

SmartMachine Security

Isolated Memory, Storage, and Network enforced at the virtualization level. Root access gives you full control over ports and processes, but not kernel level access to underlying OS.

Virtualization Level Security

Security is enforced by Joyent at the Global Zone level with Triple-A (Authentication, Access Control and Audit) controls.

Storage Security

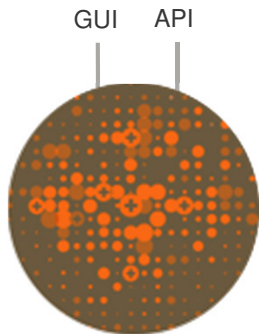
Isolated, local storage is available, as is encrypted NAS.

SmartDataCenter Security

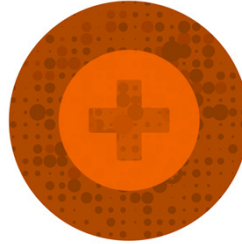
API and GUI access are authenticated and strictly controlled.

Physical Security

Secure data center facility with bio-metric access control and locked cages.



SmartDataCenter



SmartMachines

Joyent SmartOS

Resource Pool

Network Switch

Joyent Agent

Joyent Agent

Load Balancing

Instances Persistence

Each SmartMachine is a persistent with local storage and static public and private IP addresses. This smoothes rebooting, reduces complexity and reduces risk.

OS Level Security

Highly stable and secure SmartOS. Integrated virtualization reduces attack surface, centralized management reduces administrative risk

Network Security

Traffic can be isolated and restricted to dedicated VLANs. Outside the VLAN, all private IP addresses are hidden from other cloud users and traffic blocked at the switch.

Firewall

Built into HA load balancers, which also help meet scaling requirements with caching of dynamic content.