 1000 多种。不过，从 360 网站卫士拦截漏洞攻击的数量统计来看，遭黑客攻击量排名前两位的安全漏洞分别是：跨站脚本漏洞和 SQL 注入漏洞。针对这两个漏洞的攻击量之和，占到了网站卫士拦截的漏洞攻击总量的 96.6%。另据 360 网站安全检测平台的统计结果显示，在所有被检测出存在高危安全漏洞的网页中，存在上述两种漏洞的网页占到了总量的 93% 以上。

高危：SQL 注入、任意文件操作、任意代码执行、任意命令执行、文件包含等

中危：跨站脚本攻击 (XSS)、CSRF、越权访问、其他逻辑漏洞等

低危：信息泄漏、URL 跳转、暴力破解等

另据 360 网站安全检测平台的安全性评分系

图 5

信息来源：360 互联网安全中心 (2013 年 1 月)

统显示，在首次接受安全检测的十个主要类别的网站中，政府网站的成绩排名垫底，平均得分仅为 35 分（百分制）。紧随其后的是高校网站，平均得分为 37 分。这样的成绩意味着，政府和高校网站非常容易被黑客入侵、篡改数据和窃取资料。

2) 拖库风险与篡改现象日益加剧

如前所述，由于大量网站存在高危安全漏洞，就为黑客入侵网站提供了可乘之机。2012 年，网站遭遇黑客攻击的事件频频发生，拖库与篡改的案例时有发生。所谓拖库，是指黑客入侵网站后将网站数据库中的数据导出。而黑客拖库的主要目标就是窃取用户的帐号、Email 和密码。

大量知名网站遭遇拖库

国内方面，2012 年 6 月，某知名网址导航被曝因 SQL 注入漏洞致使大量用户详细资料泄露；12 月，国内某著名电商网站曝出验证码设计缺陷，用户认证缺陷，可被暴力破解，导致大量账号信息泄露。

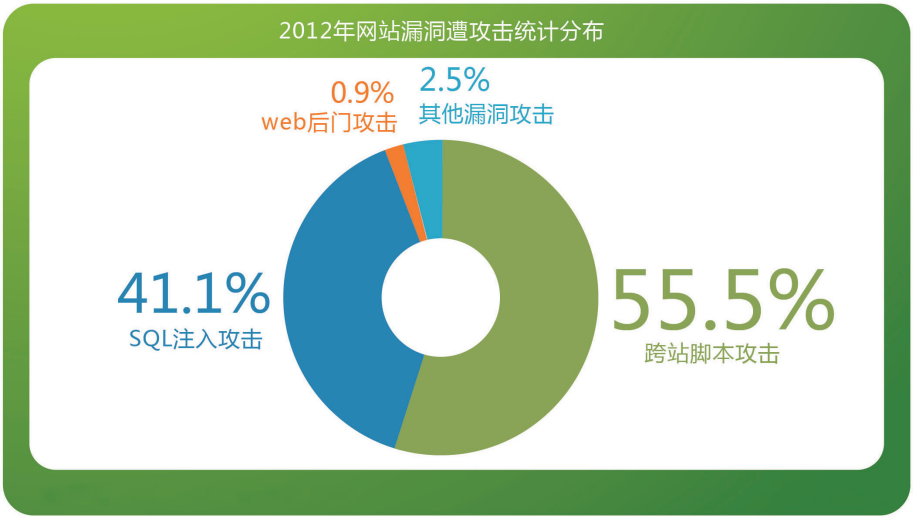
国际方面，2012 年 1 月，亚马逊旗下的电子商务网站 Zappos 被黑客入侵，2400 万用户的账户信息被窃取，被窃信息包括用户姓名、电子邮件、电话号码、住址、信用卡号的最后四位等。6 月，1500 万 eHarmony（相亲网站）密码和 3 万 LinkedIn（社交网站）密码被破解，遭破解的帐号和密码被公布在网络论坛上。7 月，雅虎旗下网站 Yahoo Voice 遭黑客攻击，45.3 万用户信息被曝光在网上，被张贴在网上的信息包括用户名和明文密码。

一个网站遭遇拖库，其他网站的用户帐号也会受到威胁。

3) 流量攻击威胁中小网站生存

除了网页篡改和拖库风险之外，中小网站往往还必须面对一种实际威胁更大的黑客攻击——流量攻击。流量攻击，简单地说就是攻击者在同一时间对某个网站发起大量的访问请求，当访问量大大超过网站服务器的承受能力时，就会造成网站系统瘫痪、服务器无响应、无法访问、无法登录等异常现象。

