

 **蓝盾** **智慧安全领导者**
BLUEDON 蓝盾股份:300297

智慧安全

领导者

疫情期间蓝盾如何保障线上办公安全



许浩伟

蓝盾学院讲师

CONTENTS

目录

第一章 信息安全发展态势

第二章 信息安全案例介绍

第三章 蓝盾保障办公安全方法



CONTENTS

章节

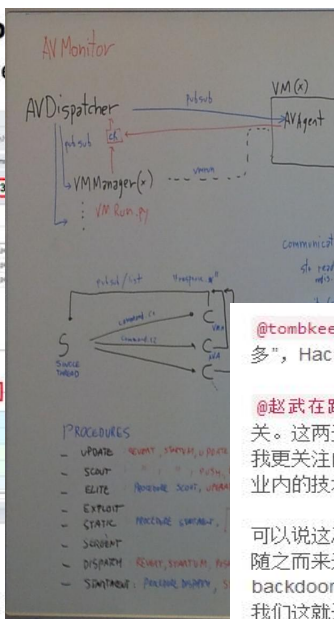
第一章 信息安全发展态势

1.1 信息安全事件



安全事件:Hacking Team数据泄露

What the function
This is what the page



Hacking Team被黑泄露400GB数据附下载地址

07月07日, 2015 资讯 APOCALYPSE 1,660次

Hacking Team是一家专业向政府及执法机构贩售入侵与监视工具的意大利黑客公司，由于Hacking Team丑陋的商业行为和该公司主导开发的监控工具“Da Vinci”，因此无国界记者组织（Reporters Without Borders）将该公司列入互联网公敌名册中。

@tombkeeper: Stuxnet 让公众知道：“原来真有这种事”，Snowden 让公众知道：“原来这种事这么多”，Hacking Team 让公众知道：“原来这种事都正经当买卖干了”。

@赵武在路上: 2011年的时候，HBGray被黑，很多人没有意识到意味着什么，因为跟国家安全相关。这两天Hacking team被黑，大家也没有意识到意味着什么。这次包括了客户清单和0day，但我更关注的是RCS的代码，以前行业内都是粗糙到不行的demo，工程化公开的很少，这次会让行业内的技术往前推进几年，尤其是黑产。

可以说这次事件和斯诺登事件的影响力是不相上下的，但HT被黑不光光是让公众知道有这回事，随之而来还有整整415G的泄漏资料！里面有Flash 0day, Windows字体0day, IOS enterprise backdoor app, Android selinux exploit, WP8 trojan等等核武级的漏洞和工具。那么废话不多说，我们这就开始导览之旅。

各种监控信息详细到令人发指。

安全事件:NSA核武泄露

黑客组织“影子经纪人”（Shadow Broker）宣称：已黑进全球顶级黑客组——美国国家安全局(NSA)“方程式”黑客小组，并盗取大量黑客工具和漏洞利用代码。

NSA在漏洞发现和利用方面的开发经费数以百万计，但颇具讽刺意味的是，这些威力堪比网络核武的零日漏洞一旦落入网络犯罪团伙、黑客甚至大众的手中，将引发一场浩劫，正如Dolan Gavitt所言：“如今十几岁的少年都会用（这些漏洞利用代码）”。

- libmelter-master.zip
- libpemelter-master.zip
- melter-master.zip
- poc-x-master.zip
- racs-anonymizer-master.zip
- racs-anonymizer-old-master.zip
- racs-backdoor-master.zip
- racs-collector-master.zip
- racs-common-master.zip
- racs-console-library-master.zip
- racs-console-master.zip
- racs-console-mobile-master.zip
- racs-db-ext-master.zip
- scout-win-master.zip
- shshget-master.zip
- soldier-win-master.zip
- test-av2-master.zip
- test-av-master.zip
- TIXATI TORRENT CLIENTS.zip
- vector-apollo-master.zip

安全事件: “永恒之蓝”

Microsoft 安全公告 MS17-010 - 严重

Microsoft Windows SMB 服务器安全更新 (4013389)

发布日期: 2017年3月14日

版本: 1.0

执行摘要

此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者向 Windows SMBv1 服务器发送特殊设计的信息, 那么其中最严重的漏洞可能允许远程执行代码。

