Reactiv SUITE – IT / Network / Security Requirements & Compliance Statement

Product: Reactiv SUITE
Company: Vizetto Inc.
Version: 3.2
Last Updated: 7/9/2025

1. Overview

Reactiv SUITE is a secure, on-premises visual collaboration platform specifically designed for enterprise deployment.
It operates independently of cloud infrastructure, external servers, or any internet-based services beyond initial activation and optional licensing verification.

Key Attributes:

- No cloud storage or synchronization.
- No user accounts or logins.
- No telemetry, analytics, or data collection.
- All data remains fully within the user's device or internal network.

2. Deployment Model

Aspect	Details
Deployment Type	On-Premise / Local Installation
Cloud Dependencies	None
Data Residency	All files and data remain local to the installation device
Authentication	Inherits Windows local or domain account permissions
Telemetry / Data Capture	None; no data transmitted to Vizetto or third parties
Software Updates	Manual or IT-admin controlled; no auto-updates

3. Network Requirements

Reactiv SUITE requires limited network connectivity, strictly for: - License activation and optional integrations with wireless display technologies: Apple Airplay, Microsoft Miracast, Google Cast.

Network Configuration Notes:

- No persistent internet connection required after activation.
- All streaming and device discovery remain within the local network.
- In firewall-restricted environments, only the specified outbound ports need to be allowed (see Appendix).

---

4. Security Considerations

Security Aspect	Status / Notes
Data Storage	Local only. No uploads or external storage.
User Management	Leverages Windows authentication (local/domain).
Data Encryption	Not applicable (no external data in transit beyond license check).
Logging / Monitoring	No external telemetry or persistent logging.
Third-Party Access	None.

---

5. Compliance and Certifications

Reactiv SUITE's on-premise architecture and strict data-locality principles align with the spirit of leading global standards, including:

- ISO/IEC 27001: Information Security Management
- SOC 2 Type 2: Trust Services Criteria (security, availability, confidentiality)
- GDPR: Privacy by Design principles
- HIPAA: Protected Health Information not collected or stored externally

Note: Due to the product's lack of cloud services, external communication, or personal data processing, direct certification under frameworks like SOC 2 or HIPAA is not required. Nonetheless, Reactiv SUITE inherently supports corporate compliance initiatives and privacy policies.

---

6. Summary

Reactiv SUITE is purpose-built for secure, local deployment in high-security, regulated, and sensitive environments. It minimizes attack surface by eliminating: - Cloud dependencies - External servers - Persistent network connections - Credential management systems

Only minimal outbound port access (for license activation and wireless display) is required, making Reactiv SUITE ideal for corporations with stringent IT and security policies.

Appendix – Port Requirements

Keyboard / File Drop Service (IWB)

Enables on-premise users to send files and keyboard commands to the Interactive Whiteboard via a browser.

Port #	TCP/UDP	Protocol
80	TCP	HTTP

AirPlay

Mirrors Apple devices to Reactiv SUITE.

Port #	TCP/UDP	Protocol
5353	UDP	mDNS
7000	TCP	Server Port
29053	TCP	Event Port
7100 – …	TCP	Data Port
2001 – …	UDP	Timing Port
61875	UDP	Audio Data Port

Miracast

Mirrors Windows 10 devices.

Port #	TCP/UDP	Protocol
7250	TCP	Server Port
7236	TCP	Control Port
51566 – ...	UDP	—
5353	UDP	mDNS Port

Chromecast

Mirrors Android and Chromebook devices.

Port #	TCP/UDP	Protocol
443	TCP	SSL/HTTPS
1900	UDP	SSDP
5353	UDP	mDNS
8009	TCP	Server Port
56086 – ...	UDP	Data Port

Why Corporations Trust Reactiv SUITE

- Air-gapped compatible: no external dependencies

- Privacy-first, data-residency assured

- Designed for highly secure environments: finance, healthcare, government

- Alignment with globally recognized security best practices and certifications