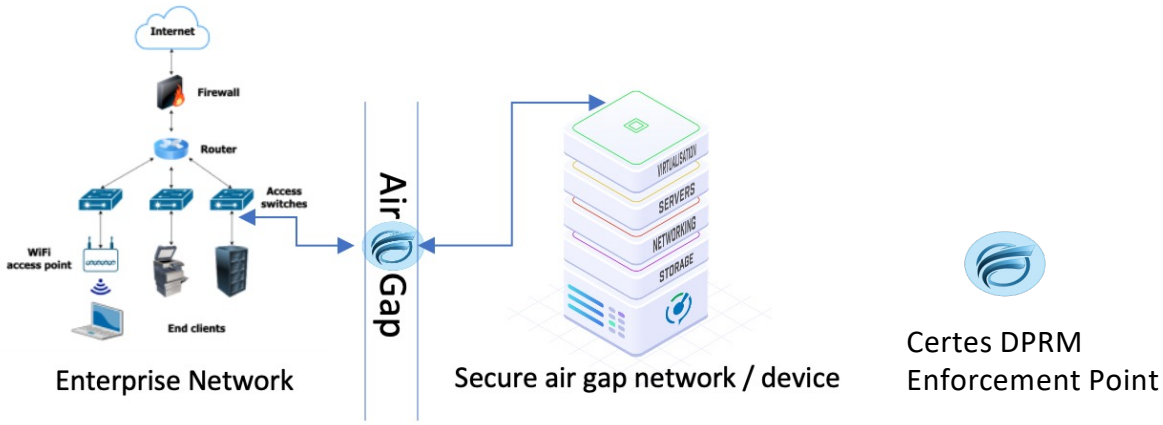
CN ”AirGap” DPRM

Companies deploy air-gapped networks primarily for **security** and **data protection** reasons. Here are some key reasons why air-gapped networks are used:

1. **Protection from Cyber Attacks:** Isolated with no remote access
2. **Safeguarding Sensitive Data:** No physical way to access the data
3. **Critical Infrastructure Protection:** IT/OT/ICS not accessible
4. **Minimizing Insider Threats:** Highly restricted access
5. **Secure Development and Testing Environments:** Ringfence sensitive labs
6. **Disaster Recovery and Continuity Planning:** Secure protected backups
7. **Mitigating the Risk of Zero-Day Vulnerabilities:** Isolated systems
8. **Cyber-Vault**: DPRM effectively acts as the isolation and protection component of a Cyber Vault

DPRM enforcement points create a boundary control point via an L2 Bridge that is under the control of a DPRM customer defined policy. The policy can allow/disallow access to the networks it is protecting as well as protecting the data payload of protected application data flowing through it. Because this access control is at L2 there are no IP addresses to ‘snoop’ and attack – DPRM is effectively an invisible customer-controlled isolation point on the network.



DPRM protects sensitive data and access to sensitive networks

Keep your data Secret,
keep your data Certes

Certes.ai
+1-412 262 2571
info@certes.ai