图 6



信息来源：360 互联网安全中心 (2013 年 1 月)

2012 年，360 网站卫士共接到遭遇流量攻击的网站求助 1297 起，平均每天拦截各种流量攻击 659 波次，平均每天约有 14% 的网站卫士用户遭到流量攻击。在网站卫士拦截的各种流量攻击中，CC（Challenge Collapsar）攻击最为常见，约占流量攻击拦截总量的 90% 以上。

根据 360 网站卫士的用户反馈：绝大多数的流量攻击都是竞争对手雇佣黑客进行的恶意攻击，也有一部分网站是因为拒绝了网上讹诈之后，遭到了黑客的报复打击。中小网站在面对流量攻击时往往束手无策，只能通过重新启动服务器的方式来恢复系统。但恢复后的系统仍然无法防御新的流量攻击。

由于流量攻击并非针对网站的任何技术漏洞，而是一种纯粹的挑战系统极限的暴力攻击，因此，理论上说只能通过增加网络带宽，提高服务器响应能力的方法来解决。但提高系统容量又势必大幅增加运营成本，这对于中小网站来说，通常是难以承受的。

4）病毒木马的绝对数量呈明显下降趋势

日均查杀黑文件数下降 25%（2011 年为 2800 万，2012 年为 2100 万），后台样本上传量和木马发现量持续下降，样本上传量从 2010 年底的日均 700 万下降到 320 万，木马日检出量从 60 万下降到 45 万。

5) 网络存储和共享成为木马新兴渠道

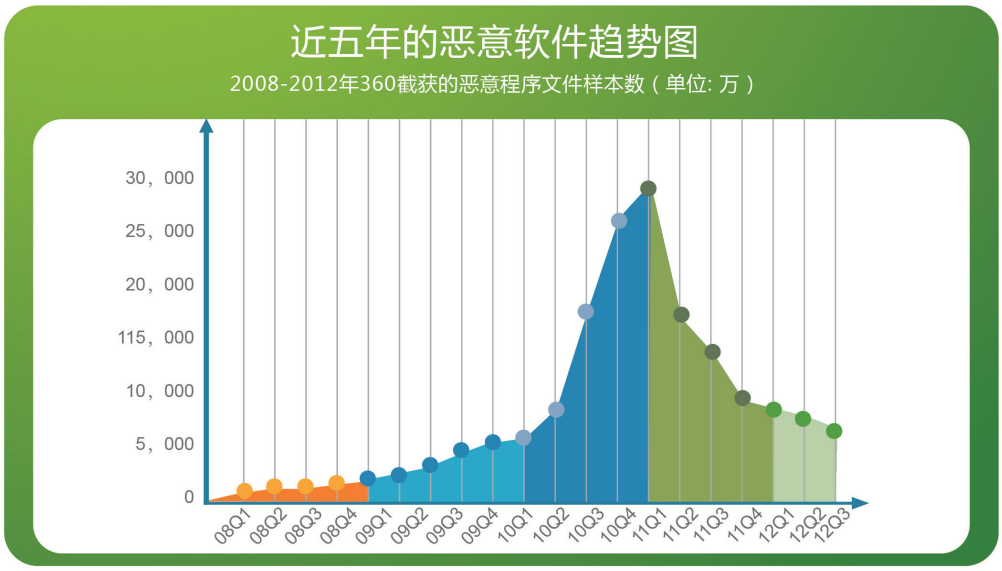
自 2010 年以后，安全浏览器的普及程度大幅提高，配合安全软件的共同使用，挂马网页的攻击成功率急剧下降。从图 8 中可以看出，360 互联网安全中心在 2011 年对挂马网页的拦截量为 2010 年的 12.9%，而 2012 年又仅为 2011 年的 14.0%。从这组统计数字来看，网页挂马对大众网民的危害已经日益减弱。

相应的，以云存储为代表的网络存储和共享服务开始被黑客利用藏毒传毒。2012 年，网盘服务流行度不断提升，娱乐、办公等用户间通过网盘分享文件愈发便利，一些黑客攻击者也开始将木马病毒伪装为热门网络资源，以分享网盘文件链接的方式进行传播。尤其是在微博等社交平台上，此类木马传播方式已相当普遍，值得用户高度警惕。