对于 Microsoft Windows 的所有受支持版本, 此安全更新的等级为“严重”。有关详细信息, 请参阅[受影响的软件和漏洞严重等级部分](#)。

此安全更新可通过更正 SMBv1 处理经特殊设计的请求的方式来修复这些漏洞。

有关这些漏洞的详细信息, 请参阅[漏洞信息部分](#)。

有关此更新的更多信息, 请参阅 [Microsoft 知识库文章 4013389](#)。



勒索病毒



安全事件:数据泄露

➤ 网易邮箱被“脱裤”

2015年10月19日, 乌云漏洞报告平台有白帽子报告称网易163/126邮箱的用户数据库疑似泄露, 网易被黑影响数量总共近5亿条, 泄露信息包括用户名、MD5密码、密码提示问题/答案(hash)、注册IP、生日等。

➤ 华住集团信息泄露

2018年8月28日, 网络爆料称, 华住集团旗下连锁酒店用户数据疑似发生泄露。从卖家发布的内容看, 数据包包含华住旗下汉庭、禧玥、桔子、宜必思等10余个品牌酒店的住客信息

漏洞概要

缺陷编号: [WooYun-2015-147](#)
 漏洞标题: 网易163/126邮箱过亿数据
 相关厂商: 网易
 漏洞作者: 路人甲
 提交时间: 2015-10-19 13:57
 公开时间: 2015-12-03 13:57
 漏洞类型: 用户资料大量泄露
 危害等级: 高
 漏洞来源: <http://www.wooyu>
 Tags标签: 无
 分享漏洞: [分享](#) [收藏](#) [评论](#)

暴躁老哥 @iOday

我也多说两句, 上次出事后, 华住的数据其实在暗网一直在更新, 基本都是当月新数据。
另, 估计他们没安全人员。

漏洞详情

披露状态: 2015-10-19: 细节已通知厂商并

简要描述: 163数据过亿交密证明数据/包含制

漏洞hash: 51e1fdd0ad0afe48e9

版权声明: 转载请注明来源 路人甲

安全_云舒 @iOday

48分钟前 来自 iPhone客户端

有认识华住安全人员的没有? 今天连你们的wifi, 电脑mac、身份证号码、手机号码, 全部明文http在网上传输, 电脑mac和手机号码还明文出现在url地址栏, 点下确定肠子都悔青了。基本的安全道理都不懂么? 就是wifiportal.huazhu.com:8008, 迟早被人网络嗅探或者脱裤, 等死吧你们。

2018/11/13 21:28

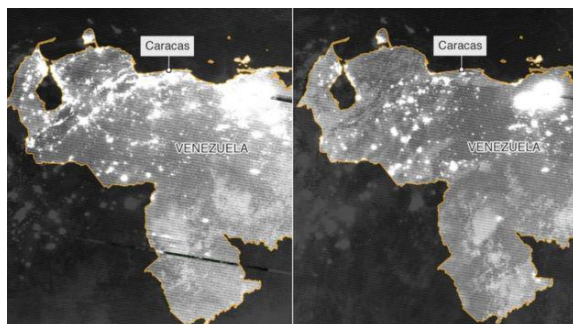


安全事件:委内瑞拉大停电

2019年3月7日委内瑞拉开始停电，此后几天，持续的停电停水让全国许多地区陷入瘫痪。

40度高温，停电停水好几天。已经混乱的国家，已经贫困的人民，在黑暗中、饥饿中、死亡的边缘挣扎……

有委内瑞拉人形容，这样过生活如同“世界末日一般”。



安全渗透进各个层面!

安全问题已经不单是一个简单的“黑客攻防”的问题，已经渗透到上至国家安全、商业安全，下至普通百姓的日常生活之中。

无所不在，无处不在，其影响只会越来越深入。

新技术的诞生，安全问题相伴相随



移动互联



万物互联

<http://46.49.100.216:8001/view1.html>



隐私画面频频曝光 网络摄像头安全何在

曾经我们希望有一天可以在千里之外就能随时监控到自己家中的画面，而随着科技的进步今天我们实现了这个梦想，但实现的背后我们的隐私去哪了？



信息安全发展态势

物联网信息安全

万物互联
等等

6

1

2011年 Hacking Team
被黑泄露400GB数据
附下载地址

2

个人信息安全

2017年 NSA网络核武扩散,
零日漏洞被公开,
wanna cry勒索病毒肆虐

信息安全发展态势

3

2015年 网易邮箱被
脱库, 数据在暗
网黑市售卖

5

2019年 委内瑞拉
大停电,
疑似国外黑客攻击

国家信息安全

4

2018年 华住
会数据泄露,
数据在暗网黑市售卖

企业信息安全



CONTENTS 章节

第二章 信息安全案例介绍

2.1 Cookie欺骗免密登录腾讯邮箱

2.2 虚假热点窃取微信资料 (图片、视频)

