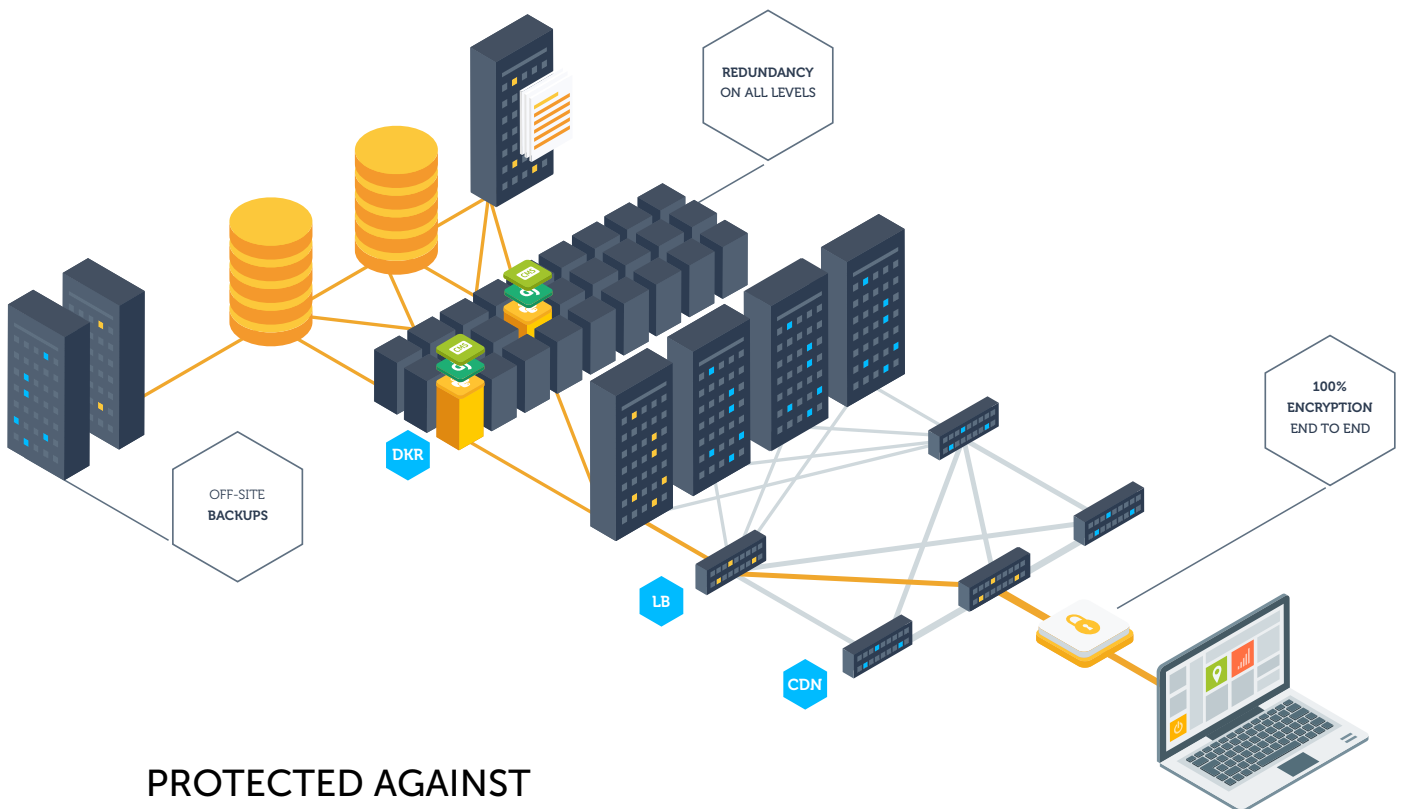


DIVIO CLOUD - SECURE BY DEFAULT

**DIVIO CLOUD IS BUILT WITH AND FOR PYTHON/DJANGO.
A STRONG FOUNDATION FOR HIGH SECURE WEB APPLICATIONS.**

Django is a web application framework implemented in Python, which has an excellent security track record. Secure by design, and hardened at all layers, Django provides great protection to those developers who don't have security experience. In fact, Django makes it difficult to write insecure code.



PROTECTED AGAINST TOP SECURITY THREATS ¹

- ✓ Cross-site scripting
- ✓ SQL injection
- ✓ Path disclosure
- ✓ Denial-of-service attack
- ✓ Arbitrary code execution
- ✓ Memory corruption
- ✓ Cross-site request forgery
- ✓ Data breach (information disclosure)
- ✓ Arbitrary file inclusion
- ✓ Local file inclusion
- ✓ Remote file inclusion
- ✓ Buffer overflow

¹Source: Wikipedia

DJANGO CMS ON DIVIO CLOUD

Divio Cloud allows django CMS projects to be run behind a Content Delivery Network (CDN), providing mitigation for DDoS attacks. All projects come with a TLS (HTTPS) certificate by default. As a further layer of protection traffic is directed through our Load Balancers (LB) before it hits the app runners that orchestrate Docker containers (DKR) that in turn make for easy and fast horizontal scaling.

All levels are redundant, including a performant PostgreSQL cluster and S3 data storage. Backups are stored separately and - like all connections and data on Divio Cloud - they're encrypted, providing further security beyond the highly-secure Django applications.