Relevant Match Desktop Cybersecurity

Applies to Relevant Match desktop version 4.1.7 and later
Jun 2023

Cybersecurity with Relevant Match optimizing software™ follows the best industry practices of layered protection. No application is 100% secure from every possible threat or compromise, but using Relevant Match (RM) desktop software provide many safeguards current to best Industry practices. Many of RM's security features are inherited from or leveraged by the host device in the Windows Operating Environment, some are enforced by the user's organization, including the physical security of the user's facilities, and some are part of the Relevant Match software architecture.

This white paper provides you and your IT security staff an orientation to the cybersecurity safeguards implemented with Relevant Match software.

RM is designed to be a single-direction application – that is, once installed onto a device, the application does not require any external connection. There are no interfaces to external services. Updates are made by a complete, new installation.

Architectural security layer	RM installs on a single computer, for operation only on that computer. It is not enterprise network enabled or web-enabled. The entire program resides on hard-drive of the User's selected device. There are no external interfaces.
Development security layer	RM is engineered and maintained by vetted professionals working in small team, who are 100% US Persons and 100% built in USA. We use no off-shore components. The software is coded and assembled in access-controlled offices which meet the standards of DoD Cybersecurity Maturity Model Certification (CMMC) program.
Engineering security layer	RM application runs within the host device security settings and only require running as an administrator in order to use your printer, import document files, and save your RM files to a place on your device directory. This is because every user on a Microsoft device has a separately profile that you log into when starting Windows. Because RM is licensed to the machine, not the person, the local administrator role is required. This setting is extremely common for desktop

	application. It is different than the network administrator, and does not allow controls and privileges to that higher level role. Your network administrator's ability to see, monitor, and control how your device works on a network is unchanged. RM's architecture makes it impossible to be distributed across a network because it is tied to that specific computer device.] RM is a lean installation which does not need access to video, audio, or Bluetooth. I requires no external connectivity, ever. All RM functions are native to the RM application, and do not require separate download after RM is installed. This is unlike a web-based application which uses web pages to display content. These apps download the UI controls across the Company network and internet, and can be exposed to threats. RM is self-contained so the threat of insertion, broken authentication, data integrity compromises, and server-side request forgery are effectively eliminated. Since RM is available on the computer for any user of the device, access to RM is further controlled by a PIN for authorized individuals, in addition to the log-in credentials of the hosting computer. In addition to the local device session management that locks the device after timeout, RM session management times out on the local machine after 24 hours. The User must reopen the application with the PIN to continue.
Distribution security layer	RM is not distributed by any third party. RM is not resold. RM is only available by direct download from our domain-registered site, hosted by IONOS. IONOS data center in Newark, NJ is certified to these standards: • American Institute of Certified Public Accountants – System and Organizational Controls (SOC) Type II • US Federal Information Security Management Act of 2002 • ISO/IEC 27001 Information security management systems RM licensing is done via secure transaction between RM named account manager and a person named for the licensing business, providing proof-of-business entity.
Installation security layer	RM is directly tied to the host device by the unique Machine ID of the device. The host Machine ID is encrypted into the activation code along with the User ID and other business information. This activation code is unique and never reused. At our offices, RM uses the current version of Advanced Installer to create a single Microsoft Installer File (msi) file, which contains all

	the functionality of RM. The MSI file is a specific type of file that must meet standardized requirements so no unauthorized code can be inserted. It is how the Windows OS manages the installation, maintenance, and removal of software. The RM .msi file can only install, maintain, or remove. No programs or code can be launched. We sign our RM files with a digital code certificate, which is issued by a third-party authenticator Sectigo, the global market leader in SSL / TLS certificates, DevOps, IoT, enterprise-grade PKI (Public Key Infrastructure) management, and multi-layered web security. They are a founding member of the Certificate Authority Security Council (CASC), an industry advocacy organization dedicated to addressing industry issues and educating the public on internet security.
Local Hosting security layer	Your Windows based computer running Windows 10 or 11 OS is a very secure platform. RM takes advantage of all the security features native to Windows, including these security features built in to the Windows Operating System.
• **Secure Boot and Trusted Boot**	Secure Boot and Trusted Boot help to prevent malware and corrupted components from loading when a device starts. Secure Boot starts with initial boot-up protection, and then Trusted Boot picks up the process.
• **Measured boot**	The Measured Boot feature provides antimalware software with a trusted (resistant to spoofing and tampering) log of all boot components that started before it. The antimalware software can use the log to determine whether components that ran before it are trustworthy, or if they are infected with malware. The antimalware software on the local machine can send the log to a remote server for evaluation.
• **Device health attestation service**	The Windows device health attestation confirms the device, firmware, and boot process are in a good state and have not been tampered with before they can access corporate resources.
• **Microsoft Defender Antivirus**	Microsoft Defender Antivirus is a protection solution included in all versions of Windows. From the moment you boot Windows, Microsoft Defender Antivirus continually monitors for malware, viruses, and security threats. Updates are downloaded automatically to help keep your device safe and protect it from threats. Microsoft Defender Antivirus includes real-time, behavior-based, and heuristic antivirus protection.

