2019
中国主机安全服务报告

2019 WORKLOAD SECURITY SERVICE REPORT OF CHINA

中国产业互联网发展联盟
腾讯标准
腾讯安全
青藤云安全

联合出品


www.qingteng.cn

中国产业互联网发展联盟

中国产业互联网发展联盟是从事产业互联网融合创新的企业、科研院所、大学院校和协会联盟自愿组成的全国性非营利社会组织。该联盟设立的宗旨是基于“平等自愿、优势互补、资源共享、共同发展”的原则，围绕工信部的中心工作，整合联盟内企业、行业内企业的专家、技术、服务、平台等资源，发挥“官产学研资”协同优势，促进产业互联网新应用、新模式、新业态的创新发展，推动传统产业的转型升级。

腾讯标准

腾讯高度重视标准化研究与应用的工作，为适应外部环境的挑战，满足内部产品与服务的需求，于2016年起组建专业的标准化团队，以“通过标准化助力互联网服务提质增效“为使命，以”立足战略、聚焦业务、开放生态“为原则，专注于跟踪政策标准、获取资质认证、参与标准研究、牵头标准制定等方面工作，助力业务发展、体现责任担当、推动行业共识。

腾讯安全

腾讯安全依托 20 年多业务安全运营及黑灰产对抗经验，凭借行业顶尖安全专家、最完备安全大数据及 AI 技术积累，提供紧贴业务需要的安全最佳实践，构建了一套自适应的闭环安全防护体系，包含基础安全防护体系，安全运营中心、业务安全服务体系等，其产品矩阵涉及终端安全、网络安全、云安全、业务安全、数据安全、安全管理、安全服务等多个安全方向，且行业解决方案涵盖了政企、金融、医疗、教育、交通等多个领域。帮助客户从技术和管理角度加强网络安全建设，提升企业竞争力，创造更大价值。

青藤云安全

青藤云安全以主机安全为核心，采用自适应安全架构，将预测、防御、监控和响应能力融为一体，构建基于主机端的安全态势感知平台，为用户提供持续的安全监控、分析和快速响应能力，帮助用户在公有云、私有云、混合云、物理机、虚拟机等多样化的业务环境下，实现安全的统一策略管理，有效预测风险，精准感知威胁，提升响应效率，全方位保护企业数字资产的安全与业务的高效开展。

张福
青藤云安全CEO

在整个安全体系保护的对象里，主机就是皇冠上的那颗明珠。随着5G、物联网、工业互联网的大发展，越来越多的数据会被存储在主机上，越来越多的业务会以数字化的形态运转在主机上，越来越多的场景会打通虚拟和现实的边界，从线上映射到线下，和人们的生活息息相关。因此，对主机的保护将会变得越来越重要。在未来，安全行业必须解决“最后一公里”的问题，安全的核心战场必然会从网络边界向内转移到主机。如何做好主机安全?如何应对变幻莫测的攻击技术?2019年主机端都遭遇到哪些挑战?希望这本详实的《2019中国主机安全服务报告》能带给大家一些答案。

黎巍
腾讯安全副总裁
腾讯云安全负责人

产业互联网时代，大量的企业业务都将依托在云上，以数据为载体的数字资产也逐渐成为企业的核心资产。与此同时，黑客们也对这些核心资产虎视眈眈。数据攻击和窃取的事件越发频繁，各类攻击手段也层出不穷。面对日益严峻的网络安全形势，企业需要建立强大的安全防御体系以不断增强对恶意攻击的抵抗能力。主机安全作为企业安全最后也是最重要的一道门，需要不断增强对恶意入侵检测的速度和准确率。腾讯安全致力于携手合作伙伴，将积累20多年的能力和经验开放，为云上客户打造更加主动、积极、智慧的安全体系。

杨志锋
中国产业互联网发展联盟秘书长

伴随着新冠病毒在全球的蔓延，全世界人民都将经历一段“与毒共舞”的特殊时期。由此带来的在线活动激增，既带动了产业互联网的深入发展，也为一些隐秘活动提供了可趁之机。

在可见的未来，无论计算的商业形态如何变化，主机安全仍将是产业互联网时代线上“防疫”的根本。产业互联网的发展之路能走多远，主要取决于我们能否从线下的疫情吸取教训，为主机安全运行提供应急使用的“口罩和防护服”，并依靠“疫苗和特效药”取得最终的胜利。

衷心希望这本主机安全报告的发布，能化作产业互联网安全发展的哨音，为线上防疫提供“救治指南”，帮助我们实现更加繁荣美好的线上生活。

01

执行摘要
EXECUTIVE SUMMARY

02

主机安全状态整体概览
OVERVIEW OF WORKLOAD SECURITY STATUS

CONTENTS

03

主机安全市场产品形态
PRODUCT FORM OF WORKLOAD SECURITY MARKET

04

主机安全产品技术分析
TECHNICAL ANALYSIS OF WORKLOAD SECURITY PRODUCTS

执行摘要

EXECUTIVE SUMMARY

主机可以为内部和外部用户提供各种服务，也可以用来存储或者处理组织机构的敏感信息，根据提供的不同服务可以分为Web服务器、电子邮件服务器、数据库服务器、基础设施管理服务器、文件服务器等。由于主机上承载的数据和服务价值巨大，因而成为黑客最喜欢的攻击目标。以下是几种常见的主机威胁示例：

A. 攻击者利用主机软件或其底层操作系统中的漏洞来获得未经授权的访问。
B. 针对服务器的DoS攻击，阻止有效用户使用其服务。
C. 截获在服务器和客户端之间传输的未加密或弱加密的敏感信息。
D. 攻击者通过失陷主机获取网络中其它未经授权的资源访问。

本报告旨在帮助各组织机构更好地保护主机安全，包括如何确保底层操作系统安全、软件配置安全、以及通过补丁、安全测试、日志监控以及操作系统文件备份来维护安全配置。

目前，主机安全的技术正在从最初的资产探测、杀毒等，开始向检测响应、隔离控制、行为检测等方向发展，未来一定会朝着主动检测、快速响应、安全适配三个方向进化。

例如，基于当下最热门的ATT&CK框架，安全从业者可以从覆盖度、检测点等方面找到自身安全检测能力的改进方向，包括如何根据ATT&CK框架去检查目前安全产品的整体覆盖度，以及如何将ATT&CK所涵盖的技术点融入到产品中。

当然，面对日趋猖獗的黑客攻击，单纯地指望通过防御和管控策略已行不通，必须更加注重检测与响应。为最大限度地、科学、合理、有序地处置网络安全事件，建立完善的响应流程尤为重要，组织机构需要根据网络安全应急响应总体策略，在每个阶段制定适当的目标，明确响应顺序和过程。

此外，随着新技术的快速发展，以容器、微服务、Serverless 为代表的云原生技术，使得企业 IT 架构发生了巨大变化，其安全挑战不容忽视。

总得来说，主机安全最佳实践应该从主机安全管理机制、主机操作系统的安全、主机软件的安全、持续的主机安全运维等角度来构建全方位的安全方案。

组织机构应当采取合适的主机管理机制，包括对主机资产的识别，以及确保信息系统资源的机密性、完整性和可用性。建议采取下列措施：

A. 配置控制管理措施
B. 持续进行风险评估和管理
C. 满足合规的要求、标准化的软件配置
D. 加大安全意识培训
E. 建立应急计划、业务连续性和灾难恢复计划

组织机构应该确保主机操作系统的部署、配置和管理满足安全需求。保护主机安全性的第一步是保护底层操作系统。如果底层服务器的操作系统配置得当，就可以避免许多安全问题。使用安全配置指南或检查列表可以帮助管理员有效地保护服务器。

组织机构需要确保主机上安装的应用能够满足安全要求。最重要的原则是安装最小数量的所需服务，并通过打补丁或升级软件来消除漏洞。保护服务器应用程序通常包括以下步骤：

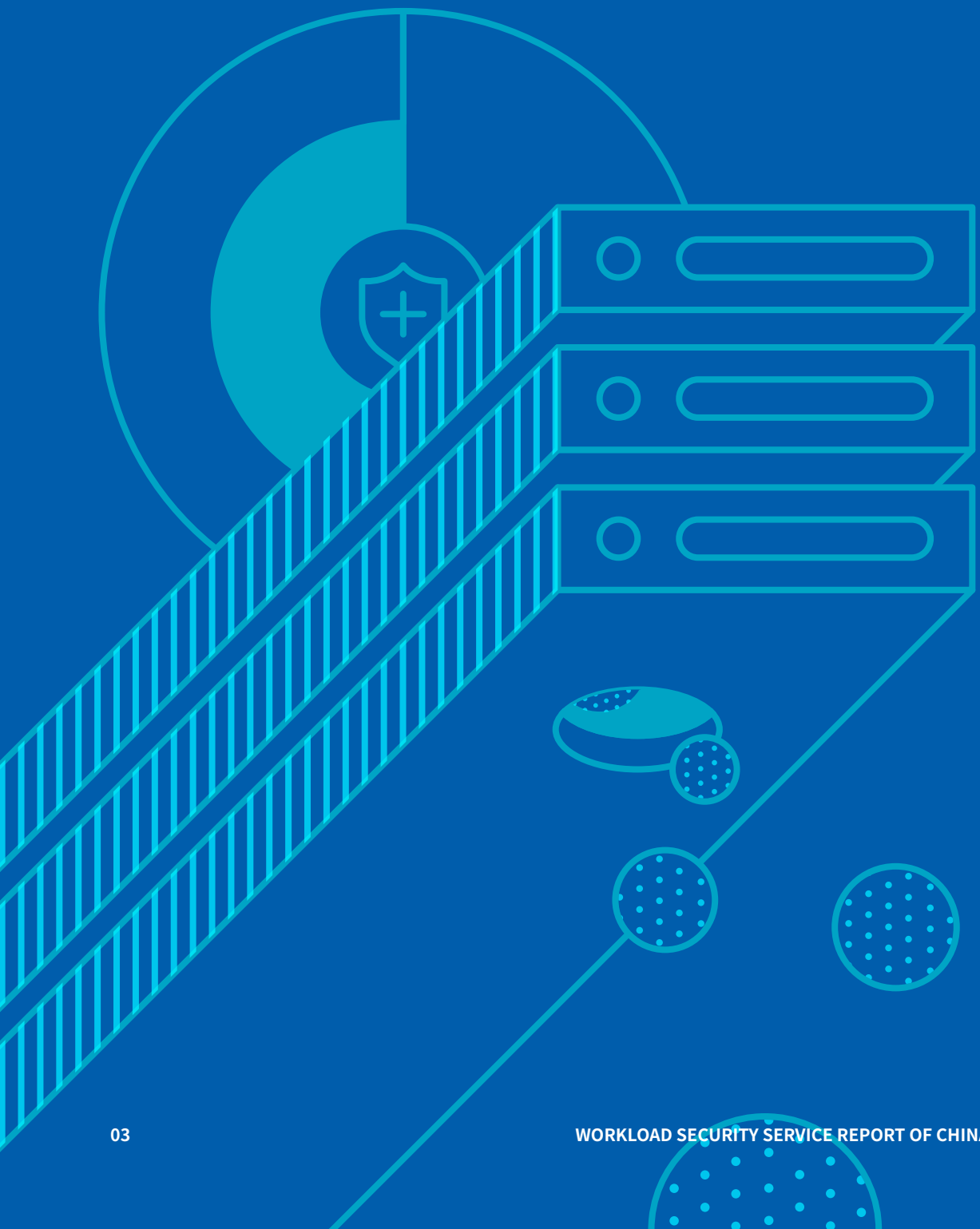
A. 打补丁或升级主机应用程序
B. 去除不必要的服务或应用
C. 配置主机用户权限和访问控制
D. 配置主机资源控制
E. 测试主机应用的安全性

组织机构需要确保服务器的持续安全性，需要采取以下行动，包括不限于：

A. 经常配置、保护和分析日志文件
B. 经常备份关键信息
C. 建立回滚策略
D. 及时测试和应用补丁
E. 定期测试安全性

主机安全状态整体概览

OVERVIEW OF WORKLOAD SECURITY STATUS



主机作为承载公司业务及内部运转的底层平台，其稳定、安全地运行是公司正常运转的前提保障。由于主机上运行着各种各样的业务，会存在着各类漏洞及安全问题。攻击者以此为目标，通过对主机进行攻击来获利，但这将会给公司发展造成严重的危害和损失。因此，主机层面的安全问题绝不容忽视，本报告将从主机资产、主机风险、主机入侵分析、主机合规分析四个方面详细分析2019年主机安全的整体概况。

01 主机资产概况

如果没有完整的、详细的主机资产清单，安全运维团队将无法确保组织机构的安全，因为任何人都无法保护“未知”事物的安全性。

虽然在过去封闭的IT环境中，通过对所有硬件、软件和网络元素进行统计和监视，安全性还是可控的。但是随着云计算、移动设备、物联网等技术的快速发展，传统网络边界已经不复存在。因此，编制一份完整的资产清单并随时进行更新，这一点愈发困难和复杂。随着资产盲点在网络环境中成倍增加，黑客入侵、数据泄露、恶意软件感染以及不合规的风险也在成倍增加。本报告通过分析大量的企业级主机核心资产情况，从而为各企业制定安全防护策略提供支持和帮助。

· 不同主机操作系统的安装情况

常见的主机操作系统有很多，比如Windows、Linux、Unix等，而在企业级主机上经常使用的都是Windows和Linux系统。通过统计分析发现，在企业级客户中，超过81.45%的主机使用都是Linux操作系统，只有18.55%主机使用的是Windows操作系统。这其中原因有很多，比如Linux兼容性更好、模块化、资源消耗少等等原因，让很多客户都会选择Linux系统。

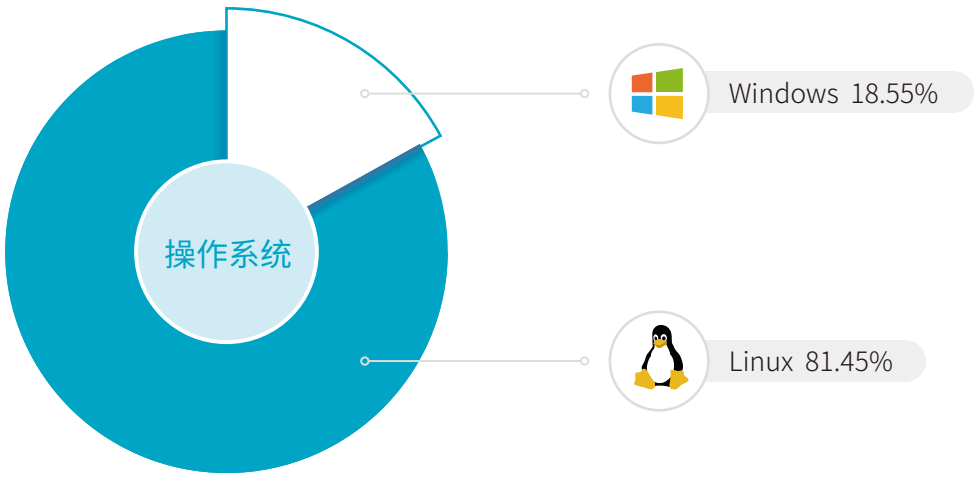


图2-1：不同主机操作系统的使用比例

在上述使用Linux操作系统的主机中，超过73%都是使用CentOS，该系统是基于Red Hat Enterprise Linux的源代码编译而成，适用于一些对主机稳定性要求比较高的企业。新版本的CentOS大约每两年发行一次，而每个版本的 CentOS 会定期（大概每六个月）更新一次，以更好地支持新硬件。

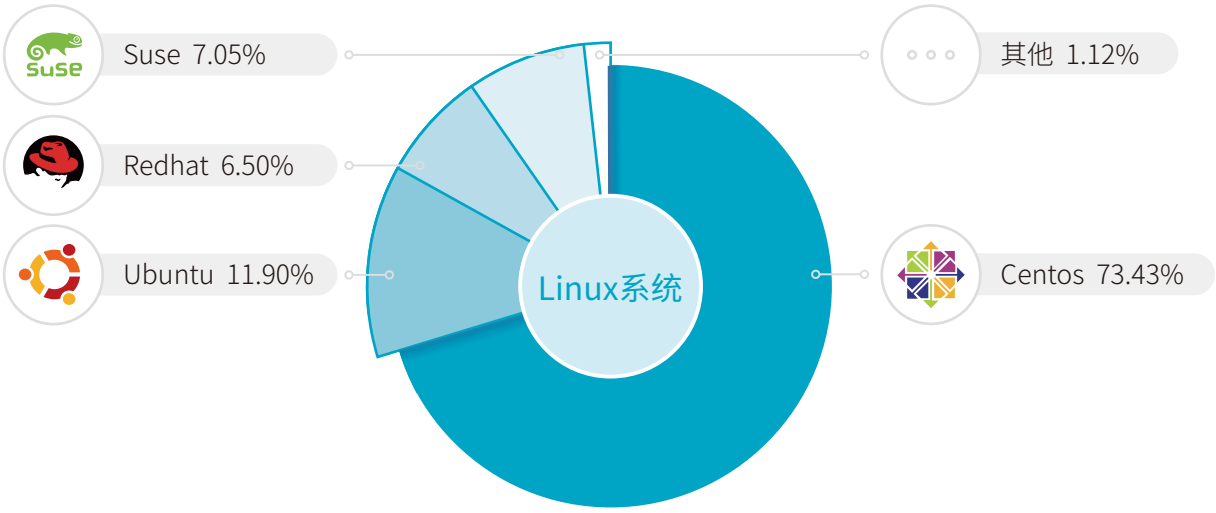


图2-2：Linux系统不同版本的使用情况

· 特殊账号清点分析

很多黑客入侵都是从账号入手，一般用软件扫描弱口令或者暴力破解登陆账号。一旦黑客拿到了特殊账号，比如Root权限就拥有了最高权限进行任意修改。如果在主机中使用默认Root账号，那么黑客只需要暴力破解密码即可。因此为了保障主机安全，一定要谨慎处理系统中特殊账号，包括UID为0、GID为0、Root权限账号、Sudo权限账号、交互登录账号等等。

例如，开发测试人员可能会要求运维人员在服务器上开放一个Root权限运行某个程序，运维人员一般会利用Sudo给其临时授权，让其以Root权限运行某个程序。但是Sudo授权也要谨慎，否则很可能被恶意提权成Root账户。

通过对样本数据的分析可知，74%的主机上都存在UID为0、GID为0、Root/Administrator账号、Sudo权限等特殊账号。这些特殊账号，往往会成为备受黑客青睐的资产，属于高危重点保护资产。

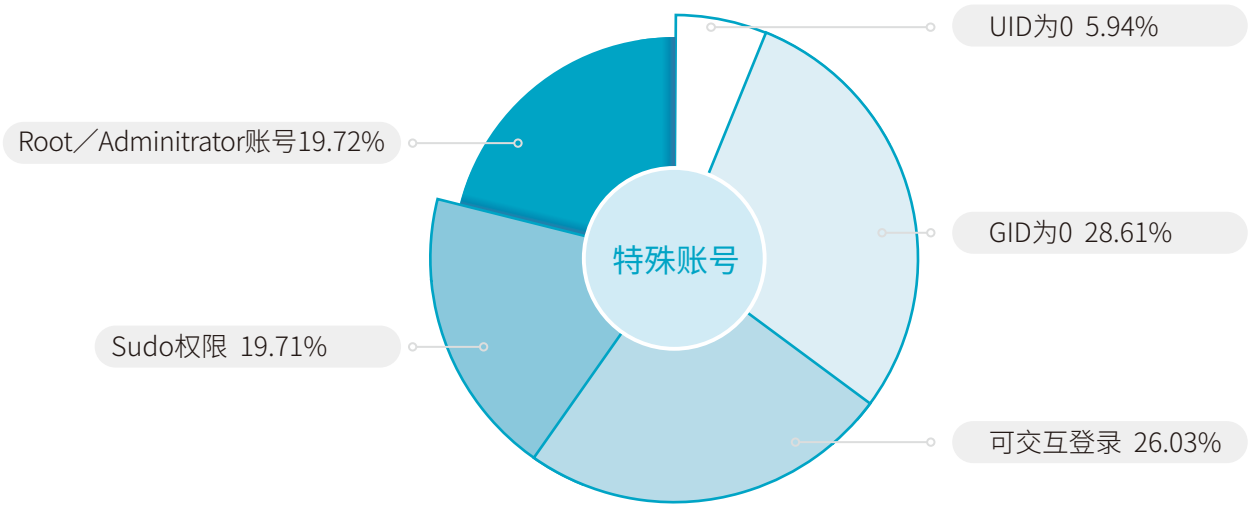


图2-3：主机特殊账号的使用情况

· Top5 Web服务应用分布

Web服务一般是指互联网上某种类型的计算机程序，可以向浏览器等Web客户端提供文档，也可以放置网站文件或者数据文件。目前最主流的Web服务包括Tomcat、Apache、Nginx 、IIS。

在样本数据分析中，发现在Linux系统中，使用最多的Web服务应用是Tomcat服务，高达58%，其次是Nginx，使用率达到了32%。

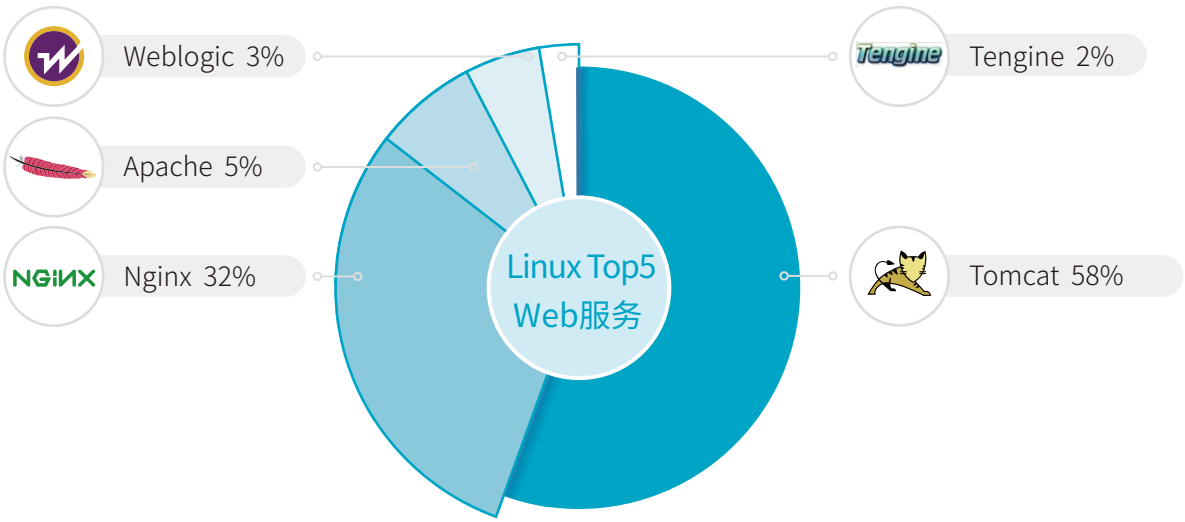


图2-4：Linux Top5 Web服务的使用情况

而在Windows环境下，IIS使用最多，达到47%，其次是Tomcat，达到36%。另外，Apache和Nginx的使用也占到了一定比例。

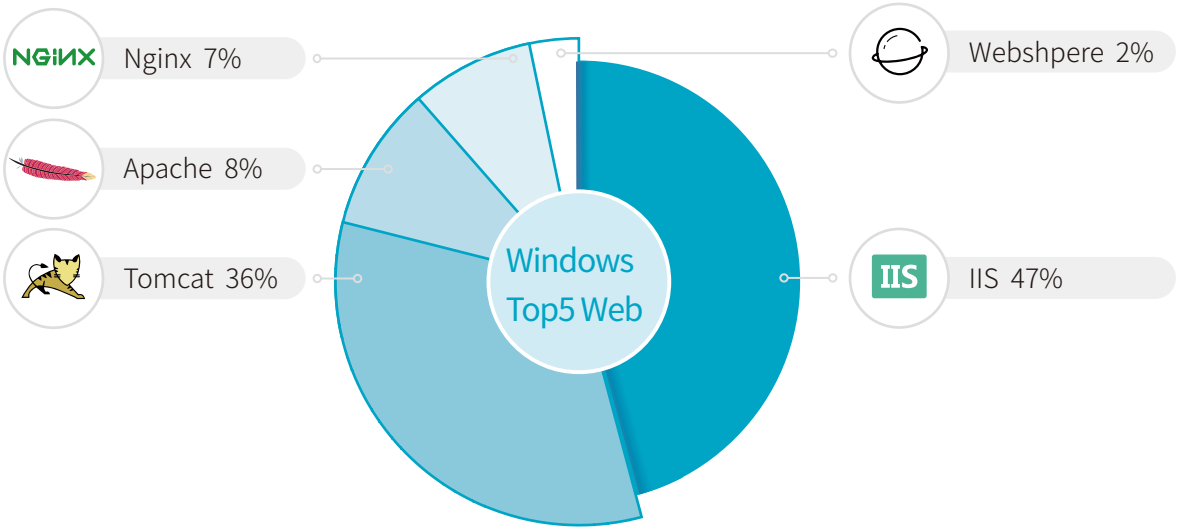


图2-5：Windows Top5 Web服务的使用情况

· Top10 Web应用框架类型

Web 应用框架是建立 Web 应用的一种方式。从简单的博客系统到复杂的 AJAX 应用，Web 框架的作用就是隐藏处理 HTTP 请求和响应相关的基础代码。

在Linux环境下，Web应用框架使用最多是Spring，达到了27%，其次是Spring MVC、Quartz、Jackson、Fastjson，其使用率也超过了10%。

