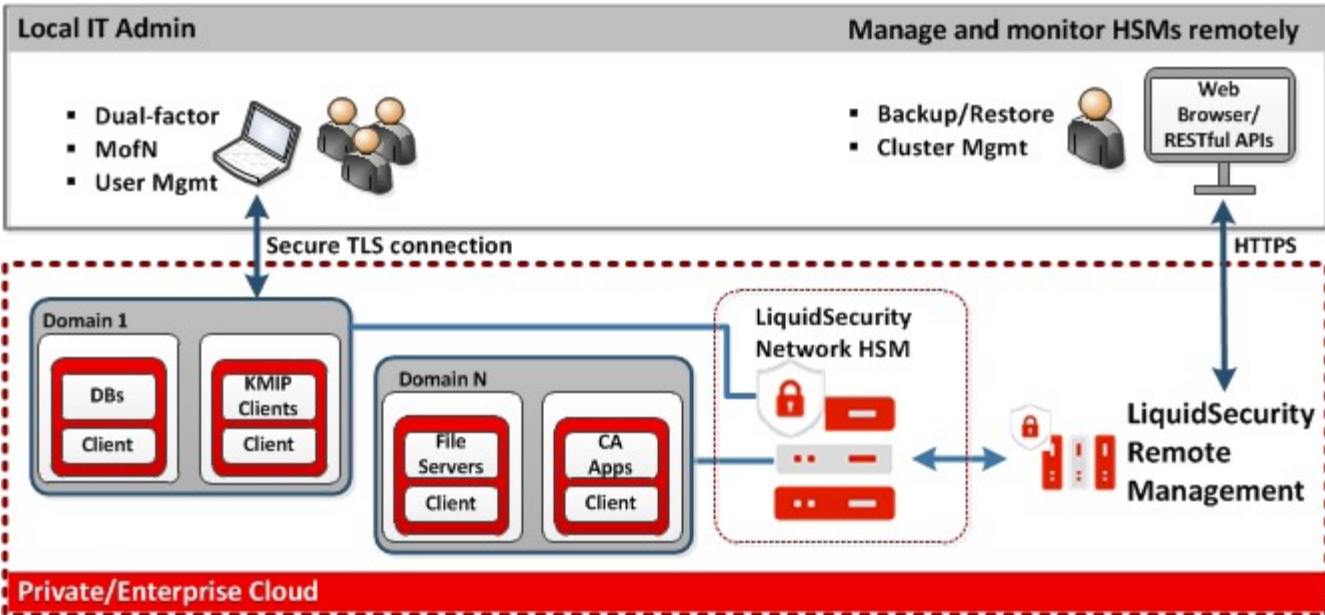


MARVELL LiquidSecurity Network HSM

Product Brief

LiquidSecurity Client Features	
<p>HSM Management Tools</p> <ul style="list-style-type: none"> • 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 <p>LiquidSecurity Client Library – Available in source code under BSD license</p> <p>Supported Crypto Stacks</p> <ul style="list-style-type: none"> • PKCS11, JCE-KSP, CNG-KSP, and OpenSSL • Partner-supported KMIP offering <p>Secure Channel – E2E (TLS-based) connectivity from the LiquidSecurity client to FIPS boundary</p>	<p>Sample Operating Systems</p> <ul style="list-style-type: none"> • RHEL7.x, CentOS 7.x, Ubuntu • Windows Server (2012 & 2016) • Windows 10 (desktop) <p>Algorithms</p> <ul style="list-style-type: none"> • 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 • 3DES/AES and SHA (1, 2), MD5 - HMAC • Key Derivation: SP800-108 Counter Mode/HMAC-KDF
LiquidSecurity HSM Features	
<p>Industry-Leading Performance</p> <ul style="list-style-type: none"> • 35K 2K RSA Sign Ops/sec • 160K Symmetric Ops/sec • 100K Asymmetric (any key size) / Symmetric key store <p>Dynamic Partition Support</p> <ul style="list-style-type: none"> • 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 <p>Marvell Trust Zone</p> <ul style="list-style-type: none"> • Certificate-based authentication between various partitions and clients to create a cluster <p>Elastic/Scalable Cluster</p> <ul style="list-style-type: none"> • Resize partition at run time including on same appliance or different appliance over the network <p>High Availability/Load Balancing Cluster</p> <ul style="list-style-type: none"> • Active-Passive (no load balancing), active-active (round robin), active-active (Weighted Round Robin) • Architected for various network models 	<p>Role-Based Access</p> <ul style="list-style-type: none"> • 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 • Secure Key Migration to/from public/private clouds <p>User/Clients Per Partition</p> <ul style="list-style-type: none"> • Support for up to 1000 users per partition • Each user can run multiple applications • Multiple thousands of applications can connect concurrently <p>Key Attestation</p> <ul style="list-style-type: none"> • Attestation of key attributes for key generation and import/export APIs <p>Audit Logging</p> <p>Support for Single- and Two-factor Authentication</p> <p>Functionality for management and key operations</p> <p>Secure Backup/Restore</p> <ul style="list-style-type: none"> • Policy-based options to meet different security requirements <p>Cloning</p> <ul style="list-style-type: none"> • Ephemeral handshake-based cloning to ensure the key rotation for the masking key

LiquidSecurity HSM Features	
Field Firmware Upgrade/Downgrade SNMP - Health checks and monitoring Provisions against Side-channel Attacks On-board Real Time Clock (RTC)	Physical Characteristics <ul style="list-style-type: none"> • 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



LiquidSecurity Network HSM Family

Device	Isolated Partitions	Key Store Size	Performance	
			2048b Asym Ops/sec	Symmetric Ops/sec
CNL3560-APL-Sec-G	32	100K	35K (2048b)	160K
CNL3510-APL-Sec-G	24	10K	13K (2048b)	65K



ABOUT MARVELL: Marvell first revolutionized the digital storage industry by moving information at speeds never thought possible. Today, that same breakthrough innovation remains at the heart of the company's storage, networking and connectivity solutions. With leading intellectual property and deep system-level knowledge, Marvell semiconductor solutions continue to transform the enterprise, cloud, automotive, industrial, and consumer markets. For more information, visit www.marvell.com.