KASPERSKY lab

企业需要自适应的安全系统

十年前，我们无法想象现在所面临的威胁情况。网络罪犯已具备入侵传统防护系统的技术，并可潜伏在系统中数月甚至是数年而不被察觉。企业应该采用以情报为基础的多层级IT安全解决方案。

“智能就是适应变化的能力。”

– 史蒂芬·霍金

企业需要自适应的安全系统

高级可持续性攻击（APT）是一种可进行针对性攻击的复杂的恶意软件，是企业面临的不断进化的新威胁之一。网络罪犯非常清楚基于边界安全的传统防护系统的局限性。这是他们寻求突破企业防护系统的第一步。

攻击者正在不断演化，而多样化的企业信息技术也沦为网络罪犯眼中的攻击向量：移动设备、网页应用、可移动存储设备、虚拟化与云计算技术。所有这些都为网络罪犯提供了可趁之机。更重要的是，单靠传统的“防御与拦截”安全技术不足以解决上述问题。

企业需要以预测、防御、检测与响应等技术为核心的具有更强适应力的全面安全解决方案。

企业自适应安全解决方案的四大核心

预测：没有人可以预言未来，但是我们可以采取措施使企业获取最新的威胁情报与相关趋势，以预测并避免攻击事件的发生。通过攻击拓展预测分析使员工认识到攻击使用的策略；取证分析安全事故可提升员工吸取教训的能力，而渗透测试则有助于发现企业网络中的薄弱环节。

防御：旨在减少攻击面。从传统意义上讲，基于特征的反恶意软件、设备控制或应用程序漏洞修复只是起到强化系统安全、为病毒攻击设置若干障碍的作用。这仅仅是整体安全解决方案中的两个组成部分，其还应具备限制病毒蔓延速度与降低其影响力的能力。

检测：卡巴斯基实验室对重大高级可持续性攻击的研究表明，复杂的攻击可潜伏数年而不被发现。平均来讲，企业威胁可潜伏200多天不被察觉1；而攻击事件发现的越早越好。最佳威胁分析所突显的检测技术表明：随着威胁的演化，最佳检测策略通常建立在发现攻击事件及其后果的能力的基础上，而该事件则意味着网络罪犯已经实施入侵。

响应：有效的企业安全解决方案能够响应并减少攻击事件的入侵影响。一方面，自动启动的程序可涉及“如果/那么”策略，如漏洞修补。另一方面，该系统可包括攻击之后的分析或借助于专业攻击事件响应团队阻止和调查网络攻击、病毒入侵以及其他安全事件，并减少相关影响。

为获得最佳效果，上述核心技术必须作为多层级安全解决方案协同工作。

全面自适应企业安全架构的关键特征包括以安全情报和策略为基础、专注于威胁、全面整合、综合性。卡巴斯基实验室可提供独一无二的自适应企业安全平台，以下为其关键特征。

情报在手，企业安全无忧

卡巴斯基实验室率先发现众多重大威胁，包括：

- Carbanak：世界上最大的银行大劫案
- 黑暗酒店（Dark Hotel）：以高级商务旅行人员为主要攻击目标
- The Mask/Careto：主要攻击企业、政府以及私募股权公司
- Wild Neutron：主要攻击跨国公司与其他企业
- Icefog：主要攻击商业供应链
- 红色十月（Red October）：利用企业系统实施大规模间谍行动

超过三分之一的卡巴斯基实验室员工专心致力于技术研发，以应对并预测不断演化的网络威胁。卡巴斯基实验室专业的情报与分析研究团队每日都会对网络威胁进行调查。

卡巴斯基实验室非常了解全球最复杂威胁的内部工作原理，因而能够研发出具有战略意义、将多层级安全技术与服务合二为一的产品，从而为企业提供全面整合

的自适应安全系统。凭借强大的专业技术，卡巴斯基实验室在权威的独立威胁检测与查杀测试中屡获第一。

预测

对网络威胁的预测能力以及由此创建的预防策略是卡巴斯基实验室的核心所在，从我们专业的全球研究与分析团队（GReAT）到卡巴斯基安全网络（KSN）以及安全情报服务（SIS）：

卡巴斯基安全网络：作为卡巴斯基实验室多层级平台的最重要组成之一，卡巴斯基安全网络是一种专门用于从全球数百万系统中收集并分析安全威胁情报的基于云的复杂分布式架构。

卡巴斯基安全网络是基于云的全球性威胁分析实验室，可在数秒种内发现、分析、高效管理未知、高级网络威胁与在线攻击来源，并且直接向客户系统发送安全情报。对于在特定数据方面存在保密性需求的企业来说，卡巴斯基实验室专门研发了卡巴斯基私有安全网络系统（Kaspersky Private Security Network）。