6) 钓鱼网站呈现快速增长势头

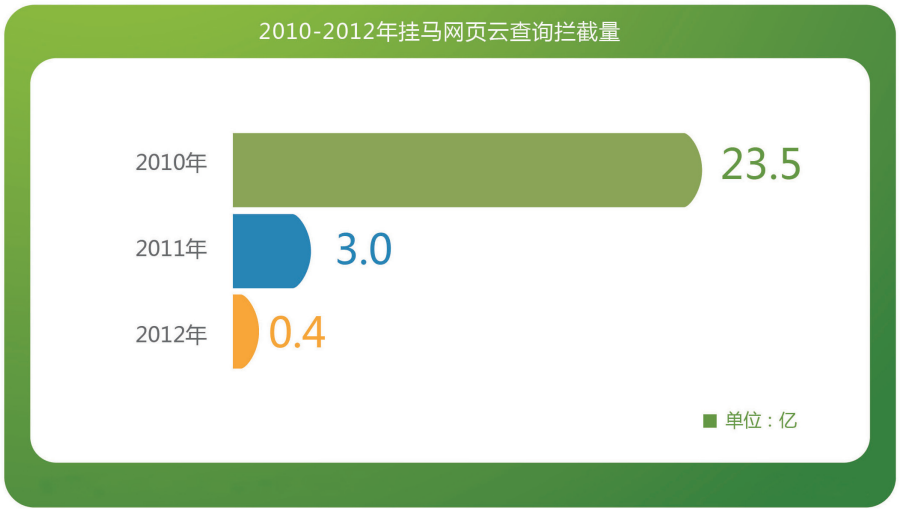
2012 年，360 互联网安全中心截获新增钓鱼网站 87.3 万个（以 Host 计算），较 2011 年增

图 7



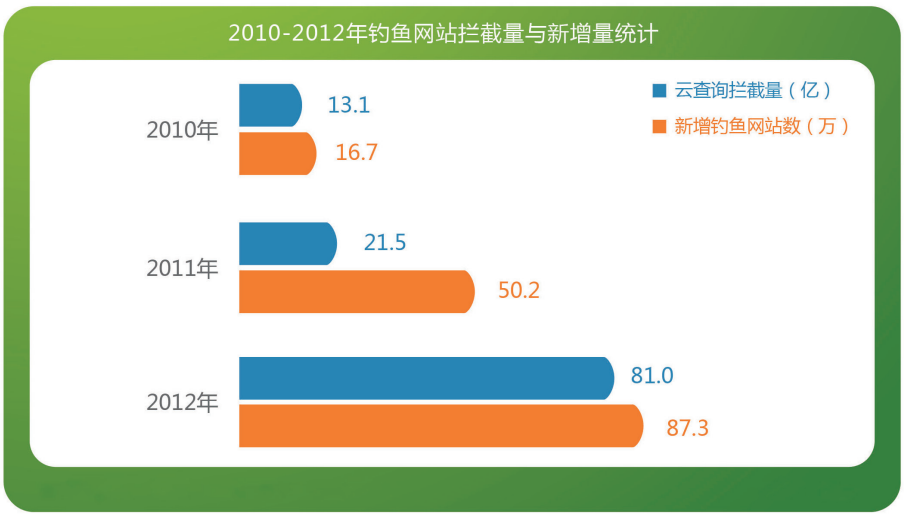
信息来源：360 互联网安全中心 (2013 年 1 月）

图 8



信息来源：360 互联网安全中心

图 9



信息来源：360 互联网安全中心

长 73.9%；钓鱼网站的云查询拦截量为 81.0 亿次，较 2011 年增长了 273.3%，是同期挂马网页拦截量的近 200 倍。图 9 给出了 360 互联网安全中心 2010-2012 年捕获的新增钓鱼网站数（万）和云查询拦截的钓鱼网站访问量（亿）。从图 9 中可以看出，钓鱼网站无论从数量上还是活跃程度上都呈现快速增长的势头。

从地域分布的角度看，钓鱼网站主要分布在境外地区（76.3%）和香港地区（13.2%），二者之和达到 89.5%。这也就为有关部门通过法律手段监管和打击钓鱼欺诈行为制造了很大的困难。现阶段，安全厂商通过技术手段来识别和拦截钓鱼网站，仍然是打击钓鱼网站最为切实可行的方式。

新型网络钓鱼的特性：

- 欺骗性：具有极大的欺骗性，网络钓鱼者利用自己的站点去模仿被钓网站的页面，类似于克隆一样，然后结合含有近似域名的网址来加强真实程度。网络钓鱼者甚至入侵正规的网站服务器，利用正规的网站进行钓鱼传播，让被钓鱼者难以分辨真假。