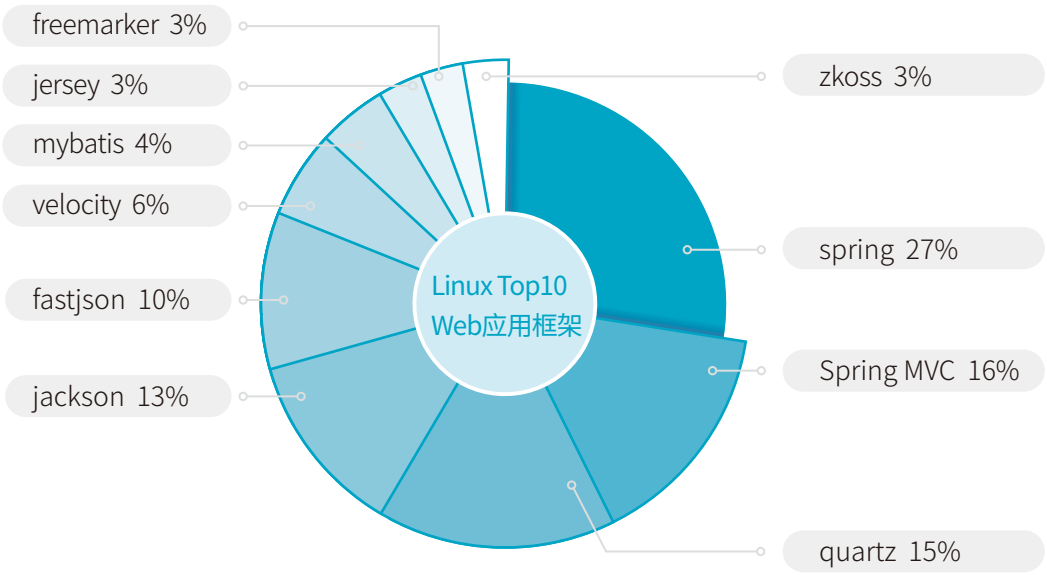


图2-6：Linux Top10 Web应用框架类型

在Windows环境下，Web应用框架使用最多也是Spring，达到了19%；其次是Jackson、Spring MVC、Fastjson、Freemark，其使用率也超过了10%。

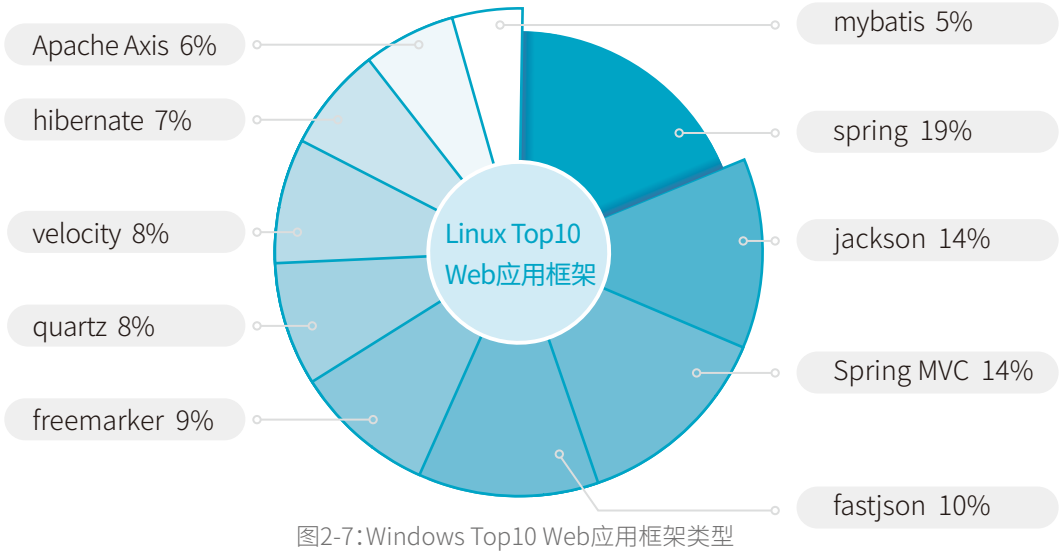


图2-7：Windows Top10 Web应用框架类型

· Top5数据库应用的分布

从整体情况看，MySQL、SQL Server、Oracle、PostgreSQL、MongoDB五大数据库产品处于遥遥领先的地位。虽然，DB2曾经是数据库的领导者，但近几年发展乏力，在持续下滑，特别是互联网行业及中小企业IT里基本没有DB2的身影，在金融等领域也面临着非常大的挑战。

在统计Linux环境样本数据中，发现MySQL、PostgreSQL、Redis占比都超过了20%，排名第四和第五的是MemCache、MongoDB。

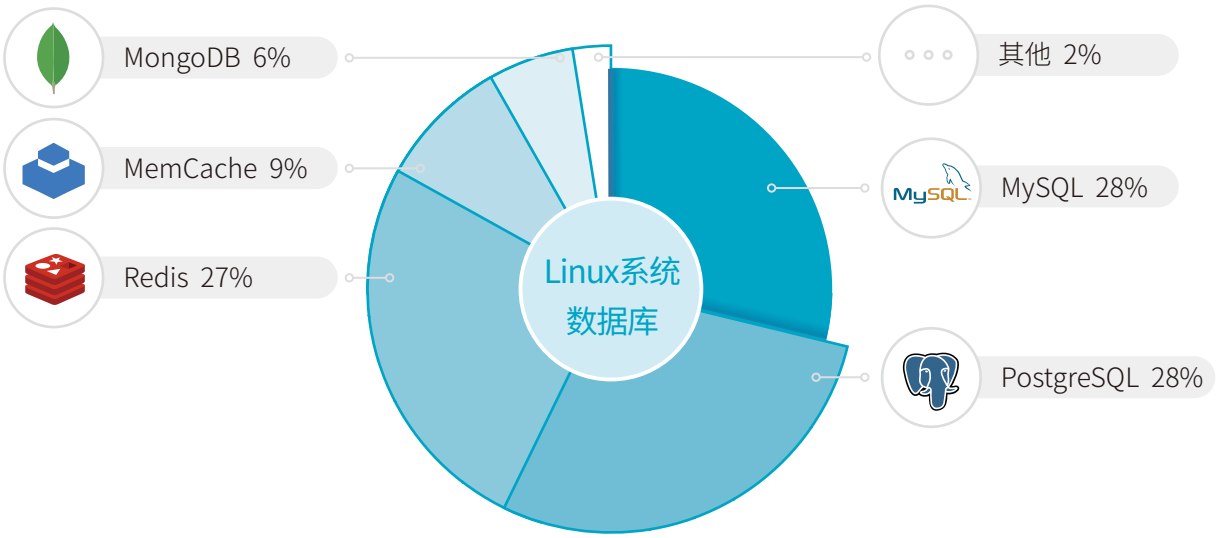


图2-8：Linux 系统中数据库的使用情况

在Windows环境中，使用最多的是SQLServer和Oracle，其中SQLServer的使用率更是达到了73.93%。

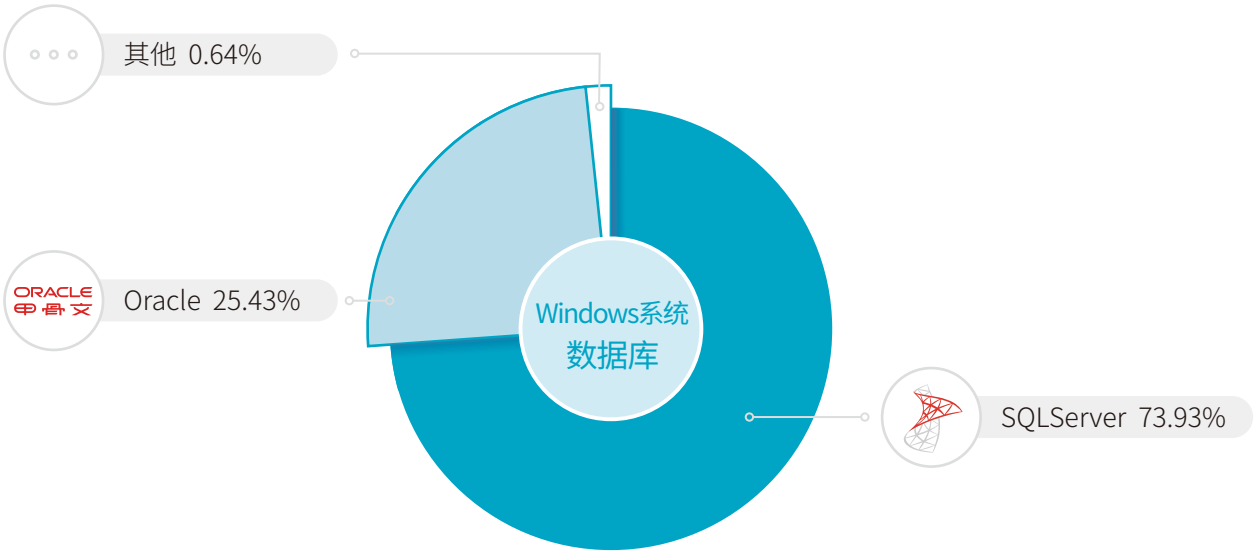


图2-9：Windows 系统中数据库的使用情况

02 主机风险总览

密歇根大学的一项研究表明，一台有开放端口或漏洞的主机连网后，在23分钟内就会被攻击者扫描，在56分钟内开始被漏洞探测，第一次被彻底入侵平均时间是19小时。软件缺陷、配置错误、代码Bug……这些问题都会导致系统存在风险。但是不论风险来源于哪，它们都不会自行消失。

为了在黑客入侵前发现系统风险点，安全人员需要通过专业的风险评估工具，对风险进行检测、移除和控制，来减小攻击面，包括安全补丁、漏洞、弱密码、应用风险、账号风险等。

· TOP10主机漏洞攻击

CNNVD将信息安全漏洞划分为26种类型，包括配置错误、代码问题、资源管理错误、跨站脚本、路径遍历、SQL注入、代码注入、命令注入、权限许可和访问控制、访问控制错误等等。

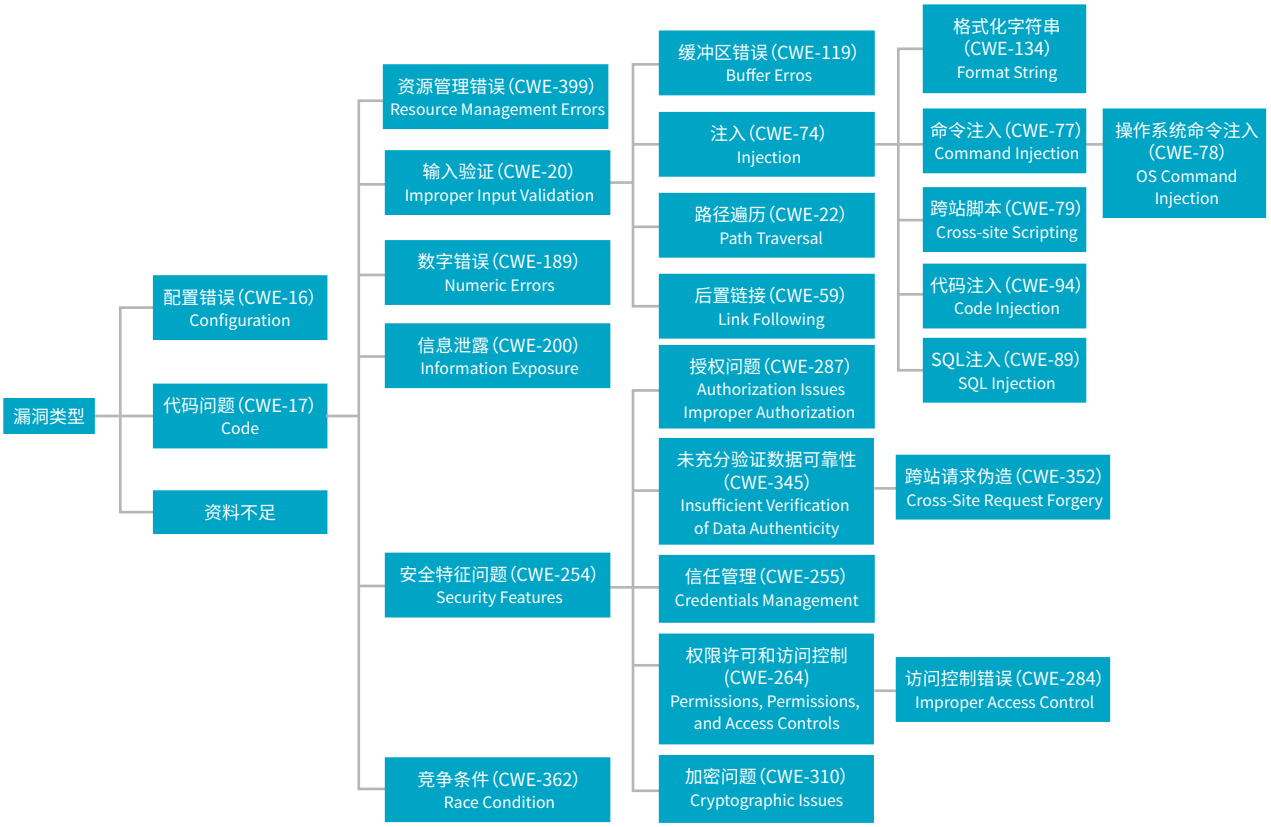


图2-10：漏洞分类层次树

基于漏洞所影响的主机数量，发现2019年影响范围最大的TOP10漏洞，有很多都是前几年的漏洞。尤其是针对那些老旧资产，补丁修复更是严重不足，因此，这些漏洞就成为了黑客入侵的突破口。

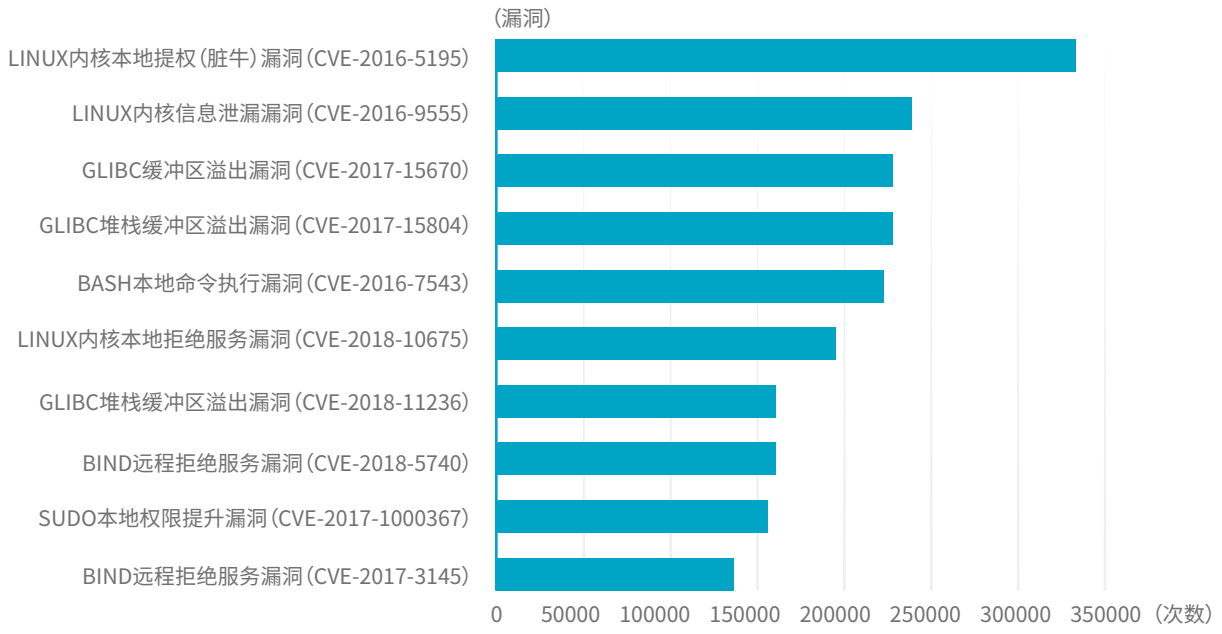


图2-11：2019年影响主机TOP10的漏洞

· 主机高危端口的开放情况

这里的高危端口是指常黑客攻击频次较高的端口。在对Web服务器等互联网空间资产做空间测绘后发现，有大量的资产开放了高危端口，存在较高的安全隐患。除了22、1900等端口之外，还有较大比重的邮件服务、数据库服务等端口暴露在公网上。

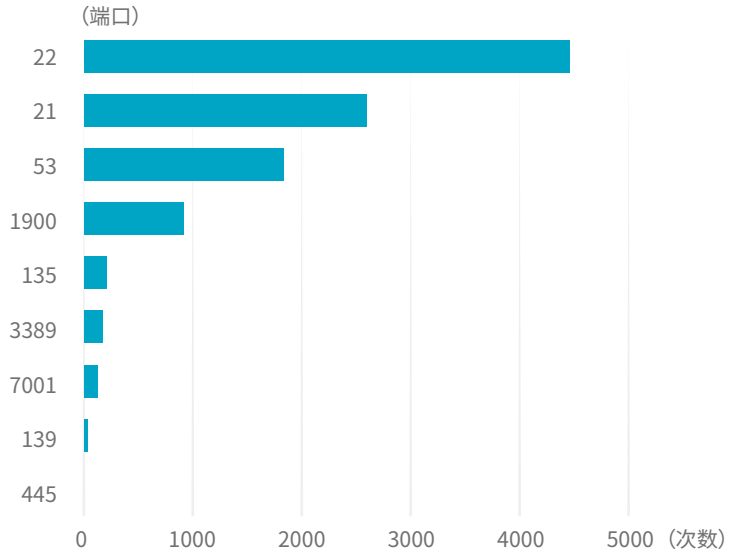


图2-12：常见高危端口的开放情况

22端口是Linux平台默认的SSH远程连接服务端口，而3389是Windows默认的远程桌面的服务（RDP, Remote Desktop Protocol）端口，通过SSH、RDP远程连接是一种非常方便的对服务器进行操作的方式，所以，很多服务器管理员都会开启22、3389端口远程桌面服务。

因此，很多黑客攻击者很喜欢尝试入侵22、3389端口，例如通过暴破。如果服务器存在弱密码登录的情况，很容易就被暴破成功，进而服务器被黑客控制。特别是今年曝光的BlueKeep（CVE-2019-0708）、Windows RDS（CVE-2019-1181），均是Windows远程桌面服务的漏洞并且危害巨大，而3389又是Windows远程桌面的默认端口，开放3389的Windows服务器更容易受到入侵攻击。建议服务器修改默认的远程连接端口，如无必要，可关闭该端口。

7001端口是WebLogic的默认端口。2019年WebLogic被曝出了多个可被远程攻击的高危漏洞，并且已有黑客组织利用最新的WebLogic漏洞入侵，投放勒索病毒。如果漏洞未能及时修复，则不排除被远程攻击、控制的可能。

1900 UDP端口源于SSDP Discovery Service服务。通过使用SSDP协议对端口1900进行扫描可以发现UPnP（即插即用协议）设备，攻击者可以利用这些设备发动DDos攻击，制造出大量流量，可导致目标企业的网站和网络瘫痪。

根据测绘结果分析，2019年服务器445端口开放的比例相对上半年有所降低，但仍有部分服务器资产开放了445端口。我们所熟悉的永恒之蓝勒索病毒就是利用445端口传播。如果这些服务器没有打上相应的补丁，那么仍然存在被勒索病毒攻击的风险，即便是打上了补丁，也仍然需要面对勒索病毒变种的攻击。

· 主机软件弱密码盘点

因为安全配置不当导致的安全问题，对主机的安全也造成了较大的影响，其中弱密码最不容忽视。定期检测并修改弱密码能有效地减少安全风险。

不同服务都有一些具有各自服务特色的弱口令，有一部分是安装时的默认密码。比如MySQL数据库的默认密码为空。通过分析发现，主机软件弱密码主要集中在MySQL、SSH、SVN、Redis、vsftpd这五类应用上，其中MySQL和SSH弱密码问题更是超过了30%。

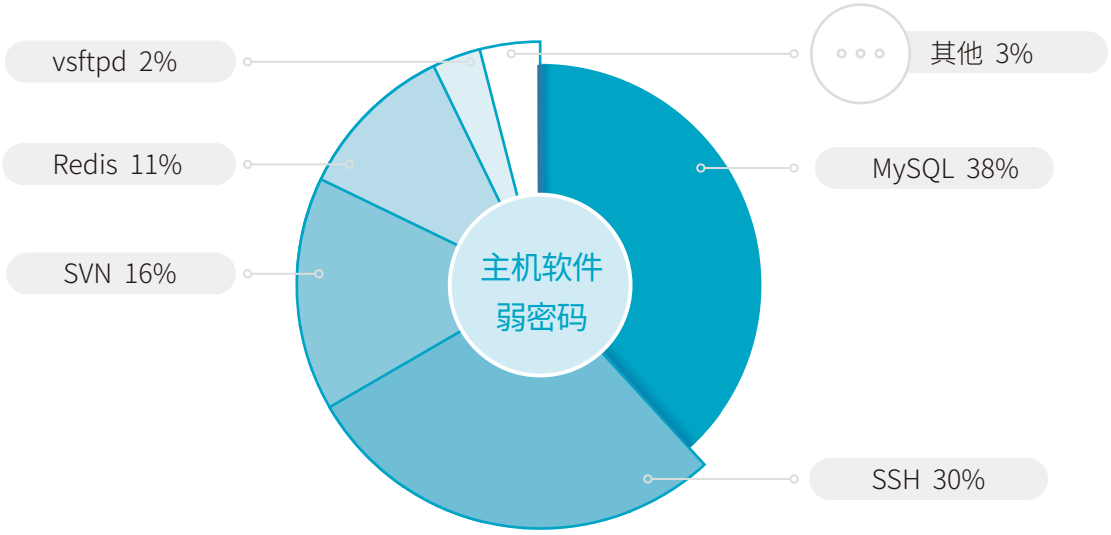


图2-13：主机软件弱密码盘点

· 主机账号危险程度分析

主机系统账号普遍存在各类风险，尤其是那些拥有Root权限的高风险账号更需要实时进行监控。根据风险账号检测结果中的信息，删除主机中无用的账号，按照权限最小化原则限制主机中可疑账号的权限。此外，还需要通过限制关键配置项，限制非管理员的文件访问权限和文件修改权限，防止未授权的访问权限和使用操作。通过主机账号分析，超过95%的账号都属于高危账号，这些高危账号通常都存在不合规的配置问题。

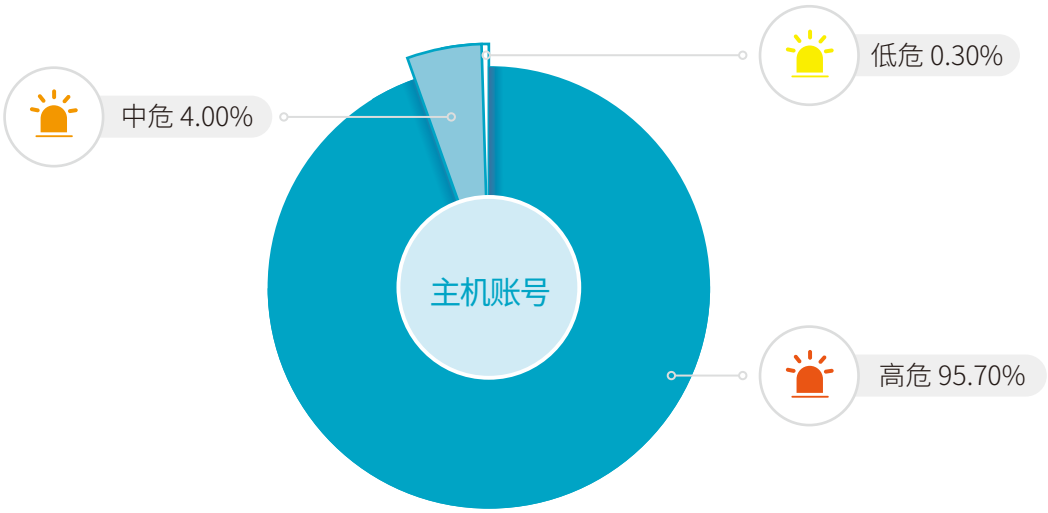


图2-14：主机账号危险程度

· 补丁修复状况分析

各种软件的漏洞已经成为大规模网络与信息安全事件和重大信息泄露事件的主要原因之一。针对主机漏洞带来的危害，安装相应的补丁是最有效、也是最经济的防范措施。对于主机数目众多、应用种类繁杂的大型网络，如果不能及时跟踪补丁的更新，将极大地威胁到网络与信息安全，造成不可挽回的损失。

从等级上来说，漏洞补丁可分为高、中、低三大类。应该着重优先解决高风险漏洞，根据安全影响的层面和组织对安全的要求适度处理中等风险的漏洞，低风险的漏洞可以适当忽略。

根据样本数据分析，未修复的补丁基本是高危或者中危的，尤其是未修补的高危漏洞更是达到了45.77%。

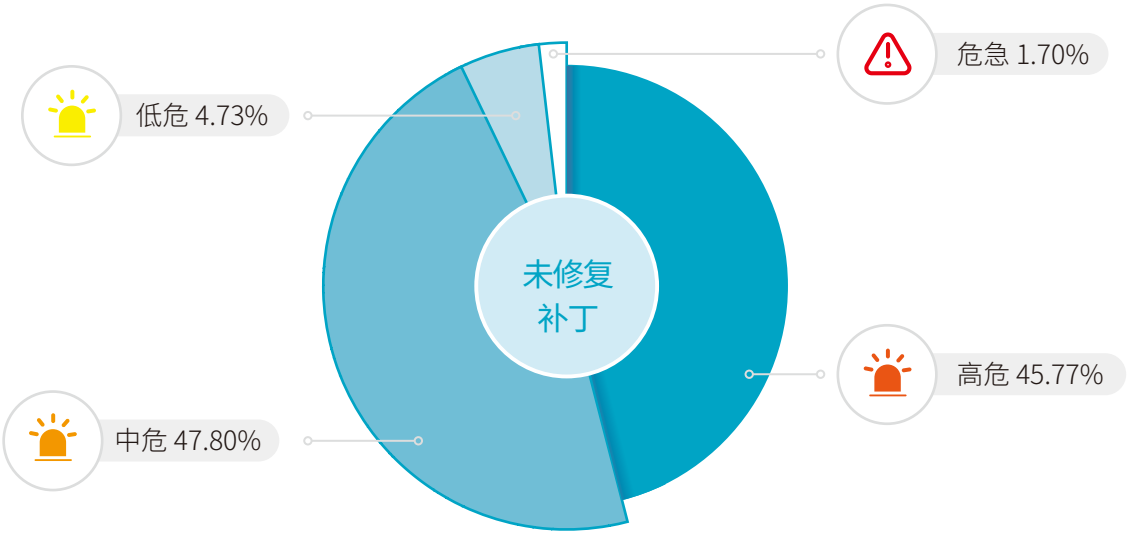


图2-15：未修复补丁情况

· 不同行业感染病毒类型分布情况

风险类软件在各行业的染毒事件中占比最高（40%以上），科技行业相对其他行业感染风险软件的比例更小。由于风险软件的感染主要是不良的上网习惯及缺乏安全意识引起的（如使用盗版软件或外挂工具等），可能科技行业从业人员的上网安全意识相对更高。

