## AD域功能

员工办公终端管理

配合网络准入

员工电脑软件管理，不能玩游戏

补丁统一安装

密码安全性管理

ADManager Plus，AD域管理工具

## 零信任

从身份来讲，我们主要关注员工在入、转、调、离等各个办公周期环节中，员工权限如何能够去跟身份快速匹配。在这个点里，很多企业在人员权限变动时，更改相关策略，常常发生错配、漏配的问题，最后导致了数据资产的外泄。

另外，员工在使用过程中也需要相关的业务保障。比如分时段上很多业务系统后，每个系统都会有单独的用户名跟密码。那如何把账号进行统一管理，让员工快速触达，然后提供相关的安全保障策略？这块在身份安全管理的角度下，也是非常重要的一个问题。

第二是网络侧，目前权限的运维，包括给员工提供多种网络的接入，对于网络运维部门，存在很多的挑战。因为网络的安全、人员的快速接入以及效率，这些之间要如何平衡？

第三是终端。刚刚提到过字节跳动当年遇到的一些问题，包括现在很多企业也同样遇到了。比如说我们有个企业客户，每个电脑上有四个端，网络准入、防病毒、虚拟专用网络、数据防泄漏，各有一个客户端，这对企业IT部门，包括网络安全、运维部门的压力是非常大的。现在他们非常想把相关产品进行整合，当然也在考虑怎么去过渡。

另外是移动端相关方案的缺失。一些企业移动性管理（EMM）方案在初创型、发展型的企业里面，落地其实是比较重的。那如何能够做到多个端的安全期限能够去统一。比如说有iOS、安卓等移动办公设备需要具备一定的安全防护手段。那这个时候，我们就可以去使用比如飞连这样的轻量化产品，去适合企业当前阶段的移动安全建设。

## IAM发展阶段

SSO：

1、解决用户体验问题

2、无特定类别的用户

3、实现一点登录，全局进入。无访问控制能力

实现统一账号管理，可以解决离职-增删账号问题

4A（Account、Authentication、Authorization、Audit）

1、关注用户、认证、权限和审计

2、面向内部员工、具备人员生命周期管理

3、具备用户登录时的访问控制

4、关注权限统一管理

5、用户身份变化和访问信息记录后可以事后审计

实现基本安全管理及技术

IAM

1、面向员工、合作伙伴、顾客、设备、应用、特权账号、物理设备等，实现全生命周期管理

2、实现Service All In的单点，将B/S、C/S不同类别的应用，不同浏览器访问的统一纳管

3、实现应用级别的细粒度权限、AP操作、数据权限统一管理

4、访问控制从静态转向动态，具备实时风险发现机制和风险闭环管理能力

1. 实现身份能力的云服务化，增强用户隐私管理

更细粒度的安全管理

开源IAM：有很多。

<https://eiam.topiam.cn/docs/introduction/overview/>

## 重点部门

运维&DBA，系统权限特别大，纵向提权的最佳目标，有种开玩笑的说法，黑掉一个运维的电脑，把所有文本文件翻个遍，找不到一个密码才是见鬼了。应当尽量限制其他人群对他们的访问。

重要业务系统的管理员，这些同学负责对公司核心业务进行运营管理，对重要后台系统具有很高的权限，一旦他们电脑被入侵，后果会很严重。比如游戏公司充值系统的后台、广告公司的客户广告投放管理系统、招聘公司的后台简历管理系统、电商的订单物流管理系统，出点事都是大事。应当尽量限制其他人群对他们的访问，同时严格限制他们的外网访问权限。

高管、HR、财务，这些同学对办公系统的访问需求比较单一，主要网络访问需求在外网，通常不懂技术，安全防护意识也最弱，也最得罪不起。他们的办公电脑集中大量公司重要数据，一旦被入侵就直接产生损失了。这部分同学可以严格限制跟办公网其他区域以及对内部系统的访问。

