Relevant Match Online Cybersecurity

Cybersecurity with Relevant Match Online (RMO) follows the best industry practices of layered protection. No application is 100% secure from every possible threat or compromise, but using Relevant Match Online provides many safeguards current to best industry practices. This white paper provides you and your IT security staff with an overview of the cybersecurity measures implemented with Relevant Match Online**.**

Architectural security layer	RMO operates as a web-based application hosted on secure cloud servers. Unlike desktop applications, it utilizes HTTPS encryption to protect data transmitted between the user's device and our servers, ensuring that all communication is secure. The application is designed with a microservices architecture, isolating different functions for better security and manageability. Access controls are enforced through robust user authentication, including multi-factor authentication (MFA), to secure user accounts.
Development security layer	RMO is developed and maintained by a team of vetted professionals who are U.S. persons, with all development conducted in access-controlled facilities in the United States. Our development practices adhere to the DoD Cybersecurity Maturity Model Certification (CMMC) program standards. We perform regular code reviews, static and dynamic application security testing, and employ secure coding practices to minimize vulnerabilities.
Engineering security layer	RMO leverages cloud-native security features provided by our hosting environment, including firewall protection, intrusion detection and prevention systems, and continuous monitoring for unusual activities. The application does not require elevated permissions on user devices, and access to its functionality is strictly controlled by user roles and permissions within the application.
Distribution security layer	RMO is accessed exclusively through our official web domain, protected by an SSL certificate issued by a trusted Certificate Authority (CA). All updates and patches are deployed directly from our secure servers to minimize risks associated with third-party distribution. Our application is not available through third-party resellers or platforms, ensuring that all users access the most secure and up-to-date version.
Installation and Access security layer	As a web application, RMO does not require installation on user devices, which reduces the risks associated with traditional software installations. User data is stored securely in our cloud environment, protected by encryption both at rest and in transit. Access to the application is managed through a secure, token-based authentication system, with additional security layers provided by regular session timeouts and login monitoring.
Hosting security layer	RMO is hosted on industry-leading cloud servers that comply with international security standards, including ISO/IEC 27001 for information security management systems, SOC 2 Type II for data integrity, and the U.S. Federal Risk and Authorization Management Program (FedRAMP) for cloud services. Our hosting provider ensures data redundancy, automated backups, and disaster recovery capabilities to maintain the highest levels of data availability and integrity.

Relevant Match Online Cybersecurity

• **Secure Boot and Trusted Boot**	Ensures that all components of the application are verified before being loaded, protecting against unauthorized alterations.
• **Device Health Checks**	Before accessing corporate resources, the application verifies that the device health status is secure and has not been compromised.
• **Antivirus Integration**	RMO is compatible with leading antivirus solutions, ensuring that any files uploaded or downloaded are scanned and free of malware.
• **Data Encryption**	All data within RMO is encrypted using AES-256 standards, both in transit and at rest, providing robust protection against unauthorized access.
• **Access Controls**	The application includes fine-grained access controls, allowing administrators to define user roles and permissions precisely, limiting access to sensitive data and functionalities.

Relevant Match Online combines robust cloud-based security measures with best practices in application security to provide a secure environment for users. Our layered security approach ensures that user data is protected at every stage, from data input to storage. By using Relevant Match Online, you can be assured that you are benefiting from one of the most secure web applications in the industry.

For any questions or further information regarding the security of Relevant Match Online, please contact us at Match@Relevantsoftware.us