企业安全威胁统一应对指南

2017最新版

FREEBUF

前言

研究背景

近年来，网络安全的国际形势日益严峻，不断增长的安全威胁给企业和个人都带来巨大的挑战。而了解2017年安全行业的威胁动态和企业能够实际采取的应对方案，有助于帮助企业做出许多重要决策。

2017年网络安全在**政策法律因素**、**IT技术发展**、**网络安全事件**及**黑色产业**多重因素影响下产生了变化。网络安全逐渐步入智能时代，而传统安全的边界日渐模糊，整体趋势呈现增长和多样化的态势。了解当前的威胁形势，熟悉企业安全应对流程并选择合适的安全产品变得尤为重要。

我们希望此份2017年度企业安全威胁统一应对指南能够帮助您了解当前形势，并通过下文内容向您提供更多有关信息安全业务决策的信息。

如需了解更多信息，请访问www.freebuf.com/paper查看过去发布的安全报告。

研究主要发现

FreeBuf是国内关注度最高的互联网安全媒体平台，同时也是信息爱好者们交流与分享安全技术的最佳社区。

本报告为FreeBuf研究院于2017年度Q3撰写的研究报告，主要针对国内外企业网络信息安全现状，梳理出了安全行业态势、发展前景、安全威胁、应对流程以及安全产品推荐名录为一体的《2017 企业安全威胁统一应对指南》。

在此份《企业安全统一应对指南》中会显示：2017年网络安全行业发展趋势、主要安全威胁、企业安全应对流程以及国内外推荐安全产品名录。

简而言之，网络安全作为企业业务的重要基础设施之一，如今得到了越来越多企业的重视。了解年度行业动态、把握安全威胁、应用安全应对流程，掌握这三个要素，是企业保障业务安全和赢得用户信任及未来稳定增长的关键。

- 信息安全智能时代悄然来临，到2020年，基于深度学习的智能机器将进行10%的渗透测试，而在2016年这一比例为0%。
- 相比较为陈旧的IDS，新兴技术有望更快地走入我们的视线，到2020年，85%的大型企业都会使用CASB技术增强企业的安全检测能力。
- 传统安防流程规划及针对新威胁的管理检测和响应同样重要，到2020年，预测将有15%的中大型企业将使用MDR，而今天却不到1%。
- 政策因素、IT技术革新和企业安全事件因素将持续驱动信息安全产业持续发展，预计未来三年内企业的安全支出仍会不断扩大。
- 企业的业务需求、应用复杂度让传统的边界不再坚固，在企业内部生产网络、测试环境和其他情况中，他们遭受威胁和攻击的可能也在日益增长。

目录

第一章 概述

2017年企业安全发展状况

当前信息技术持续高速发展的大背景下，互联网对全球政治、经济、社会和文化的影响愈发深远，网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，围绕信息获取、利用和控制的国际竞争日趋激烈，保障信息安全成为世界范围的重要议题。下面就从政策法律、技术革新、安全事件和地下产业等方面，概括一下 2017 年信息安全行业中的发展现状。

一、政策法律驱动网络安全行业发展

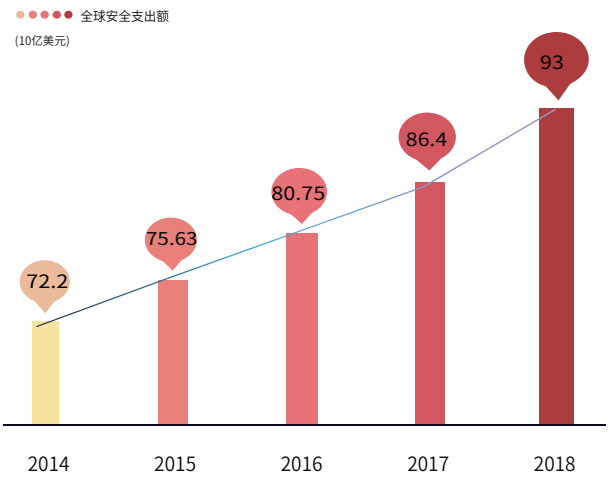
国内层面上，2017年6月1日起《网络安全法》正式施行。第十二届全国人大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，习近平主席签署第五十三号主席令，予以正式公布。《网络安全法》包括总则、网络安全支持与促进、网络运行安全、一般规定、关键信息基础设施的运行安全、监测预警与应急处置、法律责任、附则等七大章，自2017年6月1日起施行。《网络安全法》生效以来，与其相关的执法行为逐渐走向常态。作为我国第一部全面规范网络空间安全管理的基础性法律，它的施行标志着我国网络安全从此有法可依。

其次，工信部出台的《信息通信网络与信息安全规划(2016-2020)》也于今年正式发布。《规划》围绕贯彻落实习近平总书记关于网络安全和信息化工作的系重要讲话精神，立足信息通信行业网络与信息安全管理职责，紧扣“十三五”期间行业网络与信息安全工作面临的重大问题，对“十三五”期间行业网络与信息安全工作进行统一谋划、设计和部署，是“十三五”时期信息通信行业网络与信息安全工作的指导性文件。

而在国际层面，欧盟成员国将在两年的时间内将《一般数据保护条例》中规定的条款纳入本国法律，该条例将于2018年正式生效。《条例》加强了对欧盟所有企业及个人、物联网的隐私保护，并简化了数据保护的管理流程。《条例》将替代1995年的欧盟提出的《数据保护指令》，在政策指向上从原来的只提供了指导意见而不执行的转变成了具体的规则与处罚相结合的做法。《一般数据保护条例》明确规定，任何机构如果收集、传输、保留或处理涉及到欧盟任何人的个人信息，其中可能包括姓名、电邮地址、计算机IP地址、照片、社交媒体帖子、医疗信息或财务信息的话，就必须遵守GDPR 。该法规不会考虑机构的地理位置，或者个人身份信息是否关系到个人隐私、专业水平或公共生活。GDPR的处罚手段会相当严厉，不遵守《一般数据保护条例》的后果就将面临严厉的制裁及巨额罚款。

由此可以看到，2017年国内外一系列法律法规的出台，标志着网络安全在国家层面上得到的重视程度越来越高，企业及个人的安全意识也必将随之水涨船高，世界范围内的信息安全行业都将迎来更积极、更主动、以及更大的市场和舞台。

全球安全市场增长情况



二、IT技术革新注入安全行业创新动力

2017年出现的IT行业技术革命包括：基于云和传感器的物联网技术进一步普及，基于大数据分析、计算机视觉和深度学习的智能化和自动化技术也日渐成熟，AI正在逐步从学界研究走进行业，安全行业也越来越多地涉足此类技术的应用。

据德勤预计，2017-2019年，针对人工智能的投资将会达到313亿美元。基于海量数据进行复杂分析，提高企业产出绩效，技术的进步能够让工作自动化。从机器学习到深度学习，人工智能的发展目前仍处于浅智能阶段，但在特定领域的应用已经达到甚至超过人类的水准。有观点表示，未来的人工智还可能成为网络安全的救世主。

据Gartner预测，到2020年，基于深度学习的智能机器将进行10%的渗透测试，而在2016年这一比例为0%。另一方面，也有人提出警告：AI可能可以助于保护网络安全，但绝非银弹。如果机器学习如果能够学会检测恶意程序，那么它也可以被黑客用来躲避检测。其次AI在面对攻击时的表现依旧不稳定，在数据处理上的部分阶段也还有很多人工依赖。

物联网——物联网（IoT）提供了计算机感知和控制物理世界的接口和手段，它们负责采集数据、记忆、分析、传送数据、交互、控制。从2016年下半年到今年，可以看到全球物联网的机会窗口已经打开，物联网基础设施、物联网企业数据、物联网应用等技术发展趋势正在加速。

专注于物联网通讯发展的研究单位Ovum于2017年全球物联网会议（Internet of Things World 2017）上提出，低功率广域（Low Power, Wide Area，LPWA）网络、更多元的分歧需求、信息安全、大数据和机器学习、物联网即服务等新技术和新需求，将是2017年物联网产业的重要发展趋势。

新的构架平台——2017年，新的架构平台将以“云第一”为指导思想，构建更加灵活的标准化体系结构模型，总体上更高效、成本更低，可以显著提升转化率。新架构的发展趋势是更多地采用宽容的联动体系，基于核心程序联动各个应用层，发展分布式项目。其开源性同样重要，未来的企业服务如果仅仅依靠自己的员工，可能永远不会解决所有客户的需求。此外，涉及体系框架时应考虑可能出现的错误，注入系统组件，提高容错性。同时，云计算提供了强大的大规模并行计算能力，也使得数据处理能力前所未有得强大。

根据Gartner预测，2017年基于云的安全服务市场规模将达到41亿美金，云安全的发展将受益于云计算市场的快速增长。当然，伴随着机遇而来总是更多的挑战。多租户环境下的信息安全、虚拟化和私有云安全安全以及SaaS可视化和控制，将成为企业云安全建设之路上面临的几大重点问题。

三、企业安全事件频发聚焦社会关注

2017年出现多起席卷全球的勒索病毒事件和多家著名企业大数量级别的数据泄露事件，网络犯罪者、攻击者和地下产业纷纷浮出水面，网络安全事件聚焦社会各界的关注。

勒索软件席卷全球：5月12日晚，Wannacry蠕虫勒索软件袭击全球网络，对计算机内的文档、程序实施高强度加密，并向用户索取以比特币支付的赎金。100多个国家的数十万名用户中招，被认为是迄今为止最大的群体勒索事件。Wannacry利用被黑客泄露的永恒之蓝漏洞进行攻击，然而微软其实早在今年三月就已经发布了MS17-010漏洞修复补丁，但大量用户并没有及时进行更新，最终遭到攻击。

6月27日晚，乌克兰等多国遭遇NotPetya勒索病毒袭击，政府、银行等重要系统受攻击影响。这次黑客使用了NotPetya勒索病毒的变种，依旧利用永恒之蓝漏洞进行加密勒索。但更为激进的NotPetya直接加密系统的MBR导致机器无法启动，断绝恢复的可能。

企业数据泄漏事件频发：随后的下半年里，企业数据泄漏事件则开始频频发生。顶级防务公司BoozAllen Hamilton 泄露了60000 份文件，包括员工的安全凭证和美国政府系统中的密码；美国电信巨头Verizon先后发生两起数据泄漏事件；Omaha 投票选举公司的软件系统（ES& S）泄漏180万芝加哥选民的个人信息；华尔街日报的母公司道琼斯泄露了220万客户的个人资料；四大中的德勤和埃森哲也先后曝出数据泄漏问题。而近期最知名数据泄漏事件当属美国征信机构Equifax泄露事件。

该公司自5月下旬至7月起遭受黑客攻击后泄漏了1.45 亿美国公民个人敏感信息，其中包括了社会保障号码，出生日期、地址及部分驾照信息。此外，被泄露的还有20.9万美国消费者的信用卡号，部分英国和加拿大居民也受到牵连。

同样在2017年，国内也发生了多起恶性数据泄露事件。3月7日，公安部网站宣布破获一起特大窃取出售公民个人信息案，犯罪分子入侵多家国内互联网公司服务器，窃取公民个人信息50多亿条。随后网上便出现了“京东内鬼泄露50亿条公民信息”的传闻，京东发现后向公安机关提供线索协助破案。此后，58同城、优酷等网站也纷纷中招，大量用户数据信息被泄露。