## 终端安全

### 终端安全加固

终端安全加固的目的是提高安全基线，减小攻击面，事半功倍的方法是让PC终端统一加入window域，通过域控策略统一管理终端的安全策略，介绍域策略的文章很多，这里只提下几个比较重要的点：

开启屏保以及锁屏时间

域账户密码复杂度，密码更换时间

禁用guest账户

开启主机防火墙

禁止administror账户远程登录（员工自己域账户是本地管理员，可以正常登录，很多公司喜欢用ghost预装电脑，administror账户的密码绝对是个大坑）

禁止域管理员远程登录（一定要把域控和一般PC放在不同组策略下，不然这个策略害死人）

删除IPC$ C$ D$ admin$（木马经常利用）

开启审计策略，记录登录、账户相关事件

调整事件日志的大小及覆盖策略

关机清理虚拟内存页面文件

### 终端防病毒

终端防病毒肩负着具备抵御常见Nday病毒木马的能力，提高攻击成本的重任，不过传统解决方案基本就是纯粹的黑名单和基于病毒特征，似乎这一领域也是红海中的红海。可喜的是最近两年终端安全又被各大安全厂商重视起来，因为越来越多的有针对性的攻击行为被揭露，跳板都是办公终端，大家对这块越来越重视；另外新的检测技术以及解决思路落地实现，安全厂商提出了EDR的概念，即终端检测与响应。基本思路是默认攻击者始终会渗漏公司网络，让安全人员利用IoC和终端行为来快速检测任何入侵，减小攻击者造成的损害。

### 终端管理

终端管理主要解决两个安全问题：

系统、应用软件版本的管理

系统、应用软件漏洞的自动化修复

微软的WSUS以及SCCM虽然只能搞定微软系软件以及flash的问题，但是已经可以解决大部分问题了，针对类似java、chrome这类常用第三方软件的升级，就需要专业的终端管理解决方案了。

### 准入系统

准入系统可以基于员工身份做到灵活的网络权限限制，保障主机安全基线的强制执行。

## 安全区域划分

假定所有服务器都部署在IDC或者公有云上。员工和用户访问所有服务都需要通过外网。安全域内的主机互相信任，跨安全区域互相不信任，严格限制访问，我们的基本假设是，每个区域都可能被入侵。区域划分就是为了这个时候提供黑客进一步入侵的成本，为后面的入侵检测和应急响应争取时间。

### 内部服务区域

这个区域包含大量运营、人事、研发相关的重要企业数据，安全等级甚至比业务区域还要高，但是往往容易被甲方忽略，成为入侵的重灾区。原则上这个区域也只允许来自办公区域的访问。

### 测试开发区域

与内部服务器区域类似，这个区域大量开发中的产品，安全基线最差，最容易被入侵，原则上这个区域也只允许来自办公区域的访问。

业务区域、内部服务区域、测试开发区域难免业务上有需要，部分服务需要互通，这个以白名单形式开放。

各个区域针对SSH和远程桌面的访问仅信任堡垒机IP。

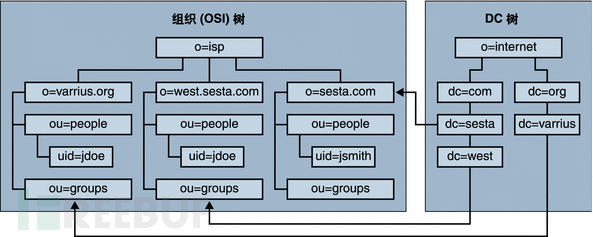
混合云模式其实也类似就不再赘述。

## 权限模型

权限模型是个非常基础但是非常重要的模型。我们先来看下公司的组织模型：

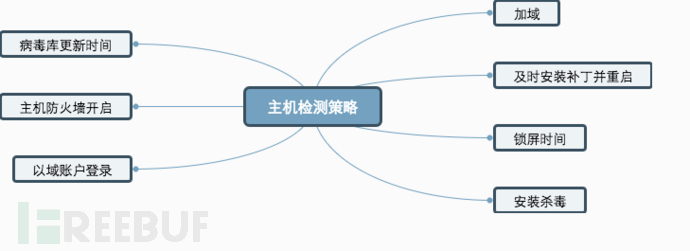
[](https://image.3001.net/images/20170207/148644506287.png)

