# Case study: Project Enclave

In 2016/2017, A publicly traded company contracted Dispel to provide a Project Center deployed external to the traditional company network and private even to company employees. In this scenario, the company doubted the security and integrity of their traditional network and additionally wanted to mitigate the possibility of insider threat. Their key priorities were to prevent theft of intellectual property and to protect the company's reputation.

Complicating this deployment, the company had a set of specialized legacy servers, and the project contributors were split amongst two locations.

Leveraging Dispel Wickets, the company integrated their legacy servers into the Project Enclave, effectively removing those servers/data repositories from both their corporate network, as well as any publicly exposed interface. Furthermore, Wickets were distributed to the two contributor locations, enabling access to the Project Enclave while also enforcing end-to-end encryption. If traveling, contributors used the Dispel application to access protected resources.

## Project Center Breakdown

*Hardware*

- Dispel Wicket$_{Int}$ (integrate legacy servers)
- Dispel Wicket$_{Ext}$ (broker encrypted transmissions)

*Access Layer*

- Dispel Traceless Network (End-to-End Encryption)

*Protected Internal Resources*

- Data Room (File Transfer)
- Team Messaging (Direct/Group Messages)
- Conference Calling (Transaction-specific Numbers)
- Video Conferencing (Unlimited Rooms)
- Integrated Legacy Servers