• **Tamper protection settings**	Tamper protection is a capability in Microsoft Defender for Endpoint that helps protect certain security settings, such as virus and threat protection, from being disabled or changed.
• **Controlled folder access**	You can protect your valuable information in specific folders by managing app access to specific folders. Only trusted apps can access protected folders, which are specified when controlled folder access is configured. Commonly used folders, such as those used for documents, pictures, downloads, are typically included in the list of controlled folders. Controlled folder access works with a list of trusted apps. Apps that are included in the list of trusted software work as expected. Apps that are not included in the trusted list are prevented from making any changes to files inside protected folders.
• **Microsoft Defender SmartScreen**	Microsoft Defender SmartScreen protects against phishing, malware websites and applications, and the downloading of potentially malicious files. For enhanced phishing protection, SmartScreen also alerts people when they are entering their credentials into a potentially risky location. IT can customize which notifications appear via MDM or group policy. The protection runs in audit mode by default, giving IT admins full control to make decisions around policy creation and enforcement.

RM can even be installed within a temporary security container or sandbox by the system administrator to test or verify that RM runs safely. This layered approach to cybersecurity is in effect from the first time RM touches your computer.

Relevant Match Online Cybersecurity

Cybersecurity with Relevant Match Online (RMO) follows the best industry practices for web-based applications. 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**.**

Cybersecurity Architecture	RMO operates as a web-based application hosted on secure cloud servers. It utilizes HTTPS encryption to protect data transmitted between the user's device and our servers. RMO uses a security architecture that includes three data security "Zones": • Zone 1 is the Account information that identifies your Company, your Account Owner, and your proposal Users (Proposal Manager or Team Members). • Zone 2 is the document upload and retention. • Zone 3 is the analysis results. Each of these three zones are within a Multi-tenant architecture, where each subscriber Company has their own secure area separate from all others. The features of this architecture include strong access controls, encryption, and isolation mechanisms, including: Shared Infrastructure: All Companies share the same physical infrastructure, such as servers and storage, but their data and configurations are logically isolated from each other. Data Partitioning: Each Company's data, including documents and analysis results, is stored in separate partitions within the same database or in entirely separate databases. This ensures that one Company's data is not accessible to another. Customization: Companies can customize certain aspects of the application, such as analysis setting, without affecting other Companies. Resource Allocation: Resources like CPU, memory, and storage are allocated dynamically based on the needs of each Company. This allows for efficient use of resources and scalability. When the Company account is closed, all Zone 2 information is deleted. Zone 1 may be retained for an unspecified period for purposes of improving RMO.

Data Security Zone 1 – Account Information	Your account information includes you Company identity and the identify of individuals in your Company that you assign as the Account Owner and the Account Users. No personal information beyond name, email, and phone number are collected or retained on RMO servers. No financial, demographics (gender, location), or Personal Identifying Information (PII: birthdate, residence, etc.) is collected or retained. No names, emails, or phone numbers are exported, replicated, or released to any other party, except if required by law.
Data Security Zone 2 – Documents	When uploaded for analysis, both the solicitation and proposal documents are held like data items in the same way as described above. The Company's Account Owner can delete any document at any time. They are retained by RMO only while the account is open for the convenience of the Company, unless requested otherwise by the Company Account Owner.
Data Security Zone 3 – Analyses	Analyses and the associated report are generated dynamically on demand, and are not retained once closed within the RMO App by the Account User.