Use Case

Dorman Account Cleanup

Case Scenario

According to studies, American workers switch their jobs every three years. The job changes could be due to internal transfers or leaving to work for different companies. Most companies are utilizing technology to improve the speed of conducting their business. Those technologies rely on computer networks and business applications. Depending the industry and sector, it's not uncommon for companies to have hundreds of applications in their environment. When there is an employee departure, properly purging/securing those accounts is essential but cumbersome. If the account cleanup is not done properly, those "zombie" user accounts can become easy targets for hackers to use as launching pads to other vital systems.

Financial company A has 5000 employees with about 200 applications running on 50+ servers. Although LDAP has been deployed to handle centralized authentications, only about 30 large

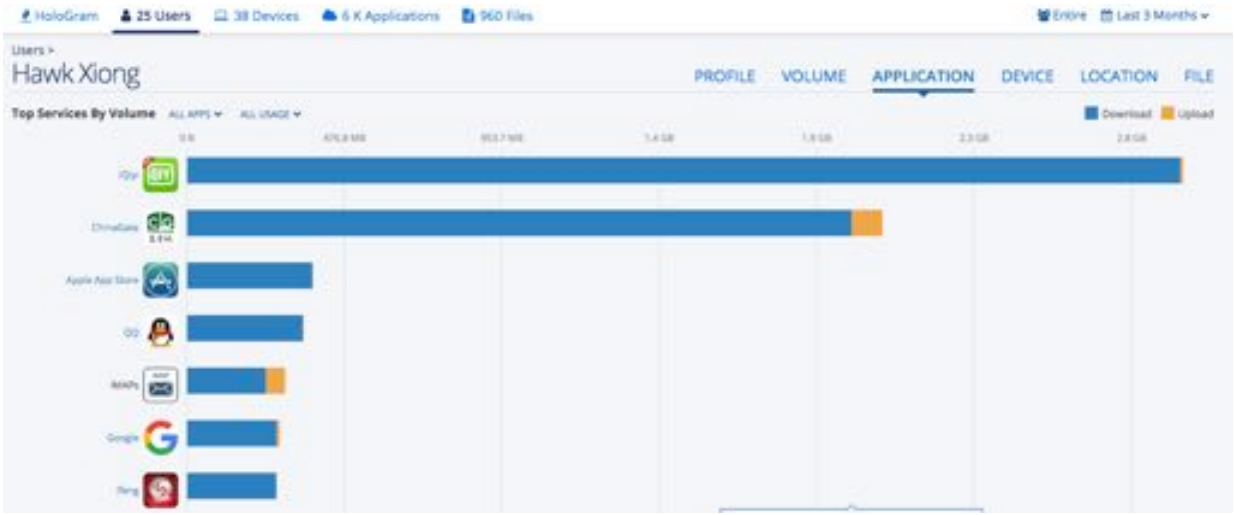
scale applications are integrated with LDAP, leaving 170 incompatible applications relying manual account management. When employees depart, their user accounts in those incompatible application systems would not be deleted automatically. The same applies when employees change their jobs via internal transfers. Their user accounts remain dormant in some application systems even though the users longer need to access them due to role changes.