规模化、产业化，暗网黑产暗流涌动：除此之外，2017年黑色产业也逐渐形成完整且发达的产业链。暗网勒索软件的定制和交易、DDoS攻击业务都浮出水面，黑产核心的变现促使产业链中出现了流量牵引、分发等分工。2017年10月Carbon Black 研究报告显示，暗网市场上的勒索软件软件产品已多达 45 000 种，在超过6300个暗网市场上进行销售。仅勒索软件定制及销售产值就从2016年的249287美元增长到6237248 美元，增长率达到惊人的2 502%。

立足2017，眺望企业安全未来

一、信息安全的智能时代正在悄然来临

随着信息安全行业中攻防技术的不断升级，以往相对完善的安全产品与体系早已不再坚不可摧，传统安全产品误报率高、维护成本高、扩展性不强、攻防不对等等问题日益显露。安全市场上的需求水涨船高，企业越来越不满足于“够用”的安全，而是提出更高的要求的防护目标。安全攻防技术升级，世界范围内越来越多的安全公司开始将人工智能、机器学习、自然语言处理等技术运用到安全产品中，加强自己的安全防御能力。深度学习技术分析用户行为区分普通行为和异常行为，对涉及企业业务的数据操作进行归类和机器分析，实现更实时高效的响应、降低误报率。

二、传统安全边界已经日渐模糊

信息化时代传统行业的数据化、在线化、移动化让企业、人和各项服务都与网络深层地绑定，过去相对独立、分散的网络已经融合为深度关联、相互依赖的整体。企业在不断连接和网络化的进程中获得了更好的产出效果，却也让传统的网络边界日益模糊。企业的业务需求、应用复杂度让传统的边界不再坚固，在企业内部生产网络、测试环境和其他情况中，他们遭受威胁和攻击的可能也在日益增长。

其次，企业员工的个人设备，尤其是移动设备的普及，也使得企业企业安全防护的边界变得模糊。BYOD（员工自带设备办公）的大规模应用打破了企业内外网的隔断，移动化的属性让企业难以对这些设备进行管理和限制，多数企业都难以防护这些个人设备上的数据交换行为。

三、安全威胁呈现多样化增长趋势

APT攻击常态化——大数据时代背景下，用户信息遍布网络，为黑产社工库提供了充分的养料。以往分散式攻击变得越来越没有效率，攻击者更加倾向施以专注、专业、持续的APT攻击，以期获取大量核心的机密数据，从而造成巨大破坏，取得最大利益。

攻击门槛日益降低——Wannacry勒索软件的源头，正是NSA永恒之蓝漏洞泄露导致的，其后又有notpetya等攻击事件接连发生。其实Wannacry勒索软件本身的技术含量并不高，但假设今后有更多类似永恒之蓝的“武器化”漏洞被公开售卖甚至开源的话，无疑会导致黑产进攻攻击的门槛进一步降低。

物联网（IoT）设备成为薄弱环节——近年来IOT设备规模增速日益提高，预计到2020年将增长到200亿以上的数量级。IOT设备的代码大多较为脆弱，大多由不同的供应商提供，且安全策略普遍不强，这将成为一个巨大的攻击面。

DDoS攻击加剧——2017年以来，DDoS攻击总体上呈现出攻击次数下降、单次攻击峰值上升的趋势，且中国依然是DDoS攻击源最多的国家，发起攻击次数占总量的46.6%，其次是美国和俄罗斯，分别占3.0%和2.0%。关键基础设施安全威胁——越来越多的国家正在构建智慧城市，电力系统、应急服务、交通控制等关键基础设施将形成巨大的攻击面。这些集成系统受到大规模破坏的可能性很高，是不法分子眼中极具价值的攻击目标。

第二章 企业安全威胁

从何着手应对各类层出不穷的安全威胁？

2017年企业面对的安全威胁层出不穷，而各种威胁手段又不断变化。

一、从威胁类型上来看，大量过去陈旧的攻击方式重新受到了青睐，如Web应用攻击、钓鱼攻击方式全球的各类攻击事件中重获新生；

二、从技术上，各类安全威胁又不断推陈出新，比如利用大量物联网设备进行大规模DDoS攻击的Mirai病毒、利用浏览器网址字符显示缺陷进行钓鱼攻击的Punycode攻击，这些新的技术对企业安全带来的新的挑战。

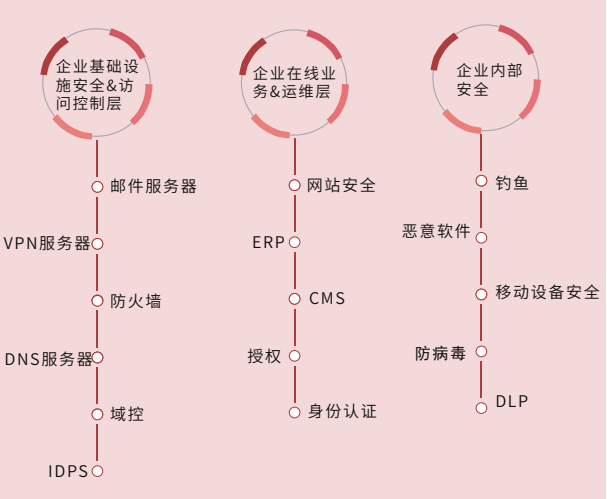
面对各类安全威胁，企业应该从何着手应对？

首先，企业要做的是知晓自己面临哪些安全，之后在此基础上寻找相应的解决方案防御、应对威胁。为此我们整理了各类企业安全威胁，对这些威胁构建三层分类的模型，帮助企业流程化地建立防御。具体来说，这个三层模型包括了如下内容：

第一层、企业在线业务与运维层安全威胁，如包含网站安全、ERP、CMS、身份认证与授权等等位。

第二层、企业基础设施安全与访问控制层安全威胁，如涉及邮件服务器、DNS服务器、VPN服务器、域控、防火墙、IDPS层面的安全威胁。

第三层、企业内部安全，如包含恶意互联网内容（常见的钓鱼、恶意软件）、终端安全（防病毒、DLP）、移动设备安全等威胁内容。



一、企业在线业务与运维层威胁

这一层的分类中包含网站安全、ERP、CMS、身份认证&授权等。

企业的服务器往往是黑客从外网入侵到企业内网的第一个环节，也是安全问题最多的一个环节，因此其中的安全问题不容忽视。从Web应用层面上讲，常见的网站漏洞包括：注入、失效的身份认证和会话管理、跨站脚本（XSS）、直接引用不安全的对象、安全配置错误、敏感信息泄漏、跨站请求伪造（CSRF）、使用含有已知漏洞的组件、未验证的重定向和转发等。

2017年，OWASPTop10威胁迎来了一次更新，在此次更新中注入漏洞仍然位居Top10威胁之首，而XSS的威胁程度从A3降到了A7。敏感信息泄露、安全配置错误、失效的访问控制等威胁均有提升，值得企业重视。与此同时，榜单中还出现了一些新的安全威胁，包括XXE漏洞(A4:2017,XML External Entity attack)、针对Java平台的不安全反序列化漏洞(A8:2017,Insecure Deserialization)以及记录和监控不足风险(A10:2017,InsufficientLogging&Monitoring)等。这些新兴的安全威胁也值得企业重点关注。

尽管网站安全问题老生常谈，并且近几年企业的安全意识也有提升，但Web应用的攻击从整体上仍然不断上升。

2017年8月，知名内容分发网络（CDN）和云服务提供商 Akamai Technologies 发布的《2017 Q2互联网安全现状报告》中指出，2017 Q2 的 Web 应用攻击比上一季度增加了5%，比去年增加了28%。

除了Web应用层面，各项其他安全威胁也有可能造成服务器出现安全问题，常见的威胁包括端口访问、主机漏洞、配置策略缺陷、补丁策略缺陷等。

事实上步入2017年之后，随着企业安全意识的不断增高，无论是Web应用层面的漏洞还是端口访问等漏洞都已显著下降。攻击者已经很难像以前一样以较低的成本寻找到漏洞，但与此同时DDoS作为一种较为古老的网站攻击手段却延续至今。

2016年秋季，爆发了利用大量物联网设备进行DDoS的Mirai事件，造成了巨大的影响。Mirai是一款恶意软件，它可以使运行Linux的计算系统成为被远程操控的“僵尸”，以达到通过僵尸网络进行大规模网络攻击的目的。Mirai的主要感染对象是可访问网络的消费级电子设备，例如网络监控摄像机和家庭路由器等。Mirai 构建的僵尸网络已经参与了几次影响广泛的大型分布式拒绝服务攻击（DDoS攻击）。通过IoT设备组建僵尸网络实施DDoS攻击，这也为攻击者提供了新的思路。

Akamai Technologies 发布的《2017 Q2 互联网安全现状报告》中已经指出，Mirai采用Pay-for-Play模式，利用其大规模的僵尸网络提供收费的DDoS服务，并且Mirai促成了DDoS攻击走向商业化。

除了公司对外的网站安全，企业内部的网络也是需要关注的业务，其中最为典型的就是企业的ERP系统。ERP系统是企业资源计划(EnterpriseResource Planning)的简称，是指建立在信息技术基础上，集信息技术与先进管理思想于一身，以系统化的管理思想，为企业员工及决策层提供决策手段的管理平台。ERP系统是很多大企业的核心系统，而近年来，针对ERP系统的发掘的漏洞也越来越多。由于ERP的实现需要大量软件，而这些软件中可能不可避免地存在着一些漏洞，这些漏洞使得攻击ERP变得更加容易。而ERP系统中存在的大量公司机密信息，也给了攻击者们充分的动机。根据Onapsis的报告，全球95%的SAP企业管理系统存在安全漏洞，可能导致严重的数据泄露。

ERP系统本身的漏洞是一个方面，而员工的安全意识

又是另一方面。许多员工使用的弱口令、默认密码等，给了黑客可乘之机。因此，身份认证和授权也是企业需要面对的问题。要想杜绝其中的安全风险，企业需要多角度地防护。企业自身的网站需要防止身份盗用，以及越权、提权等安全问题。要防止盗用，首先应该解决的是一系列的权限漏洞，包括弱口令、默认密码、访问配置缺陷等。

企业内网中同样也需要建设完善的身份认证和授权机制，因为通过钓鱼、入侵等各种攻击，黑客同样可能攻进内网。我们观察到，时至今日，钓鱼这种攻击方式仍然在 2017年被Fancy Bear等黑客组织利用，让这种看似古老的攻击方式仍然在被广泛使用。

2017年 5 月开始，美国大量能源企业遭到攻击，攻击波及到美国至少十家电力公司，其中还包括堪萨斯州的 Wolf Creek 核电站。而相关的安全研究则揭示出黑客将目标对准工控系统，并且在过去攻击的经验上，巧妙地使用“模版注入”的方式隐匿恶意文档，实施网络钓鱼，并获取相关能源企业的登录信息，由于黑客攻击时的隐蔽性，给能源企业带来的影响不可估量。

