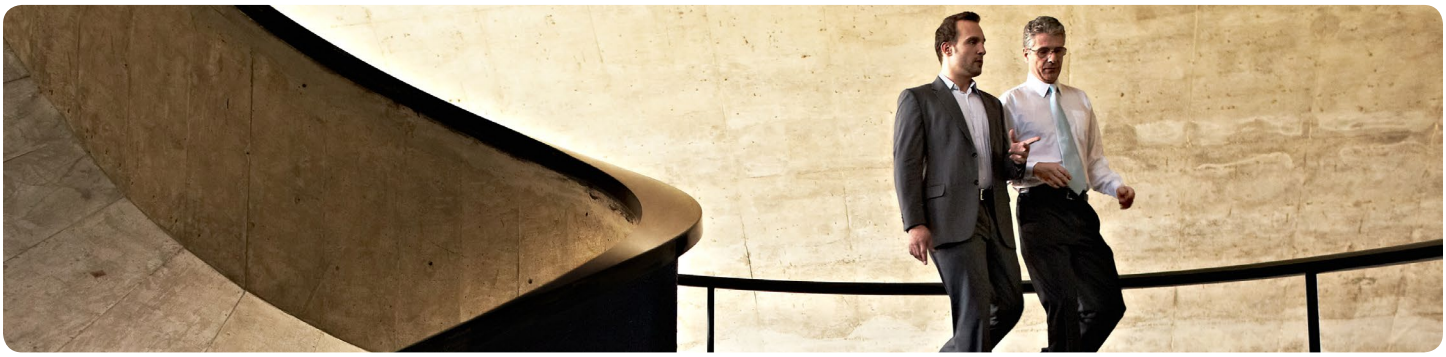
Customer Case Study

# Solutionary Boosts Security with Cisco and MapR Technologies



## Executive Summary

- **Customer Name:** Solutionary
- **Industry:** IT security and managed services
- **Location:** Omaha, Nebraska
- **Number of Employees:** 310
- **Data Volume:** Trillions of messages per year (Petabyte storage)

### Challenge

- Increase data analytics capabilities to improve clients' security
- Improve scalability as number of clients and data volume grow
- Reduce costs of expanding database solution to meet demand

### Solution

- Implemented Cisco UCS Common Platform Architecture (CPA) for Big Data with MapR

### Results

- Reduced time needed to investigate security events for relevance and impact
- Improved data availability, enabling new services and security analytics
- Enhanced agility with ability to deploy on-demand capacity

### Technology / Application Partner:

- MapR Technologies

## Managed service provider enhances security solutions and improves performance of Apache Hadoop data solutions delivered on Cisco UCS and MapR.

### Challenge

As a leading Managed Security Service Provider (MSSP) in North America, Solutionary delivers managed security services and professional consulting services to mid-sized organizations and global enterprises. Founded in 2000, the company uses proprietary security analytics technology to reduce risk, increase data security, and support compliance initiatives for its clients.

By working closely with clients and providing dedicated customer service, Solutionary maintains one of the highest client retention rates in the industry.

Part of the patented Solutionary ActiveGuard Security and Compliance Platform involves real-time analytics of client traffic, particularly massive volumes of event data, and detailed user activity. By analyzing all enterprise activity, such as patterns of behavior, anomalous activities, and attack indicators, ActiveGuard enriches and correlates data across global threats and trends to provide context and actionable alerts to clients.

ActiveGuard technology quickly and accurately identifies security events. "Our MapR/Cisco UCS clusters horizontally scale with ActiveGuard, enabling detection of advanced and sophisticated attacks through analysis of unstructured data while linking enriched structured asset and contextual data," says Scott Russmann, director of research and development at Solutionary.

In addition to growing data volumes, the need for rapid security analytics and the sharp growth of Solutionary's client base have also placed a greater demand on the company's ability to expand and quickly scale the environment. Due to this rapid growth, traditional relational database solutions need to be augmented to support dynamic scalability in a

cost-effective, high-performance environment. The Apache Hadoop solution delivered by MapR Technologies introduces a completely new way of handling big data. Unlike traditional databases that store structured data, Hadoop enables Solutionary to distribute and analyze structured and unstructured data smoothly on a single data infrastructure.

Solutionary combines the MapR solution with Cisco Unified Computing System™ (UCS®) to achieve a high-performance platform that can be easily optimized and scaled to meet growing demand. "By implementing MapR and Cisco UCS, we have achieved performance and flexibility with incredible scalability via Hadoop's clustered infrastructure. This infrastructure allows us to perform real-time analysis on big data in order to help protect and defend against sophisticated, organized, and state-sponsored adversaries," says Dave Caplinger, director of architecture at Solutionary.

## Solution

As the Hadoop technology leader, MapR brings enterprise-grade innovations to Hadoop and delivers the industry's most comprehensive Hadoop platform. The MapR M7 Enterprise Edition for Apache Hadoop, a Cisco Compatible product used by Solutionary, leverages an architecture designed specifically for high availability to offer advanced features not available with other Hadoop distributions.

The MapR Direct Access NFS feature delivers true industry-standard NFS that enables Solutionary to smoothly integrate with existing systems without sacrificing performance. Data snapshots and mirroring provide reliable data protection for enhanced data security, while monitoring through the MapR Heatmap enables staff to view cluster health and current capacity at a glance.

