

Open Source DataTurbine Security Architecture

**Matt Miller, John Wilson,
Erigo Technologies LLC**

DataTurbine is easily integrated into a layered security architecture, which relies on standard, robust IT technologies and protocols. While some security is built into the DT server itself (source-level username/password protection and hooks for third-party authentication and authorization systems) most implementations have relied on standard third-party network security mechanisms. Recommendations for DT security include:

- Firewall configuration can limit inbound data destined for a DT server from specific, known IP addresses to selectively opened UDP or TCP ports. Unidirectional UDP data transmission is preferable. Alternatively, data can be pulled into the DT server via HTTP using the HttpMonitor application (which will typically not require any firewall changes as port 80 outbound access is common).
- WebDAV/HTTP can be used for data access by clients outside the DT's LAN. DT WebDAV support is included in the Tomcat server distributed with DT, allowing architects to leverage Tomcat's mature web-based security. Tomcat supports user accounts and both HTTP and HTTPS access.
- An alternate DT data access mechanism can be provided by mirroring or routing data from an internal DT server to a DMZ server through a firewall. In this scenario, the data provider controls machines on both sides of the firewall and outside clients do not require any internal network access.
- In addition to some of these mechanisms, NASA systems have employed other technologies for DT server access, including two-stage sign-on authorization and VPN access.

The following figure shows a sample system configuration based on the above recommendations.