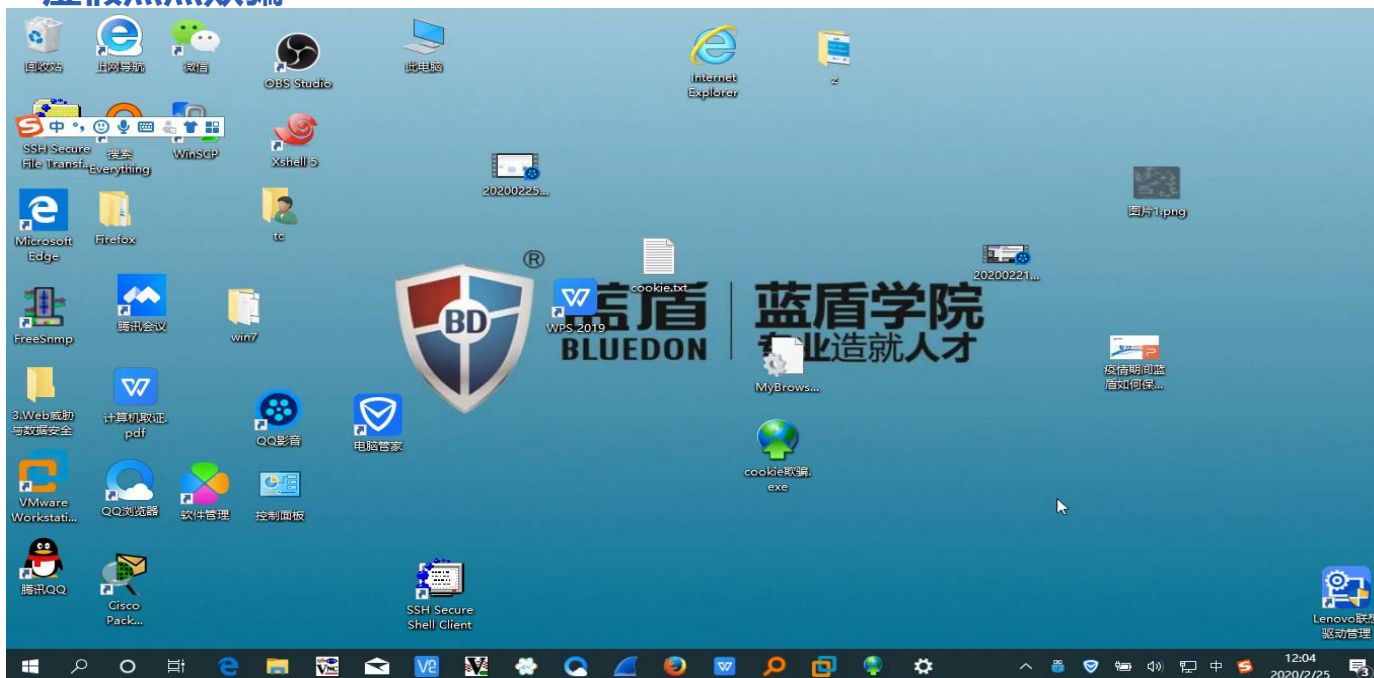
2.3 屏显内容远程窃取



Cookie欺骗



虚假热点欺骗



屏显内容远程窃取



CONTENTS 章节

第三章 蓝盾保障办公安全方法

3.1 蓝盾股份介绍

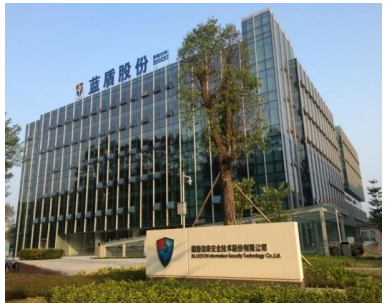
3.2 蓝盾VPN安全网关

3.3 蓝盾安全云桌面

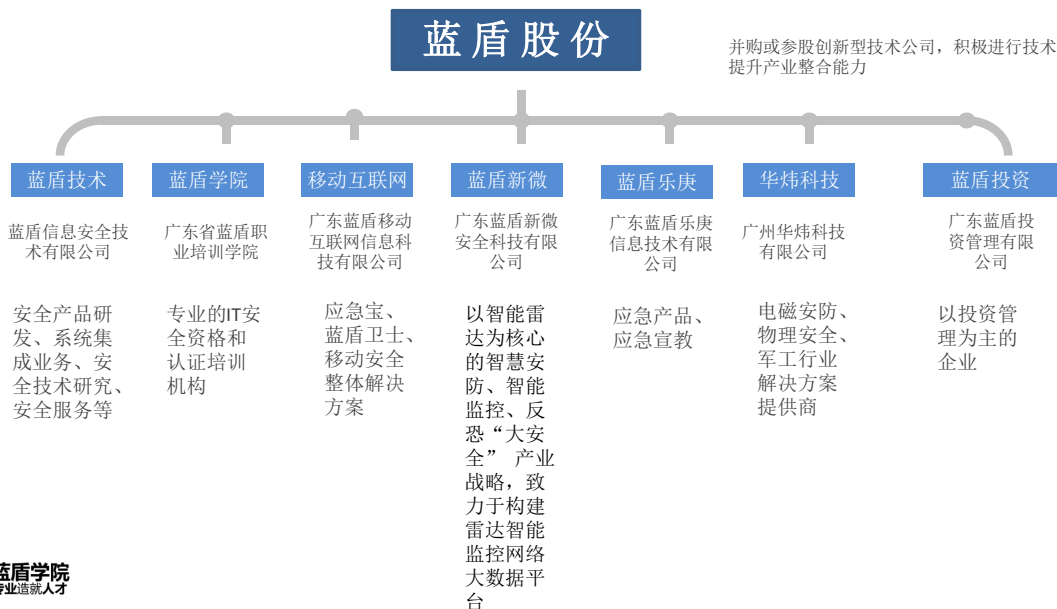


行业地位：中国信息安全龙头企业

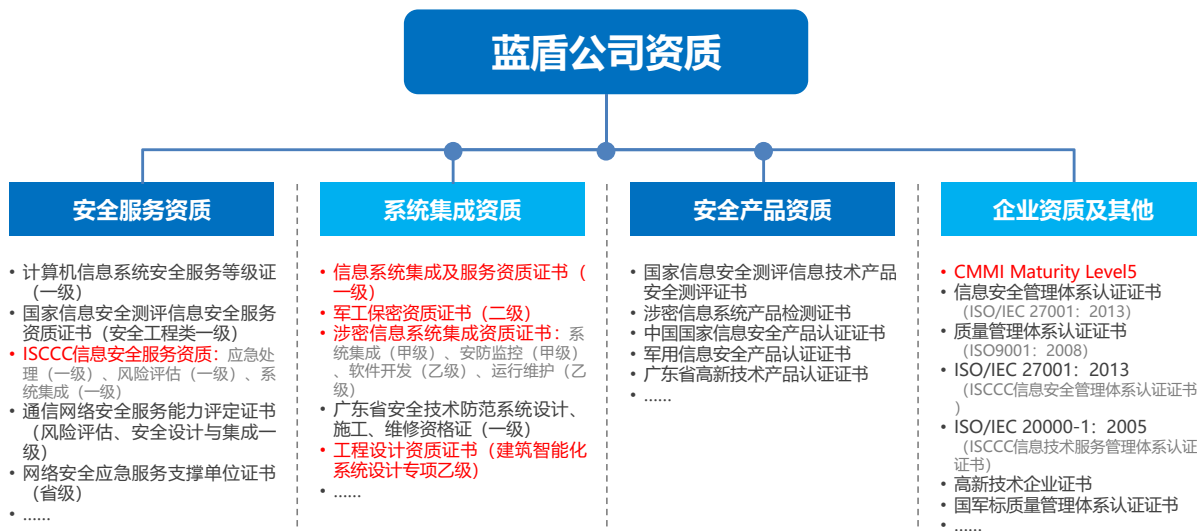
- 成立：1999年10月，注册资本12.49亿余元，民营企业，员工2798人
- 2012年3月于深交所上市(代码300297)，市值150亿元
- 国家四部委认定的：连续八年国家规划布局内重点软件企业
- 科技部认定：高新技术企业、国家重点火炬企业
- 国家及地方重大活动信息安全保障者：为第29届北京奥运会、第16届广州亚运会、“九三”抗战纪念阅兵、G20峰会、中共十九大提供信息安全产品和应急安全保障服务
- 2016年被评为“广州高科技高成长20强”企业
- 广东省经信委认定：广东省战略性新兴产业骨干企业
- 广州市政府认定：广州市总部经济企业
- 广东省博士后创新实践基地、广州市博士后创新实践基地