感染型木马在教育行业感染比例相对较高，可能和该行业频繁的文件交互传输有关。

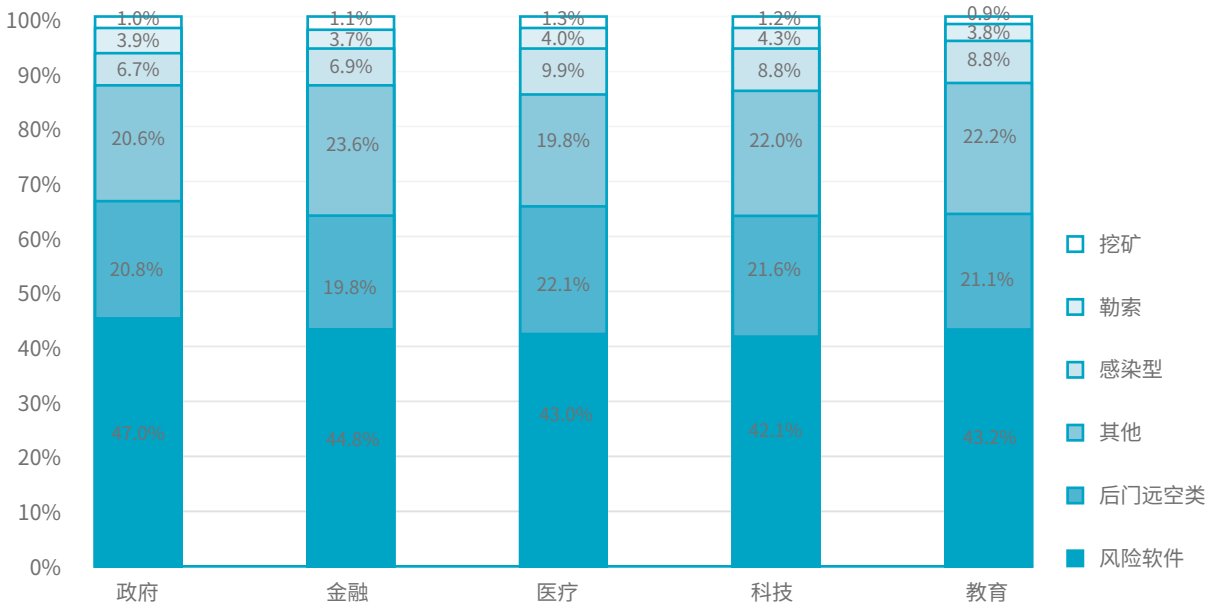


图2-16：不同行业感染病毒类型分布

后门远控类木马是除了风险软件之外感染量最大的染毒类型，占比在20%左右。后门远控类木马有着极高的隐蔽性，接受远程指令执行信息窃取、截屏、文件上传等操作，对金融科技等信息敏感行业可造成极大危害。

03 主机入侵分析

· 常见主机漏洞攻击类型

组织机构的服务器中如果存在漏洞或简单的控制可能导致灾难性的后果，许多通过黑客攻击和恶意软件进行的入侵是可以预防的。通过对暴露在公网的服务器做抽样分析发现，在常见的攻击类型中，远程代码执行（RCE）、SQL注入、XSS攻击类型比例较高，同时黑客为了获取服务器、网站的基本信息，常见的探测性扫描（Probe Scan）量同样非常高。

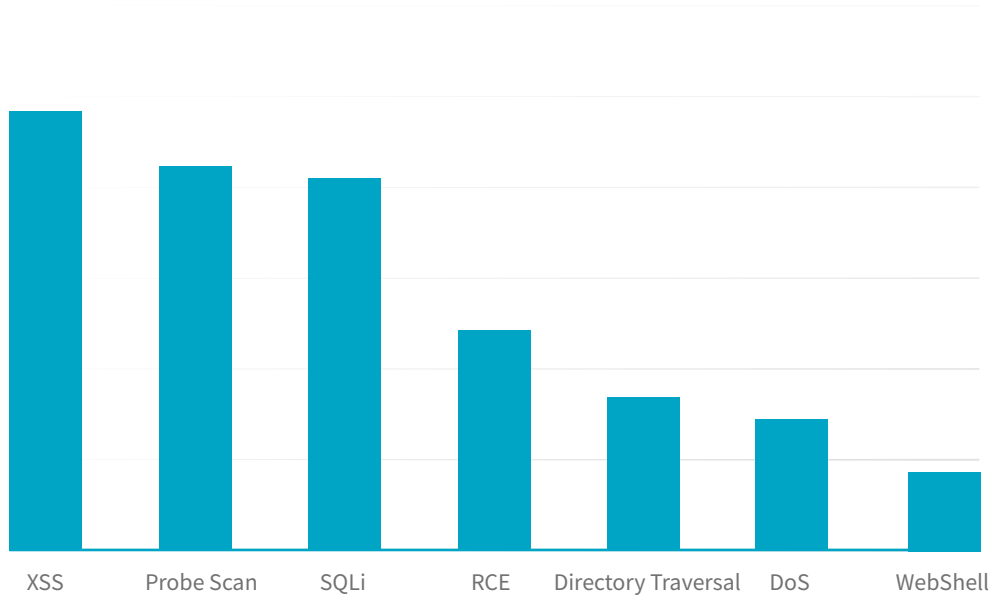


图2-17：常见主机漏洞

· 全国主机感染病毒木马的情况

2019年，全国企业用户服务器病毒木马感染事件超百万起。其中Webshell恶意程序感染事件占73.27%；Windows恶意程序感染事件占18.05%；Linux恶意程序感染事件占8.68%。

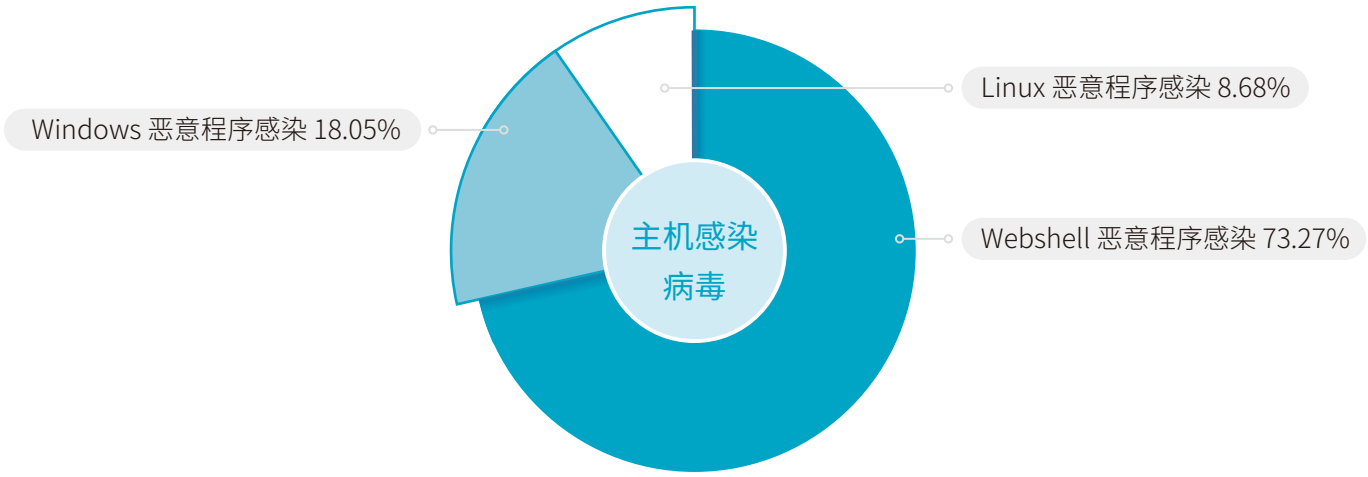


图2-18：主机感染病毒木马的情况

针对服务器的攻击事件，主要是以Webshell为主。从攻击者的角度，Webshell仍然是攻击的第一方法，且成功率高于直接向目标写入二进制可执行程序。

从感染主机中，总共发现超1万种木马病毒，其中Webshell 约占27%，Windows木马病毒约占61%，Linux木马病毒约占12%。

从比例来看，Windows平台的木马病毒的种类仍然是最多的，说明Windows平台仍然是最易受到病毒木马攻击的平台。Webshell是一类专门针对服务器攻击的恶意程序，随着云服务器的大量增长，Webshell的种类也在快速的增加。而值得注意的是Linux平台的木马病毒也是随着云时代的到来而快速增长。

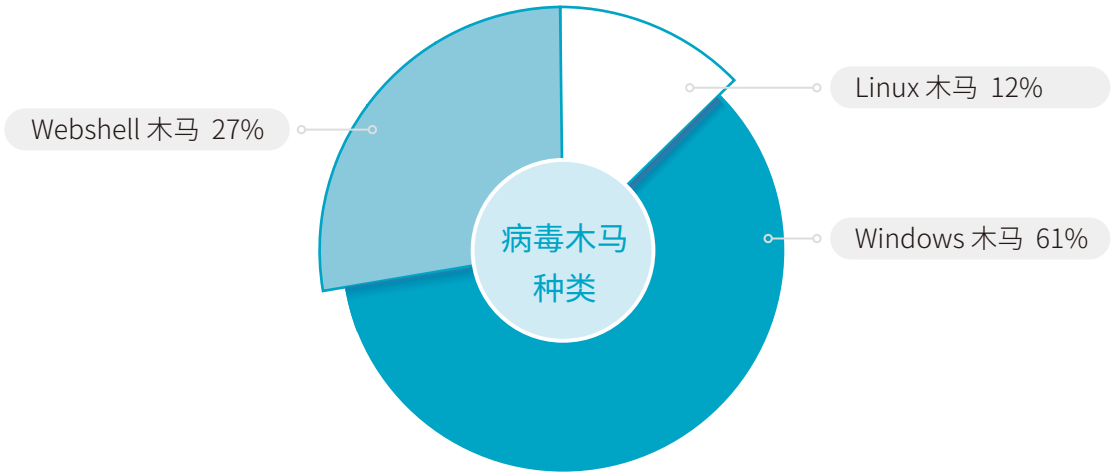


图2-19：病毒木马种类分布

如果按月份来统计，2019年感染事件多发生在年中，即3月到8月，随着企业的安全意识越来越强，安全投入越来越大，到年末感染事件呈减弱趋势。如下图所示：

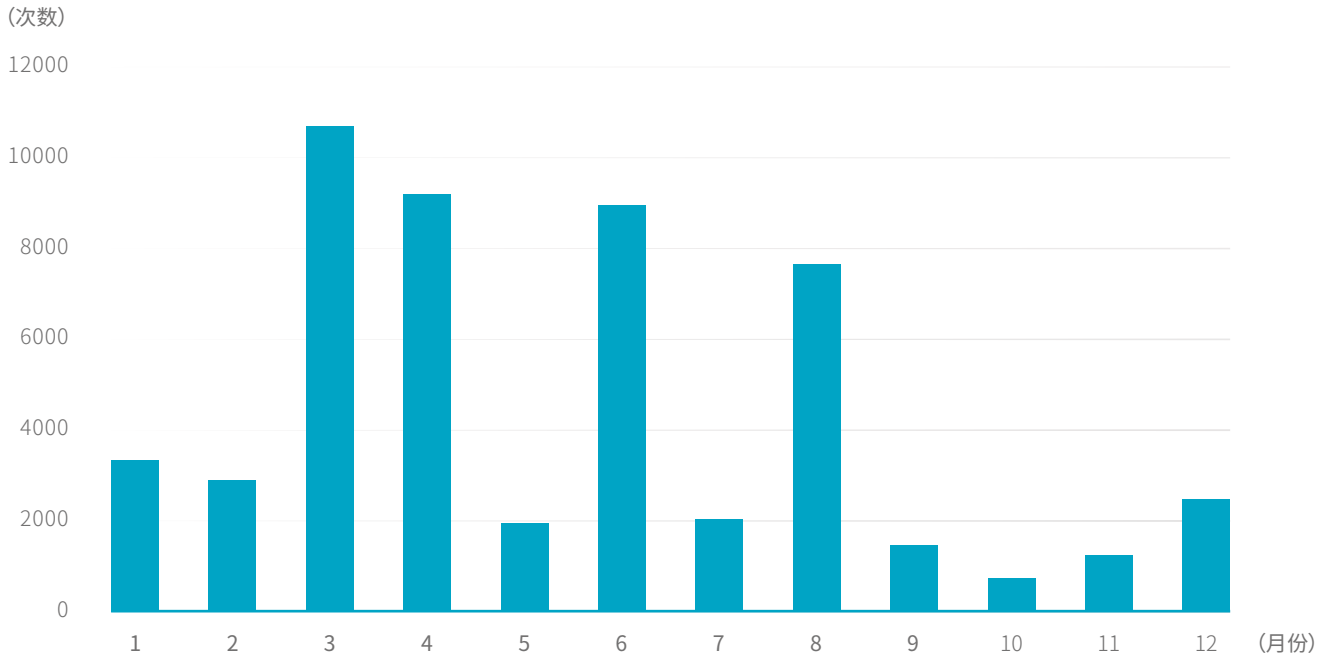


图2-20：2019年主机感染事件趋势图

· Webshell恶意程序分析

由上文可知，2019年Webshell恶意程序感染事件为近80万起，占所有感染事件的70%。从被感染服务器的数量来看，Windows服务器感染Webshell占所有Windows服务器的约44%，Linux服务器感染Webshell占所有Linux服务器的约0.2%。这说明Windows服务器更容易受到Webshell的攻击。

从感染的Webshell语言类型来看，PHP类型的Webshell是最多的，其次是ASP语言。

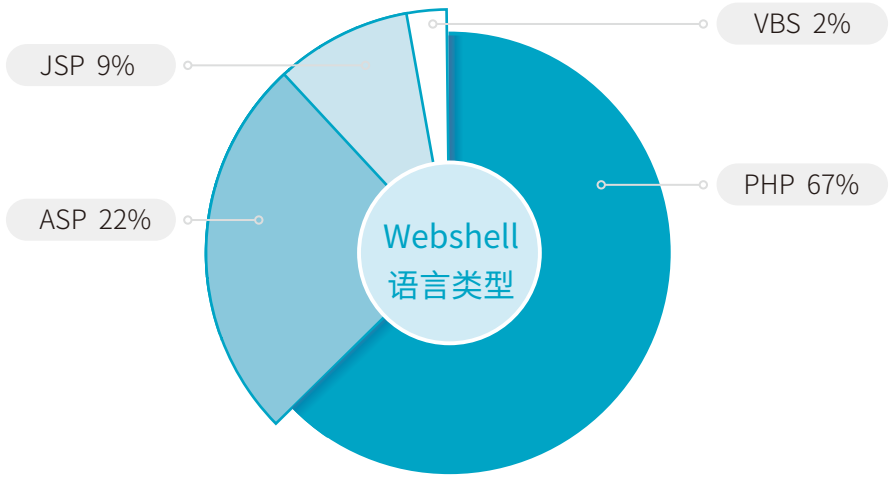


图2-21：Webshell语言类型的比例分布

根据2019年捕获的超3000类Webshell样本数据看，一句话木马的种类最多，占Webshell类型的36%。因此，对于Webshell的检测防御，需要重视一句话木马。

· 暴力破解目标及时间分布

通过系统弱密码获取进入主机的入口是攻击者最喜欢也是最容易的一种攻击方式。攻击者利用软件对那些暴露在公网上的RDP、SSH、Telnet、FTP等服务进行扫描，然后进行暴力破解。以存在弱口令的主机为基本立足点，并借此攻陷整个系统。

目前，互联网中存在大量的扫描系统会对主机是否存在弱密码进行扫描。据相关报告，端口暴露的单个Linux系统，平均遭受超过40000次/天的网络攻击，攻击频率约5次/秒。存在弱口令的Linux系统，每月大概有17000次被入侵成功。

不仅仅暴露在外网的主机会被利用，内网中存在弱口令的主机也有很大的安全风险。例如许多恶意软件都存在扫描主机弱口令的行为，一旦其进入内网当中，便会迅速的传播扩散。例如，最近几年一直在更新变种的盖茨病毒。该病毒在进入内网之后，会利用自身的字典对内网中的SSH服务进行暴力破解，一旦暴破成功，便会感染暴破成功的主机。

· 全国挖矿木马的感染情况

在本报告中，根据不同操作系统样本数据进行分析，总共发现超过3000台Windows服务器感染了挖矿木马，其中超2000台Linux服务器感染了挖矿木马。

通过对被感染的主机进行分析，发现挖矿木马主要挖比特币与门罗币。猜测其原因，可能是比特币是数字货币的开创者，其价值非常高，当仁不让地成为黑客的重点关注对象。而门罗币则是新兴的数字货币，由于主要使用CPU进行挖矿，所以黑产团伙喜欢利用入侵服务器进行挖矿。

从入侵挖矿时间的角度来看：

Windows平台挖矿事件主要出现的年初（1月-3月）和年底（12月）如下图所示：

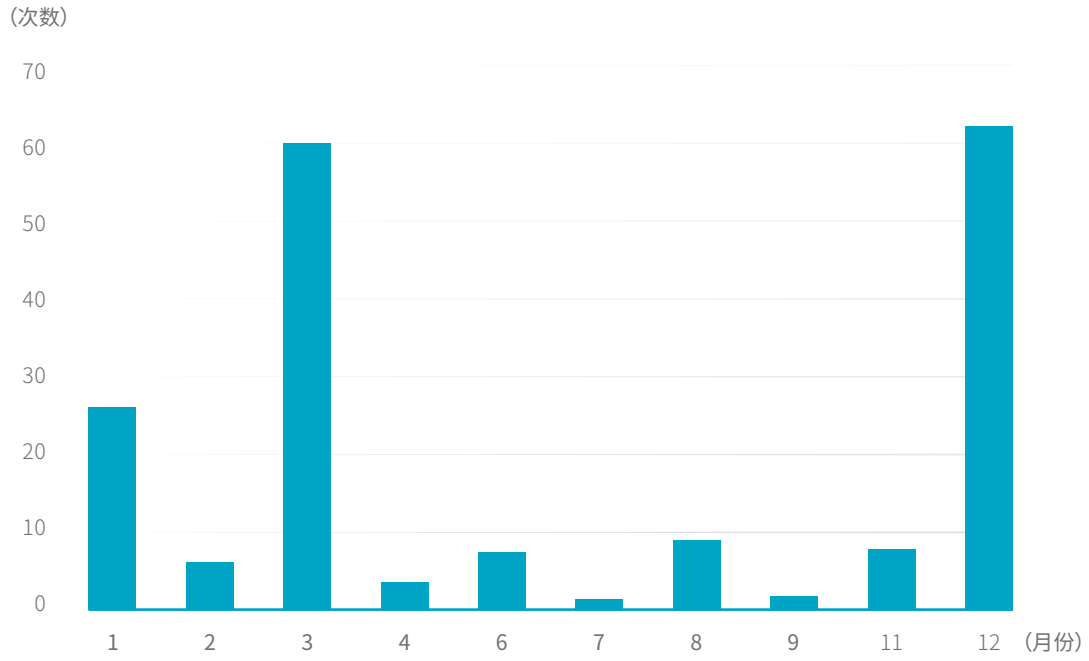


图2-22：Windows平台挖矿事件月度统计

但是，Linux平台挖矿事件主要集中在年中（4月-6月）和年底（11月-12月）：

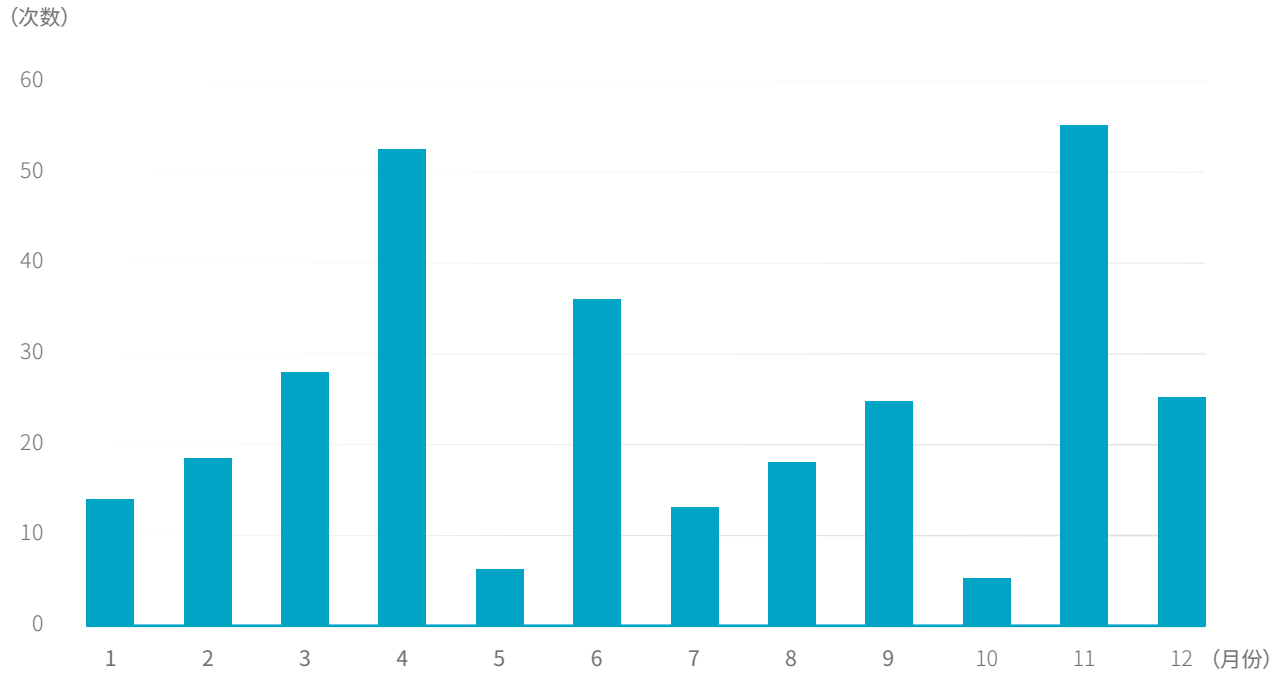


图2-23：Linux平台挖矿事件月度统计

可以看出，无论Windows平台还是Linux平台，年底都是挖矿入侵事件的高发时期，这段时间需要重点关注服务器是否出现CPU占用过高的情况。

如果以每天的入侵时间来进行统计，Windows平台挖矿事件主要发生在夜晚23点以及3点到8点之间，Linux平台挖矿事件主要发生在凌晨2点到6点之间。可以看出无论是Windows平台还是Linux平台，凌晨都是挖矿事件发生的高风险时期。

