The significant increase in attacks on corporate data makes encrypting sensitive information an absolute must. Marvell LiquidSecurity provides a next-generation solution encompassing all encryption needs in a single, easy-to-use solution and with minimal total cost of ownership (TCO). Marvell LiquidSecurity was designed to serve the needs of modern, distributed, agile, and hybrid IT environments. Delivered as a service in a wide variety of deployment scenarios, Marvell LiquidSecurity can easily adapt to any requirement.

THE PROBLEM

As organizations migrate to the cloud, encrypting and managing data encryption becomes a major stumbling block on the migration path.

- **Unified, centrally managed data encryption platform:** Migration to the cloud means there are more IT environment to manage and control. There will also be additional data encryption solutions and dashboards to manage. Result: More complexity, high TCO, less control, and less security.

- **Customer-controlled encryption keys:** From a compliance and data governance standpoint, customers must maintain complete control of the encryption keys at all times. However, managing encryption in the cloud means using the cloud native Hardware Security Module (HSM) and/or Key Management Service (KMS); i.e., customer control of the encryption keys either doesn’t exist or is flawed. Bring your own key (BYOK) doesn’t resolve the security, control, or compliance problems; it merely adds another layer of unnecessary key management to the already overly complicated encryption management.

Given that the hybrid cloud will be a reality for most enterprises, a solution that provides a unified encryption platform for all environments, and assures complete customer control of the encryption keys at all times is essential to any migration plan.

THE SOLUTION

Marvell LiquidSecurity distributed cloud HSM provides a high-performance, scalable HSM platform designed to resolve these particular problems with ease and low TCO:

- LiquidSecurity HSM powers data encryption for all leading cloud providers.
- Its unique capabilities include unlimited scalability and clustering, and the ability to create an HSM cluster across cloud and on-premises environments.
- The clusters are always managed from the on-premises deployments, assuring complete customer control at all times.
- Load balancing, high-availability, and fault-tolerance are built in. There's no need for external proxies or load balancers.
- Policies can be easily set and automated to ensure the HSM nodes in the cloud only maintain copies of keys when needed. A key is deleted when it is no longer needed.
- Elastic FIPS (Federal Information Processing Standards) boundary: LiquidSecurity maintains a FIPS boundary within the cluster. All HSM nodes participating in the cluster, regardless of where they are physically deployed, are always within the FIPS boundary.
- LiquidSecurity features strict role-based access control (RBAC) and segregation of users and roles, allowing customers to be confident with the security and privacy of their data in any deployment scenario, while providing superb general data protection regulation (GDPR) functionality.

Marvell LiquidSecurity achieves the two key requirements for migration to the cloud: a unified data encryption platform for all environments and complete customer control of the encryption keys. It’s the only solution available capable of resolving these problems.

### LiquidSecurity Network HSM Key Features

| Performance | • 35K 2K RSA Sign Ops/sec  
• 300K Symmetric Ops/sec (AES-GCM 1K byte)  
• 100K Asymmetric (any key size) /Symmetric key store |
|-------------|--------------------------------------------------|
| Multi-tenancy | • FIPS 140-2 Level 3 partitions  
• Individual appliance can be partitioned into 1 to 32 partitions at run time  
• Partition defined based on key store, symmetric/asymmetric performance, and maximum concurrent sessions  
• User/ Clients Per Partition  
• Support for up to 1000 users per partition  
• Each user can run multiple applications  
• Multiple thousands of applications can connect concurrently |
| Secure Key Management | • Secure key migration to/from public/on-prem networks  
• Attestation of key attributes for key generation and import/export APIs |
| Interfaces and Crypto Support | • Support for lights-out data center  
• Cluster creation and management utility for load balancing and high availability  
• Utility for HSM partition and user configuration  
• WebGUI, REST APIs, and C APIs  
• Field firmware upgrade/downgrade using remote management tool |
| **LiquidSecurity Client Library** | • Available in source code under BSD license  
• E2E (TLS-based) connectivity from the LiquidSecurity client to FIPS boundary |
| **Supported Crypto Stacks** | • PKCS11, JCE-KSP, CNG-KSP, and OpenSSL  
• Partner-supported KMIP offering |
| **Host Operating Systems** | • RHEL7.x, CentOS 7.x, Ubuntu  
• Windows Server (2012 & 2016)  
• Windows 10 (desktop) |
| **Crypto Algorithms** | • RSA Sign/Verify – Support for PKCS1, PSS (2K, 3K, 4K key sizes)  
• RSA enc/dec – PKCS1, OAEP (2K, 3K, 4K key sizes)  
• DSA Sign/Verify  
• ECDH/ECDSA-p-curves, b-curves, k-curves, Bitcoin curve secp256k1, Curve25519, and Brainpool curves  
• 3DES/AES and SHA (1, 2), MD5 - HMAC, CMAC  
• Key Derivation – SP800-108 counter mode/HMAC-KDF/CMAC-KDF |
| **High Availability and Clustering** | **Marvell Trust Zone** Certificate-based authentication between various partitions and clients to create a cluster  
**Elastic/Scalable Cluster** Scale the cluster size or capacity at run time, including on same appliance or different appliance over the network  
**Configurable HA-LB** • Active-Passive (no load balancing), active-active (round robin), active-active (weighted round robin)  
• Architected for various network models |
| **Security and Access Control** | **Role-Based Access** • Appliance Administrator – No access to key material on partitions, role limited to creating partitions and health checks  
• Partition Administrator – Cluster management, user management role  
• Partition User – Key management operations and crypto operations |
| **Audit Logging** | • Granular logging levels for management and crypto commands  
• Easy integration with tools like Syslog and Splunk  
• SNMP – Health checks and monitoring |
| **Authentication** | • Support for single- and two-factor authentication  
• LDAP support, single sign-on integration with AD, SAML  
• Quorum approval policy for both key management and usage services |
| **Secure Backup/Restore and Cloning** | • Policy-based backup/restore options to meet different security requirements  
• Ephemeral handshake-based cloning to ensure the key rotation for the masking key |
| **Physical Characteristics** | **Hardware Specifications** • Standard 1U 19in. rack mount chassis  
• Dimensions (inch): 16.92" x 1.71" x 27.91"  
• Weight: 26.5lbs  
• Input Voltage: 100 – 240V, 50 – 60Hz  
• Operating Temperature: 0 to 40°C  
• Regulatory Certifications: Safety, cTUVus UL, EMC, FCC/ICES, Class A |