除此之外，今年钓鱼攻击中还涌现了一些新型的手段，例如Punycode钓鱼攻击，这种攻击方式几乎无法检测，其原理是，许多Unicode字符，代表的是国际化的域名中的希腊、斯拉夫、亚美尼亚字母，看起来跟拉丁字母一样，但是计算机却会把他们处理成完全不一样网站的网址。攻击者只需要将其中的一个字符或者多个字符用Unicode字符代替就可以用来钓鱼。

另一方面，心存歹念的内部员工也可能泄露机密信息，如果缺少安全的身份认证和授权，黑客/恶意员工就有机会通过普通的身份获取到更高级别的敏感数据。

如今，众多企业所采取的方案是使用SSO方案。SSO英文全称Single Sign On，单点登录。SSO是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。它包括可以将这次主要的登录映射到其他应用中用于同一个用户的登录的机制。它是目前比较流行的企业业务整合的解决方案之一。

二、企业基础设施安全与访问控制威胁

企业的基础设施能够保证企业的各项业务能够正常工作，常见的基础设施包括邮件服务器、DNS服务器、VPN服务器。这些基础设施的安全性往往会影响到企业重要业务，因此不容忽视。

邮件服务器把控着企业对外交流合作的命脉，而且其中往往包含大量机密信息。攻击者攻击邮件服务器的主要方式包括：邮箱账号爆破、DoS攻击、系统配置漏洞。

针对邮箱账号的爆破，攻击者可以使用采集到的邮箱地址和弱口令密码，在邮箱服务器上反复尝试登录，从而盗取用户邮箱账号。而DoS攻击的成本则更低，只需要找到相关的邮箱服务器就可以利用大量流量进行攻击，最终导致邮箱服务器不可用，进而使得企业无法进行对外沟通；第三种攻击手法是使用系统配置的漏洞，比如很多系统在交付给客户时都设置了易于使用的默认配置，或者配置了空的或默认的根/管

理员密码，这就让攻击者有机会进行入侵。

而针对DNS服务器的攻击也是较为常见的安全威胁。常见的一种类型是DNS域传送漏洞。如果企业DNS服务器配置不当，可能导致匿名用户获取某个域的所有记录。带来的风险就是，攻击者可以轻易知晓企业拥有的所有域名，其中也包含一些原本没有暴露在公网环境中的域名，倘若这些域名指向的服务器存在漏洞，攻击者就有可能进行入侵。

第二种攻击方式在近几年的互联网世界比较常见，即通过入侵域名管理商劫持域名，指向其他服务器。这种攻击方式很多时候针对的是那些网站安全性较好的公司，攻击者只得旁敲侧击，尝试攻击域名托管商。百度、Google都曾遭受过此类攻击。

2017年7月，安全研究人员MatthewBryant在进行顶级域名映射的代码测试时发现，多个.io权威域名服务器（包括ns-a1.io、ns-a2.io、ns-a3.io和ns-a4.io）可以注册购买。攻击者完全可以将其指向自己的DNS服务器，将所有 .io 域名连接重定向到恶意服务器。

三、企业内部安全威胁

在完善了在线业务与运维以及基础设施安全与访问控制安全后，企业需要加强的是内部安全防御，这其中包括恶意互联网内容、终端安全以及移动设备安全等。

恶意互联网内容传播的渠道主要包含钓鱼等社会工程学手段，对于这样的安全威胁首先可以依靠企业网络中的防火墙或防病毒软件对网站流量进行过滤，对已知的钓鱼网站进行屏蔽，二是提升企业员工的安全意识，对不明的链接心存警惕。

企业内部安全的另一个方面包括终端以及移动设备的安全，为了让员工能够得到全方位的防护，我们推荐使用现有的防病毒解决方案，这样能够保证即使是安全意识薄弱的员工也能够抵御攻击。除此之外，对于各种终端设备，员工还应该即使进行安全更新。

2017年5月，一款名为Wannacry的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索交费活动，影响到近百个国家上千家企业、公共组织以及大量中国高校，其中也不乏一些大型企业，如西班牙的Telefonica、英国的国民保健署、以及美国的FedEx等。而其后爆发的NotPetya病毒，也对欧洲大量企业造成影响。企业面对这两款病毒不仅不得不支付赎金，还需要遭受数据不可恢复的损失。

而两款病毒无一例外地利用“永恒之蓝”漏洞席卷全球，如果企业使用防病毒软件经常检测威胁并且使用更新系统及时修补补丁就可以防范威胁。因此拥有防病毒软件和补丁更新机制是企业安全不可或缺的部分。

四、框架之外的其他威胁

除了上面提到的这些威胁，企业还需要注意框架以外的威胁：

赛门铁克在今年的调查中发现企业用户使用云应用的数量通常会高达900个。大量的云应用导致安全管理难度的上升。事实上，企业云面对的威胁包含多个

方面，最重要的一点是，企业云使得安全边界变得模糊，企业面对本地+云端的复杂环境，因而无法做到对敏感数据的有效管控。

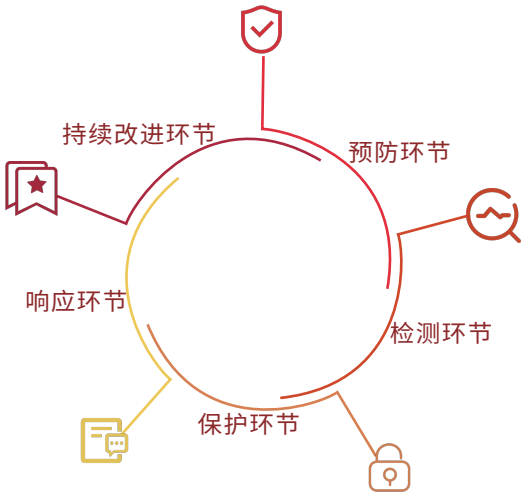
另一方面，企业也面临引入云本身带来的安全威胁，某些云平台安全性不足导致黑客入侵是一个方面，另一方面，云平台公开的属性也引入了安全风险。今年发生了大量安全泄露事件都与云服务器有关：Verizon合作伙伴泄露了超过1400万Verizon客户的个人信息记录，包括姓名，地址，账户详细信息，和一部分客户的账户PIN码；AWS S3泄露了将近1.98亿美国选民的个人资料，其数据库包含三家与共和党有关的公司信息；华尔街日报的母公司道琼斯泄露了220万客户的个人资料；埃森哲的部分业务数据被放在了公开的 Amazon S3 bucket 服务器上，这些事件的诱因都是机密文件暴露在了云服务器上。

企业对各类威胁严防死守，但员工自身引入的新设备却有可能让这些努力功亏于溃。自携设备（BYOD，Bring YourOwnDevice）是指员工使用个人行动装置进入他们工作区域并用以处理公司资讯与应用程序的作业方式。这种方式十分普遍。在巴西与俄罗斯这些快速成长的市场里，大约有75%的员工使用自携设备作业。而在发展中市场里，亦有44%的员工使用自携设备工作。而在中国，使用自己的手机处理工作事务也是常态。许多公司都相信，员工使用自携设备会更有生产力。开放使用自携设备可以提升便利性，也能节省办公成本。但是于此同时，自携设备会带来安全风险，我们知道公司往往不会对员工的个人设备进行管理，倘若员工携带的设备存在安全风险，企业对终端威胁所做的防御便会全部失效，导致各种安全威胁，轻则机密文件泄露，重则导致内网主机被入侵。

因此，除了企业本身的网络设施，传统框架之外的威胁也需要企业的重视与防范。

第三章 企业安全应对流程

面对2017年的安全态势，企业安全涉及的方面越来越复杂，积极应用传统的企业安全流程并增强对于新威胁的防范。一个健壮的企业安全应对流程应该是一环套一环，环环相扣，需要多方面协作完成。



一、预防环节

一个完整的企业安全系统，首先要做的第一步就是要做好预防措施，最常见的预防措施包括身份验证，授权和访问控制策略。这些预防措施首先可以解决一些最基本的问题，包括认出用户是谁，并且授予不同用户不同的执行权限。

整个预防环节包含三个方面，身份认证、授权、访问控制策略。

认证的目的就是为了认出用户是谁，或者说是能够识别出正确的人。如果企业是一个屋子，那么外人如果想进行破坏的话，第一步要做的就是先开门，持有钥匙的人才能开门进入屋子，那么屋子就是通过“锁和钥匙的匹配”来进行认证的，认证的过程就是开锁的过程。钥匙在认证的过程中，被称为“凭证”，开门的过程，在互联网里对应的是登录。认证实际上是验证凭证的过程。

而授权和认证相似，但又有一些区别：授权的目的是为了决定用户能够做什么。拥有高权限的用户获得的授权要比低权限的用户要多，高权限的用户可以做的事情也就比低权限用户多。而且权限多少是由最开始的认证决定的。

访问控制策略则是某个主体对某个客体实施某种操作，而系统对这种操作的限制就是访问控制。

用户身份认证和访问控制策略在整个企业安全应对流程中还是比较重要的，任何有缺陷的设计都会严重破坏整个流程。

在对整个企业安全应对流程进行部署时，安全人员往往只关注那些系统中所需要的功能，通常会建立自定义的认证和会话管理方案。但要正确实现这些方案却很难，结果这些自定义的方案往往在如下方面存在漏洞：退出、密码管理、超时、记住我、秘密问题、帐户更新等等。因为每一个实现都不同，要找出这些漏洞有时会很困难。

二、检测环节

提前做好预防措施还是不够的，时刻关注系统中可能存在的风险可以帮助企业第一时间做出决策并及时响应，减少损失。事件发生前，一个完善并准确的事件监控策略显得尤为重要。整个检测环节中企业都需要依照一定的安全策略，通过软、硬件，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

一直以来检测环节中比较常见的是IDS和DDoS检测系统，IDS在技术上也已经比较成熟，运用也相对广泛。

但到了2017年，相比市场上比较陈旧的IDS，新兴技术有望更快地走入我们的视线，在传统应对措施的基础上，2017年一些新技术的深度运用越来越多地帮助企业更好地应对威胁。

UBA（用户行为分析），它可以帮助企业或组织监测内部威胁、恶意目标的攻击和金融欺诈行为。利用UBA 技术解决内部威胁是一种新的手段方法，该技术发展到今天已经具备了能够对非结构化数据进行分析能力，甚至可以拥有一定的预测能力，并开始应用到内部威胁和目标攻击防护中去，而不再仅仅局限于行为监测了。

而更进一步的UEBA（用户实体行为分析）则将用户活动与其他部分数据结合，比如受管理终端，非受管理终端，应用（包括云端，移动端和其他的本地应用程序），网络和内部威胁。对比UBA，UEBA不仅可以监测内部的威胁，还可以监测外部的威胁，从而保护数据避免危险。

2017年企业办公系统和应用上云也对传统的监测环节提出了新的要求。调查和咨询机构 Garther 公司今年的报告同样指出，到2020年，85%的大型企业都会使用CASB技术增强企业的在云场景下的安全检测能力。