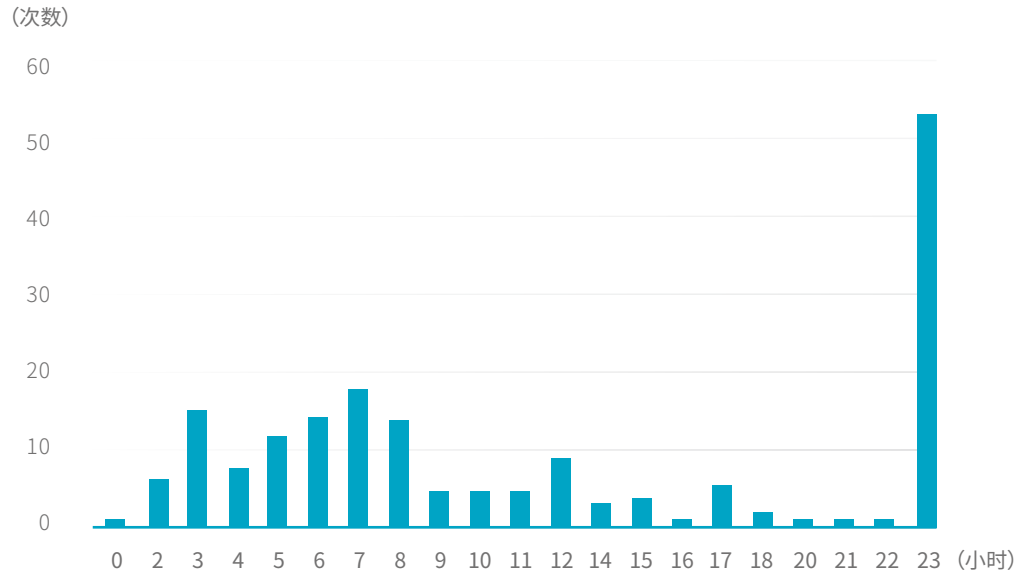


图2-24：Windows平台挖矿事件每日分布情况

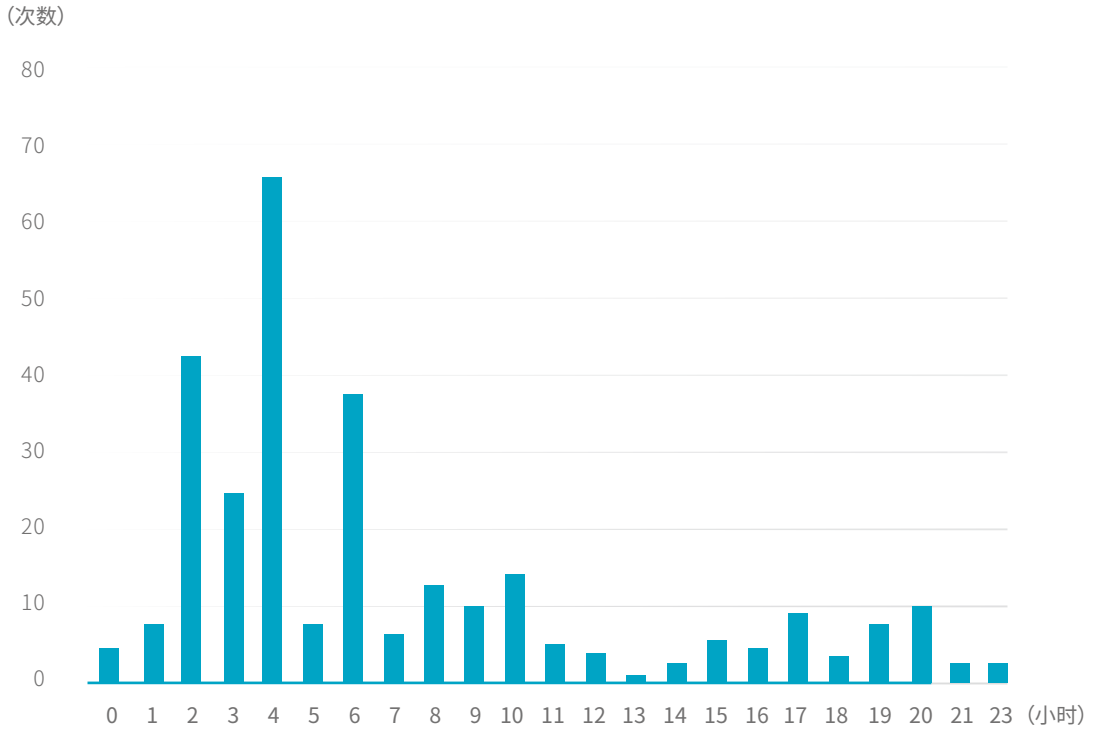


图2-25：Linux平台挖矿事件每日分布情况

· 勒索病毒情况

勒索病毒在服务器领域并不太常见。2019年共有超400台服务器感染勒索病毒，其中有约50%的服务器感染了Wannacry病毒。另外需要特别关注的是，Linux平台也出现了勒索病毒，有近百台Linux服务器感染了勒索病毒。

04 主机合规分析

所有企事业单位的网络安全建设都需要满足国家或监管单位的安全标准，如等保2.0、CIS安全标准等。安全标准，也称为“安全基线”。字典对“基线”的解释是：一种在测量、计算或定位中的基本参照，如海岸基线，是水位到达的水位线。因此，可以认为安全基线就是最低安全要求。

安全基线的意义在于为达到最基本的防护要求而制定一系列基准，在金融、运营商、互联网等行业的应用范围非常广泛。通过合规基线进行自查和自加固可以更好地帮助企业认清自身风险现状和漏洞隐患。

· 主机账号的合规分析

主机账号安全性的重要性不言而喻，但是在样本分析过程中，我们仍然发现很多账号存在不合规情况，例如未设置密码尝试次数锁定、未设置密码复杂度限制等，这不符合国家等级保护相关要求。在等保2.0通用基本要求的身份验证控制项中明确要求“应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换”、“应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施”。

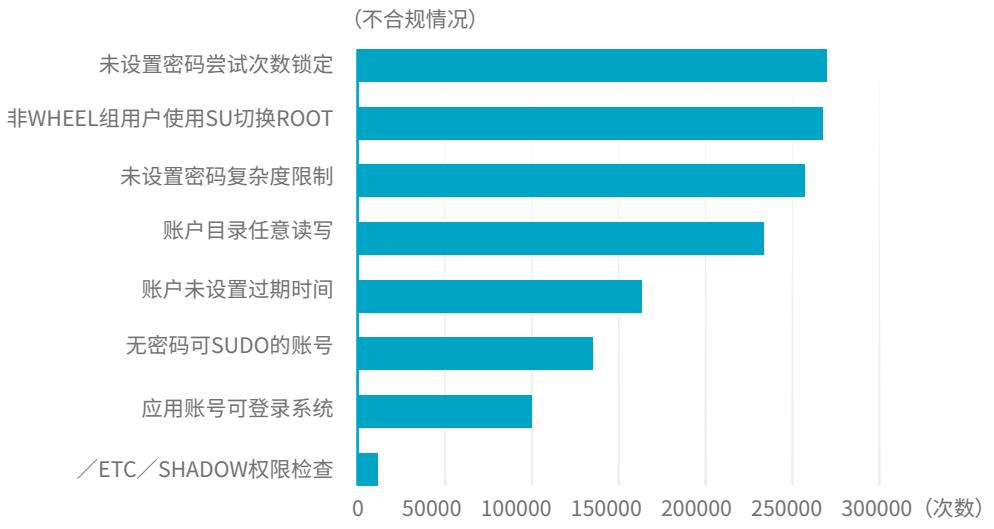


图2-26：主机账号的不合规情况

1)未设置密码尝试次数锁定

攻击者可无限次尝试登录系统，建议设置账户登录次数限制。

2)非wheel组用户使用SU切换root

建议在/etc/pam.d/su文件中增加auth required pam_wheel.so use_uid。

3)未设置密码复杂度限制

用户设置的弱口令，会让攻击者通过弱口令暴破方式获得密码。建议将存在问题的账户添加密码复杂度限制。

4)账户目录任意读写

账户目录可被任意读写，则意味着用户的变量信息或文件均可被任意改写，因此存在系统被提权或越权，或水坑攻击等风险。建议根据需要检查修改账户目录读写的权限。

5)账号未设置过期时间

用户账号密码应定期更换，若未设置密码过期时间，则用户可能不会有定期更换密码的意识，从而无法有效的保障账户安全。建议将未设置过期时间的账户添加过期时间限制。

6)无密码可sudo的账号

无密码可sudo账号往往存在一定的安全风险。请删除无密码可sudo的账号或者对该类账号添加强口令。

7)应用账号可登录系统

应用账号为应用专用，大多数情况下无需登录系统，且如果设置的密码为弱口令，存在被遗忘并被攻击者利用的风险。在不影响业务的前提下，应用账号设置为不可登录系统。

8)/etc/shadow权限检查

用chmod命令将/etc/shadow的ACL更改为400。一些系统可能需要将ACL设置为600。请参阅系统文档，以确定所需最小的ACL。用户root用户组root/shadow 例如（可根据系统不同而不同）：sudo chmod 400 /etc/shadow。

可执行如下命令进行修复：

sudo chmod 400(600) /etc/shadow

sudo chown root:root(shadow) /etc/shadow

· 主机应用合规分析

主机服务器上承载了非常多的应用，如果应用中存在不合规的情况，例如配置错误、未修补的漏洞补丁等。那么黑客通过应用就能进入主机系统内部，这将带来极大风险。

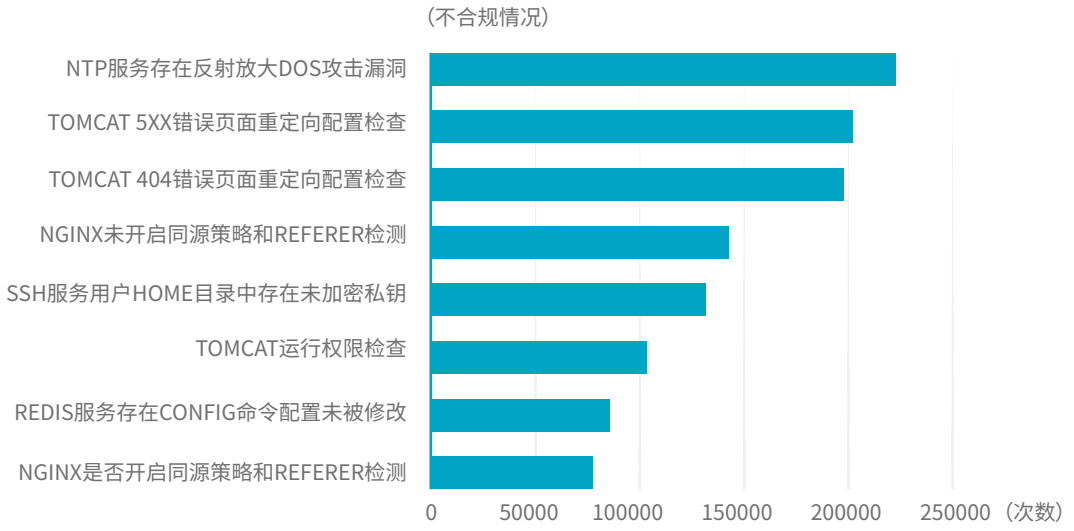


图2-27：常见应用的配置风险

1)NTP服务存在反射放大DOS攻击漏洞

NTP是用UDP传输的，所以可以伪造源地址。并且，在NTP协议中有一类查询指令，用短小的指令即可令服务器返回很长的信息。网络上一般NTP服务器都有很大的带宽，攻击者可能只需要1Mbps的上传带宽就可以欺骗NTP服务器，给目标服务器带来成百上千Mbps的攻击流量，从而造成拒绝服务攻击。如果攻击者同时向多台NTP服务器发送这种查询指令，则可以造成分布式拒绝服务攻击。

修复建议：将NTP版本更新到4.2.7p26以上，ntpd-4.2.7p26版本后，“monlist”功能已经被禁止，取而代之的是“mrulist”功能，使用mode6控制报文，并且通过实现握手过程来阻止对第三方主机的放大攻击。

2)Tomcat 5xx错误页面重定向配置检查

5xx页面未配置时，攻击者可以利用一些漏洞，如struts2远程命令执行漏洞，通过报错回显的方式获取目标的数据。配置5xx后，可以为此类攻击制造障碍，并且不易被攻击者发现和验证漏洞的存在。

检测方法：使用xml　　API解析tomcat配置文件，检查error-page节点下的error-code的值为5xx（可以为500、501等）的项，对应的location的值是否配置，如果有配置并且值不为""和nil，如果有一个5xx配置，则说明没有漏洞。

修复建议：在配置文件中添加配置500错误页面。正确配置示例：500 /noFile.htm。

3)Tomcat 404错误页面重定向配置检查

tomcat 404错误页面重定向配置检查,查看配置/conf/web.xml文件，使用xml API解析配置文件检查error-page节点下的error-code的值为404的项，如果对应的location的值有配置，并且不为""和nil，则说明配置没有问题。

修复建议：在配置文件中配置404错误页面。正确配置示例：404 /noFile.htm。

4)nginx 是否开启同源策略和referer检测

如果Nginx没有开启同源策略防护，很可能遭受点击劫持、盗链等恶意攻击。

修复建议：在配置文件中配置X-Frame-Options

如果不允许跨域访问，则删除Access-Control-Allow-Origin配置

如果允许单个域名跨域访问，则设置Access-Control-Allow-Origin值为可信域名。

如果允许多个域名跨域访问，建议使用下例方法（map中域名为可信域名）：

在nginx.conf里面找到server项，并在里面添加如下配置：

```
map $http_origin $corsHost {
default 0;
 "~http://www.example.com" http://www.example.com;
"~http://m.example.com" http://m.example.com;
 "~http://wap.example.com" http://wap.example.com;
 server
 {
 listen 80;
 server_name www.example2.com;
 root /usr/share/nginx/html;
 location /
 {
 add_header Access-Control-Allow-Origin $corsHost;
 }
 }
```

5)SSH服务用户home目录中存在未加密私钥

默认情况下，在用户的home目录中存储着未加密私钥，一旦该服务器被入侵，则可能导致该私钥泄露。私钥是登录服务器的重要凭证，如果私钥被攻击者利用，可通过私钥进行ssh登录认证获取系统权限，带来不可预知的高危风险。

修复建议：删除对应的私钥，若已经使用过该私钥对应的公钥进行登录，则应注意更换所有使用该公钥的主机的密钥。

6)Tomcat运行权限检查

Tomcat以root权限运行时，应用程序（如Struts2、jsp webshell）也拥有了root权限。因此，通过该漏洞，可以直接以root用户身份控制主机。Tomcat运行权限检查，检查tomcat运行用户的uid或gid是否为0。

修复建议：将tomcat运行账号切换至普通用户以及普通用户组。

7)Redis服务存在CONFIG命令配置未被修改

若未修改/root/redis/redis.conf中默认的rename-command CONFIG设置项，攻击者可使用CONFIG命令对Redis的数据库文件位置进行修改和变更。通过在数据库中插入攻击者的ssh公钥信息，并执行bgsave命令可以将带有公钥信息的数据库文件写入被攻击者使用CONFIG命令指定的磁盘位置。CONFIG命令未做修改的情况下，攻击者可以很方便地完成这一攻击过程并最终获取操作系统权限。

修复方法：将Redis配置文件中rename-command CONFIG 配置项更改为其他内容。

8)nginx 是否开启同源策略和referer检测的安全建议：

如果Nginx没有开启同源策略防护，很可能遭受点击劫持、盗链等恶意攻击。

修复建议：在配置文件中配置X-Frame-Options

如果不允许跨域访问，则删除Access-Control-Allow-Origin配置

如果允许单个域名跨域访问，则设置Access-Control-Allow-Origin值为可信域名。

如果允许多个域名跨域访问，建议使用下例方法（map中域名为可信域名）：

在nginx.conf里面找到server项，并在里面添加如下配置

```
map $http_origin $corsHost {
default 0;
 "~http://www.example.com" http://www.example.com;
 "~http://m.example.com" http://m.example.com;
```

```
"~http://wap.example.com" http://wap.example.com;
}
server
{
listen 80;
server_name www.example2.com;
root /usr/share/nginx/html;
location /
{
add_header Access-Control-Allow-Origin $corsHost;
}
}
```

· 主机系统合规分析

如果没有对主机底层的操作系统进行适当配置，就会引发许多安全问题。建议安全运维人员能够谨慎配置主机来满足组织机构的安全需求，并能够根据需求重新配置。通过研究分析样本数据，发现GRUB密码设置、UMASK值异常、未开启SYN COOKIE这三类问题是所有主机系统风险中所占比例最多的三类。

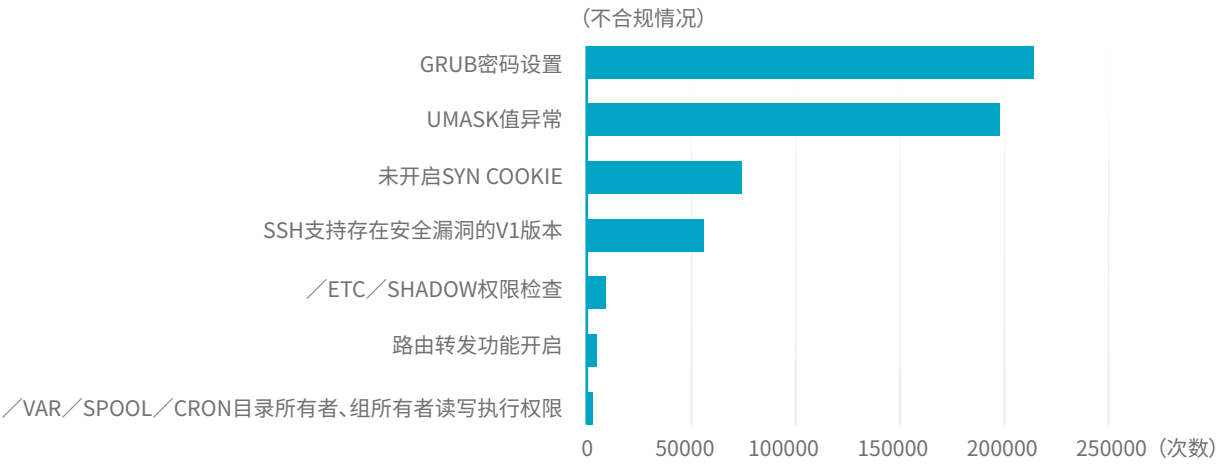


图2-28：主机系统不合规情况分析

1)grub 密码设置

如果不设置 grub，攻击者可通过 grub 对系统账户的密码进行修改。

检测 /etc/grub.conf 或 /etc/grub.d/40_custom 是否存在 password 字段，建议将 grub 设置密码。

2)umask 值异常

检测 /etc/profile、/etc/login.defs、/root/.bashrc、/root/.bash_profile、/root/.cshrc、/root/.tcshrc、/etc/bashrc、/etc/csh.cshrc、/etc/sysconfig/init 文件的 umask 值是否正常。

检测配置文件 umask 值是否为期望值。/etc/sysconfig/init 期望值至少为 022，其他配置文件期望值为 077。

3) 未开启 SYN Cookie

TCP SYN洪水攻击通过建立大量的半开TCP连接耗尽主机的资源。许多Linux发行版都能防止发生TCP SYN洪水攻击，但是这项保护功能默认是被禁用的。

设置 /etc/sysctl.conf 文件中的 tcp_syncookies 选项为整数 1 可以保护主机免受 TCP SYN 洪水攻击。

4)SSH 支持存在安全漏洞的 v1 版本

安全 shell（SSH）协议 v1 有许多安全问题都是由 SSH 协议 v2 解决。此外，.sshd_config 设置为 2 会强制使用 SSH V2。SSH v1 采用 DES、3DES、Blowfish 和 RC4 等对称加密算法可保护数据安全传输，而对称加密算法的密钥是通过非对称加密算法（RSA）来完成交换的。

手动将 Protocol 2 添加到 /etc/ssh/sshd_config 文件中。

5)/etc/gshadow 权限检查

/etc/gshadow 文件的 ACL 应当设置为 400。用户 root，用户组 root/shadow 。

/etc/gshadow 文件包含组账户的隐秘信息（例如加密的组密码和组的管理员信息）。

如果 /etc/gshadow 文件保护不当，可能导致服务器被恶意攻击、利用。攻击者可以使用该文件篡改或者利用组管理员账户，或者使用字典攻击破解加密过后的密码。

可执行如下命令进行修复：

chmod 400 /etc/gshadow

chown root:root(shadow) /etc/gshadow

6) 路由转发功能开启

启用网络接口之间的数据包转发创建一个服务器的路由功能。该功能可以被滥用来发起攻击或进行进一步攻击，并能创造威胁的高度载体。如果检查失败，路由本身没有明确要求，会把 net.ipv4.ip_forward 的值更改为 0 来明确禁用 IP 路由。服务器有面向 Internet 和内部私人的两个接口，这一点就尤其重要。下面是命令示例，你可能需要自定义您的环境：对 /etc/sysctl.conf 手动配置 net.ipv4.ip_forward=0

7)/var/spool/cron 目录所有者、组所有者读写执行权限

如果恶意用户拥有在/var/spool/cron目录创建一个文件的权限，他们可以轻松地在/var/spool/cron目录部署持久或预定恶意软件。/var/spool/cron目录的目前权限应为700。/var/spool/cron目录拥有者应该为root。/var/spool/cron应该具有root用户组所有权。

可执行如下命令进行修复：

chown root:root /var/spool/cron

chmod 700 /var/spool/cron

主机安全市场产品形态

PRODUCT FORM OF WORKLOAD SECURITY MARKET

国家互联网应急中心（CNCERT）的报告数据显示，几乎在每年CNCERT协调处置网络安全事件中，网页仿冒事件最多，其次是安全漏洞、恶意程序、网页篡改、网站后门、DDoS攻击等事件。

主机是攻击者在常规攻击或高级攻击中最主要的目标，上文所述安全问题大部分也都是发生在主机侧的一些安全威胁。因此，安全人员需要实时评估自身主机的安全防护是否可靠，以及未来的提升方向。

随着黑客攻击手段不断演进，主机安全防护软件也在不断更新迭代，衍生出了一系列不同细分类别的主机安全产品。如下图所示主机安全成熟度曲线，横坐标是攻击层面类型，包括自动化攻击、机会主义、高级攻击，而纵坐标是安全组织级别，级别1主要是临时动作，级别2是在制定一些措施，但是没有正式规定，级别3有很明确的流程，级别4是主动考虑一些攻击场景，级别5考虑到供应链、固件等管理。从下图可知，主机安全技术也一直在随着外在环境而不断进化。

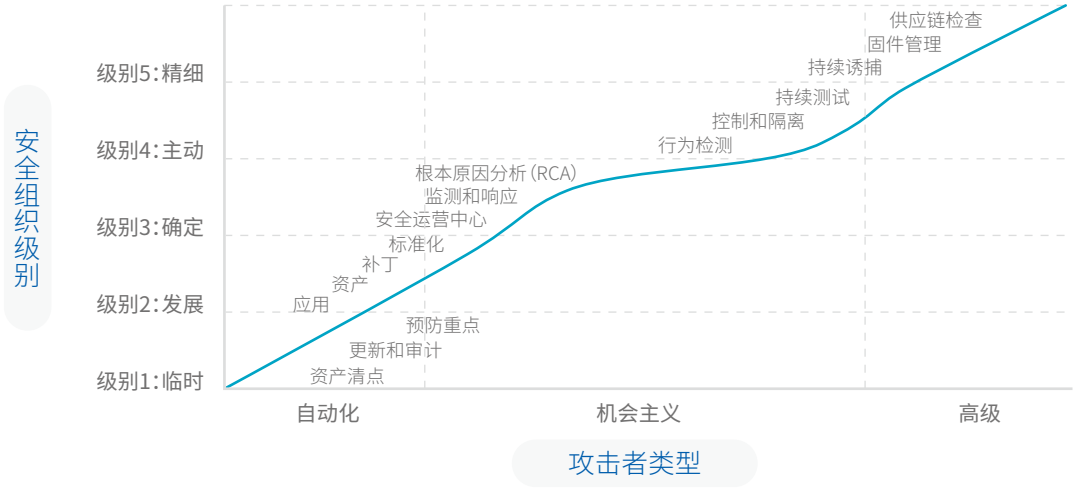


图3-1：主机安全成熟度曲线

随着主机安全产品成熟度不断提高，以“检测能力、响应能力、架构适配能力、满足合规要求能力”为核心的四大主机产品能力将成为用户进行产品选型核心参考指标，也是未来产品演进发展的关键方向。从主机安全产品发展级别来看，大体上可以概括为下述五个不同阶段的主机安全产品。

01 级别1- 基础性的主机安全产品

这个阶段组织机构需要实现的目标是一个相对清晰的资产清单，以及基础性的主机加固，能够做到防止木马病毒，防止核心数据被破坏、被偷窥、被篡改、被窃取，保证系统的安全性。

1）资产探测

没有人能够保护未知的资产，因此，制定详细的资产清单是安全防护的前提。资产发现（探测）常需要对一定范围内的主机或应用系统指纹识别（对操作系统版本、开放端口、服务版本进行识别）进行摸排。主机类资产清点产品一般具备自动探测，发现未知（未管理）资产功能，并对资产进行全生命周期管理的功能，资产类型包括主机、数据库、中间件、应用组件等。

2）主机杀毒软件

杀毒软件，主要是指从数据包级别检测主机是否感染了病毒。杀毒软件通过扫描文件来查明系统是否受到感染。扫描策略主要是静态特征扫描。这种方法对于发现已知的病毒程序非常有效，但对于发现高级或未知病毒程序并不是非常有效。例如主机受到感染，病毒程序将尝试与C&C（命令和控制）主机通信。安全人员可以根据开源威胁情报审核主机外部通信的目标IP地址，并检查目标IP地址是否是恶意的。

02 级别2-以应用为核心的主机安全产品

在这个阶段，企业组织会利用补丁管理、漏洞管理、钓鱼防护等产品进行主机的安全防护，并制定差距分析和计划来消除差距。

1）网页防篡改

网页防篡改是针对网站篡改攻击的一类产品，一般会通过文件底层驱动技术对Web站点目录提供保护，防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏。

2）补丁管理系统

补丁管理任务包括维持当前的可用补丁库，确保补丁正确安装，以及安装后测试系统。绝大多数的机会主义攻击针对的是最常见的软件。因此，修补常见系统和软件包括Windows、Office、浏览器、Adobe和Java的补丁是首要任务。

3）漏洞管理系统

漏洞管理是指识别、评估和修复组织信息系统和应用程序中存在的漏洞的过程。通过将资产分类，并按照风险级别将漏洞归类。因此，漏洞管理并不单单是指漏洞评估。漏洞管理可以为企业提供一种保护重要IT 基础设施不受安全漏洞威胁的方式。

4）特权访问管理

因能访问公司最宝贵的信息，特权账户往往成为攻击者竞相追逐的目标。组织机构必须安全有效地管理特权访问，包括提供所有特权账户的完整可见性、治理和控制特权访问、监视和审计特权活动、自动化和集成 PAM 工具。

03 级别3-以检测响应为核心的主机安全产品

为捕获更多的机会主义攻击，这个阶段的主机安全防护产品重点已经从恶意软件预防和基础主机加固扩展到检测和响应。

1）主机终端管理方案

主机终端管理方案是事件响应的主要工具，可用于检测和调查主机、终端上的可疑活动以及此类问题的踪迹和其它问题。

2）沙箱

当前的有效沙箱基本都是在专用虚拟机上执行，通过沙箱可以在与网络隔离的主机上用多种操作系统安全地测试恶意软件。安全研究人员会在分析恶意软件时采用沙箱技术，很多高级反恶意软件产品也用沙箱来根据可疑文件的行为确定其是否真的是恶意软件。因为现代恶意软件大多经过混淆加密处理以规避基于特征码的杀软，类似沙箱这样基于行为分析的反恶意软件解决方案就变得越来越重要了。