- 结合性：钓鱼者会利用网站、操作系统以及程序的安全漏洞进行钓鱼攻击，例如：利用浏览器或者网站的一些漏洞去构造钓鱼地址，或者利用漏洞等欺骗手段种植木马等等。

- 多样性：钓鱼者不会千篇一律地使用伪造网站和虚假邮件等手法，结合更多的网络服务如搜索引擎、社交网站、即时网络通信等，使用更多容易受骗的形式去骗被钓者，在更短的时间内得到最好的效果。

网络钓鱼欺诈途径：

- 基于搜索引擎的钓鱼攻击行为：

钓鱼网站与黑客进行合作、通过入侵控制权重高的政府网站、教育网站，通过劫持搜索引擎来获取流量。

- 基于木马的钓鱼攻击行为：

钓鱼网站以不可思议的低价来吸引用户浏览。让用户由网站上下载由木马伪装的“电子折扣券”或是“实物照片”。

钓鱼者通过即时通信软件的文件传输，透过社会工程学手段主动让用户接受文件，攻击者会声称某某商品大降价，请点击链接查看商品详情，点击的用户就有机会中招。

- 利用网站的 URL 跳转漏洞构造钓鱼网站链接

- 利用 HTTP Auth（基础连接认证）方式钓鱼漏洞骗取用户密码

将恶意链接作为图片网址发在论坛帖、博客文章和评论、邮件正文等处，使其他用户访问时页面自动弹出“登录框”。如果用户不加辨识，会误以为需要再次登录，就会将帐号密码发送到黑客服务器上。

2.2. 为什么企业网站容易遭到攻击?

1) 企业网站是 APT 攻击中的关键步骤

企业网站的受众主要是企业员工和客户，所以在针对企业的 APT 攻击中，攻击者往往会选择企业网站作为跳板。

360 互联网安全中心近期捕获的跨国生物制药企业凯莱英医药集团官网遭黑客入侵就是一个典型案例。黑客在其官网中英文站点均嵌入恶意代码，向凯莱英员工或来访客户电脑植入木马后门。技术分析表明，该木马传播时综合利用了 IE（三个漏洞）、Office、Adobe PDF Reader 和 Java 运行环境（JRE）的六个漏洞组合挂马，同时对攻击样本进行了变形免杀。

2) 企业网站本身安全隐患多，容易被攻陷

- **外包建站，代码质量差，缺乏后期持续的技术维护**

很多企业由于自身没有网站研发团队，将企业网站外包给建站公司制作，市面上很多建站公司开发水平参差不齐，更重要的是普遍的建站公司开发网站只考虑功能性，而不考虑安全性，在满足了企业网站的功能后便交付使用，此类网站很容易被通用的漏洞扫描程序检测出安全问题，从而进一步利用漏洞进行黑客入侵行为。由于是外包开发，当出现安全问题之后很难及时地修复安全漏洞，导致黑客可以长期控制企业网站服务器，将企业网站服务器变为黑客手里的“肉鸡”或者“跳板”，对企业自身的形象造成长期的恶意影响。

- **开源程序建站，缺乏安全运维意识**

目前市面上已经有许多开源的建站系统可供企业选择，常见的有 Dedecms、Discuz、phpcms 等。由于这些建站系统均是开源产品，意味着黑客可以通过研究这些开源建站系统

的源代码来挖掘漏洞。当黑客挖掘到一个开源建站程序的漏洞时，通过结合搜索引擎技术，批量搜索同样使用这套程序的网站，实现批量入侵。一般来说，系统开发商发现有黑客利用漏洞进行入侵行为后会尽快开发相应的补丁来告知用户，但是很多企业网站缺少专业的运维人员或者站长缺少安全运维意识，没有及时安装补丁或者根本不关注厂商官网发布的补丁更新信息，导致存在漏洞的企业网站长期暴露在互联网上，成为黑客攻击的目标之一。

- **企业网站开发人员缺乏安全编程意识**

由于人的因素不可控，导致很多企业网站在开发过程中就引入了安全漏洞，这些漏洞在测试环节缺乏有效的安全测试，上线后可以被漏洞扫描器检测，引发后续一系列的黑客攻击。网站开发人员不了解安全编程的同时也不了解黑客攻击，此类安全隐患在不借助第三方防御机制的帮助下很难被发现和修复。

3) 电子商务或在线交易的金钱诱惑

金钱对黑客来说永远是极大的诱惑。目前市面上已有很多开源的电子商务系统，同样也存在着一些安全漏洞，如果企业网站运维人员不及时安装补丁将会导致黑客入侵官网。此外，一些涉及到在线支付的企业网站通常会有很多第三方的接口，包括支付接口、授权接口、客服接口等，牵涉到第三方的接口越多，带来的安全风险越大，黑客可以通过入侵第三方的服务器来影响企业官网的整个支付流程，实现中间人劫持、伪造页面、篡改支付信息等攻击行为。

