SECURITY COMPANIES CHOOSE RIAK® KV

INTRODUCTION

Data is the backbone of any security solution. From fraud and intrusion detection to data loss prevention and document security, data is required to generate the analysis needed to provide insights. Without data, security companies are paralyzed.

As companies like Symantec and Mcafee move security software from on-premises to the cloud, ensuring data availability becomes even more critical. The distributed software environment requires modern database technology. Traditional relational databases typically have a single point of failure, or avoid that problem with a complex design. Conversely, NoSQL databases generally make it easier and less complex to ensure data is there when needed. Since data is key to selling services and growing revenue, security companies need to choose a NoSQL solution that will best meet their needs. Riak® KV is designed to deliver maximum data availability, scale linearly using commodity hardware, and lower the total cost of ownership by making the system easy to manage.

SECURITY SOFTWARE CHALLENGES

Security Companies face the same challenges as other enterprises that struggle to manage Big Data and keep that data always available in datacenters around the globe. For the average company, minutes of application downtime can mean lost sales, a poor user experience, and a bruised brand. For security companies, the stakes are even higher. Those same few minutes of downtime could translate into a data breach. In today's world where hackers and organized crime are targeting the largest companies, the financial liability could run into the millions.

With data being counted in terabytes, petabytes, and higher, systems must ensure data availability for reads/writes and analysis. Whether scaling for capacity (more and more data) or for performance (more and more users), companies need to the ability to add capacity on demand, while at the same time keeping costs in check.

WHY RIAK® KV FOR SECURITY COMPANIES?

- **HIGH AVAILABILITY**
- **FAULT TOLERANCE**
- **ENHANCED SCALABILITY**
- **GLOBAL AVAILABILITY**
- **LOWER TOTAL COST OF OWNERSHIP**

> *"Alert Logic depends on the reliable processing of massive amounts of machine data and turning that into actionable information. Our security operations center depends on this information for analysis to detect and respond to real-time security incidents that occur on our customers networks. We selected Riak KV for scalability and fault-tolerance, and it continues to be a vital component helping ensure that the Alert Logic Platform can scale to keep up with our rapid growth."*
>
> – Paul Fisher, Director of Platform Services, Alert Logic

SECURITY COMPANIES DEPEND ON RIAK KV

Security companies choose Riak KV, because it ensures constant uptime, fast performance, and the ability to scale at a lower cost than traditional relational databases. For example, Symantec selected Riak KV for a system running 26+ million concurrent connections, 38+ million unique endpoints (growing by a half million per week), and 28,000+ requests per second at daily peak. This required a massively scalable data store and the ability to replicate data across datacenters. Alert Logic switched from MySQL to Riak KV to support the development of a new analytics infrastructure required to collect and process machine data and to perform real-time analytics, detect anomalies, ensure compliance, and proactively respond to threats. Both of these deployments were possible, because Riak KV was designed for:

HIGH AVAILABILITY

Riak KV is architected for data availability, so that even in the event of hardware failure or network partition, data is available for read and write. Riak KV also ensures the system can always accept writes and serve reads at low-latency with high responsiveness, allowing security providers to do real-time analysis while meeting their customer SLAs.

FAULT TOLERANCE

Hardware malfunction, network partition, and other failure modes are inevitable. Riak KV provides a failure-resilient infrastructure by replicating data automatically within the cluster so nodes can go down but the system still responds to requests. Riak KV ensures that all replicas are valid through automatic data healing.

ENHANCED SCALABILITY

Successful security companies can grow quickly and drastically. Riak KV enables easy capacity increases. When new nodes are added, Riak KV automatically distributes data evenly to prevent hot spots in the database, and yields a near-linear increase in performance and throughput when capacity is added.

GLOBAL AVAILABILITY

Security software is global. Your users are everywhere. Riak KV has an innovative database architecture that provides fast read and write functionality for globally distributed data. Riak KV is designed for a masterless configuration. This means that administrators can deploy multiple Riak KV clusters and then replicate to keep them all synchronized. For example, if a write is received by Cluster A, then Cluster A will assure that the write is replicated to Clusters B – Z.

LOWER TOTAL COST OF OWNERSHIP

Riak KV is operationally easier to manage than traditional relational databases. You can easily add capacity on demand using commodity hardware. Riak KV Enterprise also allows replication of data to multiple datacenters, providing both a global data footprint and the ability to survive datacenter failure.

LOOKINGGLASS CHOOSES RIAK FOR THREAT INTELLIGENCE & ANALYSIS

LOOKINGGLASS
Transforming the Art of Threat Intelligence

LookingGlass Cyber Solutions has built a scalable global threat intelligence, analysis, and management solution used by large organizations including government agencies and many Fortune 1000 companies. LookingGlass stores hundreds of millions of datapoints everyday, including more than 15 million active unique threat observations.

LookingGlass customers require:

- Data persistence
- Custom search
- Data redundancy
- Horizontal scale
- Global distribution
- Real-time analytics

Why LookingGlass Chose Riak?

- Global scalability
- Custom search across growing schema-less data set
- High availability & fault tolerance
- Ease of deployment and operation

"LookingGlass products have been deployed in the most demanding, and challenging, customer environments. We have several customers that have deployed our solution in very high scale environments and one of the first things that we looked to Riak KV for was how we can store, search, and index information in an efficient manner."