安全情报服务：企业一般不具备足够的资源开发出高级别并且能够与不断演变的复杂威胁保持同步的策略性安全情报。为此，卡巴斯基实验室开发了多样化的情报服务：

教育与培训：卡巴斯基实验室面向企业用户提供全面的线下与线上培训服务，其内容涵盖普通的网络安全基本原理以及高级数字取证、恶意软件分析与逆向工程培训。除了互动游戏，还提供技术评估与综合网络安全提升课程，课时为2-5日，包括以下主题：

- 网络安全基本原理：认识网络威胁，安全地使用技术。
- 初级数字取证：建造数字取证实验室、事故重建以及工具。
- 初级恶意软件分析与逆向工程：建造安全的恶意软件分析环境，进行迅速分析。
- 高级数字取证：深度文件系统分析、恢复删除文件、事故时间轴重建。
- 高级恶意软件分析与逆向工程：分析开发壳代码、非Windows恶意软件、使用全球最佳实践。

安全评估：

- 渗透测试：从网络攻击者角度理解基础设施的安全，同时符合安全标准，比如PCI DSS。
- 应用安全测试：网络应用程序（包括在线银行与WAF启动的程序）、移动应用程序与多功能客户端分析。

威胁情报：

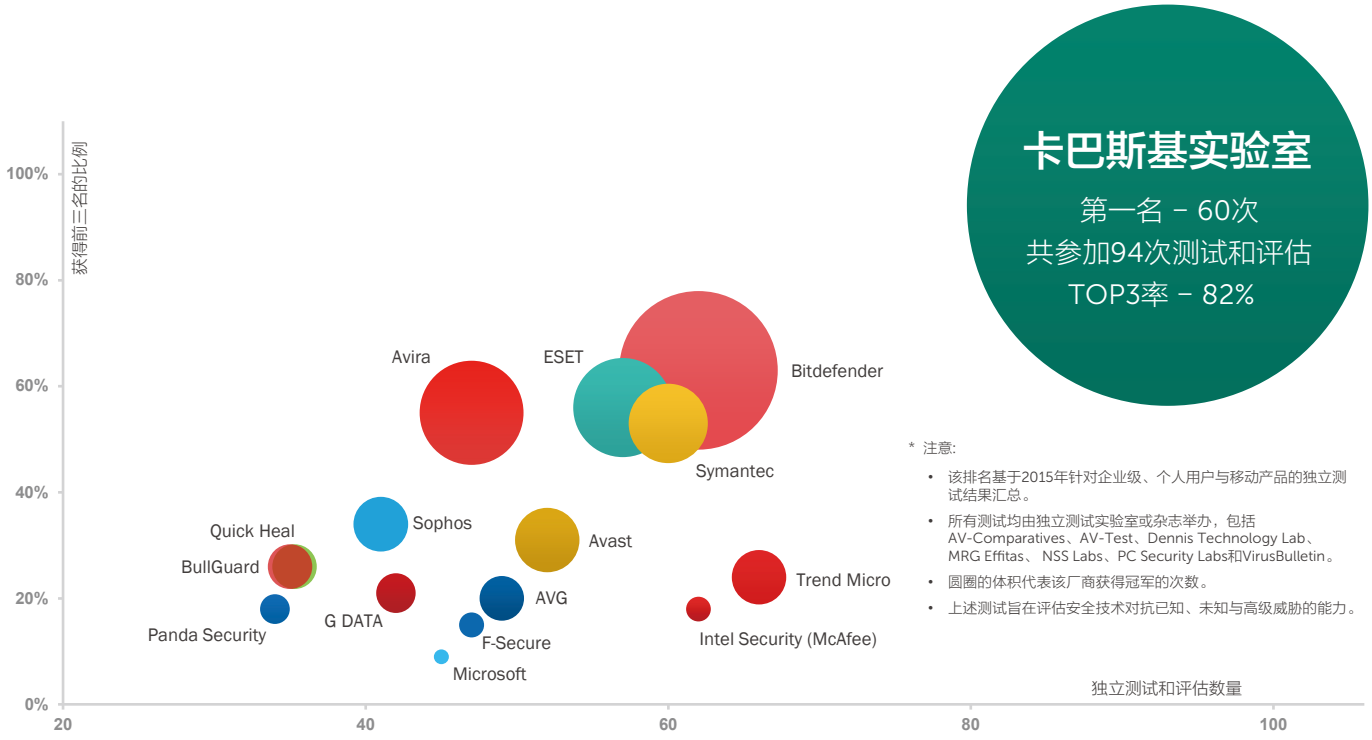
- 威胁情报是一个以GReAT专业知识为导向、由KSN支持的预警系统，包括安全威胁数据服务、僵尸网络追踪与情报报告。及早获取APT相关的配置文件和恶意软件样本以及与安全信息与事件管理整合（HP Arcsight）集成有助于企业获得综合的情报洞察力。