云访问安全代理(CASB)是一组新的云安全技术，可解决使用云应用和服务（包括SaaS和IaaS）带来的挑战。这些新的CASB解决方案的目的是通过提供这些服务的使用方式的关键可见性和控制性，使组织能够借助云应用和服务提升生产力。这能帮助信息安全团队：识别和评估所有使用中的云应用（影子IT）、在现有Web代理或防火墙中实施云应用管理策略、实施精细策略以控制敏感信息的处理，包括与合规性相关的内容、加密或标记敏感内容以保证隐私和安全、检测并阻止显示恶意活动的异常帐户行为、通过针对数据丢失防范、访问管理和Web安全的更广泛安全解决方案实现集成云可视性和控制性。

三、保护环节

时刻检测整个系统看起来十分必要，但有时也需要一些主动性的防护，旨在预先对入侵活动和攻击性网络流量进行拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报。

保护环节比较传统的是IPS，它通过直接嵌入到网络流量中而实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能够在IPS设备中被

2017年7月Gartner在安全新技术报告中提出了微分隔技术（Microsegmentation）。它的出现能够地对IPS做出了补充，攻击一旦在企业系统中站稳脚跟，它们通常会横向蔓延到其他系统中。微分隔能在虚拟数

据中心进行隔离和分段操作，就像潜艇中的舱室一样，有助于减少威胁破坏性，进行有效保护。之前，微分段技术主要用于服务器在相同层的横向通信，但如今它现在已经演化为保护虚拟数据中心的内部通信机制了。

四、响应环节

预防，检测，预防环节中主要工作还是放在防范上面，而企业在发生重大安全事故时，更需要一套完善的应急响应策略及取证分析流程。

很多时候由于缺乏紧急响应流程，或者紧急响应流程执行不到位，使得一些本来可以快速平息的安全事件，最终造成巨大的损失。

早做准备，如果有专门的一个事件响应团队，任何时间发生的攻击都可以有一个很好的应对策略。明确的事件响应规划可以帮助团队知道在事件发生之后应该做些什么，减少不必要的沟通时间。而且，制定的规划越有效，安全和技术团队就会采取更加明确安全措施来应对紧急事件，也会将损失降到最低。

及时止损，越早处理发生的安全事件，对于日后产生的影响就会越小。因为安全事件一开始如果不被及时解决，马上就会愈演愈烈，对于企业来说，要付出更多的时间和成本来处理。而如果企业提前制定了完善的应急响应规划的话，技术团队可以在安全事件刚刚发生时就可以减少损失，采取措施解决相关问题。

加强沟通，事件发生过程中，沟通往往是一个大问题，可能会造成时间上的巨大浪费，和计划上的混乱。而如果有一个可以集中交流的应急小组之后，所有的情况都会无延误的传达给安全和技术团队，这可以保证响应小组可以很快想出对策并做出行动。

整个事件响应过程就是在安全事件爆发过程中，企业的应对方式。入侵检测系统或安全监控产品的规则被触发时，根据攻击的严重程度，最终会产生“事件”或“报警”，报警建立后，开始着手建立“紧急响应流程”。整个应急响应小组应包括：技术负责人、产品负责人、最了解技术架构的资深开发工程师、资深网络工程师、资深系统运维工程师、资深DBA、资深安全专家、监控工程师、公司公关。

小组建立起来之后，第一时间就要弄清楚问题产生的原因，并协调相关的资源进行处理。保护安全事件现场，以最快速度处理完问题。

取证技术在事件响应流程中十分重要，有利于企业做出正确和及时的响应。例如，如果一家公司正在处理一起钓鱼攻击事件，取证过程就可以帮助确定一些信息，比如谁点击了钓鱼链接，谁落入了攻击者的圈套，有哪些信息泄露了或遭到了窃取。这些可以帮助安全团队策划合适的响应机制，评估上报需求。倘若公司的IP地址遭到窃取，无论是内部攻击者还是外部攻击者所为，取证技术可以帮助建立事件发生的时间线，执法机构可以以此为依据，调查或起诉攻击者。在这种情况下，取证流程符合并保存了拘留所需的证据链是十分重要的。取证分析会更加专注于防护。它将跟着数据恢复的进化方式一起进化。一旦人们开始弄丢数据，他们就会开始使用远程备份来防止数据丢失。使用计算机取证也会发生同样的事情。公司会确切落实计算机取证以防有事发生，这样他们就有数据和方

法可以追踪出到底发生了什么。他们不再需要维护硬件了。企业们会使用一个服务器，可以记录所有操作和功能，可以简单请求回顾日志。所有信息都都以取证的方式进行储存，以确保可靠无误。

同样在2017年7月Gartner在安全新技术报告中可以看到，对于中小企业而言，近年出现的安全管理检测和响应（MDR）会是他们在建立安全应对流程时的好选择。MDR提供商为那些需要改进威胁检测、事件响应和持续监控功能的买家提供服务，这些买家自身通常不具备专业的技能和资源，由于缺乏对威胁检测和应急响应方面的投资，这些MDR服务正好触及了这些中小企业的需求。

五、持续改进环节

介绍完整个响应环节之后，整个企业安全应对流程还没有结束，因为安全是一个持续的过程，还需要不断的查缺补漏，逐渐让企业的安全流程更加完善。

在整个过程中，企业需要从安全评测、安全加固、安全运营管理、安全意识、安全咨询这几个方面持续改进。

安全评测的过程，就是寻找薄弱环节并修复的过程。通过漏洞扫描，渗透测试，代码审计等方式，可以发现系统中已知的安全问题，然后通过设计安全方案，实施安全方案，最终解决这些问题。一套完善，丰富的安全评估系统可以高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。它可以全方位检测IT系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补和安全加固。

安全运营贯穿在整个体系之中。安全运营需要让端口扫描、漏洞扫描、代码白盒扫描等发现问题的方式变成一种周期性的任务。安全是一个持续的过程，管理上的疏忽随时都有可能打破之前辛辛苦苦建立起来的安全防线。假设管理工作和流程是不可靠的，就需要通过安全运营不断地区发现问题，周期性地做安全健康检查，才能让企业放心。

而在最近几年，OSS安全扫描和对DevSecOps进行软件分析也尤为重要。在整个DevOps过程中，安全架构师还必须能够进行自动化地进行安全控制，而且这种控制还要尽可能地对开发人员透明。安全分析人员还需了解软件的源码，模块，框架和类库，这样才能识别并清理OSS组件中的安全或许可问题。

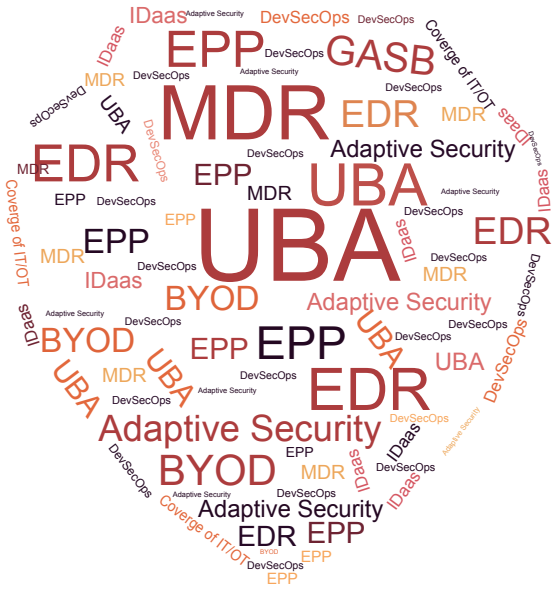
2017年卡巴斯基实验室与 B2B International 共同发布的报告中提到，每年有46%的IT安全事故是由企业员工造成的。安全作为企业生产经营的第一要素，列在企业生产经营活动的首位。从众多的安全事故案例中追溯其根源，员工的安全意识淡薄是发生安全事故的根源。因此在持续改进环节，培养企业员工的安全意识依然是值得企业关注的事情。

安全事件发生后，专业的安全咨询可以帮助客户控制并应对事件，减轻危机程度，帮助用户处理网络入侵和数据泄露，提供法律专家随时为用户提供法律专业建议，和数据隐私相关管理建议。

趋势观察

2017年企业在应对威胁时主要考虑哪些问题?

通过观察谷歌趋势,可以得到以下热点词汇的搜索态势。下面我们来详细解释一下2017年的热点词汇。



名词解释:

UBA: UBA(用户行为分析)是指帮助企业或组织发现内部威胁,目标攻击和金融欺诈。利用UBA技术解决内部威胁是一种新的手段方法,该技术发展到今天已经具备了能够对非结构化数据进行分析能力,拥有一定的预测能力,已经开始应用到内部威胁和目标攻击防护中去而不再仅局限于调查分析了。

UEBA: UEBA将用户活动和其他部分,比如受管理终端,非受管理终端,应用(包括云端,移动端和其他的本地应用程序),网络和内部威胁。对比UEA,UEBA不仅可以防范内部的威胁,还可以防范外部的威胁,从而保护数据。

SDS: Software Defined Storage,软件定义存储。数据中心中的服务器、存储、网络以及安全等资源可以通过软件进行定义,并且能够自动分配这些资源。软件定义存储的核心是存储虚拟化技术。软件定义的数据中心通过现有资源和应用程序对不断变化的业务需求提供支持,从而实现IT灵活性。

CASB: 云访问安全代理(CASB)是一组新的云安全技术,可解决使用云应用和服务(包括SaaS和IaaS)带来的挑战。这些新的CASB 解决方案的目的是通过提供这些服务的使用方式的关键可见性和控制性,使组织能够借助云应用和服务提升生产力。

EDR: EDR(端点检测和响应)工具通常会记录大量端点和网络事件,把这些信息保存在端点本地,或者保存在中央数据库中。然后使用已知的攻击指示器(IOC)、行为分析和机器学习技术的数据库,来持续搜索数据,在早期检测出漏洞(包括内部威胁),并对这些攻击做出快速响应。

MDR: 管理检测和响应(MDR)是一种可管理的网路安全服务,可以帮助企业提高威胁检测,事件响应以及持续检测服务,成本比用户自建运营相关安全团队要低很多,尤其受到中小企业的欢迎。

EPP: EPP(端点保护平台)是一种保护端点设备的软件技术,主要用来保护企业 IT 环境中的端点设备。这些端点设备包括PC,笔记本电脑,智能手机和平板电脑等。EPP是一套完整的安全解决方案,它结合了杀毒,反间谍软件,入侵检测/预防,个人防火墙,数据保护/加密和其他端点保护解决方案。

SDP: SDP(Software Defined Perimeter),软件定义边界,也称为“BlackCloud”,SDP基于

need-to-know 原则，即在访问应用程序基础架构之前要先对设备状态和身份进行验证。而应用程序基础架构是不可见的，即无法被设备检测到，没有可见的DNS信息和IP地址。SDP（软件定义边界）可以缓解大部分的网络攻击，包括：服务器扫描，DoS，SQL注入，操作系统和应用程序咯东利用，中间人攻击，XSS，CSRF等。

DevSecOps：它是糅合了开发、安全及运营理念以创建解决方案的全新方法”。企业投资防火墙、IPS等外围防御系统本身无可厚非。但是，单纯地守卫边界是不够的。DevSecOps是在DevOps方案中加入了安全理念，这需要CIO及其团队在软件开发的一开始就考虑到安全问题，而不是事后。