4) 企业间恶性竞争，攻击成本低

根据 360 网站卫士的数据分析显示，很多 DDOS 攻击都是企业所在行业内部的竞争对手发起，目前针对网站发起 CC 攻击的成本很低，通过代理或者一台普通的服务器即可发起大量 CC 攻击请求，目标网站由于无法处理大量访问请求从而导致失去响应，网站无法打开。遇到 DDOS 攻击时，企业网站自身没有有效的防御措施，只能购买安全厂商的防拒绝服务设备进行流量清洗或者使用 360 网站卫士此类的云防护解决方案。

2.3. 企业网站被攻击和入侵的危害

1) 企业被渗透，核心资料外泄等

企业网站作为防 APT 的一个环节通常是最脆弱的，黑客一旦通过企业网站将木马植入企业员工电脑中就很容易进行内部渗透，继而取得更高权限，进行窃取企业核心资料等侵害行为。

企业商业机密一旦外泄，将会给企业带来不可估量的巨大损失。

2) 在线交易等风险带来的直接财产损失

有电子商务业务的企业网站一旦被攻破，涉及财务的模块、企业收款账号等很可能被篡改，给企业带来直接的财产损失。

3) 网站被篡改、挂马导致被安全软件拦截，损失商誉

企业网站一旦被挂马、篡改等，就会被安全软件、安全浏览器拦截并提示风险网站，这样会对企业的商誉带来无形的损失。

4) 网站打不开，丧失商机

网站被 DDOS 攻击或者被当成肉鸡攻击别人，都会造成企业带宽被占满的情况，这样就会导致企业网站打不开。访问企业官网的客户打不开企业网站，会直接导致损失客户，失去商机。

信息来源：360 互联网安全中心

企业安全解决方案

1. 企业内部安全解决方案

通过边界 + 云端 + 终端的解决方案，解决传统安全防护检测手段单一、性能瓶颈、维护成本高、响应速度慢、应对手段单一问题。在云端安全中使用到分布式存储、分布式计算 / 并行计算、机器学习技术、准实时处理。边界方案中通过信息采集，进行协议还原对通信进行准入管理，攻击阻断。终端安全中实现网络准入控制、程序准入控制、硬件准入控制。

1.1. 边界防御

在企业边界部署边界防御系统，抓取和分析网络出口流量，并将样本和可疑 URL 送入沙箱，对样本进行分析。不需要完全依赖于已知的特征码，而是在沙盒机制中依赖样本执行过程当中发生的行为事实，检测来自邮件、网页、下载等的 APT 攻击，可以准确地发现使用 0day 等未知漏洞发起的攻击行为。

1) 网络嗅探模块

抓取和分析网络出口流量，并将样本和可疑 URL 送入沙盒进行分析。

2) 沙盒机制检测

通过虚拟执行引擎、高启发引擎、文件信誉云引擎、URL 信誉云引擎、QEX 和 AVE 文件和漏洞特征引擎、RVI 协议分析引擎。基于云计算和大数据技术，利用机器学习等人工智能方法，对数百亿文件和恶意网页进行鉴定，实现对未知文件和攻击的检测。鉴定程序、文档、压缩包和网址，高度启发和准确的规则，鉴别恶意行为。