防御

卡巴斯基实验室日均检测出32.5万个新兴恶意软件。检测率每增加一个百分点，就可多检出成千上万个恶意软件。众多权威独立测试结果表明，卡巴斯基实验室可提供业界最佳的防御系统。2015年，卡巴斯基实验室产品共参加94次独立测试和评估，在这些测试中，我们的产品共获得60次第一名，获得前三名的次数为77次。这就是Microsoft、Cisco Meraki、Juniper Networks和 Alcatel Lucent等设备制造商信赖卡巴斯基实验室为其自身产品提供安全方案的原因之一。

卡巴斯基实验室再次登顶2015全年测试成绩评比榜首

卡巴斯基实验室连续三年登顶互联网安全保护TOP3保护排行榜榜首，表明卡巴斯基实验室产品能够提供业内最佳的反网络威胁保护。2015年，卡巴斯基实验室产品共参加94次独立测试和评估，在这些测试中，我们的产品共获得60次第一名，获得前三名的次数为77次。



我们的企业安全解决方案将业内领先的恶意软件与多重安全技术相结合，形成以情报为导向、减小攻击面的独特综合技术。

通过多个防护层级防范已知、未知和高级威胁。这些防护层包括：

网络攻击拦截：使用已知签名扫描所有网络流量，以发现并拦截基于网络的攻击，包括端口扫描与拒绝服务攻击（DoS）。对于更深层次的保护，可选择Kaspersky DDoS Protection（KDP）作为保护方案，以防止分布式拒绝服务（DDoS）攻击。这是一个全面且综合的DDoS防护解决方案，包括全天候分析与病毒攻击报告。

启发式反网络钓鱼：通过寻找可疑活动的额外证据，以及以传统网络钓鱼数据库主导的技术，可阻止最新的网络钓鱼攻击。

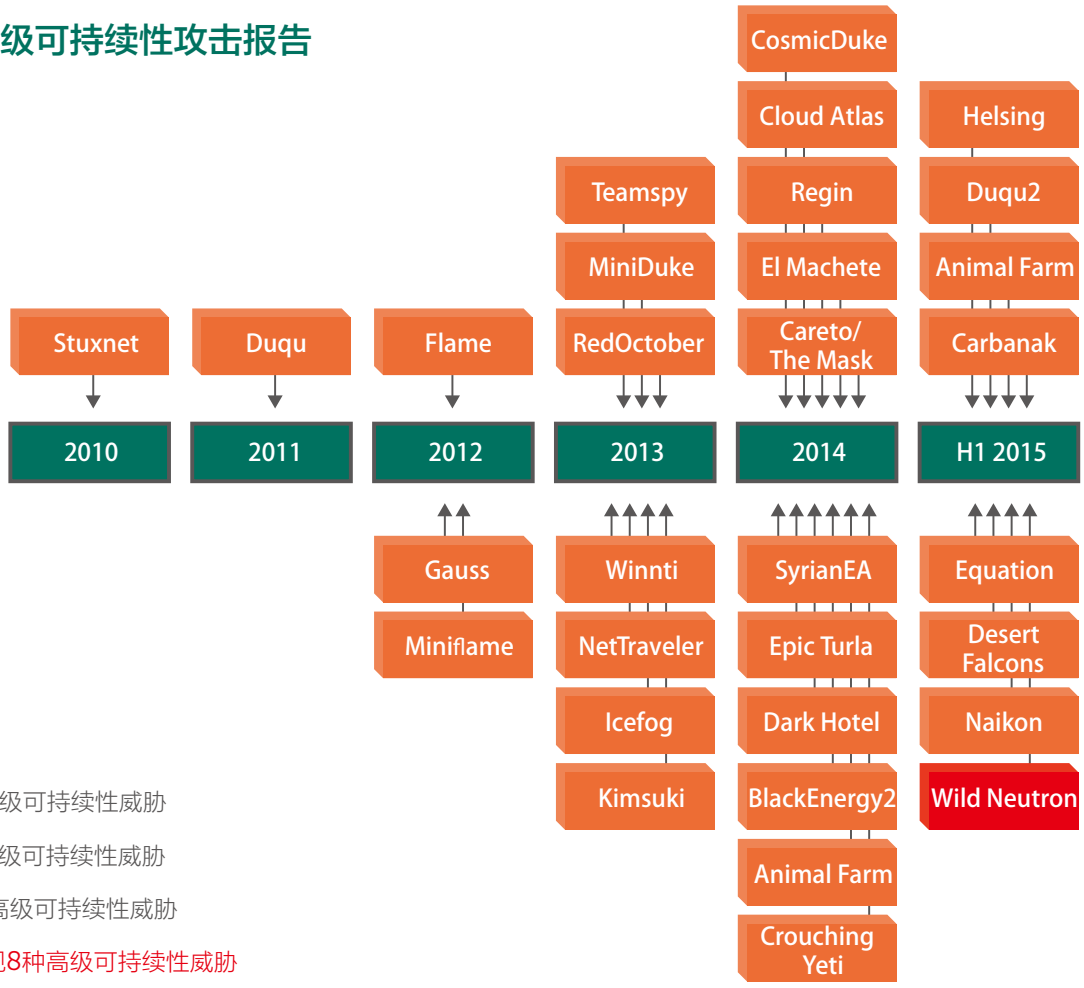
应用程序控制以及动态白名单：应用程序控制阻止或允许管理员指定的应用程序。该方案基于动态白名单、卡巴斯基实验室不断更新的信任应用程序列表以及软件类别而建立。