3）蜜罐

蜜罐和蜜网就是为诱捕攻击者而专门设置的风险系统。蜜罐是诱使攻击者盗取有价值数据或进一步探测目标网络的单个主机。

4）安全编排和自动化（SOAR）

安全编排自动化与响应，该产品聚焦安全运维领域，重点解决安全响应的问题。Gartner 将 SOAR 定义为安全编排自动化与响应，并将其看作是安全编排与自动化 (SOA, Security Orchestration and Automation)、安全事件响应平台(SIRP,Security Incident Response Platform)和威胁情报平台(TIP, Threat Intelligence Platform) 三种技术、工具的融合。Gartner 认为，SOAR 技术仍然在快速演化，内涵未来仍可能会变化，但其围绕安全运维、聚焦安全响应的目标不会改变。

04 级别4-以主动防御为核心的主机安全产品

这个阶段的主机防护重点在于减少攻击面。检测活动上升到用户行为级别。逐步使用默认的拒绝控制，如应用程序白名单、网络隔离和Web隔离，以减少攻击面，开始考虑先进的工具，如威胁狩猎等。

1）威胁狩猎（Threat Hunting）

威胁狩猎是指采用人工分析和机器辅助的方法，针对网络和数据进行主动和反复的搜索，从而检测出逃避现有安全防御措施的高级持续性威胁。一旦发现存在恶意行为，就会将新的IoAs、IoCs添加到防护设备中，形成一个预防、检测和响应的闭环。

2）应用控制

为所有不可修补的系统和面向互联网的主机部署应用程序控制，此外考虑对关键业务用户或设备的应用程序进行控制。

3）微隔离

使用网络级的微隔离将无法修补的主机和关键业务主机进行隔离。使用虚拟补丁工具，让这些无法修复的系统在从外部探测时看起来像是打了补丁。

4）欺骗防御

使用欺骗工具来检测活跃的攻击者，包括一系列更高级的蜜罐和蜜网产品，能够基于所捕获的数据为检测和防御提供更高的自动化程度。

05 级别5-新形态下的主机安全产品

随着云计算、物联网、移动互联网等新IT形态的出现，主机安全也需要有针对性地进行变化才能应对IT架构的变化。

(1) 云工作负载保护

云工作负载保护平台（CWPP）市场定义为基于主机的解决方案，主要满足现代混合数据中心架构中，主机工作负载的保护要求。它提供了一种集成的方式，通过使用单个管理控制台和单一方式表达安全策略来保护这些工作负载，而不用考虑工作负载运行的位置。

2) 固件安全（Firmware）

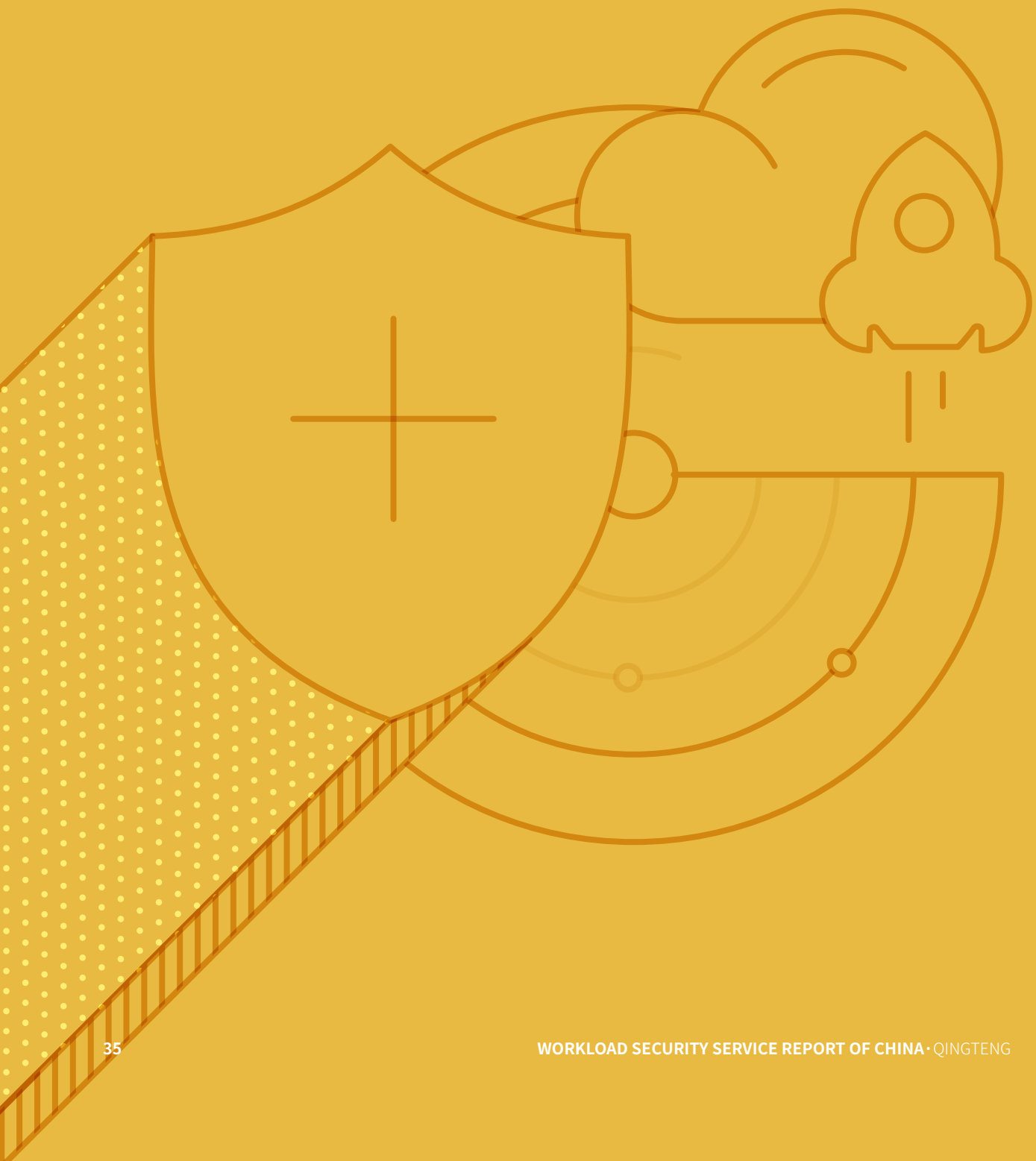
如果带有恶意目的的特殊用户对固件进行针对性的修改（hacker行为），注入恶意软件代码，然后再重新计算出新的CRC来伪装成合法的固件。这种经过伪装的固件，可以在硬盘流通和使用的各个环节通过升级方式写入，并在重新使用时驻扎硬盘内部小系统，且完全不被任何安全措施发现。固件安全类产品主要负责盘点、监控和修补固件和微控制器。

3) 供应链安全（Supply chain）

供应链攻击，也称价值链攻击或第三方攻击，是指攻击者以有权限访问企业系统和数据的外部合作伙伴或者供应商为跳板，潜入企业内部系统而发生的攻击。因为能够接触到敏感数据的供应商变得越来越多，因而，针对供应链的攻击方式也成为了最流行的攻击方式之一。

主机安全产品技术分析

TECHNICAL ANALYSIS OF
WORKLOAD SECURITY PRODUCTS



达尔文《进化论》说，进化来源于突变，而安全面对的正是“不可预知的未来”。这些层出不穷的未知威胁成为了安全进化的动力。主机安全作为该领域最重要的一个分支，也正在快速进化以应对全新的威胁。愈演愈烈的终端威胁是主机安全进化的源动力。不难预测，未来主机安全的进化方向将会像自适应安全架构那样继续朝着“持续增强的检测、响应以及架构适配”方向前进。

01 持续检测是基础

研究表明，网络攻击者平均在99天内不会被发现，攻击者不超过3天就能获得管理员凭据，超过53%的受害者是在外部通知后才知道被攻击的。

与攻击驻留时间相对应的是防御发现时间，防守者平均需要170天才能检测到一个高级威胁，而且需要39天的时间来缓解攻击，另外还需要43天的时间来恢复。

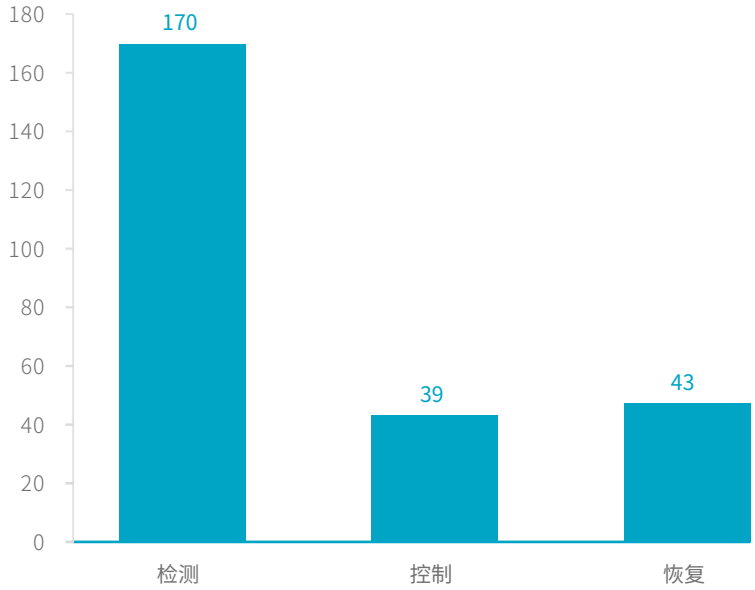


图4-1：防御所需时间

攻击者和防守者处于天然不对等的地位，传统基于报警或已存在的威胁特征的检测技术，包括防火墙、IPS、杀毒、沙箱等被动防御手段，更是让这种不平等愈发严重。很多被黑客攻陷的企业组织，虽然已经构建了一定的安全防御体系，但仍然没能及时发现或阻止威胁，将损失降到最低。主要是因为当下检测体系在应对未知威胁过程中存在一些不足，表现为以下几个方面：

A. 检测技术单一：基于签名检测技术无法检测未知威胁，更无法定位失陷主机。

B. 缺乏持续检测：只能做阶段性检测，无法覆盖威胁的全生命周期。

C. 无法进行联动：各安全检测产品独立工作，攻击告警信息割裂，无法联动。

为了持续增强检测能力，需要对攻击有更深的理解，也应该采用一些更细粒度的安全模型。对信息安全专家来说，用洛克希德-马丁公司的网络杀伤链（KillChain）来识别和防止入侵的方法可能并不陌生。但目前，较杀伤链模型更进阶和详细的模型是MITRE的ATT&CK模型。

ATT&CK有助于理解攻击者的行为、技术、战术，帮助安全人员构建检测措施，验证防御措施以及分析策略的有效性。ATT&CK包括的战术有初始访问、执行、持久化、提权、防御绕过、凭据访问、发现、横向移动、收集、命令和控制、数据获取、影响。每一个战术类别包括了一系列的攻击技术，ATT&CK提供了对每一项技术的细节描述、检测技术和分析方法，以及可能的缓释措施。在行业应用中，该模型能够帮助分析和响应人员更好地了解攻击者。帮助安全人员熟悉真实环境的对抗技巧，增强实战能力，从而更好地组织防御。

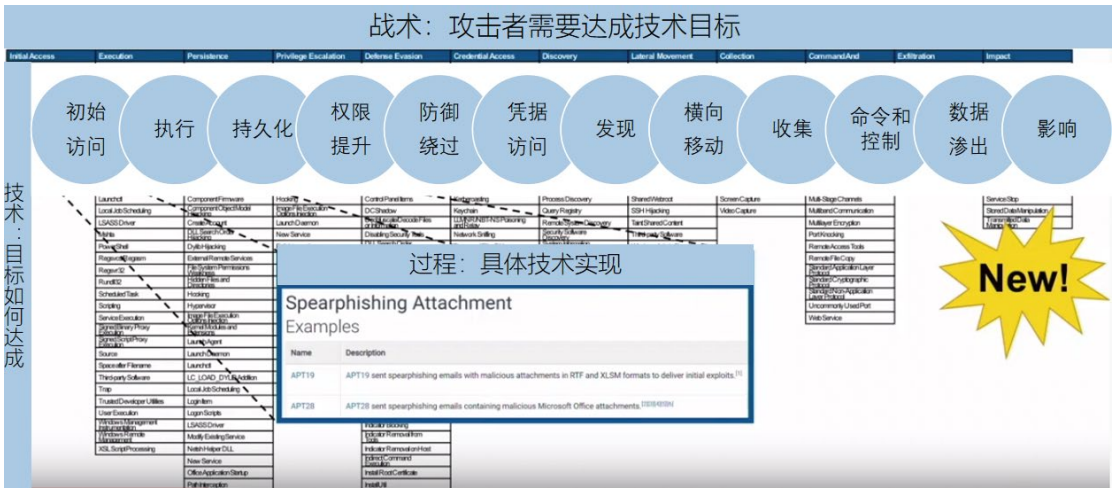


图4-2：ATT&CK矩阵的战术、技术和步骤

ATT&CK 框架对于安全从业者的最大价值就是增强其对检测能力的理解，按照其 ATT&CK 模型覆盖度和检测点，找到自身安全检测能力的改进方向。下文将从攻击角度，结合 ATT&CK 框架极其对应的战术和技术，举例分析攻击者在攻击主机时经常采用的一些套路以及缓解措施。

· 攻击持久化检测

攻击者希望尽可能减少工作量，包括减少访问攻击对象的时间。因此持久化是最受攻击者追捧的技术之一。即便运维人员采取重启、更改凭据等措施后，持久化仍然可以让计算机再次感染病毒或维护其现有连接。例如注册表Run键、启动文件夹是最常用的技术，这些注册表键或文件系统位置在每次启动计算机时都会执行。因此攻击者在启动诸如Web浏览器或Microsoft Office等常用应用时开始获得持久化。

此外，还有使用“镜像劫持（IFEO）注入”等技术来修改文件的打开方式，在注册表中创建一个辅助功能的注册表项，并根据镜像劫持的原理添加键值，实现系统在未登录状态下，通过快捷键运行自己的程序。

在所有ATT&CK战术中，持久化也是最应该关注的战术之一。如果企业在终端上发现恶意软件并将其删除，很有可能它还会重新出现。这可能是因为有漏洞还未修补，但也可能是因为攻击者已经在此或网络上的其它地方建立了持久化。与使用其它一些战术和技术相比，使用持久化攻击应该相对容易一些。

例如，Windows内置工具schtasks.exe提供了在本地或远程计算机上创建、修改和运行计划任务的功能。该工具是at.exe的替代方案，比at.exe使用更灵活。攻击者常常会使用该工具。但是，管理员、脚本和软件配置也会使用该工具。计划任务工具可用于实现“持久化”，并可与“横向移动”战术下的技术结合使用，从而实现远程“执行”。另外，该命令还具有参数来指定负责创建任务的用户和密码以及运行任务的用户和密码。/s标志将使任务以SYSTEM用户身份运行，这通常表示发生了“提升权限”行为。

ATT&CK检测技术

技术	战术	使用率
计划任务	持久化	中等

数据模型参考

对象	行动	领域
进程	创建	exe
进程	创建	command_line

实现方式—伪代码

查找是否有schtasks.exe实例作为进程运行。command_line字段对于消除schtasks命令类型之间的歧义是必不可少的，其中包括标志/create、/run、/query、/delete、/change和/end等标记。

```
process = search Process:Create
schtasks = filter process where (exe == "schtasks.exe")
output schtasks
```

· 提升权限检测

所有攻击者都会对提权爱不释手，利用系统漏洞达到Root级访问权是攻击者的核心目标之一。其中一些技术需要系统级的调用才能正确使用，Hooking和进程注入就是两个示例。该战术中的许多技术都是针对被攻击的底层操作系统而设计，要缓解可能很困难。

ATT&CK提出“应重点防止对抗工具在活动链中的早期阶段运行，并重点识别随后的恶意行为。”这意味着需要利用纵深防御来防止感染病毒，例如终端的外围防御或应用白名单。对于超出ATT&CK建议范围之外的权限升级，一种良好的防止方式是在终端上使用加固基线。例如CIS基线提供了详细的分步指南，指导企业如何加固系统，抵御攻击。

应对此类攻击战术的另一个办法是审计日志记录。当攻击者采用其中某些技术时，将留下蛛丝马迹，暴露他们的目的。尤其是针对主机侧的日志，如果能够记录主机的所有运维命令，可进行存证以及实时审计。例如，实时审计运维人员在主机上的操作步骤，一旦发现不合规行为即可进行实时告警，也可以作为事后审计存证。也可以将数据信息对接给SOC、态势感知等产品，也可以对接给编排系统。

从ATT&CK框架中可知，攻击者可以通过拦截合法安装的服务的搜索路径来提升权限。因此，Windows就会启动目标可执行文件，而不是所需的二进制文件和命令行。同时，当二进制路径中有空格并且该路径未加引号，也会启动目标可执行文件。正常情况下，搜索路径拦截绝不是合法正常行为，极有可能是攻击者利用了系统不合规或者系统配置导致的。使用一些正则表达式，可以通过截获的搜索路径来识别执行的服务。

ATT&CK检测技术

技术	战术	使用率
可访问性功能	持久化、提升权限	高

数据模型参考

对象	行动	领域
进程	创建	command_line
进程	创建	image_path
进程	创建	parent_exe

实现方式—伪代码

查看创建的服务时，主要观察第一个参数是否为加引号的路径。假设这些路径都是绝对路径，请查找命令行中有空格但exe字段不属于命令行的情况。这表明执行者的目标是另外一个进程，但是路径因为前一个空格而被拦截了。

```
process = search Process:Create
services = filter processes where (parent_exe == "services.exe")
unquoted_services = filter services where (command_line != "\"*" and command_line
== "* *")
intercepted_service = filter unquoted_service where (image_path != "* *" and exe not
in command_line)
output intercepted_service
```

· 凭据获取检测

毫无疑问，攻击者最想要的是凭据，尤其是管理凭据。如果攻击者可以登录，为什么要用0Day或冒险采用漏洞入侵呢?这就犹如小偷进入房子，如果能够找到钥匙开门，没人会愿意砸破窗户进入。

任何攻击者进入企业都希望保持一定程度的隐身。他们将希望窃取尽可能多的凭据。他们当然可以暴力破解，但这种攻击方式噪声太大了。还有许多窃取哈希密码及哈希传递或离线破解哈希密码的示例。最后，攻击者最喜欢的方式是窃取明文密码。明文密码可能存储在明文文件、数据库甚至注册表中。攻击者入侵一个系统、窃取本地哈希密码并破解本地管理员密码并不鲜见。应对凭据访问的最简单办法就是采用复杂密码。建议使用大小写、数字和特殊字符组合，目的是让攻击者难以破解密码。最后一步就是监视有效帐户的使用情况。在很多情况下，是通过有效账户发生的数据泄露。

当然最稳妥的办法就是启用多因素验证。即使存在针对双重验证的攻击，有双重验证（2FA）总比没有好。通过启用多因素验证，可以确保破解密码的攻击者在访问环境中的关键数据时，仍会遇到另一个障碍。

例如，通过Mimikatz之类的凭证转储工具可以从内存中读取其他进程的数据。检测入侵行为时，可以查找有没有进程正在请求特定权限以读取LSASS进程的各部分内容，以此来检测何时发生凭证转储。但这种方法也存在的一个缺点是，过分关注Mimikatz使用的常见访问方式。

· 横向移动检测

攻击者在利用单个系统漏洞，通常会尝试在网络内进行横向移动。甚至通常一次只针对单个系统的勒索软件也会试图在网络中移动以寻找其它攻击目标。攻击者通常会先寻找一个落脚点，然后开始在各个系统中移动，寻找更高的访问权限，以期达成最终目标。

在缓解和检测对该特定技术的滥用方面，适当的网络分段可以在很大程度上缓解风险。将关键系统放置在一个子网中，将通用用户放置在另一个子网中，将系统管理员放置在第三个子网中，有助于快速隔离较小网络中的横向移动。在终端和交换机级别都设置防火墙也将有助于限制横向移动。

遵循CIS控制措施 14——基于需要了解受控访问是一个很好的切入点。除此之外，还应遵循控制措施4——控制管理员权限的使用。攻击者寻求的是管理员凭据，因此，严格控制管理员凭据的使用方式和位置，将会提高攻击者窃取管理员凭据的难度。此控制措施的另一部分是记录管理凭据的使用情况。即使管理员每天都在使用其凭据，但他们应该遵循其常规模式。发现异常行为可能表明攻击者正在滥用有效凭据。

除了监视身份验证日志外，审计日志也很重要。域控制器上的事件ID4769表示，Kerberos黄金票证密码已重置两次，这可能表明存在票据传递攻击。或者，如果攻击者滥用远程桌面协议，审计日志将提供有关攻击者计算机的信息。

举个例子，Microsoft操作系统内置的远程桌面协议（RDP）允许用户远程登录到另一台主机的桌面。它允许交互式访问正在运行的窗口，并转发按键响应、鼠标点击等。网络管理员、高级用户和终端用户可以使用RDP进行日常操作。从攻击者的角度来看，RDP提供了一种横向移动到新主机的方法。在高度动态的环境中，确定哪些RDP属于攻击者行为绝非易事，但对于确定入侵范围将很有用。

可以通过多种方式检测远程桌面：

A. 网络连接到端口3389/tcp（假设使用默认端口）
B. 数据包捕获分析
C. Windows安全日志（事件ID 4624、4634、4647、4778）
D. 从mstsc.exe检测网络连接
E. 执行进程rdpclip.exe
F. 如果启用了剪贴板共享，则在RDP目标机器上将剪贴板共享作为剪贴板管理器

· 命令和控制入侵的检测

现在大多数恶意软件都有一定程度的命令和控制权。黑客可以通过命令和控制权来渗透数据、告诉恶意软件下一步执行什么指令。对于每种命令和控制，攻击者都是从远程位置访问网络。因此了解网络上发生的事情对于解决这些技术至关重要。

在许多情况下，正确配置防火墙可以起到一定作用。一些恶意软件家族会试图在不常见的网络端口上隐藏流量，也有一些恶意软件会使用80和443等端口来尝试混入网络噪音中。在这种情况下，企业需要使用边界防火墙来提供威胁情报数据，识别恶意URL和IP地址。虽然这不会阻止所有攻击，但有助于过滤一些常见的恶意软件。

如果边界防火墙无法提供威胁情报，则应将防火墙或边界日志发送到日志服务处理中心，安全引擎主机可以对该级别数据进行深入分析。例如Splunk等工具为识别恶意命令和控制流量提供了良好的方案。

恶意攻击者可能会重命名SysInternals等工具提供的内置命令或外部工具，以更好地融入环境。在这种情况下，文件路径名称是任意的，并且可以很好融入背景环境中。如果对这些参数进行仔细检查，则可能会推断出攻击者正在使用哪些工具，并了解攻击者目前正在做什么。对于存在共享相同命令行的合法软件则可以根据预设参数加入白名单中。

02 快速响应是动力

当前安全攻防对抗日趋激烈，单纯指望通过防范和阻止的策略已行不通，必须更加注重检测与响应。企业组织要在已遭受攻击的假定前提下，构建集防御、检测、响应和预防于一体的全新安全防护体系。这从2019年6月网络演习的规则也能看得出来，不强制要求系统不被入侵，而是强调入侵之后的快速响应能力。

为最大限度科学、合理、有序地处置网络安全事件，建议建立完善的响应流程，包括查询、排序、可视化、获取、分析、工作流，总共7个阶段的工作。根据网络安全应急响应总体策略对每个阶段定义适当的目标，明确响应顺序和过程。

查询	快速、实时、自然语言查询工具，快速发现攻击的IOC类型
排序	根据时间严重性，以及受影响资产的业务价值，对风险进行优先排序
可视化	点击攻击链可视化工具，使调查人员可从数据中获取或钻取更多信息
获取	可自动获取可疑文件或内存和磁盘转储
分析	自动集成分析云或沙箱中的可疑进程／文件
工作流	提供警报管理工作流的调查工具，轻松解决安全事件

建立完善的响应流程之后，应急响应人员需要结合对应工具处理安全事件。下文将结合不同场景，详细阐述主机安全应急场景。

· 恶意挖矿事件响应

概述

挖矿恶意软件基本上可以分为基于Web的恶意软件和基于主机的恶意软件。基于Web的挖矿恶意软件托管在网站上在用户浏览受感染的页面时自动激活。它通常用JavaScript编写，并作为本地计算机上的Web应用程序执行。这种类型的恶意软件通常会挖掘货币，例如Monero，它非常适合通过CPU进行挖掘。基于Web的矿工很难检测或停止，因为它们虽然没有将自身安装在本地计算机上，却出于用户自己的目的而利用本地计算机，这是用户所不知道的。这类攻击的潜在后果包括严重的性能下降，导致移动设备过热甚至是崩溃。

基于主机的挖矿恶意软件是系统上本地安装的恶意应用程序，通常是由dropper型木马安装的。通常，恶意软件只是在后台以无窗口模式运行的标准挖掘软件。例如，该恶意软件可能使用进程注入技术来执行，然后在合法的系统进程中掩盖挖掘应用程序的进程，从而使用户和防病毒解决方案更难以识别和删除它。基于主机的恶意软件可以更好地访问系统资源，包括计算机的GPU，使其对于网络犯罪分子来说可能更有利可图。

事件分析

客户反馈服务器异常卡顿，并且接收到云服务商的邮件告警，提示服务器资源负载过高，严重影响正常运行。ssh进系统，top了下，发现某进程占用了大量主机CPU和内存资源。

```
[root@                    peng]# ps aux|head -1;ps aux|grep -v PID|sort -rn -k +3|head
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root     19252 449  0.0  12636   660 ?        S<   17:52   0:08                                    _load.sh
root     17371 34.6  0.0 1560948 24780 ?       Tl   17:50   0:47                 -d
root     21836  4.9  0.0 154000  7872 pts/2    S+   17:46   0:17 top
root        34  0.6  0.0      0     0 ?        S     2016 3893:01 [rcu_sched]
```

