DWR Security Overview

Digital WarRoom adheres to policies, controls, procedures, and auditing at levels that meet or exceed ISO 27001, SOC, PCI-DSS, and FISMA NIST SP 800 Series cybersecurity guidelines. Digital WarRoom also takes regulatory frameworks such as Monetary Authority of Singapore Act and HIPPA into consideration to all our provided services. Our contractual obligations provide the strongest remedies in our industry.

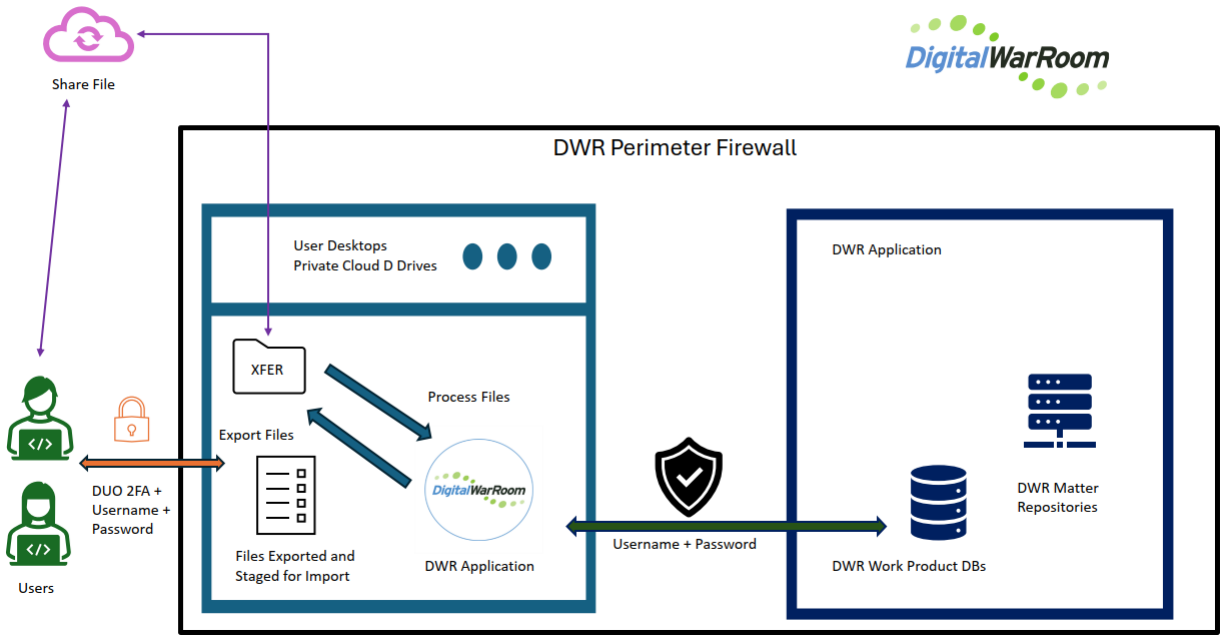
We are fully compliant, but do not purchase annual third-party certification.

Data connections to DWR managed infrastructure are maintained to both physical and logical levels. Connection to the DWR Hosted environment and Private Cloud services are tightly controlled. We enable only limited and specific TCP/IP ports, and implement narrow, targeted IP address access rules. All data communications with DWR adhere to Federal Information Process Standard (FIPS) 140-1 validated encryption methods.

Additional measures are in place across multiple operational domains at Digital WarRoom. We can respond to any specific risk or control, and our policy, procedure, and mitigation posture where needed. We would be happy to extend this discussion during a call or demonstration.

DWR requires, deploys and manages the following security measures to ensure the best protection for our customers client sensitive data:

- Two-factor authentication for all logins in the DWR environment (2FA)
- Separate login to the DWR application hosting documents and databases with customer work product. (image)
- A separate white label ShareFile system for uploading and downloading data. Branded XREF, the document transfer system is independent and disconnected from the hosting application.
- A 7x24 SOC monitoring facilitated by agents on every physical or virtual machine in the DWR environment.
- White Label IP access, informed by our Dual authentication system. Most IP addresses are blocked; only customer-centric IP addresses are allowed to access DWR.
- We have an independent and external Chief Information Security Officer (CISO) that oversees regular audits, testing, and guidance. Our CISO provides approval of evolving internal processes and procedures, including in-transit and staged document limitations and control.
- We perform regular, weekly maintenance intervals to ensure OS upgrades and patches are applied across all systems. This includes firewall upgrades and maintenance audited by a premium service.



Some specific areas, related to the operation of the Digital WarRoom (DWR) Hosted Services include, but are not limited to:

ACCESS

- DWR uses DUO Two Factor Authentication (2FA) – when you login you will need to verify on cell phone in addition to username and password.
- Connections to DWR servers are encrypted at the highest level available for the client computer. Unencrypted connections are rejected, flagged as an alert, and follow up.
- Obscurity - Client access via IP address (not a shared web portal) is unique to each customer in a manner not traceable to the client or DWR.

ARCHITECTURE

- Remote encrypted and monitored (security) sessions enhance the speed and security of document review – during review files do not move between private cloud host and review client, only screen shots are transmitted.
- Client-side web apps, downloads, applets, and other code that would run on a client computer are complete eliminated and excluded from impacting DWR client environments.

HOSTING

- All DWR equipment is based in the US, managed behind a locked rack with biometric access and other physical security controls. DWR colocation facilities housing the internet services utilized our customers are located in the USA are resident at TX1 Data Center[1] (NTT) in metro Dallas, TX.

[1] https://datacenters.ragingwire.com/ntt-global-data-centers-americas-texas-tx1-overview

- DWR owns and manages its servers and infrastructure – no third parties have access to your data. We are unique in the industry in this regard; no other provider can certify compliance with a protective order or other restrictions.
- If your client is averse to Amazon (AWS), Microsoft (Azure), Google or other IaaS providers, DWR provides a neutral solution. Only DWR employees, no third parties, no Amazon, AWS, or who knows who holds your data.

CUSTOMER DATA

- Content based scanning (virus, trojan, malware, etc.) in use at multiple points of entry for data in motion and periodically on all data in at rest
- Servers providing Private Cloud include Microsoft BitLocker encryption; data is stored and transported encrypted.
- All client data is segregated; DWR cannot access your data without direct permission.
- DWR does not operate on, ingest, review, manage, export, classify, or otherwise handle client data except as specifically directed by a client

MONITORING

- Firewalls, network monitoring, login and access audit, malware, and other active measures to manage traffic are actively employed and controlled by DWR employees with professional backgrounds, certifications, and credentials in InfoSec.
- All DWR devices are actively monitored by Sentinel One using device agents and adaptive perimeter controls, as well as permit / deny screens per client

We stand behind our commitment to your client's security. DWR agreements include some of the strongest security and remedy language in the industry.

To review our agreements, please fill out the form on the pricing page of our DWR website:
https://www.digitalwarroom.com/products/single-matter/request-contract

Consider scheduling a call to discuss your security concerns:
https://www.digitalwarroom.com/meeting