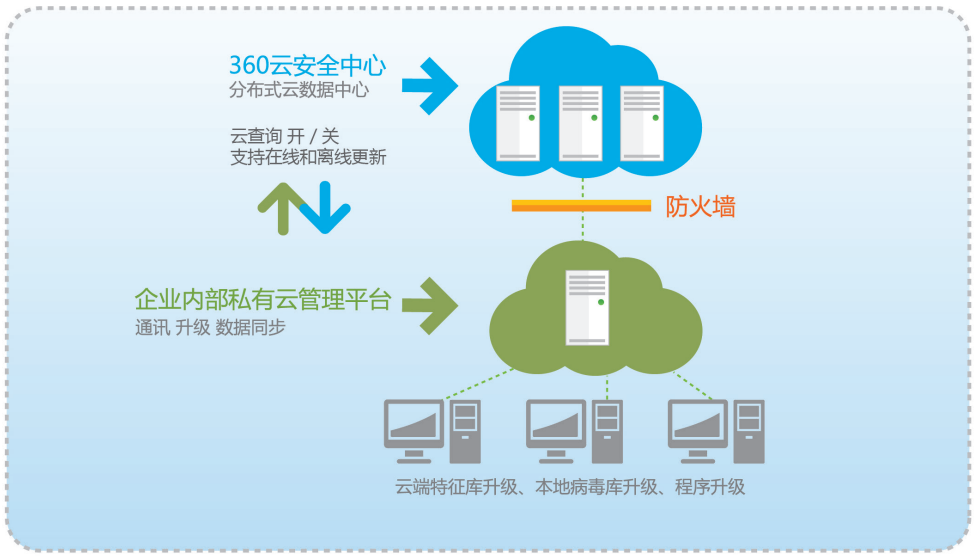
1.2. 云端防御

把云安全体系移植进企业内网，让企业用户享受云安全技术带来的高效及便利。建立私有云安全系统为企业打造的高度可控云安全解决方案。面对企业复杂的网络环境，提供内网云安全服务，能最大限度保障业务系统和数据安全，有效降低资源占用和运营成本。

1) 基于白名单技术

使用白名单技术，默认只允许白名单中的文件被执行，不在白名单中的文件都会自动被

图 1



信息来源：360 互联网安全中心

拒绝。即使这个木马利用了 0day，甚至有数字签名，也会被自动检测出来，从而有效防范未知的威胁。

2) 定制私有黑白名单

根据企业独有的合规性需求，自定义文件的黑白属性，形成私有黑白名单。同时，提供灵活的工具构建并更新安全基线。

3) 分级安全策略

根据不同的安全要求，预设安全区域分为核心区、办公区、客户区、自由区几种分级，每个分级应用不同的安全策略。这种分级既保证了核心区的安全，也满足了企业对安全控制的灵活程度的需求。

比如：跟业务数据相关的核心服务器，可以在同一套系统下享受更高规格的安全保护，未经管理员认证的程序，一律禁止运行并自动报警。这样，就算普通员工的计算机被突破了，想要获取公司机要数据还是非常困难。

4) 实时监控和预警

对终端进行实时监控，用户掌握过去每一台终端的文件活动（包括文件什么时候出现、在什么终端出现、文件路径、文件名、公司名、数字签名、文件大小等），并了解防护范围实时的情况，快速鉴定恶意软件从何而来并立即阻止恶意软件继续运行。

未知文件出现时管理员可获得及时通告预警。

1.3. 终端防御

1) PC 终端解决方案

为解决缺乏统一终端管理的安全问题，建议使用简单高效的管理控制中心，统一管理终端的安全软件，解决企业对安全统一管理的需求，能够提供全网统一体检、杀病毒、补丁修复、开机加速、软件管理、发送公告、流量监控、IT 资产管理等功能，解决企业用户普遍的网络安全问题，让网络安全管理变得很简单。同时，还能有效减少移动应用和 APT 攻击带来的威胁。

此外通过基于白名单的“非白即黑”软件准入技术，实现对终端的严格安全管控，只有在白名单中的软件方可安装和运行。

2) 移动终端解决方案

纵观 2012 年的手机安全形势，从持续激增的数据，到不断出现的新特点，都预示着用户将面临更多、更为严重的安全威胁。为此 360 互联网安全中心强烈建议广大手机用户，提高手机安全意识，通过如下四大建议确保用户手机安全。

- **尽量选择正规渠道购买手机**

报告显示，水货手机是目前木马和恶意软件的主要传播源头，其多会在出货前被“刷机”植入吸费、流氓推广木马等，且由于已嵌入系统底层，很难通过常规方式卸载清除。为此，360 手机安全专家建议用户在购买新手机时应尽量选择大型正规卖场购买手机，购买手机后，建议安装如“360 手机卫士”等专业安全产品对其进行扫描，避免手机暗藏恶意软件。

- **选择正规站点、渠道下载应用**

报告指出，通过下载应用而感染恶意软件的比例惊人，为保护用户的正常下载安全，360 安全专家建议用户尽量选择专业、可信的应用市场、官网，以及如 360 手机助手、360 软件宝盒等经过安全检测的渠道下载应用。

- **下载安装应用前，细心留意应用权限**

当前，通过篡改、伪装正常应用威胁手机安全的恶意软件，实际会在安装权限中有细微体现，如要求获取的权限与正常应用的获取列表有明显不同，如莫名要求得到敏感高危权限等，为此，建议用户在下载安装应用前，细心留意应用权限，避免被获取后威胁手机安全。

- **BYOD 解决方案**

有效地管理和控制自带设备的网络访问，提高自带设备用户的使用体验和工作效率。提供了接入点、控制器、安全、网络管理等所有必需的基础设施和基础架构，可帮助创建安全、高性能、支持更多设备访问的网络。