图4-3：存在异常进程占用较高CPU

该恶意挖矿脚本xxx_load.sh名称和企业重要业务名称极其近似，并在其后增加load字样，具备一定的迷惑性，同时通过守护进程使得该挖矿进程被结束后能够很快重新启动。

通过一系列分析发现：由于该主机Redis服务的6379端口暴露于公网中且存在弱口令，导致恶意攻击者通过暴力破解方式连接Redis服务。通过crontab反弹shell直接获取该主机root用户权限，随后该主机被用于挖矿。

· 内网入侵事件响应

概述

内网入侵事件同样在应急响应事件中占据着显著地位，然而内网入侵的成因和方式多种多样。入侵行为被发现的起因通常是因为出现主机无法登录、触发内网蜜罐、bash审计异常、主机异常登录、主机异常连接等情况。通过详细排查，被入侵的主机通常情况下存在以下三个特点：

A. SSH/RDP服务存在弱口令。
B. Web业务存在文件上传或远程命令执行漏洞。
C. 操作系统或服务使用存在明显漏洞的版本。

通过对入侵事件的分析发现，弱口令问题仍是导致服务器被入侵的最大原因。一些手段较为高明的攻击者往往会重新编译安装自己精心制作的后门应用来替换系统自带命令，起到一个隐蔽自身的效果。常被用于替换的命令包括：ps，netstat，top，ls，cd等，但有些攻击者水平往往无法控制好上述操作，入侵行为更加容易被发现。

事件分析

客户反馈有部分内网主机始终无法通过SSH正常登录系统，存在类似问题的主机逐渐增多，然而运维人员在近期内并未对相关主机进行任何操作。专业服务团队通过远程管理卡配合recovery模式进入系统进行信息收集和分析，终于确认了问题的原因。

攻击者通过弱口令方式入侵该企业主机后，尝试编译安装SSH后门，加载恶意PAM模块，实现不修改root密码的情况下添加自己的密码，绕过正常SSH登录验证流程。但由于该攻击者在编译安装时出现错误，PAM模块损坏，导致该主机SSH仅能通过攻击者后门中的密码登录而正常root用户无法使用自身密码登录。攻击者没有察觉到该情况使得用户始终无法登录root用户进而被察觉。工程师通过该服务器的远程管理卡不断进入recovery模式对PAM模块下的so文件进行逐一分析，最终定位到了问题。

图 4-4：某恶意SSH后门so文件部分代码

类似以上入侵行为一旦没有出现明显纰漏将具备较强隐蔽性，可能会在长时间内无法被用户察觉。

· 勒索病毒事件响应

概述

勒索病毒和挖矿在入侵的方式上有一定的相似之处，但是在对受害主机的影响程度上，勒索病毒往往更胜一筹。常规的挖矿事件往往通过杀死挖矿进程，清理掉生成文件和部分配置后即可恢复服务器正常运行。然而勒索病毒常常会对受害主机硬盘、文件或数据库进行高强度加密或删除操作，并要求向某指定加密货币账户打入指定金额才可能予以解密或还原。

事件分析

在一起MongoDB勒索病毒事件中，发现攻击者主要通过MongoDB未授权访问漏洞对该数据库中数据进行了删库处理，且要求支付0.5BTC才能归还数据。通过查询相关日志分析，该删库行为发生在两年前。由于时间间隔较大，且属于删库而非加密行为，因此数据无法恢复，只能通过对该主机进行相应安全加固避免类似事件再次发生。

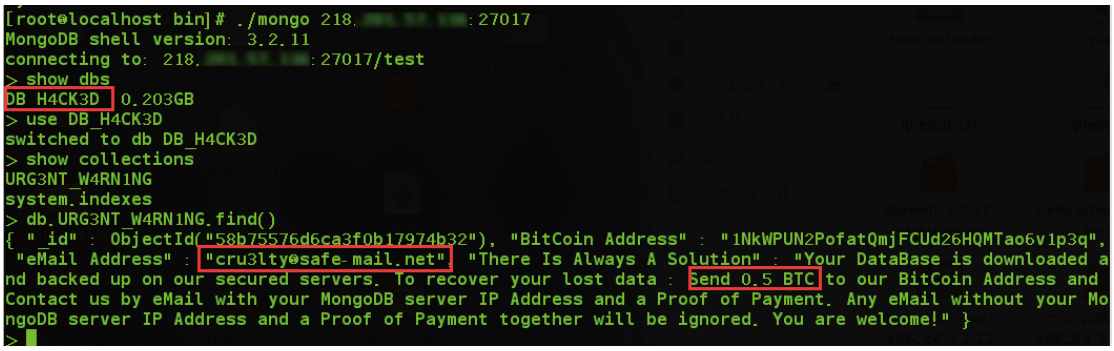


图4-5：某客户MongoDB被恶意删库

在这里也提醒各位用户，一旦发现类似勒索事件，可以咨询专业安全公司尝试能否通过逆向分析或数据恢复手段进行止损，不要听信攻击者警告或怀侥幸心理尝试给攻击者转账，遇到能恢复的情况真的非常稀少。

· 网页挂马事件响应

概述

网页挂马是攻击者在后攻击阶段的行为之一。不同于10年前利用Java或者Flash传播网页木马，现在的攻击者常常利用目标网站的流量或权重，将包含博彩、色情、暴力的网页链接隐藏于目标网站的网页中。企业往往通过搜索引擎或用户反馈得知自己的域名经常和涉及博彩、色情、暴力的关键词组合出现，或用户点击链接跳转至相关恶意页面。

在部分网页挂马应急响应事件中发现，攻击者往往在挂马前就通过各种方式已经获取目标主机的命令执行权限。对于如何挂马，攻击者常见的思路有两种：(1) 直接下载相关挂马网页的压缩包，解压到Web目录。(2) 下载挂马页面生成脚本，直接运行一键生成大量挂马页面。

事件分析

在网页挂马的应急事件中，通过挂马页面生成脚本方式进行挂马的情况远远超过直接下载网页压缩包的情况。在应急响应过程中发现黑客经常登录受害主机执行以下PHP脚本自动生成大量挂马页面。

app.php

```php
<?php
@error_reporting(E_ERROR);
@date_default_timezone_set("Etc/GMT-8");
@ini_set('memory_limit', '2048M');
@set_time_limit(0);
$config = array();
$config['网站www路径']      = "/home/web/www/health";
$config['生成路径']         = "/smsb/";
$config['文件存放路径']        = "./";     //默认不要改动，除非包含生成，改为绝对路径，避免修改的时候忘记修改这个路径了。
$config['自删除开关']          ="ON";
$config['关键字文件']       = "zi.txt";
$config['文章文件']         = "wen.txt";
$config['模板文件']         = "moban.txt";
$config['描述文件']         = "miaoshu.txt";
$config['站点编码']         = "UTF-8";          //必须大写
$config['生成模式']         = "数字";           //新增加 页面字母
$config['多线程开关']       = "OFF";
$config['递归模式']      = "OFF";
$config['递归模式数量']       = "500";
```

图4-6：批量生成挂马网页脚本

如上图所示，该PHP文件即为生成挂马页面的主PHP之一，只需访问或直接执行即可在Web目录下生成大量挂马页面。

相较于方式(1)，方式(2)消耗的流量更小、更隐蔽，且即使挂马页面被删除，只要相关生成脚本还在，攻击者可随时“借尸还魂”。

此外，随着近年来黑帽SEO技术的发展，很多黑产人员也自然而然将目光转到了具备高流量、高权重的热门网站。挂马的对象除常见的HTML、PHP、ASP等静态/动态页面外，有时也会在JS、CSS、图片中存在，可以说手段更加隐蔽，让人防不胜防。

03 全面适配是未来

随着云计算市场快速发展，多云和云原生趋势将渐渐成为主流。面对多云、云原生等新型架构的出现，安全成为了新的挑战。为迎接新发展，各大云服务商、安全厂商、企业组织都要做好充分技术准备及应对策略。因此，原有的主机安全产品也需要去适配这些新的架构。

· 构建云原生的安全运营中心

云原生不但可以很好的支持互联网应用，也在深刻影响着新的计算架构、新的智能数据应用。以容器、服务网格、微服务、Serverless 为代表的云原生技术，带来一种全新的方式来构建应用。企业 IT 架构也随之发生巨大变化，而业务又深度依赖 IT 能力。这带来了一定程度的复杂性和挑战性，尤其是其安全挑战不可忽视。

云原生 (Cloud Native) 最初是由 Pivotal 公司的 Matt Stine 于 2013 年提出的。Pivotal公司先后开源了云原生的Java开发框架Spring Boot 和Spring Cloud。随后，Google 在2015年成立了CNCF(Cloud Native Computing Foundation)，使得云原生受到越来越多的关注。

结合主流机构对于云原生安全的理解，其实就是四个方面的安全考虑：第一、云原生基础设施安全，尤其是容器安全。第二、DevSecOps的安全加成，也就是整个流程的安全工具链。第三、CI/CD的持续集成和持续交付的过程，可以让整个安全的修复做到非常自然，在一次持续交付过程中就可以把相关漏洞修复上线，可以跟着整个软件交付的周期来内生植入安全，同时也可以做凭证的更换等。第四、微服务安全，这个领域目前越来越受到关注，例如微服务的基础API安全，也是未来应用的交互方式。除了API本身，对于微服务的发现、隔离等安全内容也有其特定价值。

随着云原生应用的快速发展，如果将传统的安全理念、管理思路及产品技术“照搬”到云上并不能真正建立有效的云上安全运营体系，并且会存在大量的安全风险。例如：

A. 无法实现对各类型云资产的动态盘点；
B. 无法对云原生基础设施的配置风险进行检测；
C. 无法对合规风险持续的自动化评估；
D. 缺乏对云上特有的新型威胁的检测；
E. 缺乏云上自动化响应处置机制与能力；
F. 缺乏全面的云上调查溯源能力。

面对云上安全的新挑战，云上安全体系建设的安全理念、产品技术及管理思路都需要升级，需要构建云原生的安全运营体系。本报告倡导构建“一个中心、三个基本点”的安全运营中心，如下图：

图4-7：云时代的安全运营中心

构建云时代的安全运营体系应当“以云原生为中心思想，以安全左移为基本前提，以数据驱动为基本要求、以自动化为基本手段”。结合安全运营经验及广泛的云上客户调研，结合下述的云原生安全的IPMDR体系，可以帮助公有云客户全面建设云上安全运营体系，提升云上安全水平。

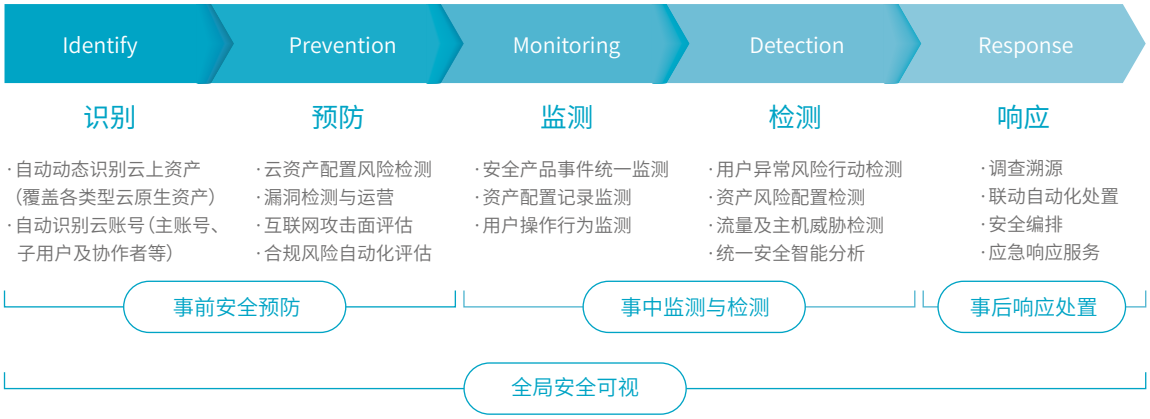


图4-8：云原生安全的IPMDR体系

根据IPMDR体系可分为，事前安全预防、事中监测与检测、事后响应处置三个阶段：

A. 首先，需要构建事前安全预防体系，即在安全事件发生之前提升整体安全水平，防患于未然。例如对云上各类资产进行自动动态盘点，并对各类云产品配置风险、漏洞及互联网攻击面等进行定期识别与加固。

B. 其次，需要构建事中的统一监测和威胁检测体系，将云上安全产品的安全事件统一收集实现安全统一监测和全局管理。同时，针对云上特有的新型威胁需要搭建检测机制与手段，例如用户风险操作、异常API调用及SecretKey泄漏监测等。

C. 同时也需要构建完善的事后响应处置体系，在发生安全事件后能够及时响应阻断与配置加固，并积极采用自动化的手段提升事件处置效率。同时，也需要构建云上安全事件的统一调查溯源平台，将安全各类相关的数据统一采集汇聚，在发生安全事件后做到可溯源。

D. 最后，在事前、事中及事后全程需建立全程的安全可视体系，例如仪表盘监控、大屏监控、安全报表等，以降低安全运营管理难度，提升安全运营效率，让云上安全态势可视可感知。

· 容器安全解决方案

对于云原生的应用，越来越多的企业开始利用Docker容器来快速构建和维护新服务和新应用。但是，容器本身也存在重大的安全风险，例如Docker宿主机安全、Docker镜像安全、运行环境的安全问题、编排安全等，这都意味着保护容器安全将是一项持续的挑战。

1）主机安全

容器与宿主机共享操作系统内核，因此宿主机的配置对容器运行的安全有着重要的影响，比如宿主机中安装有漏洞的软件可能会导致任意代码执行风险，Sudo 的访问权限没有按照密钥的认证方式登录可能会导致暴力破解宿主机。从安全性考虑，容器主机应遵循如最小安装化，不应当安装额外的服务和软件以免增大安全风险，及时给操作系统打补丁等原则。

2）镜像安全

容器镜像是由若干层镜像叠加而成的，包括根镜像、赋能层、应用层，是通过镜像仓库分发和更新的。镜像安全可以从镜像构建安全、仓库安全以及镜像分发安全三个方面加固镜像安全能力。

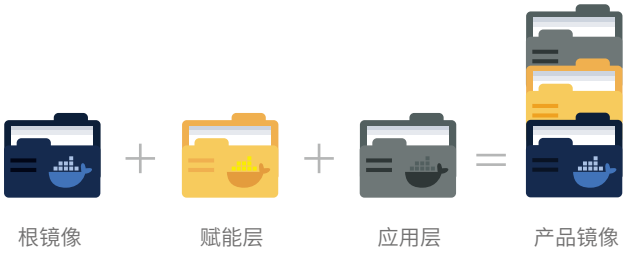


图4-9：容器镜像的组成

3）运行时安全

容器以进程的形式运行在主机上，运行的容器进程是隔离的，它拥有自己的文件系统、网络以及独立于主机的进程树。有别于传统环境，为了保证容器的稳定运行，在容器环境下需要从主机、容器实例、镜像等多个层面进行监控审计。采用基于行为控制的方式对容器运行时状态进行监控。运行时容器基本上都是单服务，每一个容器只运行一个服务，所以环境足够单纯。每一个容器都像一个采集器，有助于收集数据，然后通过机器学习进行行为分析，一旦发现异常行为就能够及时报警。此外通过容器研究和流量分析也能够建立对应基线。当然也可以采用白名单对工作负载进行微隔离。

4）编排安全

容器技术的成熟推动着微服务的发展和落地，越来越多的企业开始采用微服务架构来组建自己的应用，其中，容器编排工具管理着承载各类服务的容器集群。无论是 Kubernetes 社区还是第三方安全机构均针对 Kubernetes 中组件和资源的安全进行了相应改善和安全加固，包括计算资源安全、集群安全及相关组件安全等。对此，需要全面考虑隐私管理、授权管理、身份防控制、编排控制面、网络证书等都各个方面。

图4-10：容器编排安全

针对各类容器安全问题，目前，国际市场上涌现了一批容器安全产品安全厂商，如Neuvector、Twistlock、StackRox、Aqua等等，国内自研容器安全产品的厂商则有青藤云安全。从容器安全产品的技术方案上来看，目前大部分的容器安全厂商均使用了平行容器的方式对宿主机上的容器进行安全防护，也有一部分安全厂商采用了基于宿主机Agent解决方案进行安全防护。这两种技术方式有何不同，会产生怎样不同的安全防护效果呢？

平行容器技术方案：利用容器的隔离性和良好的资源控制能力，在容器的宿主机中启动一个容器，该容器通过挂载宿主机的所有文件系统，而后在容器内部对这些文件系统进行实时监控和处理响应，以实现对容器进行防护的作用。

基于宿主机的Agent解决方案：即基于全生命周期的主机防护能力，监控宿主机上容器相关的文件、进程、系统调用等信息，增加对于容器的清点、监控、防护能力，从而通过一种安全解决方案，即可实现宿主机安全、容器安全两种防护效果。国内新一代主机安全厂商青藤云安全是此类方案的践行者。

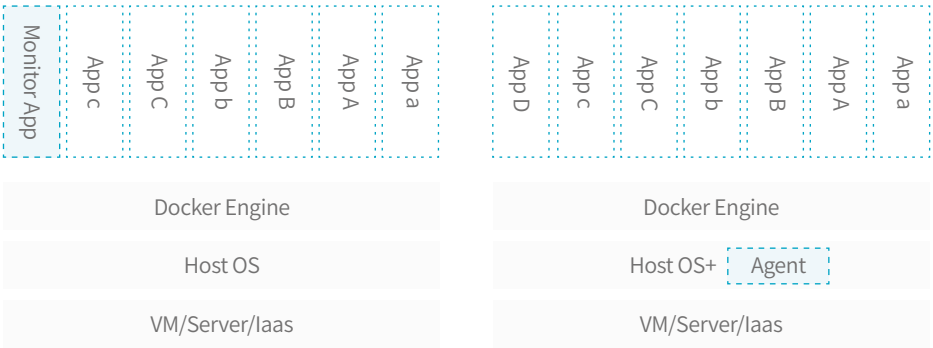


图4-11：平行容器技术方案与基于宿主机的Agent解决方案

根据容器安全解决方案，容器的安全能力应覆盖容器的整个生命周期，即构建、分发、运行三个阶段。下图展示了容器环境的安全工作流程。

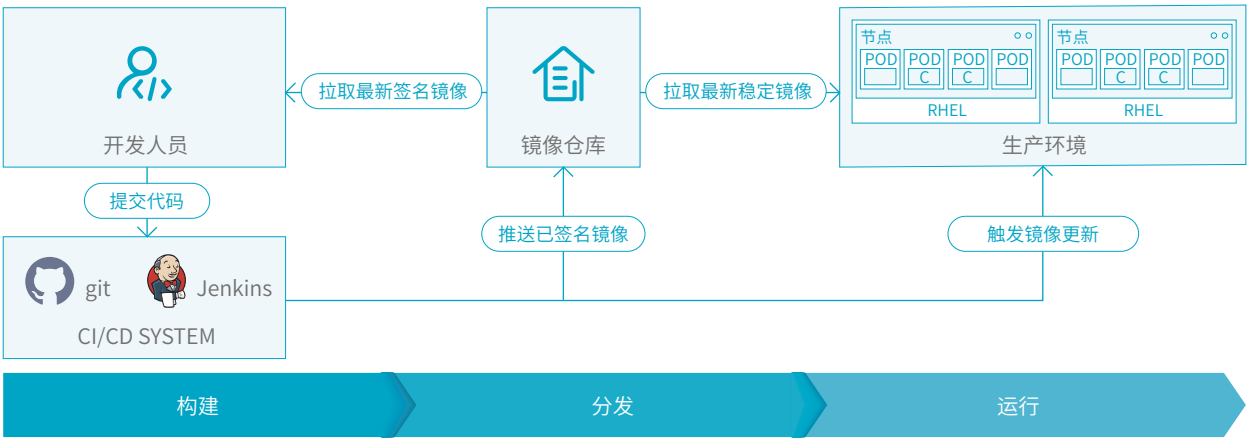


图4-12：容器环境安全工作流程

· 云工作负载保护平台

云工作保护平台（Cloud Workload Protection Platform）简称CWPP。CWPP的定义是基于主机安全的解决方案。在现代混合的数据中心架构中，主要的保护目标是服务器的工作负载。这种架构是由本地服务器、虚拟服务器以及不同公有云环境组成。CWPP与普通终端管理平台（EPP）的分野就此开始。CWPP主要解决的问题在于数据中心维度，跟EPP解决问题的PC维度是不一样的。CWPP强调了混合数据中心架构需要统一的管理、Linux系统的重点支持、杀毒软件的无效、定价灵活性以及跟云平台的对接和API与DevSecOps的结合等等。

从技术角度来看，最核心的是跟云平台原生的对接，利用AWS或者Azure提供的接口来进行相关安全措施的处理。比如说通过VPC接口可以做到相关业务的微隔离，也可以通过traffic flow log来进行流量的安全分析。之前存在的混合云的接受度问题在现在基本不是问题，当下大部分企业都是按照此类方式在规划建设。如下图所示，现在对CWPP产品能力要求在近几年中也变化最小：

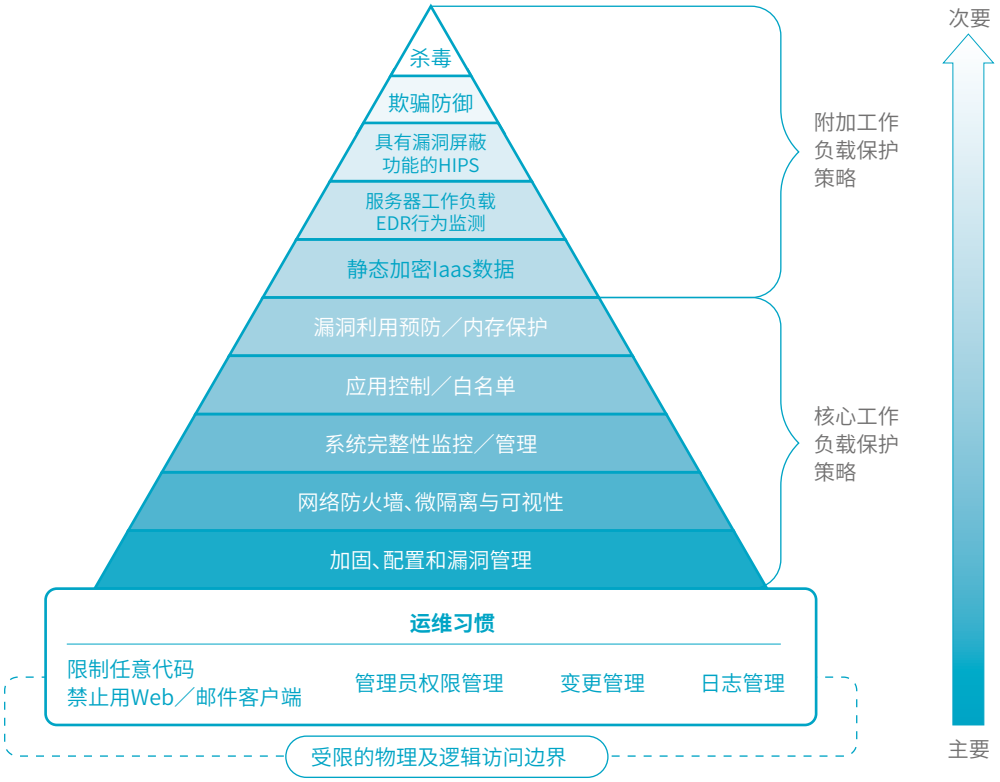


图4-13：2016年CWPP产品能力金字塔

这个产品能力（需求）的金字塔说明了对CWPP产品能力的定义，越是靠近基座的功能越重要，越是靠近塔尖的功能越次要。而到了2017年，除了对CWPP产品本身的理解又有了新的进步，也加入了一些外部场景来完善云安全的整个大局观。包括了工作负载外的服务和云基础架构的安全评估。CWPP产品解决了数据层面的问题；而外部的其他服务也是为了保证云工作负载的安全，包括了WAF、Firewall和IPS等。同时加入了控制层面的安全措施，保证云使用上的安全，其中包括IAM配置、网络配置以及管理员访问等。

同时提出了一个免疫架构的变化趋势。因为容器的出现，导致用户无法对线上系统进行处理，为此，需要将安全措施前移到开发环节，从而保证上线之后就是免疫的。运行时的应用控制和容器的锁定作为免疫系统的手段。相应架构上的要求就有对SDL流程的支持，与自动化CI/CD工具的结合，要求API可以灵活调用，将安全检查前移。

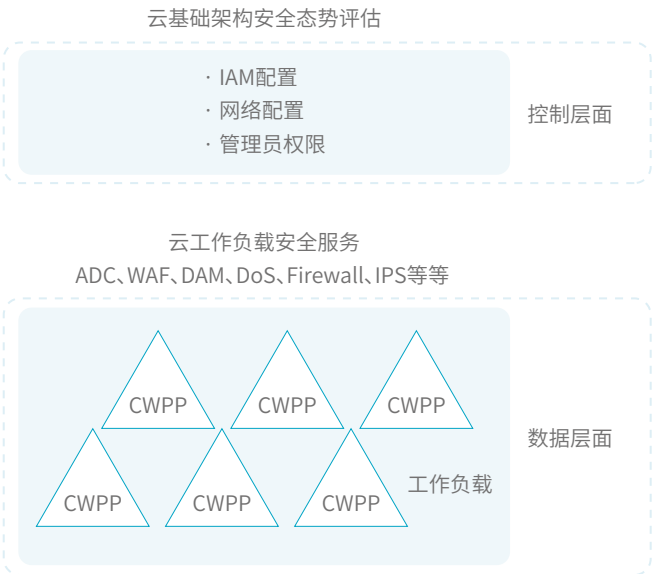


图4-14：2017年CWPP以外的安全手段

Gartner强调了大部分机构都在使用至少两个云计算服务厂商。在这种异构的云环境下，CWPP可以提供统一的安全策略管理并且迅速减少企业的知识鸿沟。提出CWPP管理的自动化，可以更好地与DevSecOps相结合。在企业自动化生成工作负载的时候，相关的软件或安全策略可实现自动化安装和配置。Serverless计算方式所带来的安全问题已经被提及，但CWPP厂商并不能很好地解决此类问题，这也是CWPP产品面临的挑战。