主机入侵防御系统（HIPS）：控制应用程序的行为，并限制执行具有潜在危险的程序，而不影响授权的安全应用程序性能。

检测

卡巴斯基实验室具有检测全球范围内最复杂安全威胁的独一无二的专业技术，可直接应用于企业安全威胁检测系统中。2008年以来，卡巴斯基实验室率先发现了众多史上最复杂的网络攻击。这些经验和情报被直接运用到我们的产品开发当中。卡巴斯基实验室不仅拥有一流的复杂企业攻击的检测能力，还利用从发现重大的金融威胁病毒，如Carbanak病毒所获得的洞察力，来研发针对金融欺诈威胁的检测方案。

卡巴斯基实验室高级可持续性攻击报告



2012年–发现3种高级可持续性威胁

2013年–发现7种高级可持续性威胁

2014年–发现11种高级可持续性威胁

2015年上半年–发现8种高级可持续性威胁

响应

在适应性安全架构中，响应威胁的能力与预测和预防威胁的能力同等重要—同样能够为企业节省时间和金钱。另外值得一提的是，提升检测能力的直接结果就是响应能力的提高。卡巴斯基实验室从技术和服务两个层面来解决“响应”问题：

系统监视程序：卡巴斯基实验室的独家主动监测程序能够应对复杂的系统事件，如驱动程序的安装和检测可疑行为。

调查服务：卡巴斯基实验室可帮助实时解决安全事故。从恶意软件分析到数字取证、报告与事件响应，在减轻攻击影响和恢复受损系统的同时，用户可从中吸取教训。

以情报为导向的企业安全解决方案

恶意软件被“广泛传播”这样的说法不免有些轻描淡写：高级威胁可避开传统拦截技术。只花几个小钱就能购买到现成的恶意软件工具包——从一个恶意软件自动创建多个定制变体的工具。而这些都只不过是大规模恶意软件的冰山一角。

威胁日趋复杂，因此企业需要多层级的自适应安全解决方案。该方案应结合多种整合技术，能够全面检测和防御已知、未知和高级威胁以及其它以企业为目标的威胁。

卡巴斯基实验室在发现最复杂的威胁方面成绩斐然。结合其业界领先的技术和服务，卡巴斯基实验室可提供企业所需要的全面的自适应安全系统。卡巴斯基安全网络以全球范围内逾6000万节点产生的实时情报为基础；同时，卡巴斯基实验室全球研究与分析团队为威胁研究提供了独家技术和专业知识，从而能够开发出对抗复杂威胁的解决方案。

企业、政府与监管部门值得信赖的合作伙伴

卡巴斯基实验室是一家私营企业，因此能够不受短期市场的约束而在产品研发方面大力投资。我们拥有3000名员工，其中将近半数从事研发工作，专注于开发创新技术，调查网络战争、网络间谍活动和所有类型的威胁与技术。

卡巴斯基实验室专注于优质内部研发，被公认为IT安全技术领域的领导者。这就是世界100多家设备制造商信赖卡巴斯基实验室并制定我们为其产品提供安全方案的原因之一，包括Microsoft、Cisco Meraki、IBM、Juniper Networks 和 Alcatel Lucent等。

也正是因此，我们成为了政府、执法机构和世界各地大型企业信赖的合作伙伴。一些知名的权威组织机构，包括国际刑警组织、欧洲刑警组织和众多计算机应急响应小组，都邀请卡巴斯基实验室与其合作并为其提供持续的咨询服务；除了为国际刑警组织和许多国家的警务人员提供定期的培训课程之外，我们还协助创办了国际刑警组织的数字取证实验室。

关注卡巴斯基官方微信
获取实时权威安全资讯

公众号　　订阅号

卡巴斯基实验室
www.kaspersky.com.cn

关于互联网安全：
www.securelist.com

寻找附近的合作伙伴：
www.kaspersky.com.cn/partners

KASPERSKY lab