Workload Security for Financial Services

Security Drivers for Financial Services

- Requirement to build in security and compliance to private cloud deployments
- Secure credit card processing and publicly facing apps on private cloud infrastructure
- Compliance risk prevents or slows public cloud deployment
- Need for robust key management solutions
- Provision known-secure workloads quickly and efficiently
- Desire to encrypt all types of workload including linux bare-metal
- Requirement to encrypt workloads in-flight and at-rest
- Protection against insider threats and admin errors
- Eliminate risk of "virtual admin" caused by excessive privileges etc

How do Carbon Cloud Help?

Initial Proof of Concept

Understand risk profile

Build strategy

Manage change program

Implement and Integrate

CloudControl

- Policy based governance and control for workloads
- Eliminate privileged account misuse
- Avoid Admin mistakes
- Remove infrastructure air-gaps
- Automated support for audit and compliance

DataControl

- Automated encryption for multi-cloud environments
- Retained ownership of keys whilst operating in the cloud
- Protects workloads in-flight
- Near-zero overhead
- Avoids downtime in initial encryption and re-keying

BoundaryControl

- Meet compliance by controlling where workloads can run
- Ensure the virtualisation host can be trusted
- Logically restrict workloads to trusted hosts
- Geo-fencing
- Data decrypts only on specific hosts (data sovereignty)

CloudAdvisor

- Discover where sensitive data is located
- Monitor who is accessing sensitive data
- Implement policy and controls to protect data
- Detailed audit over sensitive data to meet regulatory compliance requirements
- Implement policy on discovered workloads