Container Security：Docker 容器（Container Security）也不是完全安全的，对docker容器安全质疑最大的一点就是其隔离的彻底性，与其对比就是当前成熟的虚拟机（VM）技术。相对于VM，docker容器只是对进程和文件进行虚拟化，而VM做到了OS级别的虚拟化。

BYOD：BYOD (Become Your Office Device)即在你自己的设备上安装很多公司的软件，以便可以让你使用公司的资源。当员工的设备比如iphone上安装了这样的管理软件，员工自己的手机就变成了公司的手机，那个Agent就不停的和服务器同步。虽然这是员工的自带设备，但此时BYOD就从自带设备转换成了自带的办公设备。

Adaptive Security：自适应安全是一种保护安全的新手段，它对威胁的定义不仅仅局限于感染病毒的文件和代码，而是检测系统中存在的有威胁性的行为。该方法最重要的特点就是就是可以很快适应并应对不断变化的复杂环境进行预警。而且它还可以主动预测，识别，处理恶意软件和黑客行为。跟踪应用程序和系统行为，并识别出其中不正常的行为，追踪这些行为的源头。自适应安全可以帮助企业更好地应对日益增强的企业威胁。

本章小结

整个企业安全应对流程中，可以发现每个环节之间连接都相当紧密，对于企业来说，每个环节都不能掉以轻心，平时也要加强员工安全意识的培养，出现问题的时候，有一套提前预演过的应对流程，对于决策和方案都有一个很好的指示作用，对于安全事故的发生，寻求专业人士，从而得到专业的建议。只有每个环节都做好足够的准备，在事故发生的时候，企业才能将损失降到最低。

第四章 企业安全产品推荐名录

一、安全产品名录研究背景介绍

在确保候选列表阶段，FreeBuf主要采取的是资料搜集、走访企业客户以及专家访谈的形式进行调研。

FreeBuf经过统计后得出推荐安全产品的候选列表。为了进一步提升名录的严谨性和公信力，评定小组还参考了国内外信息安全领域的各类主要奖项、Gartner魔力象限及多家专业机构发布的权威报告，并对上榜企业的融资情况进行了深入调查。

随后，FreeBuf研究院对每个入选候选列表的安全产品进行评分。每位专家会对每个产品进行六个维度的打分（品牌影响力、整体创新性、技术先进性、市场占有率、产品体验及用户口碑），我们通过一定的统计方法按照权重汇总后，最终得到推荐名录。

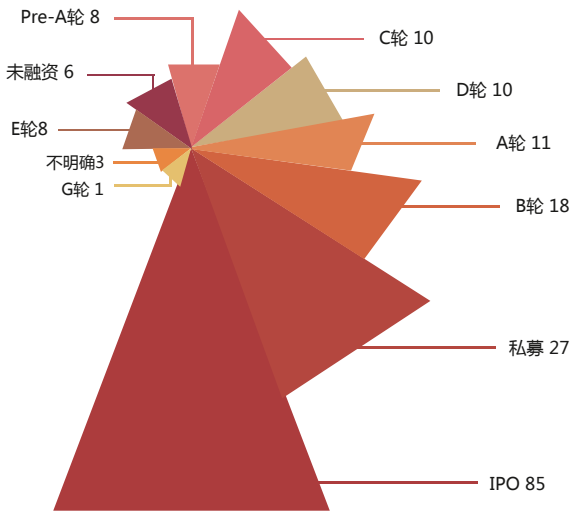
历时近两个月的评分后，最终9个大类、29个小类共190个优秀产品脱颖而出，我们可以在这一章节从各个角度来了解到这些上榜产品的情况，如入选企业的融资情况、整体得分情况，最后还会以雷达图展现每类产品的得分情况。

二、入选企业融资情况一览

入选的190项安全产品来自于国内国外的187家企业。其中国内企业为90家，国外企业为家97家。

获得Pre-A轮为8家，A轮融资的企业为11家，获得B轮融资的企业为18家，获得C轮融资的企业为10家，D轮的则是10家，E轮8家，G轮1家。而获得了IPO的企业共计85家。

此外，获得私募融资的企业为27家，情况不明或者不需要融资的企业为9家。



入选产品的企业整体融资占比

而从企业的融资情况来看，IPO的企业占据多数，约占45.45%的入选产品企业已经获得公开募股上市。而14.44%的企业通过了私募方式获得融资。剩下的入选产品居多是处在A、B、C轮、D轮的早期融资阶段之中。

我们可以看到5.88%的企业处于A轮阶段，9.63%的企业处在B轮，5.35%的企业处在C轮阶段。此外，约占10% 的企业处在晚期融资阶段，还有约占5%

的企业不需要融资或融资情况不公开。

其次，我们还可以按照入选安全产品的大类产品分类，来了解每一类型产品的整体融资阶段。

我们可以发现，除了大趋势中我们可以看到半数入选产品名录的企业是上市企业之外，安全运营类别、威胁预警类别中的安全产品中，分别有56.52%以及56.25%的所属企业已经处在IPO阶段，说明在这两类产品已经较为成熟。而身份认证类别、主动防御类、安全评测与加固类别中都有不少新兴企业的产品入选名录，在后续市场中可能还有更大的潜力有待发挥。

三、各大类产品得分整体情况

下面将按照威胁预警、访问控制、身份认证、事件监测、主动防御、事件响应与取证分析、安全评测与加固、安全运营管理、安全意识与咨询这九大分类，展开每一层的产品分类描述。经过评分，本次入选名录的190个产品来自187家企业。

威胁预警类产品下分为威胁情报、态势感知和舆情监控三种细分类别，我们可以看到威胁情报国外产品居多，而态势感知类别和舆情监控类别主要是国内产品。

访问控制类产品中分为防火墙和VPN两种细分类别，该类产品中国内、国外的产品占比较为均衡。

身份认证类的产品则分为SSO、云身份认证两种细分类别，该类产品国外产品居多，得分分布较广。

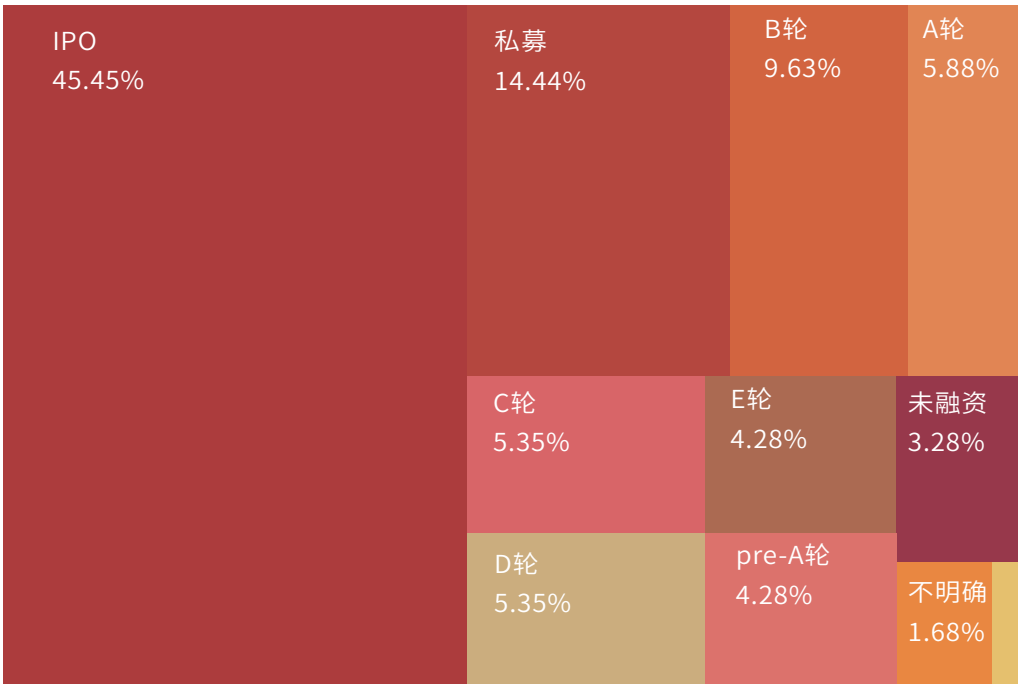
事件响应与取证分析产品中，则可以分为取证与漏洞响应两种细分类别。

安全运营产品中，可以分为SOC、容灾备份、准入控制三种细分类别，国内外产品较为均衡。

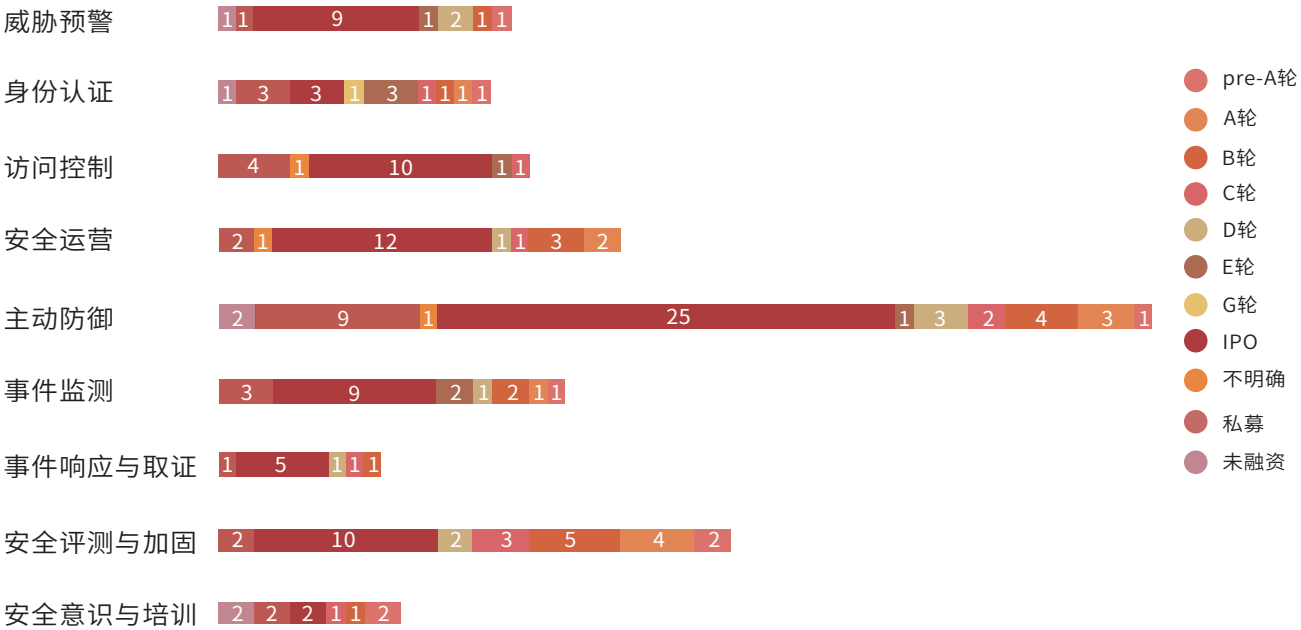
事件监测产品之中，网络类、Web类、数据库类、日志类、移动终端、主机类不同类别中，国内产品占据多数且网络类产品入选居多，但产品的得分较为分散。