Challenge

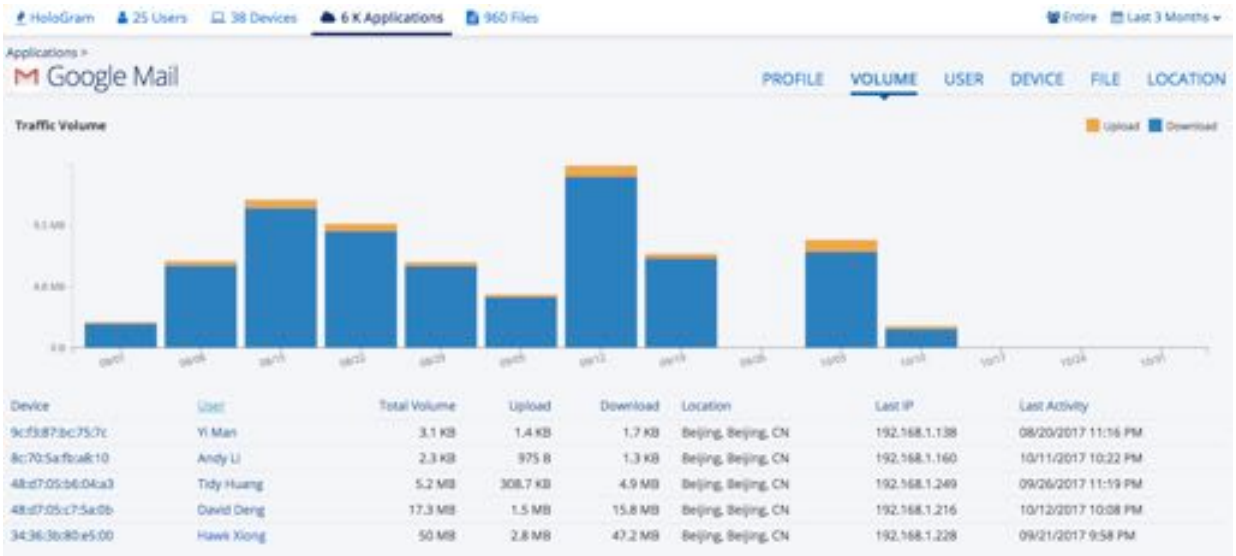
- "Zombie" user accounts pose significant risk to organizations when employees depart. Deleting accounts from hundreds of application systems are manual and labor-intensive tasks. Since IT does not know exactly which user uses which application, they could be resorted to manual examination of each system to delete accounts. Even if companies have a low 10% turnover rate, it could still result in heavy workload for IT team. To preserve resources, it's not uncommon for IT department to perform semi-annual system/account clean ups.

Solution

- ✓ OnFire is a real time security camera for the Cyber world that can record and link data, application, devices to actual users, proving unprecedented full mesh hologram. With the full mesh linkage and correlation technology, OnFire link and correlate each application, each piece of sensitive data, each device to an actual user. With this precise correlation, OnFire can provide accurate anomaly alerts and minimalize false alerts.
- ✓ After company A installed OnFire, it starts the linkage and correlation process immediately. After 2~3 months, OnFire have learned and built full mesh data holograms for users and applications. (internal and cloud based) When an employee departs, all is needed is to search the user account name in OnFire, it will show a complete list of all the application that user has accessed. All IT staffs must do is to delete the accounts in the list rather than blindly searching through hundreds of applications.



✓ For internal job transfers, access to applications in his/her previous department could no longer be needed. (Like when an employee switches from accounting to marketing, access to financial report should no longer be needed) As the employee is still with the company, IT team does not always know whether he/she would still need to access applications for his/her previous role. Should the employee change roles in the company multiple times, his/her application accounts could easily reside in many application systems. An application holding vital records with access limited to a dozen can turn out to be accessible to ten folds more users due to legacy "zombie" accounts that never been properly disposed of. Since that application contain sensitive and vital data, "zombie" accounts pose significant risks. OnFire links and correlates each application to users and devices. As shown in diagram below, in the past three months only four users have accessed this application. Other user accounts are likely "zombie" accounts. IT can delete them to mitigate the risk.



✓ Besides the features above, OnFire can provide additional functionalities below with data from user application activities and data volume.

1. User might have left the company: An employee typically accesses 50 or more applications with data volume in the multi gigabytes ranges. In the past three months there were no application accessed by the user and zero application data volume. Based on these data, that user could have left the company or transfer to a different location. IT team can follow up on the user account.
2. Users no longer needed access to those applications: If an employee frequently switch departments, he/she could have accumulated hundreds of accounts. OnFire has made detailed record of all the applications the user has accessed. Looking at user data for past three months, IT found that user only access about 20 applications. IT team can disable and later deleted the rest of the accounts the user no longer need access to.