公司战略架构



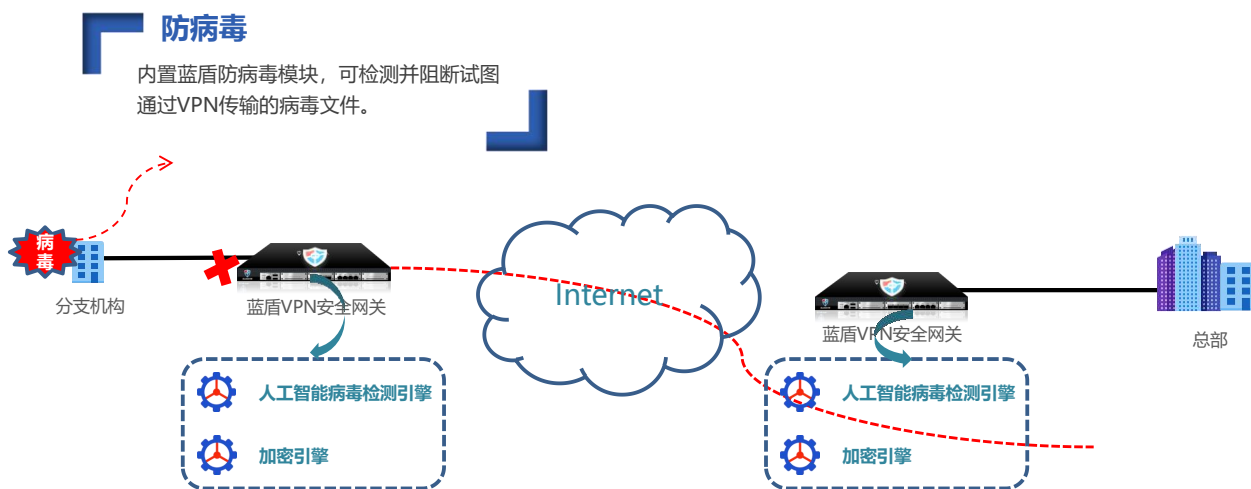
公司资质介绍



※ 部分主要资质证书



安全性. 防病毒

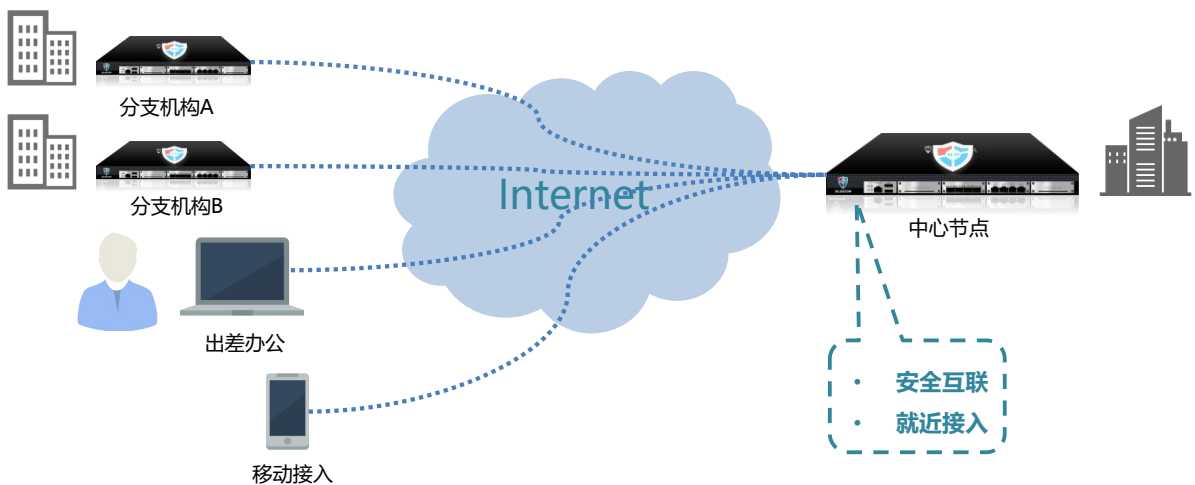


远程应用发布

将应用程序运行的实时图像通过加密隧道传输到客户端，再传回客户端的用户操作，如鼠标点击、键盘输入、手势操作等，实现对应用程序的操作和控制。轻松实现应用跨平台发布、访问。