Solutionary particularly appreciates the MapR JobTracker HA feature, which helps to ensure that all jobs complete successfully. In addition to boosting performance speeds, this feature requires less manual management from the infrastructure staff. "MapR has taken Apache Hadoop to a new level of performance and manageability," says Caplinger. "It integrates into our systems seamlessly to help us boost the speed and capacity of data analytics for our clients."

Solutionary launched MapR in the Cisco® UCS CPA for Big Data environment with two clusters of 16 Cisco UCS C240 M3 Rack Servers. With high density, the enterprise-class Cisco UCS C240 Servers are designed to work well with data-intensive applications and storage-intensive infrastructure workloads, making it the ideal hardware for Hadoop solutions. The Cisco UCS CPA for Big Data environment reduces the total cost of ownership while increasing scalability and business agility.

Working with Cisco UCS Manager, Solutionary gains unified management over server and network resources. Cisco UCS 6200 Series Fabric Interconnects provide high-bandwidth and low-latency connections to servers and act as unified management points for all connected devices. High scalability enables the fabric interconnects to support the large number of nodes needed for MapR clusters. Cisco UCS 2200 Series Fabric Extenders extend the network into each rack, improving scalability even further.

"MapR and Cisco UCS have many of the same values: high performance, efficient management, and ease of use," says Caplinger. "Using both solutions together enables us to scale our security analysis services while keeping complexity and cost under control."

"MapR and Cisco UCS have many of the same values: high performance, efficient management, and ease of use. Using both solutions together enables us to scale our security analysis services while keeping complexity and cost under control."

— **Dave Caplinger**
Director of Architecture
Solutionary

## Results

Working with the data-processing capabilities of Cisco and MapR's Hadoop implementation, Solutionary can rapidly evolve its data modeling and predictive analysis of events while expanding the amount of traffic the ActiveGuard Platform can process. For example, in traditional hardware deployments and data structure, the lifespan of useful data available to ActiveGuard for analytics was limited.

Hadoop has significantly increased the amount of data analysis and contextual data that ActiveGuard can access, which provides a greater view of attack indicators, expanding global correlation and true understanding of attackers' goals and techniques. This capability also enables Solutionary to cost-effectively and quickly identify global, cross-client patterns.

Superior performance allows the Solutionary ActiveGuard platform to perform far more complex processes. If new threats are discovered, Solutionary can now globally detect and analyze activity across all clients within milliseconds. With the previous environment, even this seemingly simple task would be considerably more difficult and costly to do, taking as long as 30 minutes even with a preplanned, optimized environment.

"With the speed and sophistication of today's attacks, along with the large amount of data produced by enterprise environments, Solutionary needed a high-performance and scalable infrastructure to quickly respond to the ever-growing attacks against clients. Solutionary found its solution in the MapR and Cisco UCS CPA for Big Data environment, which dramatically increases performance and ability to analyze big data allowing Solutionary to defend and minimize the impact of attacks on clients", says Russmann.

The streamlined Cisco environment simplifies management for Solutionary staff. Devices and connections can all be provisioned and controlled using Cisco UCS Manager. The Cisco UCS fabric interconnects act as centralized management points for the Cisco infrastructure, eliminating the need to manage each element in the environment separately.

Automated provisioning and configurations in Cisco UCS Manager further streamline management and enhance scalability by reducing the time needed to modify the environment. "With our previous infrastructure, adding new equipment was a long and intensive process," says Caplinger. "Cisco UCS enables us to scale our infrastructure on-demand to meet our dynamic and growing business need with greater agility."

## Next Steps

Using Hadoop technologies in the Cisco UCS CPA for Big Data and MapR environment, Solutionary plans to expand its analytical capabilities, extending machine learning, predictive modeling and analysis to improve Advanced Persistent Threat (APT) detection, which typically includes sophisticated techniques utilizing zero-day vulnerabilities. "Cisco UCS and MapR give us the ability to enhance our global security intelligence, and expand our current services. It also enables advanced behavioral analysis, and machine-learning in near real time that previously was not possible on traditional platforms, due to the precision and speed of attacks buried within petabytes of data," says Russmann.

## Product List

### Data Center Solutions

- Cisco Unified Computing System (UCS)
- Cisco UCS C240 M3 Rack Server

### Routing and Switching

- Cisco Catalyst 6500 Series Switches

### Fabric Interconnects

- Cisco UCS 6200 Series Fabric Interconnects
- Cisco UCS 2200 Series Fabric Extenders

### Network Management

- Cisco UCS Manager

### Applications

- MapR M7 Enterprise Edition for Apache Hadoop

Compatible

## For More Information

To find out more about Cisco Unified Data Center, please visit: www.cisco.com/go/unifieddatacenter.
To find out more about Cisco UCS Big Data Solution, please visit: www.cisco.com/go/bigdata.
To find out more about Cisco UCS Big Data Solution with MapR, please visit: www.cisco.com/en/US/docs/unified_computing/ucs/UCS_CVDs/Cisco_UCS_CPA_for_Big_Data_with_MapR.html.
To find out more about MapR Technologies, please visit: https://marketplace.cisco.com/catalog/companies/2032.
To find out more about MapR M7 Enterprise Edition, please visit: www.mapr.com/products/mapr-editions/m7-edition.

Available in the Cisco Developer Network Marketplace



**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



COO-XXXXXX-00 11/14