RACKTOP

Implementing Multi-Level and Multi-Category Security in Classified Environments

BrickStor's Attribute-Based Access Controls Deliver Unmatched Simplicity, Security, and Performance

Classified environments face increasing challenges from cyberattacks and unauthorized breaches. Multi-level security (MLS) and Multi-category security (MCS) both serve as essential frameworks to ensure information integrity and confidentiality across highly sensitive operations.

Federal policies require organizations to use separate environments for different classifications and projects, or to adopt MLS and MCS-approved solutions. MLS and MCS solutions reduce cost while improving data security, operational efficiency, and mission outcomes. With BrickStor, organizations now have a cost-effective solution to easily implement MLS and MCS to address evolving security demands in government and contractor environments.

Security Framework	Definition	Example Use Case
Multi-Level Security	Classifies data hierarchically, from Unclassified to Top Secret, ensuring the strictest access control.	A Top Secret user accesses all classifications, while Unclassified users are restricted to only Unclassified data.
Multi-Category Security	Segments data by compartments or categories within a classification level. There is no concept of moving data up or down in levels of sensitivity.	Intelligence reports separated by region or project, accessible only to authorized users.

Classified Environment Scenarios with MLS and MCS

Intelligence Agencies - Intelligence data often needs to be segmented by mission or department to ensure compliance with strict security protocols. MLS and MCS enable agencies to achieve this, reducing the risk of unauthorized access while maintaining operational efficiency.

Special Access Programs - Special Access Programs - Highly sensitive information needs to be accessed and managed by a few individuals; this demands a solution that is easy to use, easy to manage, and scalable.

Defense Industrial Base - Easily comply with NIST 800-171 standards to protect Controlled Unclassified Information (CUI) within a typical enterprise IT environment. Enable users to properly label CUI data with minimal changes to their workflow and enable secure team collaboration and information sharing.

Data-Centric Zero Trust Security with BrickStor

Advanced Data Classification and Control

- **Classify and Categorize** - BrickStor enables unlimited categories for fine-grained control over data access. This ensures compliance with security requirements and allows seamless integration into existing workflows.
- **Mandatory Access Control (MAC)** - BrickStor enforces dynamic, policy-driven access at the storage layer, aligning access with clearance levels and need-to-know requirements.

Built-In Cyber Resilience

- **Active Defense** - BrickStor actively monitors and responds to insider threats, cyberattacks, and data theft in real time.
- **ImmutaVault™** - BrickStor protects sensitive data and logs with immutable datasets that prevent unauthorized changes.

Cloud Integration and Disaster Recovery

- **Secure Cloud Tiering** - Transparent Data Movement (TDM) securely tiers data to object storage while maintaining security labels.
- **Integrated Backup and Disaster Recovery** - Immutable snapshots and replications provide robust protection against cyber threats and natural disasters, supporting recovery times under 1 minute.

Flexible Deployment Options

Deploy on-premises, in the cloud, or in hybrid environments with seamless data movement and integrated disaster recovery.

Since 2020 BrickStor has been a comprehensive, trusted storage solution for MLS and MCS environments. With seamless integration, active defense against cyber threats, and deployment flexibility, organizations can confidently safeguard their most sensitive data.

Email fedsales@racktopsystems.com to learn more.

Accredited MLS solution for over 5-years
Designed and developed in the USA