产品部署·多分支/移动办公企业环境



跨终端协同办公趋势

移动设备已经成为办公、服务不可或缺的终端设备，而且在办公环境下，跨终端无缝切换，已经成为新型办公形态的主要诉求之一。

服务与业务云化趋势

与传统的服务、业务局限在本地环境不同，目前服务与业务云化进程正风起云涌，云化后如何保证安全，困扰广大政企。

强化信息安全保密趋势

近年来安全事件愈发频繁，《网络安全法》发布，等保2.0的条例落实，意味着安全已经得到了广泛关注。基于人为导致的安全事件，也愈发得到关注。

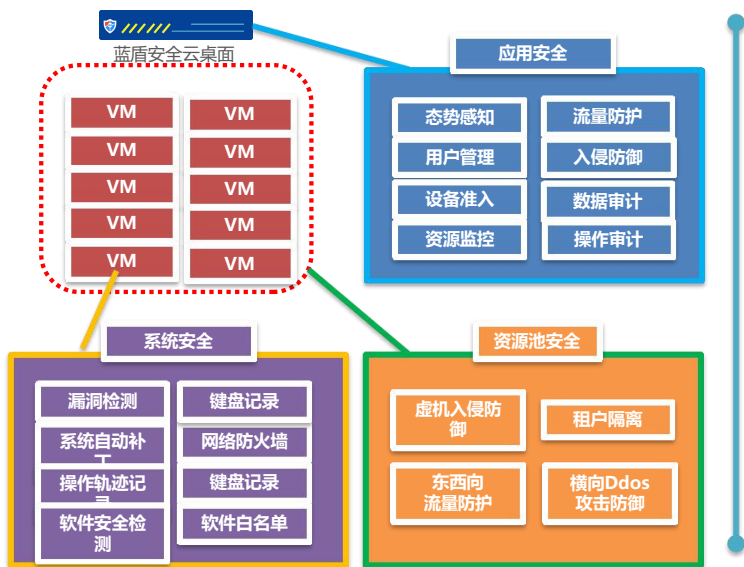
多终端协同管理趋势

多终端协同办公，同时也带来新的管理困难，无论是终端环境的安全与管控，抑或终端设备丢失衍生的安全管控问题，已经成为横亘在管理人员面前的难题。



云化、多终端协同、安全保密等诉求对业务系统、服务、办公等都提出了全新的管理要求。

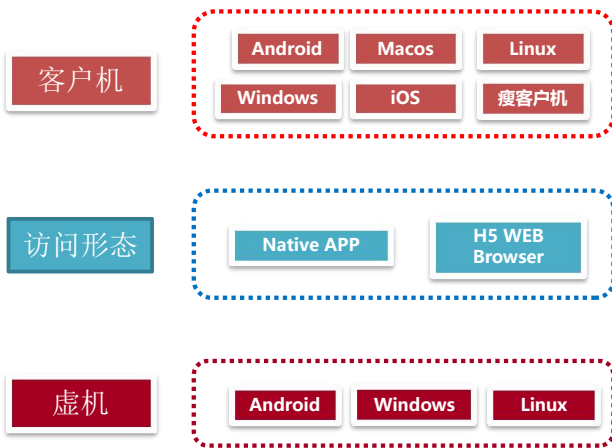
产品介绍 . 云桌面安全



