Security

Overview of OneOffice Security Features

OneOffice

Introduction

- OneOffice was designed & built to offer best-in-class security features. Our security parameters far exceed industry standards as well as the nearest competitor
- As a monolithic system we minimize attack vectors (by reducing reliance on third-party software with their own vulnerabilities & eliminating integration risks)
- The latest version of SSL/TLS libraries are built-in manually to avoid reliance on outdated / hacked OS-level libraries
- The heavy-lifting is done via our own framework in C/C++, no reliance on “hacky” scripted-frameworks

Single Point of Entry

OneOffice includes its own web server with SSL / TLS termination

- The application acts as a firewall, preventing unauthorized access
- All services (DB, Redis, storage, document editor etc.) sit BEHIND the application server in a private network
- Strong session controls at the access-level prevent any further actions until user permissions are validated, and all actions are permitted only based on RBAC
- Delegated administration allows organizations to allocate administration privileges to the concerned teams

Intrusion Detection

- **Host Intrusion Detection**
  We monitor all activities to detect anomalies in user behavior & block malicious attempts system-wide
- **Protocol-Based Intrusion Detection**
  HTTP / HTTPS / IMAP / SMTP / Websocket servers are built-in and disconnect on any attempts to alter protocol behavior. We do not honor SSL requests from older encryption technologies
- **Anomaly-Based Intrusion Detection**
  The typical patterns of behavior are well-known in advance. Any deviation is given a score, above which attempt is logged & the session is terminated

Intrusion Prevention

- **Strong Session Controls**
  Each user's session is linked to device / IP and cannot be hacked by third party
- **XSS – Cross-site Scripting**
  By design, our system is not vulnerable, as our applications are Websocket / REST – based which only query data (no HTML generation)
- **SQL Injection**
  Our queries are prepared & compiled during startup time preventing any attempt to alter or access the database
- **Password Flood Controls**
  All access protocols (HTTPS / IMAP / SMTP) share 'flooding' database system-wide.
- **Live list of Malicious IP / Domains**
  We download from multiple services the most up to date lists of malicious actors
- **Viruses**
  User apps never run on server, all uploads are scanned. Our code is compiled on safe clean machines
- **Zero-day malware**
  The anti-virus engine downloads hourly latest signatures from top-tier cybersecurity organizations
- **Long hashes & high entropy**
  We use long alphanumeric random strings with very high entropy, negating "birthday attacks"

Separate Instance

OneOffice

Each organization gets its own instance of OneOffice

- Separate database sandbox
- Separate file storage
- Talk chats & video calls routed through your server
- All push / web notifications through your instance straight to the platform (e.g. Chrome / Firefox / Apple / Google)
- Customized security rules (e.g. password, MFA, session duration etc.)
- Customized country, IP access controls & geo-fencing
- Each customer has a different Web SSL certificate

MS 365 & Google Workspace use shared database & file storage.
A vulnerability / hack exposes all its tenants to attacks.

End-to-end Encryption

End-to-end (E2E) secures the most sensitive communications

- Strongest defense vs. weak networks & Man-in-the-middle (MIM)
- Only platform to offer E2E on ALL communication
- Strong AES 256-bit key encryption
- Rotating keys with randomized delays
- RSA 4096-based key exchange with fresh keys
- Server validation during key exchange to prevent MIM

Ransomware / Data-loss Protection

- All servers are protected by strong key-based & IP authentication
- Historical versions of files are kept as backup, so you can quickly revert any data loss
- Deleted emails are stored in built-in backup
- Built-in auditing tools allow you to track unauthorized access
- Fine-tuned sharing rules
- All uploads are scanned for file types, no uploads are ever executed on server

Strong Sharing Protection

Internal and External shares controlled by administrators

- Admins can fine-tune external share rules (e.g. password protection, duration, groups, access type, target audience etc.)
- Automated video call for verification during file access
- Multiple shares for same files with different permissions
- Version history is kept for all changes (even by external actors)

MS 365 and Google Workspace do not allow you to customize your sharing rules or to have multiple share permissions for the same file

Server-side File Editing

- Online document (Word, PPT, Excel, Visio) editor is server-side
- Streaming engine sends a “view” of the file, not its content
- Uses same technology as streaming games
- Blocks all downloads
- Real-time collaboration is server-controlled avoiding conflicts

MS 365 and Google Docs send the file to your browser for editing, allowing users to get a copy (even if you disable downloads)

Security Controls

- All communication is encrypted
- Enforced password policy (length, history, life-cycle, login attempts, common passwords, checking for breached passwords etc.)
- Brute-force protection
- Rate-limiting
- Content Security Policy (block XSS etc.)
- Same-site cookies only
- Machine-learning suspicious login detection
- IP blocks / whitelists (e.g. only allow access from company IP)
- Multi-factor authentication
- Advanced country & IP based access controls

Activity & Event Logs

All user activity are logged

- Your / employee file shares
- All file modifications
- All communication between your employees & externally
- New or deleted files
- Download of files
- New comments or tags
- Calendar invitations
- Incoming calls or chat requests

Email Security

- Strong DKIM signatures
- SSL certificates renewed every 2 months (to prevent man-in-the-middle)
- Sending servers are fully validated
- Spam / Phishing detection using leading-edge AI filters
- Email quarantine system
- Industry IP block lists
- Anti-virus using most advanced commercial virus signatures
- Ability to block by domain / IP
- Executable (.exe .pkg etc.) blocking
- Detection of file type based on binary content (vs. extension)
- Malicious HTML filtering
- In-page JavaScript removal
- Link analysis and testing
- Macro-filtering in Office documents
- Filtering of compressed archives

Thank you.

Please feel free to contact us
info@oneoffice.ca