安全的SmartMachine

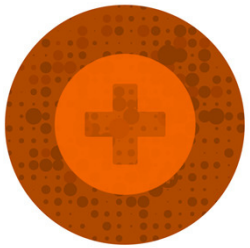
在虚拟层上，每个虚拟机上的内存、存储空间以及网络建构都是独立的。根访问为您提供了对端口和进程的完全控制，但不是内核级别的底层操作系统访问。

安全的虚拟化技术

Triple-A（认证，访问控制及审计）的安全机制。

安全的存储

有经过网络存储器加密的独立本地存储空间。



SmartMachines

Joyent的SmartOS

资源池

事件连贯性

每个SmartMachine都有本地存储空间和持久的公共和私有IP地址，降低了重新启动时的风险和复杂性。

安全的操作系统

高稳定高安全的SmartOS。集成的虚拟化可以减少受攻击的机会，集中控制降低了管理风险。

安全的SmartDataCenter

应用程序编程接口和图形用户界面访问需要经过严格的身份验证和控制。

安全的物理环境

采用生物度量接入控制和锁笼来保证数据中心设施安全。

图形用户界面（GUI）

应用程序接口（API）

SmartDataCenter

网络交换机

Joyent代理

Joyent代理

负载均衡

安全的网络

数据访问可以被隔离并被限制到专用的虚拟局域网。在虚拟局域网外，所有私有IP地址都会对其他云用户隐藏，且没有授权的数据访问会在交换机处被拦截。

防火墙

内置的高可用性负载平衡，以满足带动态数据缓存在扩展时的要求。