虚拟机系统安全

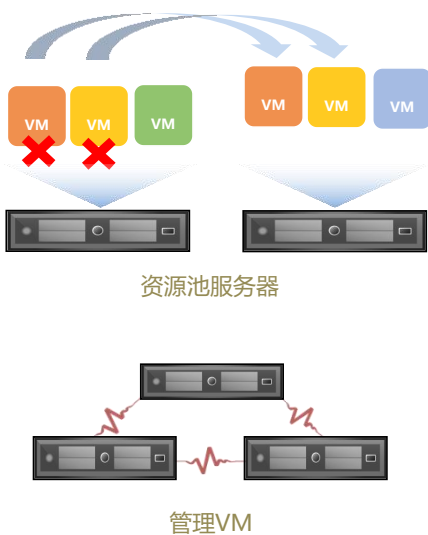
- 支持整合蓝盾主机涉密审计
- 支持整合蓝盾漏洞扫描
- 支持虚拟机本身操作行为轨迹捕获 (用于大数据分析建模)
- 支持键盘记录
- 网络流量支持防火墙过滤
- **满足等保三级**





全平台支撑

- 提供各种主流系统的客户端
- 支持使用浏览器的方式进行访问
- 虚拟机支持部署windows、linux、android, 实现移动系统的全平台访问



高可用

- 支持管理节点、服务器和VM故障恢复, 避免数据丢失

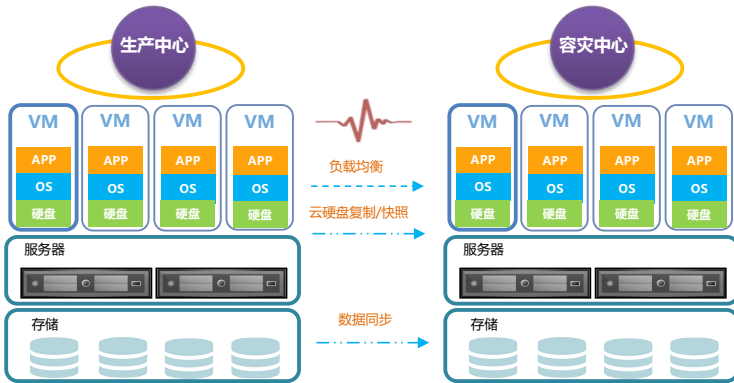
资源池

实时心跳检测, 当服务器或VM异常宕机时,
 >> 自动在选择可用服务器
 >> 在可用服务器上重启VM

管理节点

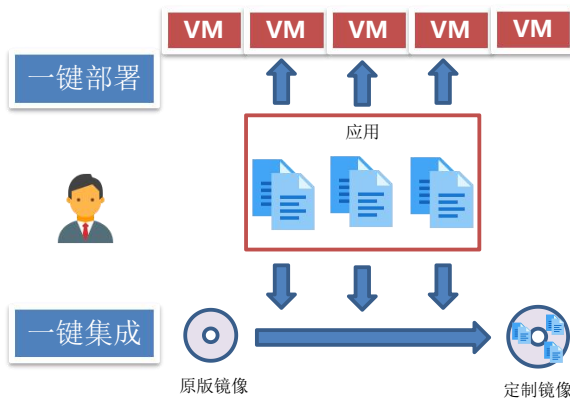
实时心跳检测, 当出现异常时,
 >> 自动选择可用节点
 >> 将节点的服务自动接管到可用节点