主动防御类别中，共分为网络类、防病毒、主机防护、web/waf以及数据保护、蜜罐类六种细分类别。国内国外产品均有入选，且国外产品稍微占比更高，得分较为分散。

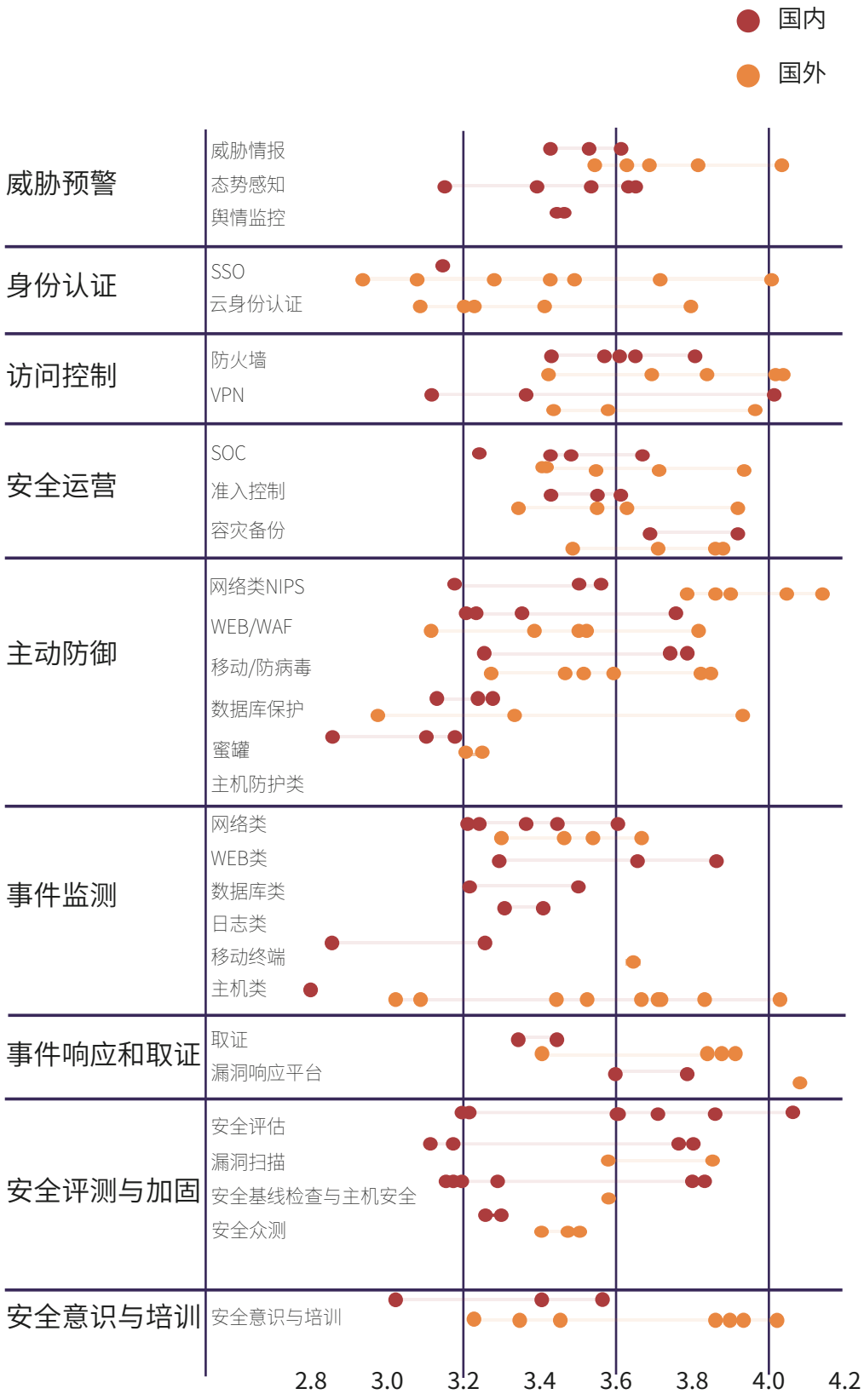
入选产品的企业整体融资占比



每类产品整体融资阶段



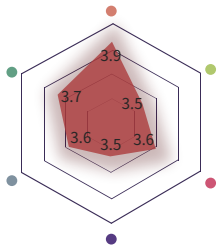
入选产品得分情况一览


国内
国外
威胁预警
威胁情报
态势感知
舆情监控
身份认证
SSO
云身份认证
访问控制
防火墙
VPN
安全运营
SOC
准入控制
容灾备份
主动防御
网络类NIPS
WEB/WAF
移动/防病毒
数据库保护
蜜罐
主机防护类
事件监测
网络类
WEB类
数据库类
日志类
移动终端
主机类
事件响应和取证
取证
漏洞响应平台
安全评测与加固
安全评估
漏洞扫描
安全基线检查与主机安全
安全众测
安全意识与培训
安全意识与培训
2.8
3.0
3.2
3.4
3.6
3.8
4.0
4.2

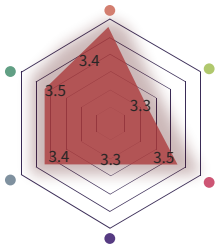
安全评测与加固类别中，分为安全评估、漏洞扫描、安全基线检查与主机安全、安全众测这四种细分类别，产品的得分比较集中，国内产品居多。

此外通过对每类产品进行最终得分的均分计算，我们可以绘制雷达图的形式得到就九个大类产品各自的能力雷达图。

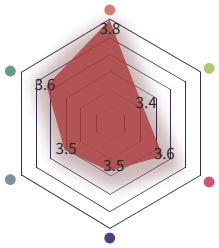
安全意识与培训



事件检测

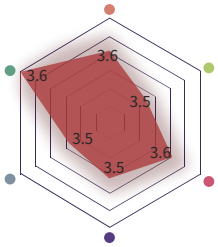


威胁预警

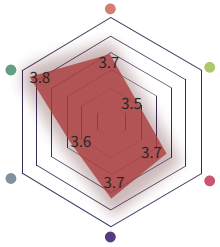


- 平均值/品牌影响力
- 平均值/整体创新性
- 平均值/技术先进性
- 平均值/市场占有率
- 平均值/产品体验
- 平均值/用户口碑

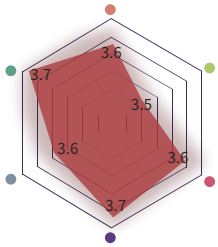
安全评测与加固



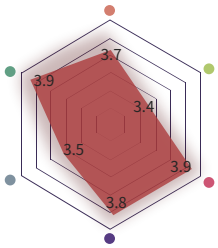
访问控制



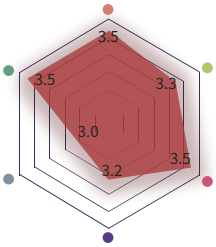
安全运营



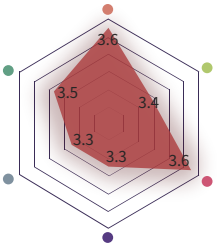
事件响应和取证



身份认证



主动防御



四、细分分类下安全产品推荐名录

FreeBuf在了解了入选企业的融资情况、整体得分情况后，在下面这一部分中我们将会以更细致的视角观察每个产品的得分情况，并以雷达图形式展现每类细分产品在六个维度上的得分对比。

急速增长的针对性网络攻击直接催生了威胁情报服务。威胁情报包含两个不同的层面。第一种威胁情报是“战略层面”的，也就是供人阅读的。这类威胁情报不需要非常技术，主要为各类高管准备，让他们能够了解威胁对于业务连续性的影响，帮助他们做出正确的决策。这类威胁情报的典型呈现方式就是报告。另一类是“可操作层面”的，或者说是可机读的数据——安全设备能够利用这些数据来加固安全性。这些可操作的威胁情报能够帮助SOC分析师、事件响应团队，甚至到做出决策的管理层。

1. 威胁情报产品推荐名录

入选本次威胁情报名录的产品包括：FireEye、卡巴斯基、IBM、Crowdstrike、赛门铁克、微步在线、AlienVault以及奇虎360的威胁情报产品。

威胁预警	威胁情报	FireEye
	威胁情报订阅服务	卡巴斯基
	X-Force情报社区	IBM
	DeepSight Intelligence	赛门铁克
	Falcon	Crowdstrike
	VB(VirusBook.cn)	微步在线
	OTX开源威胁情报社区	AlienVault
	天擎终端、天堤防火墙、天眼APT检测	奇虎360
	Enterprise Security Counter Threat Platform	Secureworks (Dell)

2. 态势感知产品推荐名录

本次入选态势感知名录的产品包括：阿里云盾、360态势感知、亚信安全态势感知、安恒明鉴以及任子行网络安全态势感知平台。

态势感知	阿里云盾	阿里云
	360态势感知	奇虎360
	亚信安全态势感知	亚信安全
	明鉴	安恒信息
	任子行网络安全态势感知平台系统	任子行

3. 舆情监控产品推荐名录

本次入选舆情监控名录的产品包括：乐思网络舆情监控系统以及军犬舆情监控系统，这两家都是国内企业。

舆情监控	乐思网络舆情监测系统	乐思
	军犬舆情监控系统	中科点击

4. 身份认证SSO产品推荐名录

入选身份认证SSO名录的产品包括：微软，Okta、Centrify、OneLogin、RSASecurity、SecureAuth 、九州云腾、PerfectCloud、卫士通以及Ping的身份认证工具。

身份认证/SSO	Azure Active Directory	微软
	Okta Identity and Mobility Management	Okta
	centrify identify service	Centrify
	onelogin Secure Single Sign-on (SSO) Solution	OneLogin
	RSA SECURID	RSA Security
	SecureAuth IdP	SecureAuth
	九州云腾生成令牌IPG	九州云腾
	PerfectCloud SmartSignin	PerfectCloud
	身份认证管理系统	卫士通
	Ping Identity PingOne	Ping

5. 云身份认证产品推荐名录

入选云身份认证名录的产品包括：微软、Okta、BioCatch、Netiq以及SecureAuth的产品。入选的产品均为国外公司产品。

身份认证云身份	Azure Active Directory	微软
	Okta Identity and Mobility Management	Okta
	BioCatch identity proofing&Continuous Authentication	BioCatch
	netiq Identity Manager	Netiq
	secureauth Multi-Factor Authentication	SecureAuth

6. VPN产品推荐名录

入选访问控制VPN名录的产品包括：深信服VPN、思科ASA 、Array Networks、Juniper SSG、江南信安综合网关以及天融信VPN。

VPN	深信服 VPN	深信服
	Cisco ASA	思科
	Array Secure Access Gateway	Array Networks
	Juniper SSG	Juniper
	江南信安 VPN综合安全网关	江南信安
	IPSec VPN	天融信

7. 防火墙产品推荐名录

入选防火墙名录的产品包括：CheckPointNGFW，PaloAltoNGFW，FortinetNGFW，深信服NGFW，思科NGFW，华为NGFW，天融信NGFW，绿盟NGFW，H3C NGFW，山石网科NGFW 以及Juniper NGFW。