员工的网络权限往往和他的工作内容相关，对应的就是部门属性，所以最简化的模型就是直接从组织模型转化，用户对应到不同的角色，角色对应一个或者多个部门。角色的定义就是具有相同网络访问权限的员工的集合。对应的微软域控也是这种层次结构：uid对应用户名，ou对应部门。

[](https://image.3001.net/images/20170207/14864450764875.png)

## 主机检查策略

主机检测策略需要结合公司实际情况，我简单描述下比较通用的几个：

[](https://image.3001.net/images/20170207/14864450981709.png)

强烈建议PC都加入域，这样主机检查可以非常简化，大量的安全加固策略可以通过域的组策略强制下发给终端。

我们采用了一个折衷的方案，就是把用户名和硬件做了绑定，指定的用户名只能在指定的硬件上使用，其中核心的是硬件的识别，具体思路就是获取若干硬件信息，形成一个硬件向量，任意一个影响向量变化都判定硬件改变，需要后台重新绑定，否则即使密码正确也会判定认证失败，这个是提高硬件伪造的成本，其中任一变量其实都是可以伪造的，大家不要太纠结。下面列举各个厂商经常使用的一些硬件信息，具体实现时建议大家增加一些其他变量：

### CPU序列号

目前存在的CPU几乎都支持CPUID指令。这个指令不仅可以获取CPU生产厂商等基本信息，还可以获取其他有关CPU的硬件信息，包括CPU序列号。

### MAC

网卡MAC是具有国际标准的地址编号，能够确保世界上的每一块网卡具有唯一的序列号。

### 硬盘序列号

除了一些特殊硬盘外，大部分硬盘都有自己唯一的硬件序列号，而且不可修改。

### 硬盘分区序列号

首先要说明，硬盘分区序列号和硬盘物理序列号是不同的东西。硬盘物理序列号是硬盘厂商指定的，而分区序列号是分区软件指定的。每次重新分区的时候，这个序列号会变动。对于GPT硬盘分区来说，每一个分区都使用全球唯一的UUID来标识，具有良好的唯一性和可用性。另外对于RAID设备来说，分区序列号同样存在并可用。

### 主板序列号

## 其他

**这里列举一般办公主机的需求项：**

* 病毒防御（本地查杀选用国外厂商的产品，能接受云查杀选用国内厂商的产品，没有重要机密的内容的）；
* 入侵检测防御（说白了就是HIDS或者HIPS产品，一般国内都是和杀毒软件集成的）；
* 漏洞防护（打补丁，一般国内也是集成在杀软里面的）；
* 软件管控（软件中心功能，一般对win平台比较常见）；
* 日志记录；
* 管控场景（禁止起SSID等、数据防泄漏DLP）

**这里用来解释一下日志需求：**

* 日志记录一般可以做两件事情被攻击的响应追查和主动攻击的追踪溯源；
* 日志可以记录邮件、进程、服务、命令等等；

### 办公主机安装和在线率提高方案

* 全员检查
* 内网做准入
* 虚拟桌面后台强制安装

### 工作三部曲

* 推全员安装
* 做准入推全员再现
* 推漏洞补丁自动安装并接受实时日志

### 重点管控对象

* 人力资源部门
* 法务财务部门
* 高管要职群体
* 助理秘书群体
* 投资融资部门
* 其他关键人员

### 重点效果预期

* 自主防御能力提升化
* 漏洞补丁修复自动化
* 敏感数据传存安全化
* 病毒爆发场景预知化
* 攻击失陷发现简单化