容灾备份

- 业务级备份
 - 虚拟机快照
 - 虚拟机迁移
 - 虚拟克隆
 - 负载均衡
- 数据级备份
 - 本地容灾
 - 同城双活容灾
 - 远程容灾



镜像快速定制

- 快速整合客户端应用到批量镜像
- 应用一键批量安装到所有虚拟机



产品介绍 . 整合BYOD设备管理

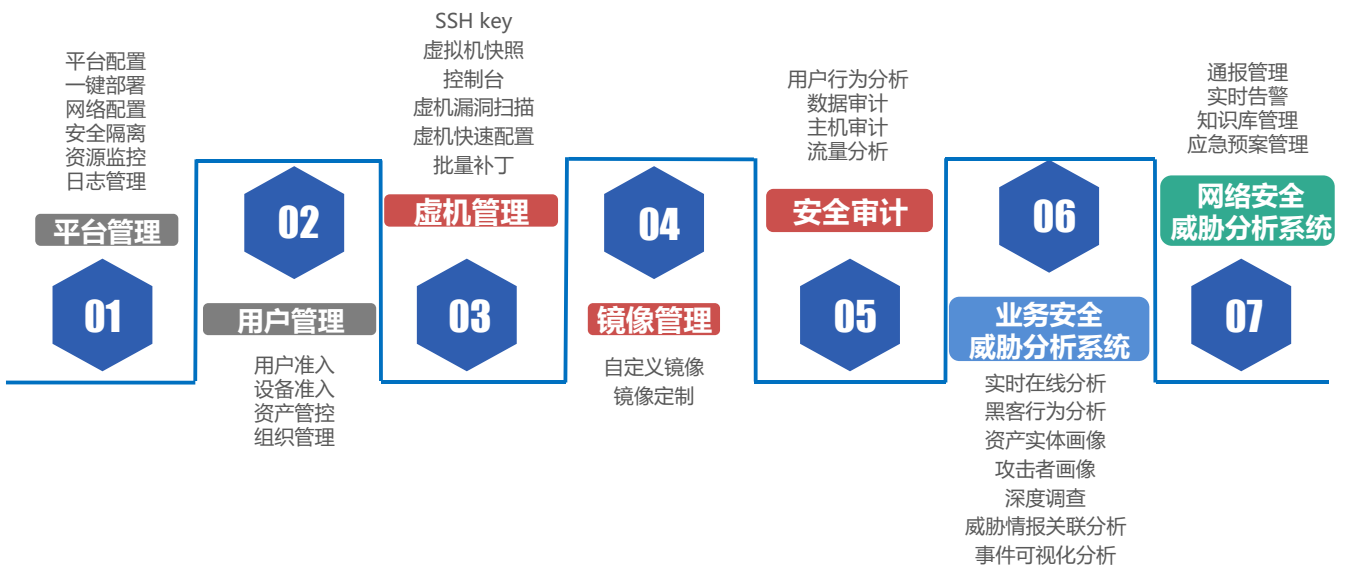
蓝盾股份 300297

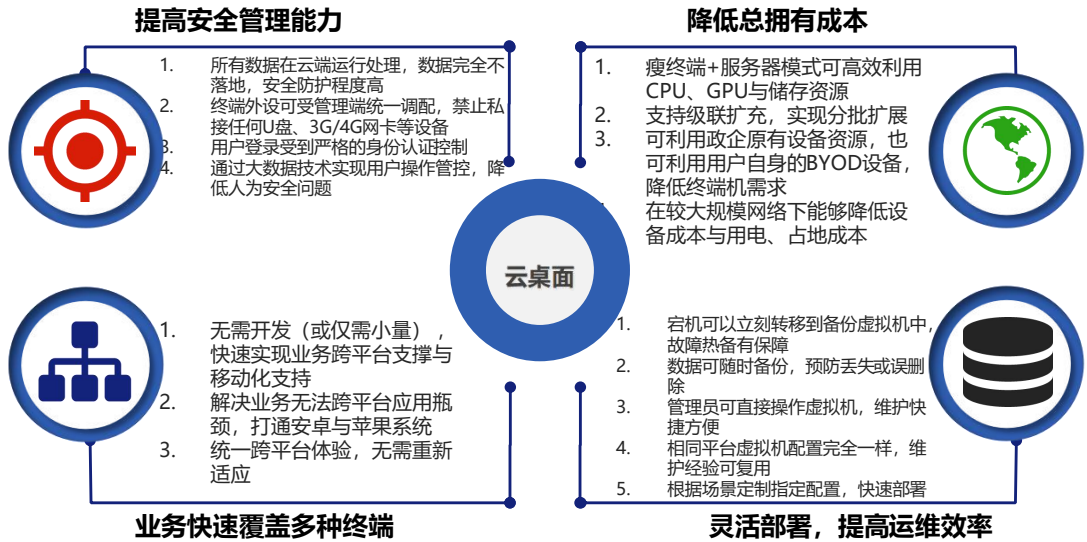
BYOD设备管理依赖EMM系统的设备管控功能，需要实现双系统整合。



产品介绍 . 基本功能介绍

蓝盾股份 300297





抗疫公益蓝盾在行动...

产品符合保密要求，拥有涉密专家团队

政、医、教、企 免费云桌面产品使用1年 捐赠行动于2月11日正式开始，至2020年5月之前，符合条件单位均可提交捐助申请。

捐助产品

“非接触式”云桌面管理系统 低带宽 桌面业务不中断，完美支持 Win7、WinXP系统。全外设支持——全场景覆盖

客服热线: 肖旭东 18688863910