- 利用通过 MDM 集成实现的附加安全层保护移动设备
- 了解接入网络的人员、设备及位置，确保适当人员具有对适当信息的适当访问权限
- 基于网络和端点的设备识别和感知
- 对以有线或无线方式从设备传输到控制器或接入交换机的数据提供安全保护并进行加密
- 通过灵活的授权逻辑满足所有组织的策略访问控制需求
- 结合使用现有智能基础设施和可扩展的灵活实施机制

1.4. APT 攻击检测防御

传统的防火墙、入侵检测和防护系统等技术，难以有效发现 APT 攻击；以上边界 + 云端 + 终端的防御解决方案，通过建立基于大数据分析，多层次的检测防护方式，构成防御 APT 攻击的体系架构。

2. 企业网站安全解决方案

网站安全是一个综合性、多元化的问题，包括系统安全、数据安全、交易平台安全等，全方位解决安全问题需要完善的管理机制和专业技术保障。360 网站安全检测平台建议，网站应该从以下四个方面提升安全性：

2.1. 强化网站安全意识

1) 由专业技术人员进行安全维护

有些网站的 WEB 程序是外包开发的，而且网站程序的开发人员没有安全编程经验，极易造成各种漏洞。

图 2

信息来源：360 互联网安全中心

2) 及时为服务器操作系统和网站程序打好补丁

有些网站使用版本陈旧的程序，服务器操作系统也不注意更新补丁，存在大量广为人知的漏洞，当然会轻易被黑客利用入侵，成为傀儡主机。

3) 严谨的测试流程

在任何网站应用上线前，都应从安全角度进行测试，去除不必要的风险因素。

在用户交互环节，更应注意控制权限，过滤可能出现的威胁。

2.2. 定期进行网站安全检测

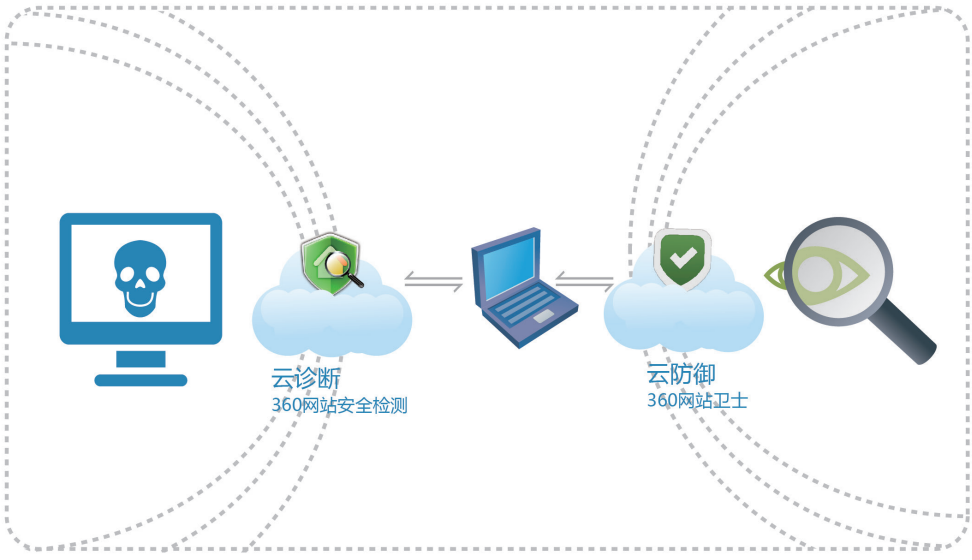
一些网站管理者认为，“在网络中不断部署防火墙、入侵检测系统、入侵防御系统等设备，就可以提高网络的安全性”。其实这样的认识存在误区，网站安全性低下根本原因在于，传统的网络安全设备难以抵御应用层的攻击，最有效的网站安全解决方案是修复漏洞。

在网站安全检测方面，360 网站安全检测平台提供了集“漏洞检测”、“挂马检测”和“篡改检测”于一体的一站式免费服务平台，拥有国内最全的网站漏洞检测库及强大的蜜罐集群检测系统，能够识别常见 WEB 服务器软件如 Apache、IIS、ngnix 等的一些常见安全漏洞；对 SQL 注入漏洞和跨站脚本 (XSS) 漏洞有较为准确的识别能力；能够对常见的 WEB 安全配置问题，如目录列表、管理页面暴露等常见安全配置漏洞进行检测外，还可在第一时间为高危 0day 漏洞提供修复建议。