之前的CISPA现已被重新命名为CSPM，并且作为云安全的三个新兴产品（CWPP、CASB、CSPM）之一诞生了，同时加强了CSPM的内涵，比如加入了存储配置。

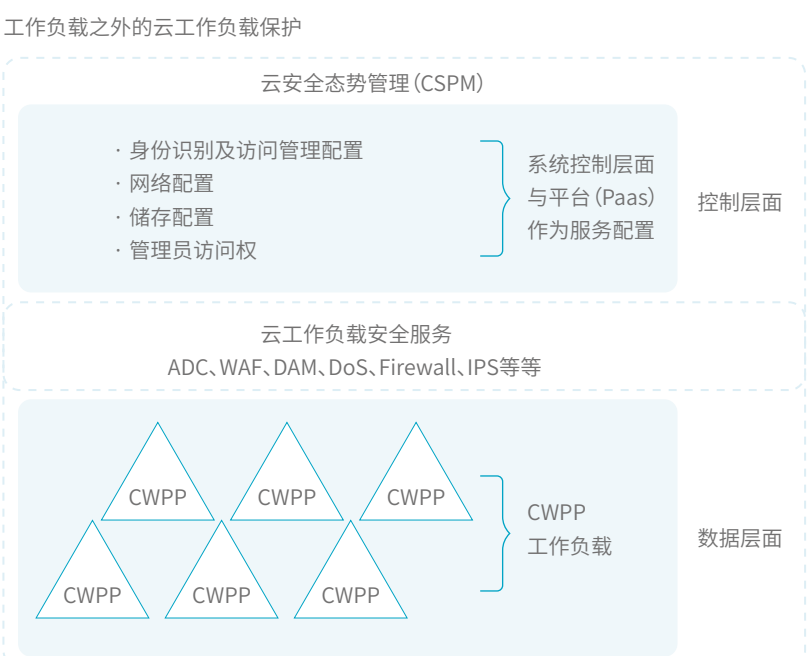


图4-15：2018年CWPP以外的安全手段

2018年，机器学习加成CWPP能力被提出。机器学习可以加强CWPP产品能力金字塔的各个层面，比如微隔离，机器学习可以先学习和观察正常的情况，然后建立白名单，随着时间的推移不断更新和修正策略以达到不用人工介入就可设置安全策略的状态。反观在EDR领域，很多使用机器学习来进行病毒发现以及异常行为监控的产品已经出现，比如Crowdstrike和Cylance。CWPP与EDR相比，更多是在数据中心安全管理领域，而EDR更多是在终端安全监测领域。

2019年是变化最大的一年。首先将工作负载的外延和内涵进行细粒度解释，根据抽象度的不同分为物理机、虚拟机、容器和Serverless。可以看出这几种工作负载从虚拟化水平到单位的计量再到生命周期都有很大的区别。这样来看，这才是“云工作负载”这一名称真正的意义所在，如果只是服务器安全或者云主机安全，是无法覆盖容器以及Serverless场景的。

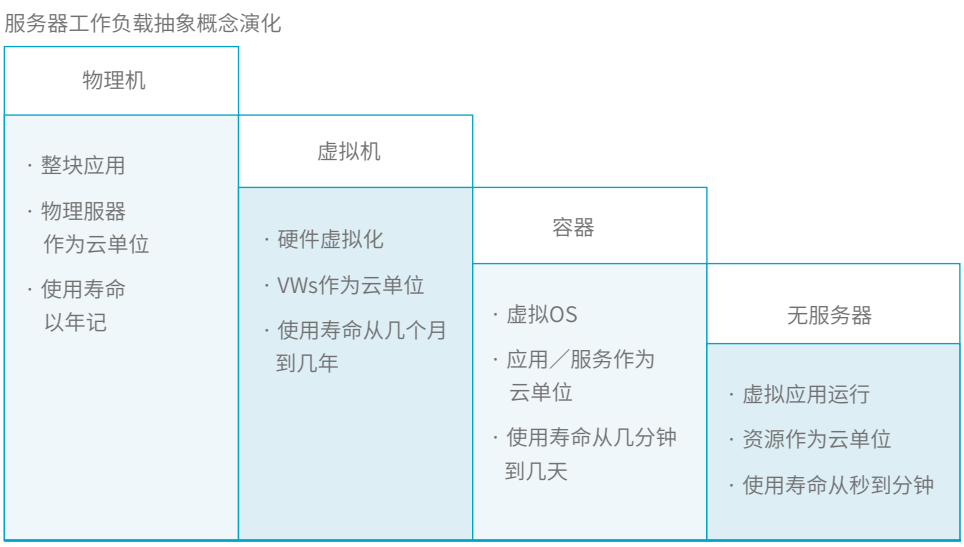


图4-16：工作负载粒度和抽象度

安全能力图也终于迎来一次大的更新。从原来的11个能力删减到8个能力，并且将最底层的“运维习惯”与“加固、配置与漏洞管理”进行了整合。删掉了“欺骗防御”能力，因为欺骗/蜜罐系统是单独产品提供。同时数据的静态加密大部分情况下都有云厂商提供，比如AWS的EBS加密和Azure的磁盘加密，因此“静态加密laas数据”这个能力也从能力金字塔中删掉了。但是加强了对威胁检测和响应的要求，相当于要学习EDR的能力。

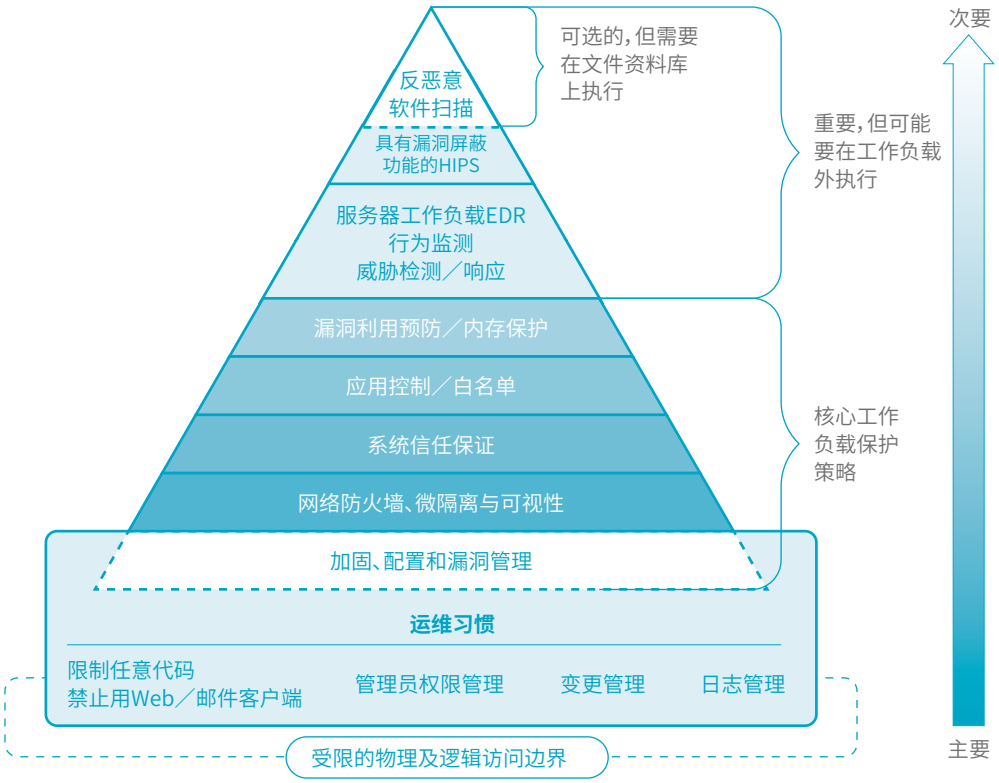


图4-17：2019年CWPP产品能力金字塔

CWPP加入了容器服务以及编排的安全要求。Kubernetes成为容器编排的事实标准，对于K8s的安全支持变为硬性要求，包括Amazon的EKS，Azure的AKS，Google的GKE以及Red Hat的OpenShift。

Serverless的函数保护被提及出来，这是一个非常新的领域。在这个保护领域，计算环境对于客户是不可见的，包括服务器、VM甚至是容器，所以基于基础架构进行的防护基本无效。考虑Serverless的解决方案更多是从应用安全入手解决，可能出现的认证信息偷窃、OWASP的漏洞、持续性攻击与容器投毒等都是需要考虑的安全场景，而实现方式更多是从代码层面和接口方面考虑。

利用机器学习分析加强安全能力的场景包括网络隔离、应用控制、服务器EDR、杀毒等。

综上所述，CWPP产品以及市场越来越成熟，客户的需求越来越统一，各家的产品能力越来越集中。但是特色的功能依然作为区分点，比如EDR能力、容器安全、合规为主或是微隔离为主，都让客户根据实际情况进行选择。从终端安全到CWPP分野，大部分厂商都会将这两类产品分得很清晰。从炒作曲线来看，非常可能迅速地从幻灭期进入爬升期，并且大家对这种产品的接受度逐渐加强，同时也是云安全建设中首先要考虑的产品之一。

目前国内也有一些公司推出了相关产品方案，例如腾讯云CWPP安全产品就可以实现“跨云，混合云统一管控”、“开放API”、“提供container和Severless app 安全”等重要功能。

1）跨云，混合云统一管控

企业在数字化转型进程中，混合云和跨云架构将成为常态。腾讯云CWPP安全产品将以统一的技术管控界面，让企业级用户对物理服务器、虚拟主机、容器以及无服务器模式的云上负载实现全面管控，同时腾讯云CWPP产品将提供行业领先的安全解决方案，让用户无需担心云上负载的位置和形式，都能获得可持续的安全保障。

2）开放API

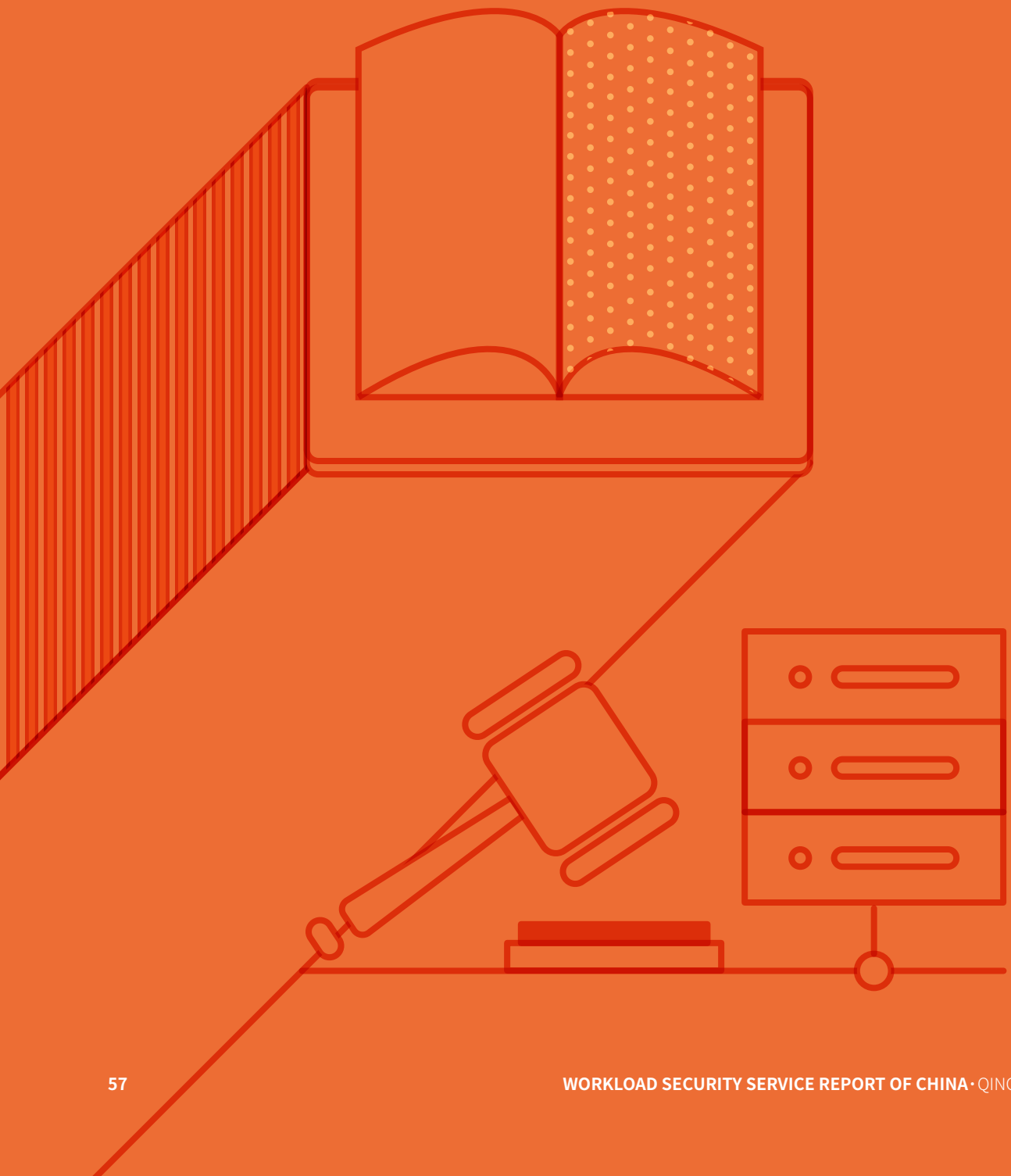
腾讯云CWPP安全产品为企业级用户提供API接入模式，让IT管理人员以及开发人员能够通过开放的API更加便捷地实现对云上负载的自动化安全策略配置，并实现自动化持续监控管理，让防护手段更加智能和高效。

3）提供Container和Severless app 安全

随着服务架构的发展，云原生应用通常由VM，Container和Serverless PaaS组成来进行交付，工作负载的粒度在变化，腾讯云CWPP产品要适配这种粒度变化。

主机安全领域法律法规

LAWS AND REGULATIONS ON WORKLOAD SECURITY



自中华人民共和国《网络安全法》于2017年6月1日正式实施以来，我国网络安全相关法律法规及配套制度逐步健全，逐渐形成综合法律、监管规定、行业与技术标准兼备的综合化、规范化体系。随着我国网络安全工作法律保障体系不断完善，网络安全执法力度持续加强，国家相关部门正在加快建立关键信息基础设施保护制度，出台数据安全法、数据安全管理办法等系列法律法规，规范数据采集、使用、共享。例如，2019年6月工信部发布的《网络安全漏洞管理规定(征求意见稿)》，已经开始面向社会公开征求意见。

在2019年12月1日，《信息安全技术 网络安全等级保护基本要求》即等保2.0的正式开始实行。标志着《网络安全法》第二十一条所确立的网络安全等级保护制度有了具体的实施依据与有力抓手。相较于2007年实施的《信息安全等级保护管理办法》所确立的等级保护1.0体系，等保2.0在国家支持、定级备案、密码管理等多个方面进行了更新与完善，以适应现阶段网络安全的新形势、新变化以及新技术、新应用发展的要求。尤其在移动互联、云计算、物联网等新的业务环境均提供安全建设标准和指导。必将极大地促进全社会对网络安全的重视，推动整个网络安全行业的全面发展。

01 等保2.0下新一代主机安全实践

等保2.0的发布将为我国网络和信息安全筑起重要防线，为政企安全防护体系的构建提供新思路。一方面，通过开展等保工作，发现相关机构、单位和企业网络和信息系统与国家安全标准之间存在的差距，找到目前系统存在的安全隐患和不足；另一方面，通过安全整改，提高网络安全防护能力，降低系统被各种攻击的风险。

等保2.0新标准名称由原来的《信息安全技术 信息系统安全等级保护基本要求》变更为《信息安全技术 网络安全等级保护基本要求》，与《中华人民共和国网络安全法》保持一致。等级保护对象由原来的“信息系统”改为“等级保护对象（网络和信息系统）”，包括基础信息网络（广电网、电信网等）、信息系统（采用传统技术的系统）、云计算平台、移动互联、物联网和工业控制系统等。新版安全要求在原有通用安全要求的基础上新增安全扩展要求，安全扩展要求主要针对云计算、移动互联、物联网和工业控制系统提出了特殊安全要求。等保2.0通用要求基本框架也原来大不相同，如下图所示。

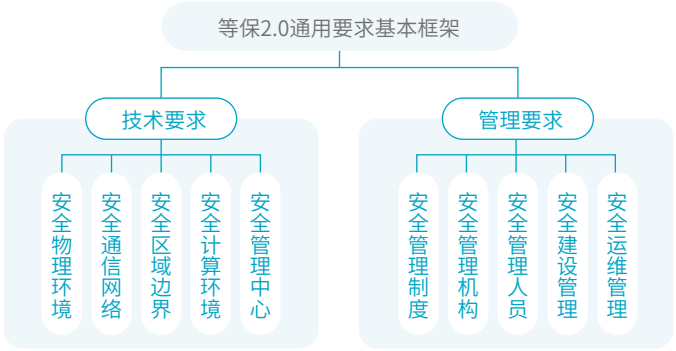


图5-1：等保2.0通用要求基本框架

在等保2.0标准对安全计算环境的描述中，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等几个方面提出了具体的要求。

1）身份鉴别

	控制点1	测评要求项
	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	1）应核查用户在登录时是否采用了身份鉴别措施。 2）应核查用户列表，核查用户身份标识是否具有唯一性。 3）应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户。 4）应核查用户鉴别信息是否具有复杂度要求并定期更换。
0分情况	1)存在自动登录或默认账户默认口令或默认账户无口令。 2）对口令复杂度和更换周期均无要求，或存在空口令或弱口令（6位数字及以下）。 3)操作系统和数据库系统的用户名不具有唯一性。	
满分情况	1）对登录操作系统和数据库系统的用户进行身份鉴别。 2）不得使用默认用户和默认口令。 3）口令由数字、大小写字母、符号混排，无规律的方式。 4）用户口令的长度至少为8位。 5）口令每季度更换一次，更新的口令至少5次内不能重复。 6）操作系统和数据库系统的用户名具有唯一性。	

	控制点2	测评要求项
	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	1）应核查是否配置并启用了登录失败处理功能。 2）应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能。 3）应核查是否配置并启用了远程登录连接超时并自动退出功能。
0分情况	1)无登录失败处理功能或未启用登录失败处理功能。	
满分情况	1）已启用登录失败处理功能。 2）限制非法登录尝试次数，超尝试次数后实现锁定策略。 3）设置网络连接超时自动退出。	

	控制点3	测评要求项
	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。
0分情况	当对主机进行远程管理，鉴别信息明文传输。	
满分情况	当对主机进行远程管理，鉴别信息非明文传输。	

	控制点4	测评要求项
	应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	1)应核查系统是否采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户身份进行鉴别。 2)应该检查是否其中一种鉴别技术使用密码技术来实现。
0分情况	采用一种鉴别技术。	
满分情况	采用两种或两种以上组合的鉴别技术（采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个及以上的组合）。	

2）访问控制

	控制点1	测评要求项
	应对登录的用户分配账户和权限。	1) 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况。 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。
0分情况	1) 未根据业务需要设置访问控制策略。 2) 只配置一个管理人员。 3) 存在兼任。	
满分情况	1) 制定安全策略。 2) 根据安全策略控制用户对资源的访问。(对重要文件的访问权限进行限制，对系统不需要的服务、共享路径等可能被非授权访问的客体（文件）进行限制）。 3) 操作系统的特权用户与该操作系统中安装的数据库系统的特权用户权限进行分离，且权限互斥。	

	控制点2	测评要求项
	应及时删除或停用多余的、过期的账户，避免共享账户的存在。	1) 应核查是否不存在多余或过期账户。 2) 应访谈网络管理员、安全管理员和系统管理员不同用户是否采用不同账户登录系统。
0分情况	存在无用账户或多人共享账户。	
满分情况	1) 不存在过期和无用账号。 2) 做到账户和人一一对应。	

	控制点3	测评要求项
	应重命名或删除默认账户，修改默认账户的默认口令。	1) 应核查是否已经重命名默认账户或默认账户已被删除。 2) 应核查是否已修改默认账户的默认口令。
0分情况	使用默认账号和默认口令或存在弱口令。	
满分情况	1) 合理限制默认账户的访问权限。 2) 重命名默认账号。 3) 修改默认口令。	

	控制点4	测评要求项
	应授予管理用户所需的最小权限，实现管理用户的权限分离。	1) 应核查是否进行角色划分。 2) 应核查访问控制策略，核查管理用户的权限是否已进行分离。 3) 应核查管理用户权限是否为其工作任务所需的最小权限。
0分情况	所有操作均使用超级权限账户进行管理。	
满分情况	所有账户采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行处理配置和安全设置，安全审计员只能维护审计信息等）。	

	控制点5	测评要求项
	访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。
0分情况	访问控制的粒度未达到主体为用户和进程级，客体为文件、数据库表级。	
满分情况	访问控制的粒度达到主体为用户和进程级，客体为文件、数据库表级。	

	控制点6	测评要求项
	应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	1) 应核查是否有管理用户负责配置访问控制策略。 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则。 3) 应测试用户是否有可越权访问情形。
0分情况	未根据业务需要设置访问控制策略。	
满分情况	1) 制定安全策略。 2) 根据安全策略控制用户对资源的访问。(对重要文件的访问权限进行限制，对系统不需要的服务、共享路径等可能被非授权访问的客体(文件)进行限制)。	

	控制点7	测评要求项
	应对重要主体和客体设置 安全标记，并控制主体对有安全标记信息资源的访问。	1) 应核查是否依据安全策略对敏感信息资源设置了安全标记。 2) 应测试是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。
0分情况	1) 未设置敏感标记功能。 2) 未依据安全策略实现功能控制。	
满分情况	1) 能对重要信息资源设置敏感标记。 2) 对重要资源设置敏感标记，并制定了访问控制策略。	

3) 安全审计

	控制点1	测评要求项
	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	1) 应核查是否开启了安全审计功能。 2) 应核查安全审计范围是否覆盖到每个用户。 3) 应核查是否对重要的用户行为和重要安全事件进行审计。
0分情况	1) 未启用审计功能。 2) 审计内容未包括重要用户行为（如用超级用户命令改变用户身份，删除系统表等）。	
满分情况	1) 启用审计功能。 2) 审计范围覆盖到主机和重要客户端上的每个用户。 3) 审计策略覆盖系统内重要的安全相关事件，至少包括用户标记和鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用等。	

	控制点2	测评要求项
	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	应核查审计记录信息是否包括事件的日期和时间、用户、事件类型，事件是否成功及其他与审计相关的信息。
0分情况	审计记录未包括事件的时间、主体标识、客体标识和结果等。	
满分情况	审计记录包括事件发生的日期和时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等。	

	控制点3	测评要求项
	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	1) 应核查是否采取了保护措施对审计记录进行保护。 2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
0分情况	审计记录只在本地存储。	
满分情况	1) 采取措施对审计记录进行保护。 2) 记录至少保存半年。	

	控制点4	测评要求项
	应对审计进程进行保护，防止未经授权的中断。	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。
0分情况	审计进程可被非授权中断。	
满分情况	审计进程受到保护，无法未授权中断或未授权修改配置。	

4）入侵防范

	控制点1	测评要求项
	应遵循最小安装的原则，仅安装需要的组件和应用程序。	1）应访谈系统管理员是否遵循最小安装原则。 2）应确认是否已经关闭非必要的组件和应用程序。
0分情况	存在明显能被利用的安全漏洞。	
满分情况	1）遵循最小安装原则，仅安装需要的组件和应用程序。 2）未启动多余的服务和端口。	

	控制点2	测评要求项
	应关闭不需要的系统服务、默认共享和高危端口。	1）应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享。 2）应核查是否存在非必要的高危端口。
0分情况	存在明显多余系统服务、共享及高危端口。	
满分情况	1）遵循最小安装原则，仅安装需要的组件和应用程序。 2）未启动多余的服务和端口。 3）设置升级主机实现对主机的补丁升级。 4）操作系统和数据库系统补丁为厂商新公布的补丁版本。	

	控制点3	测评要求项
	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	应核查配置文件是否对终端接入范围进行限制。
0分情况	未限制终端登录。	
满分情况	远程登录限制终端接入方式和网络地址。	

	控制点4	测评要求项
	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块。 2) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。
0分情况	未采用第三方监控管理软件对系统服务水平进行监视。	
满分情况	1) 通过第三方监控管理软件进行监视。 2) 第三方监控管理软件具有报警功能，且设置了报警门限值。	

	控制点5	测评要求项
	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	1) 应进行漏洞扫描，核查是否不存在高风险漏洞。 2) 应访谈系统管理员是否在经过充分测试评估后及时修补漏洞。
0分情况	存在明显能被利用的安全漏洞。	
满分情况	1) 设置升级主机实现对主机的补丁升级。 2) 操作系统和数据库系统补丁为厂商新公布的补丁版本。	

	控制点6	测评要求项
	应能够对重要程序完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。	1）询问管理员是否利用一些检查工具和脚本对重要文件的完整性进行检查，如对比校验等。 2）是否对重要的配置文件进行备份，查看备份演示等。
0分情况	无法检测重要程序的完整性。	
满分情况	1）通过第三方软件对重要程序进行完整性检测。 2）检测到完整性受到破坏后具有恢复措施。	

	控制点7	测评要求项
	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	1）应访谈并核查是否有入侵检测的措施。 2）应核查在发生严重入侵事件时是否提供报警。
0分情况	重要主机上不能检测到对重要主机的入侵行为。	
满分情况	1）能够在重要主机上检测到入侵的行为。 2）保存有攻击源IP、攻击类型、攻击目标、攻击时间等相关入侵检测记录。 3）发生入侵事件能够报警（如声音、短信、Email等）。	