防火墙	CheckPoint NGFW	CheckPoint
	新一代防火墙	Palo Alto Networks
	Fortinet NGFW	Fortinet
	深信服NGAF下一代防火墙	深信服
	Cisco NGFW	思科
	华为下一代防火墙	华为
	天融信NGFW®下一代防火墙	天融信
	绿盟NF防火墙系统	绿盟科技
	H3C SecPath系列防火墙	H3C
	山石网科下一代防火墙	山石网科
	Juniper NGFW	Juniper

8. SOC产品推荐名录

入选SOC名录的产品包括：IBM的Qradar，HP Arcsight，启明的泰合SOC，Splunk，瀚思安信的HanSight下一代安全管控平台，LogRthythm的NGSIEM，东软的NetEyeSOC，Fortinet的FortiSIEM，Trustwave的SIEM，以及360网神的SecFox-SNI。

SOC	Qradar	IBM
	HP Arcsight	惠普
	泰合信息安全运营中心（SOC）	启明星辰
	Splunk	Splunk
	HanSight下一代安全管控平台	瀚思安信
	Next-Gen SIEM	logRhythm
	NetEye安全运维管理平台（SOC）	东软
	FortiSIEM	Fortinet
	SIEM Enterprise	Trustwave
	安全管理平台SecFox-SNI	360网神

9. 容灾备份产品推荐名录

入选容灾备份名录的产品包括阿里云、EMCData protection suite，Veritas NetBackup 华为灾备解决方案，VeeamAvailability。

容灾备份	阿里云	阿里云
	EMC Data protection suite	EMC
	IBM数据备份容灾解决方案	IBM
	NetBackup	Veritas
	业务连续性灾备解决方案	华为
	Veeam Availability Orchestrator	Veeam

10. 准入控制产品推荐名录

入选准入控制名录的产品包括：CiscoSecure Access Control，PulsePolicySecure，盈高科技的ASM6000，以及ArubaClearPassPolicy Management，联软科技的网络准入控制系统，以及ExtremeNetworks的ExtremeControl。

准入控制	Cisco Secure Access Control System	思科
	Pulse Policy Secure	Pulse Secure
	ASM6000	盈高科技
	Aruba ClearPass Policy Manager	Aruba Networks
	网络准入控制系统UniNAC	联软科技
	ExtremeControl	Exterme Networks

11. 主动防御-WEB/WAF产品推荐名录

入选主动防御-Web／Waf名录的产品包括：Akamai technologies 的Web Application Protector，长亭科技的雷池NGFW，Cloudflare的CloudWeb ApplicationFirewall，DenyALLrWeb，Imperva WEB应用程序防护，服云科技的网站安全狗，天融信网页防篡改，绿盟网站安全防护，以及F5Networks的BIG-IP应用安全防护。

WEB/WAF	Web Application Protector	Akamai Technologies
	雷池 (SafeLine) 下一代Web应用防火墙	长亭科技
	Cloud Web Application Firewall	Cloudflare
	DenyALL rWeb	Rohde & SchwarzCybersecurity
	imperva WEB 应用程序防火墙	Imperva
	Next-Generation Web Application Firewall (WAF)	Signal Sciences
	网站安全狗	服云科技
	天融信网页防篡改	天融信
	绿盟网站安全防护	绿盟科技
	BIG-IP Application Security Manager	F5 Networks

12. 蜜罐产品推荐名录

入选蜜罐名录的产品分别为NetBait，Keyfocus的Kfsensor，锦行网络的幻云系统，长亭科技的谛听内网感知系统。

蜜罐	NetBait	NetBait
	Kfsensor	Keyfocus
	幻云	锦行网络
	谛听内网感知系统	长亭科技

13. 主动防御-数据库保护产品推荐名录

入选主动防御-数据库保护名录的产品包括：McAfee数据中心保护，Imperva数据保护产品，安华金和数据安全产品，安恒信息明御数据防火墙，天融信TDSM-DBFW，甲骨文的Secernodatawall。

数据库保护	McAfee Data Center Security Suite for Databases	McAfee
	imperva Data Protection and Compliance	Imperva
	安华金和数据安全产品	安华金和
	明御数据库防火墙	安恒信息
	TDSM-DBFW	天融信
	Secerno datawall	甲骨文

14. 主动防御-网络类产品推荐名录

入选主动防御-网络类名录的产品包括：FireEye网络安全，思科下一代网络安全防护，趋势科技TippingPoint，McAfee网络安全防护，IBM，Fortinet，华为NIP6000，绿盟网络入侵防护系统，Alert logic网络入侵防护，山石网科入侵检测防御产品。

网络类NIPS	FireEye Network Security	FireEye
	cisco Next-Generation Intrusion Prevention System	思科
	TippingPoint Next-Generation Intrusion Prevention System	趋势科技
	McAfee Network Security Platform	McAfee
	Network security and protection	IBM
	Fortinet Advanced Threat Protection (ATP)	Fortinet
	NIP6000 下一代入侵防御系统	华为
	绿盟网络入侵防护系统	绿盟科技
	Managed Network Intrusion Detection System	Alert logic
	山石网科入侵检测 / 防御产品	山石网科

15. 主动防御-移动防病毒类产品推荐名录

入选主动防御-移动防病毒类名录的产品包括：赛门铁克的诺顿手机安全防护，McAfee的移动安全防护，腾讯手机管家，奇虎360的360手机卫士，卡巴斯基安卓安全，Sophos的移动安全防护应用，Avast的手机安全软件，趋势科技的移动安全应用，永杨安风的LBE安全大师，Avira的安卓反病毒防护软件。

移动/防病毒	诺顿手机安全软件	赛门铁克
	McAfee® Mobile Security	McAfee
	腾讯手机管家 7	腾讯
	360手机卫士 7.0	奇虎360
	卡巴斯基安全软件 安卓版	卡巴斯基
	Sophos Mobile Secure Enterprise Mobility Management	Sophos
	Avast 免费手机安全软件	Avast
	trend Mobile Security for Enterprises	趋势科技
	LBE安全大师	永杨安风
	Free Antivirus for Android/iphone	Avira

16. 主动防御-主机防护产品推荐名录

入选主动防御主机防护名录的产品包括：赛门铁克端点防护，微软反病毒防护，IntelMcAfee，Sophos端点防护，PaloAlto的Traps端点防护，F-secure的Server Security，趋势科技的云安全软件，Signal的RASP，Cylance的ThreatZero以及椒图科技主机安全。

主机类/主机	Symantec Endpoint Protection	赛门铁克
	Microsoft antivirus protection	微软
	Macfee终端安全保护产品	Intel security
	Sophos端点防护	Sophos
	Traps Advanced Endpoint Protection	Palo Alto Networks
	F-secure Server Security	F-secure
	PC-cillin 2017 云安全软件 全功能增强版	趋势科技
	The Signal Sciences RASP	Signal sciences
	PROTECT+ ThreatZERO	Cylance
	JHSE椒图主机安全环境系统	椒图科技

17. 事件监测-WEB类产品推荐名录

入选事件监测-Web类名录的产品包括：360企业安全的360网络服务监控，安恒信息的明鉴网站安全监测平台，新华三的H3CSecPath云安全监测中心。

WEB类	360网站服务监控	360企业安全
	明鉴®网站安全监测平台	安恒信息
	H3C SecPath云安全监测中心	新华三

18. 事件监测-日志类产品推荐名录

入选日志类名录的产品包括：绿盟科技的安全日志审计，启明星辰的安全运营日志审计。

日志类	绿盟安全审计系统[日志审计]	绿盟科技
	泰合信息安全运营中心系统-日志审计系统	启明星辰

19. 事件监测-数据库类产品推荐名录

入选事件监测-数据库类名录的产品包括：启明星辰的天玥网络安全审计系统，H3C的Secpath数据库审计系统。

数据库类	天玥网络安全审计系统	启明星辰
	H3C Secpath 数据库审计产品	新华三

20. 事件监测-网络类产品推荐名录

入选事件监测-网络类名录的产品包括：LogRhythm的NGSIEM，亚信安全威胁发现设备TDA系列，SplunkEnterpriseSecurity，LogPoint，绿盟网络入侵检测系统，兰云科技的兰天平台，AlienVault的统一安全管理平台，山石网科的入侵检测及防御系统，瀚思安信的HanSight 3。

网络类	Next-Gen SIEM	LogRhythm
	威胁发现设备TDA系列	亚信安全
	Splunk Enterprise Security	Splunk
	State-of-the-Art European SIEM	LogPoint
	绿盟网络入侵检测系统	绿盟科技
	兰天	兰云科技
	AlienVault 统一安全管理平台 (USM)	AlienVault
	山石网科入侵检测和防御系列	山石网科
	HanSight Enterprise 3	瀚思安信

21. 事件监测-移动终端类产品推荐名录

入选事件监测-移动终端类名录的产品包括：恒安嘉新的移动互联网恶意程序检测系统以及卫士通的移动安全管理中心。

移动终端	移动互联网恶意程序监测系统	恒安嘉新
	移动安全管理中心	卫士通

22. 事件监测-主机类产品推荐名录

入选事件监测-主机类名录的产品包括IBM的IBM Tivoli。

主机类	IBM Tivoli	IBM

23. 漏洞响应平台产品推荐名录

入选漏洞响应平台名录的产品包括HackerOne，漏洞盒子，补天漏洞响应平台。

漏洞响应平台	HackerOne	HackerOne
	漏洞盒子	斗象科技
	补天漏洞响应平台	360企业安全

24. 取证分析产品推荐名录

入选取证分析名录的产品包括：IBM的X-Force，FireEye的Mandiant，HerjavecGroup，安恒的明鉴，Opentext的Guidance，以及美亚柏科取证产品。

取证	X-Force	IBM
	Mandiant	FireEye
	HerjavecGroup	Herjavec Group
	明鉴®网络安全事件应急处置工具箱	安恒信息
	guidance	Opentext
	美亚柏科	美亚柏科

25. 安全基线检查与主机安全产品推荐名录

入选安全评测与加固-安全基线检查与主机安全名录的产品包括：启明安全配置核查，绿盟的安全配置核查系统，Tenable的Nessus，亚信安全的NSG-SMP 安全管理平台，青藤云安全Analyzer，以及椒图科技的主机安全系统。

安全基线检查与主机安全	启明星辰安全配置核查管理系统	启明星辰
	绿盟安全配置核查系统	绿盟科技
	Nessus	Tenable
	亚信科技 NSG-SMP安全管理平台	亚信安全
	JHSE椒图主机安全环境系统	椒图科技
	青藤云安全Analyzer	青藤云安全

26. 安全评估产品推荐名录

入选安全评估名录的产品包括：绿盟科技远程安全评估系统，安恒明鉴远程评估系统，斗象科技网藤ARS，启明星辰天镜扫描，Janus移动安全威胁数据平台，天融信脆弱性扫描系统。

安全评估	绿盟远程安全评估系统RSAS	绿盟科技
	明鉴远程安全评估系统	安恒信息
	网藤ARS	斗象科技
	天镜脆弱性扫描与管理系统	启明星辰
	Janus 移动安全威胁数据平台	犇众信息
	脆弱性扫描与管理系统TopScanner	天融信

27. 安全众测产品推荐名录

入选安全众测名录的产品包括：Hackerone，Bugcrowd，Synack Pen Test，漏洞盒子众测平台，以及360补天平台。

安全众测	Bugcrowd	Bugcrowd
	Hackerone	Hackerone
	Synack Pen Test	Synack
	漏洞盒子众测	斗象科技
	360补天	奇虎360

