RMS(one) Solutions

Architected for High Availability and Resiliency

High availability and resiliency are core business requirements for any insurance technology. The ability to support business-critical workflows, modeling, and analytics processes at all times and under any conditions is critical. Not only for companies meeting current business demands, but also to position themselves for future growth in an increasingly competitive and complex industry.

Modern catastrophe modeling poses significant technological challenges, with complex calculations requiring significant computing power and robust analytics capabilities. Evolving data privacy concerns challenge companies to meet current regulations and anticipate new ones. Cyber threats are both persistent and increasingly sophisticated. Yet the very nature of the insurance industry demands that systems remain available, secure, and compliant at all times.

Insurance companies have historically relied on their hardware to meet these demands. However, this approach was inflexible and expensive, as a hardware failure also meant an application failure. Today's modern approach means companies are building availability and resiliency directly into their product architecture and applications. This enables companies to lower hardware costs and provides insurance companies with greater flexibility and scalability.

RMS(one)® is an open, big data and analytics, risk management platform purpose-built for the data structures, workflows, and analytics specific to the insurance industry. Unlike federated or legacy systems, the RMS(one) platform operates entirely from a modern cloud environment to deliver the high availability and resiliency insurance companies need and the business results their stakeholders expect.

Cloud Architecture Purpose-Built for High Availability

The RMS(one) platform is built leveraging cloud-first technologies and delivers a timely and consistent view of risk across all users in a cost effective manner. The services within the platform are architected for high availability and reside within the Microsoft Azure cloud for additional redundancy at the hardware and infrastructure layer, delivering resiliency and solution flexibility.

The Microsoft Azure network enables multiple terabit connectivity to more than 70 points of presence. Multiple paths to providers reroute traffic around internet failures. Data is continually replicated for durability and high availability.

At the application layer, the RMS(one) platform further enhances availability through Apache Mesos – a purpose-built resource allocator and instrumentation framework. Built on open-source code and unique to RMS, Mesos lets you manage compute nodes by defining and allocating specific hardware resources for each task in your workflow. Once configured, the framework maintains platform availability by continually monitoring performance and adjusting or allocating resources in response to service failures or fluctuations in workload.

The RMS(one) platform is also application-aware. That means the allocation framework quickly spots and logs failed services, replaces them with new services, and then automatically validates new ones. Communication among services is conducted via the secure HTTPS protocol. Related security information resides within a centrally managed cloud service – a current industry best practice. These capabilities are replicated within Microsoft Azure to ensure consistent performance throughout the platform.

The RMS(one) platform also delivers high availability and resiliency through its individual services. The analytical engine on top of Apache Spark allows us to scale horizontally and run analytical computations across multiple nodes, delivering fast speeds to process complex calculations. Additionally, our purpose-built data layer uses columnar databases to ensure fast responses to complex queries.

Lastly, we continually test its performance to multiple levels of the expected load.

The services within the RMS(one) platform are architected for high availability and reside within the Microsoft Azure cloud for additional redundancy at the hardware and infrastructure layer, delivering resiliency and solution flexibility.

Progressive Security for Business Continuity

The RMS information security team incorporates security principles and best practices throughout our organization, while helping provide assurance to our customers that data is secure and protected during transmission, processing, and storage.

No component of the platform ships until it is declared free of all severity 1- and 2-level bugs. Our security framework extends beyond our development teams to include our legal, monitoring, information security, and cloud operations.

We approach security from two unique verticals: **Application Security** and **Infrastructure Security**.

No component of the platform ships until it is declared free of all severity 1- and 2-level bugs.

Application Security

RMS(one) solutions are secured at multiple levels and entry points. We test for vulnerabilities in the user interface through direct attacks from legitimate user accounts. Application integrity is tested through foreign data placement, and we deploy a variety of tools to perform dynamic scans of the code base. These tests include static application security testing (SAST), dynamic application security testing (DAST), and open-source scanning (OSS). We also maintain a rigorous patching schedule.

Internal product experts conduct penetration tests weekly. We also engage trusted third-party organizations to conduct penetration tests frequently as well as a “bug bounty” program that is unique in the insurance industry, and offers financial rewards similar to programs at leading cloud organizations like Amazon and Google.

Infrastructure Security

RMS infrastructure security combines advanced and hardened firewalls, network segmentation, and intrusion detection and prevention systems, as well as ongoing log monitoring and analysis for threat detection. We regularly test our infrastructure components for vulnerabilities (including the OWASP Top 10) and engage trusted third-parties to do the same.

The RMS(one) platform is secured with Microsoft Azure cloud services. Each Azure facility employs measures to protect your operations from power failure, physical intrusion, and network outages. Azure cloud services comply with ISO 27001 and SOC 2 standards for physical security and availability.

Our production management network, which hosts customer data, is segregated from our corporate network. Access to the network is restricted to individuals on a need-to-know basis and requires multi-factor authentication. There are no paths from the RMS corporate network into a client tenant.

Continuous Compliance

RMS security practices comply with the most widely accepted industry standards and regulations, including ISO 27001 and SOC 2. We view General Data Protection Regulation (GDPR) as an important step toward streamlining the data protection requirements across the EU, as well as an opportunity to deepen our commitment to data protection. Similar to our existing compliance with the European Data Privacy Directive, we are continuing to build on and execute our GDPR plans to be compliant by May 2018. As further guidance continues to emerge from data protection authorities, we will adjust our processes and practices, as needed, to comply with applicable laws.

Compliance

- ✓ ISO 27001
- ✓ SOC 2

RMS
7575 Gateway Blvd.
Newark, CA 94560 USA

For Sales Inquiries:
+1.510.505.2500
+44.20.7444.7600
sales@rms.com

www.rms.com

RMS is the world's leading catastrophe risk modeling company. From earthquakes, hurricanes, and flood to terrorism, agriculture, and infectious diseases, RMS helps financial institutions and public agencies understand, quantify, and manage risk.

20170000