5）恶意代码防范

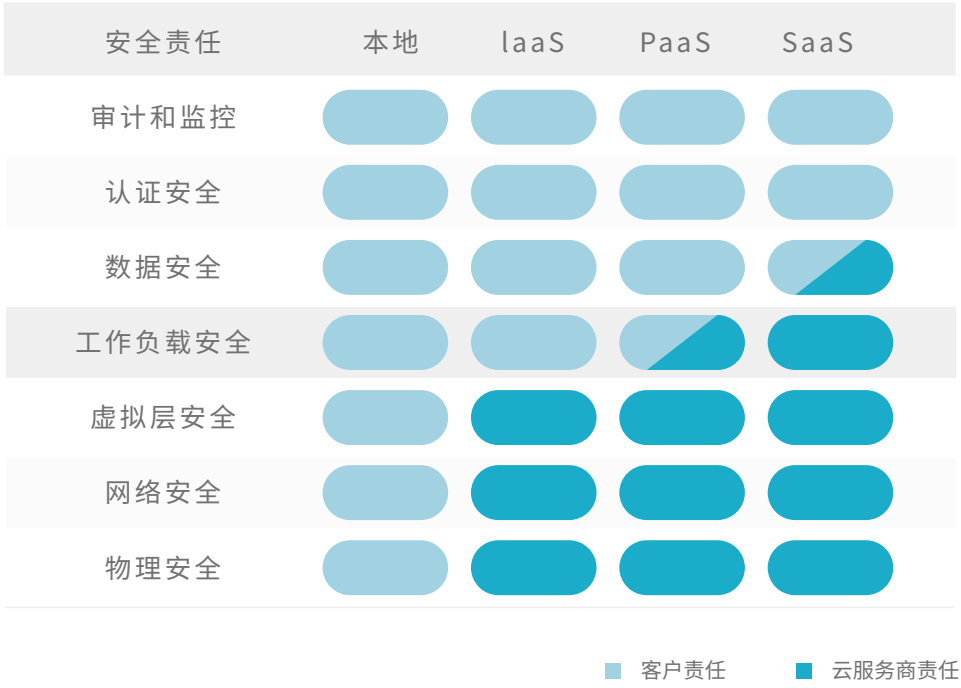
	控制点1	测评要求项
	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	1）应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或核查是否采用可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证。 2）应核查是否有保护重要系统程序或文件完整性的措施。 3）当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
0分情况	未安装防恶意代码产品或安装防恶意代码产品未及时升级。	
满分情况	1）安装防恶意代码软件。 2）防恶意代码软件为最新版本。 3）恶意代码库定期更新，且为最新版本。	

02 云等保安全合规要求

云等保不是新鲜的事物，而是在原等保框架下的扩展要求。云等保的各环节与传统等保相同，包括定级、备案、建设整改、测评、监督检查等，因此只需要对原有等级保护相关工作的具体内容进行扩充并统一。

传统信息系统的网络架构伴随业务变化而变化，系统各组件功能与硬件紧耦合，在安全防护上强调分区域和纵深防御。直观上来说，就像铁路局各管一段，信息系统通常以物理网络或者安全设备为边界进行划分。但是，云计算系统网络架构是扁平化的，业务应用系统与硬件平台松耦合，犹如航空运输。如果信息系统的划分，单纯的以物理网络或安全设备为边界进行划分，将无法体现出业务应用系统的逻辑关系，更无法保证业务信息的安全和系统服务的安全，这就犹如以机场划分各航空公司一样不适用。

在对云计算系统进行测评时应同时满足安全通用要求和云计算安全扩展要求部分的相关要求。在这个过程中根据云上系统的责任分担不同，要对安全通用要求和云计算安全扩展要求做拆分，云服务商和云服务客户针对相应要求采取对应安全保护措施。



云等保的建设整改/测评对象与传统信息系统建设整改/测评对象大不相同，如下表所示。云计算系统保护对象中增加了虚拟化、云管理平台、镜像文件等云计算独有内容。

层面	云计算系统保护对象	传统信息系统保护对象
安全物理环境	机房及基础设施	机房及基础设施
安全通信网络 安全区域边界	网络结构、网络设备、安全设备、综合网管系统、**虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台**	网络设备、安全设备、 网络架构、综合网管系统
安全计算环境 （设备和计算节点）	主机、数据库管理系统、终端、网络设备、安全设备、**虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、网络策略控制器**	主机、数据库管理系统、终端、 中间件、网络设备、安全设备
安全计算环境 （应用和数据）	应用系统、中间件、配备文件、业务数据、用户隐私、鉴别信息、**云应用开发平台、云计算服务对接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器**	应用系统、中间件、配备文件、 业务数据、用户隐私、鉴别信息等

云平台在安全建设中，强调安全能力集成，包括统一身份认证、统一用户授权、统一账户管理、统一安全审计等。在平台内部强调通讯加密与认证、动态监测预警、快速应急响应能力建设、安全产品合规等。

这时我们要考虑几方面因素，首先要确定被测系统是云计算平台还是业务应用系统。其次，确定被测系统使用哪种服务模式，以此来确定保护责任。

03 建设新基建趋势下的主机安全标准

在2018年底的中央经济工作会议上，首次提出新型基础设施概念，指出要“加快5G商用步伐，加强人工智能、工业互联网、物联网等新型基础设施建设”。2020年初突发疫情，新型基础设施的作用进一步凸显，加快建设新型基础设施的呼声和共识更加强烈。中国政府高度重视新型基础设施在抗击疫情、支持复工、促进投资、稳定经济方面的作用，密集提出加快新型基础设施建设的任务要求和方向指引。

安全可靠推进新型基础设施的建设，是新基建快速推进的基础保障。其中，无论是物理网、人工智能，还是5G通信设施，都需要一个安全可靠的主机能力。在以往云计算平台的主机安全能力基础上，我们可以预想主机安全的能力要求必将需要与新型基础设施的技术要求相比配合一致。腾讯标准化团队联合腾讯安全团队在2020年初，积极参与国家信息安全标准化委员会牵头编制的《网络安全标准实践指南　远程办公安全防护》，为重大公共卫生事件发生中和发生后带来的社会工作协同方式的变化，贡献大量的专家意见和技术实践。新型基础设施的应用，将带来大量的工作和生活形式，甚至个人身份的信息化的变化，例如，健康码在本次新冠疫情中对疫情防范和复工复产的作用，我们可以预计将来会在更多的场景下的广泛应用。在这种情况下，如何保障应用安全，数据安全，个人信息保护的有效实施，急需强大的主机安全能力，为新型移动应用提供强大的安全保障。腾讯标准团队协同腾讯产品团队和腾讯安全团队，共同贡献最先全面推广健康码的深圳地方团体标准《防疫通行码参考架构和技术指南》，以及产业互联网发展联盟归口的全国范围联盟标准《防疫健康信息码技术指南》标准。我们还会在更多的领域，探索和提供出更多的主机安全能力应用和技术建设标准，为新型基础设施建设贡献腾讯智慧“科技向善”。

主机安全建设实践指南

WORKLOAD SECURITY CONSTRUCTION PRACTICE GUIDE

主机安全将会是企业安全建设的必需品。由于安全人员紧缺，企业往往选择安全服务和产品来保护主机安全。本报告提供了一些主机安全实践的最佳办法，可以帮助安全人员将风险降至最低，确保主机上数据的安全性。

01 制定主机安全计划

想要确保主机安全，最关键是在主机安装、配置、部署之前制定详细的安全计划。许多主机的安全问题和性能问题都可以追溯到缺乏计划或管理控制。在许多组织机构中，IT架构高度分散，这种碎片化导致配置管理不一致，而这些不一致可能导致安全漏洞和其他问题。

在主机规划阶段，需要考虑以下几个方面内容：

1）确定主机的用途、位置、提供的服务信息。

2）确定在该主机上提供的服务，例如HTTP、FTP、SMTP。

3）确定要安装在主机和其它关联主机上的软件服务。

4）识别主机、主机用户、用户类别，确定主机和主机用户的权限。

5）确定主机的管理方式（例如，本地管理、从内部网络远程管理、从外部网络远程管理）。

6）确定如何对用户进行身份验证，以及如何保护身份验证数据。

7）确定资源访问执行，能够细粒度地将root级活动限制为仅对授权用户有效。

8）能够细粒度控制数据访问，能够禁用不必要的网络服务。

9）记录主机活动以检测入侵情况。

10）提供主机级别的防火墙限制流量。

11）提供必要的物理级安全防护。

02 底层操作系统安全

如果对主机底层的操作系统进行适当配置，就可以避免许多安全问题。运维人员需要通过配置主机来满足组织机构的安全需求，并能够根据需求重新配置。可以采取以下基本步骤来保护操作系统：

1）补丁以及更新操作系统

一旦安装了操作系统，通过打补丁或更新升级来解决已知的漏洞。尤其是在主机暴露在不受信任的环境之前，需要解决主机的操作系统漏洞。

2) 加强和配置操作系统，以充分解决安全问题

管理员应该执行以下步骤来加强和安全地配置服务器操作系统，包括移除不必要服务、应用、控件，配置操作系统用户权限，对资源控制进行适当配置。

3) 部署和配置额外的安全控制

操作系统通常不包括所有必要的安全控制，以充分保护操作系统、服务和应用程序。在这种情况下，管理员需要选择、安装、配置和维护额外的软件来提供缺少的控件。通常需要的控制包括反病毒软件、IDPS、主机防火墙、补丁管理和风险管理。

在规划安全控制时，服务器管理员应该考虑安全控制将消耗的资源。如果服务器没有足够的内存和处理能力来处理控件，那么它的性能可能会下降。服务器管理员还应该考虑任何基于网络的安全控制，如网络防火墙和入侵检测系统，它们可以为服务器提供额外的保护。如果基于主机的安全控制对服务器来说资源过于密集，或者在其他方面不可行的话，服务器管理员可能需要通过使用额外的基于网络的安全控制来保护服务器的操作系统、服务和应用程序来进行补偿。对于许多服务器，除了基于主机的安全控制之外，还使用基于网络的安全控制来提供额外的安全层。

4) 测试操作系统的安全性，以确保前面的步骤充分解决了所有安全性问题

操作系统的定期安全测试是识别漏洞、确保现有安全预防措施有效和安全控制配置正确(例如，使用所需的密码算法来保护网络通信)的重要方法。测试操作系统的常用方法包括漏洞扫描和渗透测试。漏洞扫描通常需要使用一个自动化的漏洞扫描器来扫描网络上的一个或一组主机的应用程序、网络和操作系统漏洞。渗透测试是一个使用攻击者的工具和方法来破坏网络的测试过程。它涉及迭代地确定和利用网络的最薄弱区域，以获得对网络其余部分的访问，最终危及网络的整体安全。漏洞扫描应定期进行，至少每周至每月进行一次，渗透测试至少每年进行一次。

03 主机运行软件安全

在确保主机操作系统安全后，下一步就是确保主机上软件性，例如通过CNNVD确定是否有已知的漏洞和相关补丁可用。

此外，在所有软件都安全安装、打补丁和配置之前，应尽可能限制内部网络访问。不安全的服务器在被放到互联网上几分钟内就会受到威胁。当然软件放到网络上之前想要进行全面加固并不总是可行的。例如，一些应用程序开发工具组合不能在预先加固的OS和Web服务器配置上安装、配置和测试。在这种情况下，逐步强化或增量强化是一个可行的选择，在生产部署时对加固进行全面验证。

1）安全安装软件

总体原则是只安装服务器所需的服务，并通过补丁或升级消除任何已知的漏洞。安装过程完成后，应立即删除安装的任何不必要的应用程序、服务或脚本。

如果可能，组织应该考虑使用非标准的目录名、目录位置和文件名安装服务器。许多针对服务器的服务器攻击工具和蠕虫只寻找默认位置的文件和目录。虽然这不能阻止坚决的攻击者，但会迫使他们付出更大的代价，而且还会增加攻击检测的可能性，因为访问默认文件名和目录的尝试失败，而且执行攻击需要额外的时间。

2）配置访问控制

大多数服务器操作系统提供了为该主机上的文件、设备和其他计算资源单独指定访问权限的功能。服务器可以使用这些控件访问的任何信息都可以潜在地分发给访问服务器的所有用户。服务器软件可能包括提供特定于其操作的附加文件、设备和资源访问控制的机制。为操作系统和服务器应用程序设置相同的权限非常重要;否则，可能会授予用户过多或过少的访问权限。服务器管理员应该从两个角度考虑如何配置访问控制来保护服务器上存储的信息。

适当设置访问控制可以帮助防止泄露敏感或受限制的信息。此外，访问控制可用于在针对服务器的DoS攻击事件中限制资源的使用。类似地，访问控制可以通过确保服务器管理员不能修改服务器日志来强制职责分离，并可能确保服务器进程只允许附加到日志文件。

3）服务器资源限制

为了减轻某些类型的DoS攻击的影响，配置服务器以限制它可以消耗的资源的数量。服务器操作系统生成的日志信息有助于识别此类攻击，因此管理员应该尽可能将服务器日志存储在集中的日志服务器上，最好是本地存储日志。因为服务器一旦被攻击，攻击者可以修改或删除本地存储的日志来隐藏攻击信息，而在集中式日志服务器上维护日志的副本，可以让管理员获得更多的信息。除了上面提到的控件之外，通常还需要配置超时和其他控件来进一步减少某些DoS攻击的影响。

如果打开的连接最大数量设置为一个较低的数量，攻击者就可以很容易地使用非法请求(通常称为SYN泛滥)来消耗可用的连接。将最大值设置为大得多的数字可能会减轻这种攻击的影响，但代价是消耗额外的资源。

4）选择并部署身份验证和加密技术

许多服务器都支持多种用于识别和验证具有不同访问权限的用户技术。没有用户身份验证，服务器就无法对不同权限的用户进行访问限制。此外，如果没有加密，流量数据可以轻易被窃取和篡改，这将违反机密性和关键信息的完整性。

组织应该定期检查服务器上可访问的服务和信息，并确定必要的安全需求。对于敏感信息，组织应该检查每组资源可访问的用户或用户组。对于需要某种级别的用户身份验证的信息，组织应该确定哪些验证技术或方法将提供适当级别的验证和加密。每种方法都有其独特的收益和成本，应该与客户和组织的需求和策略仔细权衡。

04 持续主机安全运维

在完成服务器部署之后，运维人员需要确保主机的持续安全性，包括处理和分析日志文件、定期执行文件备份、主机故障恢复、定期测试主机安全性、以及安全地执行远程管理，当然也包括前面所提倡的操作系统和软件补丁和更新，配置管理和安全控制。

1) 日志记录

日志记录是安全运维的基础，日志文件通常是可疑行为的唯一记录，需要准备好的工具来处理和分析日志文件并检查警报通知。网络和系统日志很重要，特别是在通信加密的情况下，网络监控的效率较低，而主机侧的日志数据显得尤为重要。主机日志可以针对可疑行为发出警报，通过日志可以追踪攻击者活动，当服务器被攻陷后可以帮助恢复工作，协助事后调查，也可以为法律提供相关支持。

2) 主机备份程序

服务器管理员最重要的功能之一是维护服务器上数据的完整性。服务器管理员需要定期对服务器执行备份。服务器可能由于恶意或无意行为或硬件或软件故障而失败。此外，出于法律和财务方面的原因，还应该定期备份服务器数据。

3) 安全恢复

大多数组织机构都会面临自己网络上主机被入侵的情况，因此，组织机构需要建立必要的流程以应对入侵。大多数组织机构都建立了自己应急响应团队。服务器运维人员应该按照既定的规则和流程，在怀疑或者确认安全事件发生后，在采取具体行动之前第一时间与应急响应团队保持沟通。可以采取以下流程步骤：

A. 向组织应急响应团队报告入侵情况
B. 隔离已被入侵的系统或采取其它步骤来遏制攻击，以便收集更多信息
C. 在必要的情况下，与管理层、法律顾问和执法部门迅速协商
D. 调查相似主机，以确定攻击者是否也危害了其他系统
E. 入侵分析，包括服务器状况（网络连接、内存转储、时间戳、登录用户）、修改服务器软件配置、攻击者留下的痕迹、系统日志、入侵检测和防火墙日志
F. 恢复服务器，如不可行，重新部署
G. 测试服务器确保安全性
H. 重新连接网络

I. 监视服务器和网络，寻找攻击者试图再次访问服务器或网络的迹象

J. 经验总结文档

4）主机安全性测试

定期对服务器进行安全测试至关重要。没有定期的测试，就不能保证当前的保护措施是有效的，或者应用的安全补丁是正常的。尽管存在多种安全测试技术，但漏洞扫描是最常见的。漏洞扫描帮助服务器管理员识别漏洞并验证现有的安全措施是否有效。渗透测试也被使用，但它使用频率少很多。

A. 漏洞扫描

漏洞扫描器是用来识别漏洞和主机错误配置的自动化工具。许多漏洞扫描器还提供关于缓解已发现漏洞的信息。漏洞扫描器可以帮助识别过期的软件版本、缺失的补丁或系统升级，可以验证是否符合或偏离组织机构的安全策略。为了实现这一点，漏洞扫描器识别运行在主机上的操作系统、服务器软件和其他主要软件应用程序，并将它们与漏洞数据库中的已知漏洞进行匹配。

然而，漏洞扫描器有一些明显的弱点。通常，它们只识别已经暴露的漏洞，无法输出主机整体风险级别。尽管扫描过程本身是高度自动化的，漏洞扫描器可能有很高的误报错误率。此外，漏洞扫描器通常不能识别自定义代码或应用程序中的漏洞。

B. 渗透测试

渗透测试对于安全防护有着非常大的价值，使用攻击者使用的相同方法和工具测试网络，验证网络是否存在漏洞，并展示如何利用这些漏洞，获得更大权限。

5）远程登录管理

启用远程登录的风险因服务器在网络上的位置而异。对于位于防火墙之后的服务器，可以从内部网络相对安全地实现远程登录，一般情况下不允许从位于网络外部实现远程登录，除非通过远程访问解决方案(如VPN)在组织控制的计算机上执行。如果是必须启动远程登录，应该尽可能尝试以下方式确保安全性，包括：

A. 严格的身份认证机制（包括私钥/公钥、双因子认证等）

B. 限制用户、限制IP、限制内网、VPN等方式来控制可远程登录主机的方式

C. 使用SSH、HTTPS等安全协议对密码和数据进行加密，不使用FTP、NFS、HTTP等

D. 远程登录最小权限，包括最小访问权限

E. 除非采用VPN，否则禁止从互联网直接远程登录内部服务器

F. 使用支持服务器身份验证的远程管理协议来防止中间人攻击

G. 更改远程管理实用程序或应用程序的任何帐户或密码

总结

SUMMARY

由于主机可以为内部和外部用户提供各种服务，也可以用来存储或者处理组织机构的敏感信息，因此，主机上承载的数据和服务价值巨大，因而成为备受黑客青睐的攻击对象。保护主机安全的重要性不言而喻。

本文件首先从宏观角度入手，介绍了主机安全行业的发展现状。包括从主机资产、主机风险、主机入侵和主机合规四个方面介绍了主机安全行业的整体概况。然后针对主机行业存在的风险和问题，介绍了主机安全市场上存在的不同级别的安全产品。这些安全产品，按层次从低到高分别为基础性的主机安全产品、以应用为核心的主机安全产品、以检测响应为核心的主机安全产品、以主动防御为核心的主机安全产品和新形态下的主机安全产品。本文件针对不同级别的主机安全产品，分别介绍了其所采用的控制措施以及达到的安全防御效果。

但是，随着技术发展的突飞猛进，黑客的攻击技术也在加速迭代更新，攻防对抗愈发激烈，仅仅通过防范和阻止已无法满足主机安全要求，这就需要注重检测和响应。最近两年发展得如火如荼的ATT&CK框架对主机安全防护带来了很大的便利。在检测方面，本文件则介绍了基于ATT&CK框架的主机入侵检测，主要描述了如何检测和缓解黑客最常用的攻击战术，例如持久化、权限提升、凭据获取、横向移动、命令和控制。在应急响应方面，本文件对恶意挖矿、内网入侵、勒索病毒、网页挂马四大最常见的事件为例，介绍了在发生安全事件时，该如何做出应急响应。

另外，随着云计算市场的快速发展和5G时代的到来，企业上云为安全带来了新的挑战。本文件从这一时代背景出发，从云原生的安全运营中心、容器安全解决方案和云工作负载的保护方面，对新型架构下的主机安全适配能力进行了介绍。

与此同时，网络安全的法律法规也日趋完善。各项法律法规的出台与颁布，为主机安全防护设定了基准要求，进一步夯实了网络安全的基础。

最后，本文件从主机安全的不同层面出发，给出了针对性的安全防护措施，对于各企业的主机安全防护具有一定的指导作用。

总体来讲，本文件首先介绍了主机安全市场的整体状况，说明了当前市场上存在的不同安全产品，让安全从业者和各大企业对主机安全市场的发展现状有了一个整体的了解。然后，介绍了如何基于最先进的ATT&CK框架进行检测，并给出了具体的应急响应示例，对于安全人员有很好的借鉴意义。另外，本文件还介绍了在当今云计算发展的时代背景下，该如何防护主机安全。最后，文档还介绍了当前法律法规的完善情况，并从不同层面出发，给出了主机安全的最佳实践指南。总之，本文件希望通过对主机安全行业概况、发展现状、具体的检测和响应方式、以及未来的发展趋势的介绍，让各大组织机构更加清晰地了解如何保护主机安全，以及如何应对未来发展。

参考文献

REFERENCE

[1] GB/T 22239-2019 信息安全技术网络安全等级保护基本要求。

[2] GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求。

[3] GB/T 28448-2019 信息安全技术网络安全等级保护测评要求。

[4] GB/T 28449-2018 信息安全技术网络安全等级保护测评过程指南。

[5] GB/T 25058-2019 信息安全技术网络安全等级保护实施指南。

[6]GB/T33561-2017 信息安全技术安全漏洞分类。

[7]国家计算机网络应急技术处理协调中心。2017年中国互联网网络安全报告。[R]中国工信出版集团，人民邮电出版社，2018年6月。

[8]国家计算机网络应急技术处理协调中心，2018年中国互联网网络安全报告。[R]人民邮电出版社，2019年4月。

[9]国家互联网应急中心，CNCERT互联网安全威胁报告。[OL]
http://www.cert.org.cn/，2019年4月。

[10]Mitre Group.CAR-2019-04-004: Credential Dumping via Mimikatz.[OL]
https://car.mitre.org/analytics/CAR-2019-04-004/,Oct.30,2019.

[11]Cylance, 2019 Threat Report. [OL]
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf?_ga=2.194100014.207560192.1557408928-1034628078.1557241850, Jan. 20, 2020.

[12]Qualys, Narrowing the Security Gap with Automated Configuration Assessment.[OL]
https://www.qualys.com/forms/whitepapers/narrowing-security-gap-automated-configuration-assessment/,Jan.18,2020.

[13]SANS, Stronger Security with Global IT Asset Inventory.[OL]
https://www.sans.org/webcasts/stronger-security-global-asset-inventory-107930,Jan.30,2020.

[14]CrowdStrike, 2019 CrowdStrike Global Security Attitude Survey.[OL]
https://www.crowdstrike.com/resources/reports/global-security-attitude-survey-2019/,Jan.16,2020.

[15]Qualys, Keep Calm and Prioritize:Top 5 Requirements for Prioritizing Vulnerability Remediation.[OL]
https://www.cloudpapers.com/keep-calm-and-prioritize-top-5-requirements-for-prioritizing-vulnerability-remediation/, Feb.10,2020.

[16]Qualys, Top 6 Security Use Cases for Automated Asset Inventory.[OL]
https://techpapers.co.uk/qual_111/,Jan.14,2020.
[17]Neil MacDonald. Market Guide for Cloud Workload Protection Platforms. [OL]
https://www.gartner.com/en/documents/3906670/market-guide-for-cloud-workload-protection-platforms, Nov. 30, 2019.
[18]Keith Mokris. 2019 Gartner Market Guide for CWPP: What You Need to Know.[OL]
https://www.twistlock.com/2019/04/25/2019-gartner-market-guide-cwpp-need-know/, Dec.25,2019.
[19]TANIUM , 2018 Endpoint Security Survey.[OL]
https://www.google.com/search?q=TANIUM+%2C+2018+Endpoint+Security+Survey.&oq=TANIUM+%2C+2018+Endpoint+Security+Survey.&aqs=chrome..69i57.976j0j8&sourceid=chrome&ie=UTF-8, Nov. 28,2019.
[20]McAfee, Foundstone Host Security Configuration Assessment. [OL]
https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-host-security-config-assess.pdf, Dec. 20,2019 .
[21]IDC, Worldwide Cloud Security (Software-Defined Compute Workload Security and Firewall Fabric) Market Shares, 2018: Protecting Workloads in Hybrid and Multicloud. [OL]
https://resources.trendmicro.com/IDC-Cloud-Workload-Security-Report_ThankYou.html,November 30, 2019.
[22]Andras Cser, The Forrester Wave™: Cloud Workload Security Q4 2019. [OL]
http://www.bitdefender-cn.com/downloads/datasheet/The_Forrester_Wave_Cloud_Workload_Security.pdf, December 9, 2019.
[23]Department of Computer Science Computing Guide, Host Based Security Best Practices. [OL]
https://csguide.cs.princeton.edu/security/host,Jan.10,2020.
[24]ExamCollection, How to establish host security.[OL]
https://www.examcollection.com/certification-training/security-plus-how-to-establish-host-security.html, Nov. 20, 2019.
[25]Andreas M. Antonopoulos, Host-based security controls. [OL]
https://www.networkworld.com/article/2326592/host-based-security-controls.html, Dec. 20, 2019.

让安全之光照亮互联网的每一个角落