–Allan Thomson, CTO, LookingGlass Cyber Solutions

SECURITY SOFTWARE USING RIAK KV

According to Gartner, the cybersecurity market is $77 billion dollars in 2015 and will more than double to $170 billion by 2020. The list of related security specialities is long, and all of them share the need to perform read/write and analysis on massive volumes of data. Here are a few examples of security software applications using Riak KV:

FRAUD DETECTION

Preventing fraud is a complicated and expensive endeavor requiring real-time data management and analysis. In order to spot suspicious activity early, the data must be always available. However, availability is meaningless without high performance to go with it, because systems need the capacity to analyze massive amounts of data. For example, in order to know if a customer's network has been breached, Alert Logic analyzes over five terabytes of data per day — as it streams in from over 2,000 customers, 5,000 appliances, and hundreds of thousands of data sources on customer networks. With their data volume growing more than 50% a year, Alert Logic chose Riak KV to keep their data always available, even at massive scale.

DETECTING MALICIOUS EMAILS

Security companies offering malware and other email protection solutions must deal with massive amounts of unstructured data. A database with a schemaless key/value design makes it possible to use machine learning to process and analyze email for malicious activity. Symantec chose Riak KV as the distributed NoSQL database behind its cloud-based service, SPOC (Single Point of Contact), to ensure push email notifications are always available to warn customers about suspicious activity.

DOCUMENT SECURITY

Enforcing usage policies, revoking access after distribution, monitoring, and auditing sensitive data all require a robust database. Using a distributed architecture helps document security companies avoid a single point of failure, which is why Covata embeds Riak KV as its highly available, distributed database for managing user access control and document data.

INTRUSION DETECTION

To defend against security threats and address compliance mandates, such as PCI and HIPAA, security companies collect and process machine data to perform real-time analytics, detect anomalies, ensure compliance, and proactively respond to threats. To handle increasingly distributed systems, databases must offer advanced replication technology. Alert Logic relies on Riak KV Enterprise for multi-cluster replication to deploy clusters that can handle different priority workloads. This ensures the primary cluster is always available to receive and write customer-specific analytic data, even during times that require extreme scale.

DATA LOSS PREVENTION (DLP) SYSTEM

Data loss prevention requires accessing and analyzing vast amounts of content. Security companies offering DLP services need a highly available and scalable backend database. Kolab Enterprises uses Riak KV for integrating data loss prevention systems to store groupware object histories in real-time for future audit and rollback. Kolab chose Riak KV, because it is robust, scalable, and easy to deploy.

CONCLUSION

High availability is the key to success for security companies that rely on data to power their daily operations. It is critical that the data backing the service offerings be readily accessible. If the data is not available, the service is not available.

Whether a mega-company like Symantec, security-as-a-service companies like Alert Logic, or a threat intelligence and threat defence companu like LookingGlass Cyber Security, today's security companies need state-of-the-art database systems to support their business processes. Detecting malicious emails, preventing data loss and fraud, and securing documents are just some of the security offerings that traditional relational databases are not designed to cope with. Security companies are switching to NoSQL systems to handle the enormous amounts of unstructured data required for security analysis and insights.

Riak KV is architected to better handle a variety of security-sector challenges, including storing fast-growing unstructured data, and ensuring globally distributed reads and writes are fast. Riak KV is a distributed NoSQL database architected for high availability and massive scalability, and stands out among its peers for ease of use and operationalization. If a node or cluster fails, you won't know it. And no matter how massive the data, it's always available for reads and writes.

When the data is available, your service is available, and your customers are secure.

> *"Unlike traditional databases where clustering can present significant development hurdles, Riak KV delivers resilience and scalability out of the box with amazingly little tweaking necessary for a production deployment."*
>
> – Aaron Seigo, Senior Technologist and Evangelist, Kolab Systems

ABOUT BASHO TECHNOLOGIES

Basho is a distributed systems company dedicated to developing disruptive technology that simplify enterprises' most critical data management challenges. Basho has attracted one of the most talented groups of engineers and technical experts ever assembled devoted exclusively to solving some of the most complex issues presented by scaling distributed systems.

Basho's distributed database, Riak® KV, the industry leading distributed NoSQL database, and Basho's cloud storage software, Riak® S2, are used by fast growing Web businesses and by one third of the Fortune 50 to power their critical Web, mobile and social applications. The Basho Data Platform helps enterprises reduce the complexity of supporting Big Data applications by integrating Riak KV and Riak S2 with Apache Spark, Redis, and Apache Solr. Basho is the organizer of RICON — a distributed systems conference. Riak is the registered trademark of Basho Technologies, inc.

basho

SEATTLE - HEAD OFFICE
10900 NE 8th Street
Suite 1580
Bellevue, WA 98004
617.714.1700

WASHINGTON, D.C.
12930 Worldgate Drive
Suite 120
Herndon, VA 20170
617.714.1700

LONDON
Fourth Floor
South Warwick House
65/66 Queen Street
London, EC4R 1EB
+44 020 3201 003

PARIS
6th Floor
105 rue Anatole France
Levallois-Perret, Paris
92300 France
+33 1 73 44 66 71

TOKYO
Basho Japan KK
NK7 Building 3rd Floor 2-9
Yotsuya Shinjuku-ku
Tokyo, Japan 160-0004
03-5953-1780