2.3. 实时监控网站安全状况

网站被挂马篡改，会降低用户对其的信任度，更严重危害网络安全造成不良影响。此外，360 网站安全检测平台提供了实时的挂马监控和篡改监控功能，一旦发现网站被挂马被篡改，能够自动以邮件等方式通知站长，将网站蒙受损失的风险降到最低。

图 3



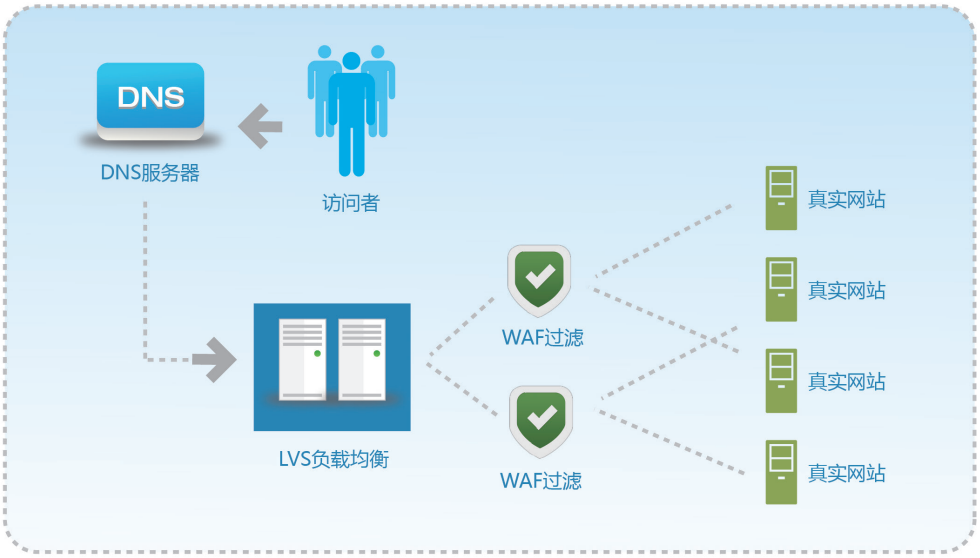
信息来源：360 互联网安全中心

2.4. 建立网站云防御体系

相对于传统安全厂商的网站安全解决方案，如 360 网站卫士提供了一种新的“隐身”模式，集成了 DDOS 攻击拦截系统、CC 攻击拦截系统、网站加速系统、抗攻击 DNS 系统，单服务器抗 DNS 攻击性能达到 500 万 QPS 防护能力，加入 360 网站卫士的网站会自动隐藏自己的 IP 地址，网站卫士将自己的 IP 信息暴露在外面，黑客和网站攻击者无法找到网站的真实 IP 信息，所有的 DDOS 攻击和 web 入侵都会经过 360 网站卫士的服务器，经过了 360 网站卫士的流量清洗和攻击识别过滤，将非正常的网站请求过滤掉，保证网站的正常请求访问。

通过此类云防护方案，企业网站可以做到“零部署、零安装”，能够快速将企业网站接入到云防护平台中，最大限度地减少部署安全防护机制中所需的人力、财力成本，实现实时高效稳定的整体安全防御。

图 4



信息来源：360 互联网安全中心

信息来源：360 互联网安全中心

关于 360 互联网安全中心

奇虎 360 科技有限公司（NYSE:QIHU）是中国领先互联网安全公司，360 为超过 4.5 亿用户提供高品质的免费互联网及手机安全服务。基于领先的云安全体系，360 为互联网用户解决上网时遇到的各种安全问题。

自从 2005 年 9 月成立以来，360 的员工人数已经超过 3500 名。2011 年 3 月 30 日，360 在美国纽约证券交易所挂牌上市（股票代码 QIHU），是迄今为止最早独立上市的中国互联网安全公司，目前 360 公司总市值已近 100 亿美元。正是基于不断进取和持续创新，创业八年来，360 公司的飞速发展堪称业界奇迹。

用户基数

- 360 的 PC 端产品和服务的月活跃数达到 4.61 亿，市场渗透率达 96%
- 360手机卫士的智能手机用户总数约3.38亿，市场渗透率达 70%
- 360 浏览器的用户数达到 3.3 亿，市场渗透率达 69%

360互联网安全中心

产品和服务

核心安全产品：

- 360 安全卫士
- 360 杀毒
- 360 手机卫士

云服务

- 云安全体系

平台产品

- 360 浏览器
- 360 手机助手
- 360 个人起始页
- 360 安全桌面

在线广告

- 在线广告服务
- 360 搜索

互联网增值业务

- 第三方网页游戏

操作系统

- 远程技术支持
- 网站安全服务