28. 漏洞扫描产品推荐名录

入选漏洞扫描名录的产品包括：Acunetix扫描，绿盟科技Web漏洞扫描，安恒信息明鉴扫描，Netsparke的扫描器，四叶草感洞，天融信脆弱扫描。

漏洞扫描	Acunetix Web Vulnerability Scanner	Acunetix
	绿盟Web应用漏洞扫描系统WVSS	绿盟科技
	明鉴Web应用弱点扫描器	安恒信息
	Netsparker Web Application Security Scanner	Netsparke
	四叶草感洞	四叶草安全
	脆弱性扫描与管理系统（Web扫描）	天融信

29. 安全意识与培训产品推荐名录

入选安全意识与培训名录的产品包括IBM，Pwc普华永道，EY安永，KnowBe4，赛宁网安，AT&T，谷安天下，InspiredeLearning，PhishMe，以及易安在线。

安全意识与培训	IBM	IBM
	pwc普华永道	Pwc普华永道
	EY安永	EY安永
	KnowBe4	KnowBe4
	赛宁网安	赛宁网安
	AT&T Network Security	AT&T Network Security-AT&T Consulting Enterprise Security Assessment (ESA) Service
	谷安天下	谷安天下
	Inspired eLearning	Inspired eLearning
	PhishMe	PhishMe
	易安在线	易安在线

附录：企业安全推荐产品名录

威胁预警	态势感知	阿里云盾态势感知	阿里云
		360态势感知	奇虎360
		亚信安全态势感知	亚信安全
		明鉴网络空间态势感知	安恒信息
		任子行网络安全态势感知平台系统	任子行
	威胁情报	威胁情报	FireEye
		威胁情报订阅服务	卡巴斯基
		X-Force情报社区	IBM
		DeepSight Intelligence	赛门铁克
		Falcon	Crowdstrike
		VB(VirusBook.cn)	微步在线
		OTX开源威胁情报社区	AlienVault
		天擎终端、天堤防火墙、天眼APT检测	奇虎360
		Enterprise Security Counter Threat Platform	Secureworks (Dell)
	舆情监控	乐思网络舆情监测系统	乐思
		军犬舆情监控系统	中科点击公司
身份认证	SSO	Azure Active Directory	微软
		Okta Identity and Mobility Management	Okta
		centrify identify service	Centrify
		onelogin Secure Single Sign-on (SSO) Solution	OneLogin
		RSA SECURID	RSA Security
		SecureAuth IdP	SecureAuth
		九州云腾生成令牌IPG	九州云腾
		PerfectCloud SmartSignin	PerfectCloud
		身份认证管理系统	卫士通
		Ping Identity PingOne	Ping
	云身份认证	Azure Active Directory	微软
		Okta Identity and Mobility Management	Okta
		BioCatch identity proofing&Continuous Authentication	BioCatch
		netiq Identity Manager	Netiq
		secureauth Multi-Factor Authentication	SecureAuth
访问控制	VPN	深信服 VPN	深信服
		Cisco ASA	思科
		Array Secure Access Gateway	Array Networks
		Juniper SSG	Juniper
		江南信安 VPN综合安全网关	江南信安
		IPSec VPN	天融信
	防火墙	CheckPoint NGFW	CheckPoint
		新一代防火墙	Palo Alto Networks
		Fortinet NGFW	Fortinet
		深信服NGAF下一代防火墙	深信服
		Cisco NGFW	思科
		华为下一代防火墙	华为
		天融信NGFW ® 下一代防火墙	天融信
		绿盟NF防火墙系统	绿盟科技
		H3C SecPath系列防火墙	H3C
		山石网科下一代防火墙	山石网科
		Juniper NGFW	Juniper
安全运营	SOC	Qradar	IBM
		HP Arcsight	惠普
		泰合信息安全运营中心 (SOC)	启明星辰
		Splunk	Splunk
		HanSight下一代安全管控平台	瀚思安信
		Next-Gen SIEM	logRhythm
		NetEye安全运维管理平台 (SOC)	东软
		FortiSIEM	Fortinet
		SIEM Enterprise	Trustwave
		安全管理平台SecFox-SNI	360网神
	容灾备份	阿里云	阿里云
		EMC Data protection suite	EMC
		IBM数据备份容灾解决方案	IBM
		NetBackup	Veritas
		业务连续性灾备解决方案	华为
		Veeam Availability Orchestrator	Veeam

	准入控制	Cisco Secure Access Control System Pulse Policy Secure ASM6000 Aruba ClearPass Policy Manager 网络准入控制系统UniNAC ExtremeControl	思科 Pulse Secure 盈高科技 Aruba Networks 联软科技 Exterme Networks
主动防御	WEB/WAF	Web Application Protector 雷池（SafeLine）下一代Web应用防火墙 Cloud Web Application Firewall DenyALL rWeb imperva WEB 应用程序防火墙 Next-Generation Web Application Firewall (WAF) 网站安全狗 天融信网页防篡改 绿盟网站安全防护 BIG-IP Application Security Manager	Akamai Technologies 长亭科技 Cloudflare Rohde & Schwarz Cybersecurity Imperva Signal Sciences 服云科技 天融信 绿盟科技 F5 Networks
	蜜罐	NetBait Kfsensor 幻云 谛听内网感知系统	NetBait Keyfocus 锦行网络 长亭科技
	数据库保护	McAfee Data Center Security Suite for Databases imperva Data Protection and Compliance 安华金和数据安全产品 明御数据库防火墙 TDSM-DBFW Secerno datawall	McAfee Imperva 安华金和 安恒信息 天融信 甲骨文
	网络类NIPS	FireEye Network Security cisco Next-Generation Intrusion Prevention System TippingPoint Next-Generation Intrusion Prevention System McAfee Network Security Platform Network security and protection Fortinet Advanced Threat Protection (ATP) NIP6000 下一代入侵防御系统 绿盟网络入侵防护系统 Managed Network Intrusion Detection System 山石网科入侵检测 / 防御产品	FireEye 思科 趋势科技 McAfee IBM Fortinet 华为 绿盟科技 Alert logic 山石网科
	移动/防病毒	诺顿手机安全软件 McAfee® Mobile Security 腾讯手机管家 7 360手机卫士 7.0 卡巴斯基安全软件 安卓版 Sophos Mobile Secure Enterprise Mobility Management Avast 免费手机安全软件 trend Mobile Security for Enterprises LBE安全大师 Free Antivirus for Android/iphone	赛门铁克 McAfee 腾讯 奇虎360 卡巴斯基 Sophos Avast 趋势科技 永杨安风 Avira
	主机类/主机	Symantec Endpoint Protection Microsoft antivirus protection Macfee终端安全保护产品 Sophos端点防护 Traps Advanced Endpoint Protection F-secure Server Security PC-cillin 2017 云安全软件 全功能增强版 The Signal Sciences RASP PROTECT+ ThreatZERO JHSE椒图主机安全环境系统	赛门铁克 微软 Intel security Sophos Palo Alto Networks F-secure 趋势科技 Signal sciences Cylance 椒图科技
事件监测	WEB类	360网站服务监控 明鉴®网站安全监测平台 H3C SecPath云安全监测中心	360企业安全 安恒信息 新华三
	日志类	绿盟安全审计系统[日志审计] 泰合信息安全运营中心系统-日志审计系统	绿盟科技 启明星辰
	数据库类	天玥网络安全审计系统 H3C Secpath 数据库审计产品	启明星辰 新华三
	网络类	Next-Gen SIEM 威胁发现设备TDA系列 Splunk Enterprise Security State-of-the-Art European SIEM 绿盟网络入侵检测系统 兰天智能安全平台 AlienVault 统一安全管理平台（USM） 山石网科入侵检测和防御系列 HanSight Enterprise 3	LogRhythm 亚信安全 Splunk LogPoint 绿盟科技 兰云科技 AlienVault 山石网科 瀚思安信

	移动终端	HanSight Enterprise 3 移动互联网恶意程序监测系统 移动安全管理中心	瀚思安信 恒安嘉新 卫士通
	主机类	IBM Tivoli	IBM
事件响应和取证	取证	X-Force Mandiant HerjavecGroup 明鉴®网络安全事件应急处置工具箱 guidance 美亚柏科	IBM FireEye Herjavec Group 安恒信息 Opentext 美亚柏科
	漏洞响应平台	HackerOne 漏洞盒子 补天漏洞响应平台	HackerOne 斗象科技 360企业安全
安全评测与加固	安全基线检查与主机安全	启明星辰安全配置核查管理系统 绿盟安全配置核查系统 Nessus 亚信科技 NSG-SMP安全管理平台 JHSE椒图主机安全环境系统 青藤云安全Analyzer	启明星辰 绿盟科技 Tenable 亚信安全 椒图科技 青藤云安全
	安全评估	绿盟远程安全评估系统RSAS 明鉴远程安全评估系统 网藤ARS 天镜脆弱性扫描与管理系统 Janus移动安全威胁数据平台 脆弱性扫描与管理系统TopScanner	绿盟科技 安恒信息 斗象科技 启明星辰 犇众信息 天融信
	安全众测	Bugcrowd Hackerone Synack Pen Test 漏洞盒子众测 360补天	Bugcrowd Hackerone Synack 斗象科技 奇虎360
	漏洞扫描	Acunetix Web Vulnerability Scanner 绿盟Web应用漏洞扫描系统WVSS 明鉴Web应用弱点扫描器 Netsparker Web Application Security Scanner 四叶草感洞 脆弱性扫描与管理系统（Web扫描）	Acunetix 绿盟科技 安恒信息 Netsparke 四叶草安全 天融信
安全意识与培训	安全意识与培训	IBM pwc普华永道 EY安永 KnowBe4 赛宁网安 AT&T Network Security 谷安天下 Inspired eLearning PhishMe 易安在线	IBM Pwc普华永道 EY安永 KnowBe4 赛宁网安 AT&T Network Security --AT&T Consulting Enterprise Security Assessment (ESA) Service 谷安天下 Inspired eLearning PhishMe 易安在线

关于报告

报告撰写团队

FreeBuf 研究院：廖文 乐朱樑 孟雷 施凯东 王峰 徐钟豪 张志鹏

鲍弘捷 王鹏 余桂茗 朱伊琳 朱嘉豪

美术设计：姚媛媛

关于FreeBuf

FreeBuf 是国内关注度最高的全球互联网安全媒体平台，同时也是爱好者们交流与分享安全技术的最佳社区。

在网络安全的形势日益严峻的 2017 年，FreeBuf 研究院对安全行业的威胁动态和企业应对方案进行了不同维度的调查，分别在3月、6月、11月和12月发布了四份研究报告。

除了此份《2017企业安全威胁统一应对指南》之外，还有《2017金融行业应用安全态势报告》，《2017 年度移动App安全漏洞与数据泄露现状报告》以及《深渊背后的真相之「薅羊毛产业」报告》。

如需了解更多信息，请访问 www.freebuf.com/paper 查看过去发布的安全报告。

企业安全威胁统一应对指南报告

FREEBUF

FreeBuf研究院

2017年12月