

账户清除

**用例分析**

Account Deleting

**Use Case**



据不完全统计，在科技相关的领域，员工平均每三年换一次工作，或在本企业内部，或跳槽。不论是企业还是其它组织机构，人来人往已是家常便饭。在信息化，数字化的今天，几乎没有人可以离开电脑和网络可以工作的。在日常工作中，根据职位和分工的不同，每个人都会使用几种甚至十几种应用，这些应用或运行在企业内网，或在云端。

位于美国加州的某娱乐集团（Resort）有1600名员工，在近三十台的服务器上运行了近一百个应用软件，其中一部分运行微软的协作软件，为不同部门提供内部资料分享。因为系统已经运行多年，各个部门人员流动很大，包括辞职和新增员工，IT部门对每台服务器到底还有哪些员工在使用，该不该使用等情况一无所知。当某个员工离职时，因为IT部门其使用的应用和软件没有一个准确的了解，所以无从下手彻底清理其账户。

* 在分享的文档中，许多都涉及到公司的商业机密和客户信息，尤其是VIP客户。公司对这些应用唯一的控制方法就是账号管理。岗位调动的员工或离职员工仍然拥有原服务器应用的账号，无疑是企业安全的巨大风险。然而，当一个员工离开时，要从30个服务器上，近百个应用中逐个清除其账号是非常繁重的工作。因为IT部门并不清楚离职员工曾经用过哪些应用，唯一的方法就是手动地从近百个应用中一个一个地查找去删除。
* 客户原计划使用终端安全软件(Varonis)，并已经进行了POC，但IT部门认为终端软件维护工作量大，对每个应用的总体使用情况仍然缺乏完整的可视性。不能够完全解决问题。
* 客户在其四个三层交换机侧各部署一个OnFire数据采集探针，并将探针上采集到的日志送到安装在其私有云上的分析展现模块处理。
* OnFire是一个网络虚拟世界的监控摄像头，实时精准地将所有网络活动与人，设备，数据，和应用相关联并记录，提供了一个前所未有的网络活动全息图。OnFire基于这种完整的全息图，对每个网络使用者，对连接到网络上的每一台设备，对用户所使用的每一个应用，甚至对每个敏感文件都进行准确画像，从而对每个员工所使用的账号一清二楚，对每个服务器／应用的使用情况也一目了然，如下图所示，IT部门可以对每个服务器的使用者一一核查，清除安全隐患。



