OneOffice Security in layman's terms (sort of)

To summarise, OneOffice has stronger security than MS 365. And this is by design. Many companies will add additional services like MimeCast or Barracuda to secure their emails on top of MS365. Not needed here. And this is mostly owing to the fact that many of our partners just provide infrastructure and expect us to provide a comprehensive solution.

Here is a short summary list to give you the assurance you need, feel free to revert if any point needs clarity

1. First, OneOffice is security-first monolithic, meaning all services are built-in, rather than external services with their own vulnerabilities. This makes for a very "strongbox" that is very hard to pierce
2. Web / internet proxy is built-in -- we talk to the socket directly, no third-party with their own agenda in the way
3. SSL -- The SSL engine is fully baked / compiled in, and we start with TLS 1.3 which is the recommended encryption protocol (TLS 1.2 is considered "compromised" as it's getting easier to hack)
4. We generate all SSL certificates directly on the server (including key generation, validation, renewal etc. -- keys never leave the server)
5. Inbound and outbound emails are encrypted -- specifically no password exchange ever occurs on plain
6. DDoS built-in -- we can sustain medium level attacks with no additional servers (higher level of attacks are typically state actors, and will need the infra itself to block)
7. Brute-force detection built-in with exponential delays
8. Live list of malicious IPs updated to block on-access (before requests even get processed) with a nano-second IP fast search to prevent malicious attempts to overload the server
9. Email standard protection is built-in -- Sender policy framework, reverse DNS, email signing, email signature validation etc.
10. As you can see from the diagrams in the security doc (and attached architecture doc -- strictly confidential) OneOffice has one public

access point only (again, owing to its monolithic design), and all services are behind it. An active firewall prevents any attempt to reach backend services. You cannot access any service except via the application (which requires authentication etc.)

11. Built-in antivirus, AI spam engine, malware detection, macros, executables etc.
12. Emails are parsed, cleaned and then rebuilt (like GMail does), so the emails are never exactly what is received, full HTML cleaning is performed and the HTML is rebuilt from 'clean'
13. We are the only platform that detects file type from the binary itself before it is uploaded, so gets rejected before upload is even attempted
14. We have a 2-step storage system, when files or emails come in they stay in the "dirty" pile before they are analysed, only then do they go to secure remote storage
15. And finally, we don't use any of the common script-based frameworks (PHP, Python, Node) which are loaded with issues (including performance), we built our own in native language (C/C++) so best-in-class performance

A case in point, which is not public yet, we are also replacing Cisco Security Mail Gateway in some installs (e.g. Saudi Telecom), so security is bullet-proof based on penetration testing, analysis, etc.