



SecureWorks

## SecureWorks Slashes the Cost of Storage with Dell | Cloudera Solution

### Overview

In the time it takes to read this brief article, [Dell SecureWorks](#) may already have collected and analyzed information on millions of IT events that took place during the same interval at thousands of customer sites around the world. This is all part of the work of an information security services organization that never sleeps. Dell SecureWorks is on deck 24 hours a day, 365 days a year, to help protect the security of its customers' assets in real time.

To meet its enormous data processing challenges, Dell SecureWorks requires leading-edge technologies for cost-effectively storing, scaling, and analyzing massive amounts of information in real time. And that's just what it found in the [Dell | Cloudera® Solution](#) for high speed data processing, analysis, and mining.

Providing information security services is very different from selling security products. With the services business model, the security provider's relationship with customers is just beginning when the technology is deployed. Once the service is up and running, customers rely on the service provider day in and day out. That's the case with Dell SecureWorks, which offers world-class information security services to help thousands of organizations worldwide to protect their IT assets, comply with regulations, and reduce security costs. These managed security services customers include many Fortune 10, Fortune 100, and Global 2000 companies, along with small and midsize organizations. Regardless of size, they all count on Dell SecureWorks to have highly trained, expert security analysts on duty around the clock to help them identify and protect against potential security threats.

In its nonstop work, the SecureWorks organization can process ~20 billion events per day in real time. An event is a single transaction for a security device, such as a firewall or an intrusion prevention system (IPS), or a log event from an application or operating system.

## Key Highlights

### Industries

- Technology
- Information Security Services

### Location

- USA

### Business Applications Supported

- Managed information security services
- Threat intelligence

### Impact

- Reduced data storage costs from \$17 per GB to ~\$0.21 per GB
- Easy scalability for future growth
- High availability for critical services
- Flexibility to analyze structured and unstructured data

### Technologies in Use

- Hadoop Platform: Dell | Cloudera Solution
- Servers: Dell PowerEdge C2100
- Cloud Installer: Dell Crowbar
- Networking: Dell Force10

### Big Data Scale

- 38 TB

## The Challenge

Each day, the SecureWorks organization investigates ~1,000 potential security incidents and analyzes ~20,000 pieces of malicious software. Leveraging this global intelligence enables SecureWorks to offer improved threat protection on behalf of its customers. To deal with the massive amounts of information it collects, SecureWorks requires highly scalable solutions for processing, storing, and analyzing big data in a cost-conscious manner.

Historically, the SecureWorks organization met this need with proprietary technologies. Then a few years ago, it started looking for next-generation solutions, including those based on open-source software and industry standard hardware. This search culminated in the deployment of the Dell | Cloudera Solution, comprised of [Apache Hadoop](#) open source software, [Dell PowerEdge C](#) servers, [Force10™](#) switches, and services from [Cloudera](#) and [Dell](#).

## The Solution

Hadoop is an open-source analytics platform, built from the ground up, to address today's big data challenges. Hadoop enables organizations to load and consolidate data from various sources into an extremely scalable distributed file system for data storage, the [Hadoop Distributed File System \(HDFS\)](#). This data can then be processed using highly distributed compute jobs through the [MapReduce](#) framework. Hadoop excels at supporting complex analyses, including detailed, special-purpose computation, across large collections of structured and unstructured data.

"Hadoop had all of the attributes that we needed," said Robert Scudiere, director of engineering for SecureWorks. "It was a highly scalable system. It had availability built into it. It had technology to enable very-high-analytics types of activities, and it was very active in the market in terms of ongoing development to further enhance the technology over time."

The SecureWorks engineering team went down the path of evaluating Hadoop before the company was [acquired by Dell in February 2011](#). "When we joined the company, we were pleased to learn that Dell had a big data initiative under way, had built out a reference architecture, and had selected Cloudera as a partner - a partner we were actively working with," Scudiere says.

Dell partnered with Cloudera to create the Dell | Cloudera Solution, comprised of Cloudera's distribution of Apache Hadoop ([CDH](#)) running on optimized Dell PowerEdge C2100 servers, delivered with joint service and support. The Solution includes the [Crowbar](#) software framework, a Dell-developed software to speed and ease bare-metal deployments. The Solution also includes a reference architecture and a detailed deployment guide. The combined resources of Dell and Cloudera helped SecureWorks accelerate the deployment of a robust Hadoop environment by more than six months, Scudiere said. These resources also helped the organization slash its cost of storage—thanks in particular to the built-in economies offered by PowerEdge C2100 servers at the core of the environment.

Dell PowerEdge C servers provide a low cost, easily managed, easily maintained platform to run Hadoop, which is designed to work with industry standard hardware. While offering a solid hyperscale design and a good balance of disk, memory, and cores, PowerEdge C servers do not have some of the features found in more conventional servers such as extensive systems management.

### **Impact: Reduced TCO**

“The PowerEdge C2100 server has been great,” Scudiere said. “It’s provided us with a fantastic price/performance curve. As an example, our storage cost per gigabyte is ~\$0.21. We thought we had great economics previously when we were spending about \$17 per gigabyte. When you look at the volumes of data that we currently have, it has been a great win for us from an economic standpoint to drop that cost to ~\$0.21.”

Those cost advantages can grow over time as SecureWorks moves more of its systems to the PowerEdge C platform running CDH, Scudiere said. “We expect the entire investment for this initiative to have about a one-year payback as we look to retire much more expensive storage solutions in our environment.”

Looking ahead, Scudiere sees ongoing savings as SecureWorks continues to scale out its global data centers to accommodate ever-larger amounts of data. “The data in our business doubles about every 18 months. And so as we think about expanding over the next three years based on the growth numbers we’re expecting from being part of the larger Dell organization, there can be significant cost savings for us as we scale out.”

### **Impact: High Scalability, Low Risk**

Fast time-to-market and dramatic cost savings are just chapters in a larger story of business benefits. The Dell | Cloudera Hadoop Solution is also helping Dell SecureWorks reduce the risk that comes with the deployment of new technologies, maintain high availability for critical security systems, and gain the cost-effective scalability it needs to keep pace with rapid data growth.

“Our business is very much about data, and being able to use that information—both learned and applied—and turn it back into better protection for our customers makes all the difference,” Scudiere said. “With Cloudera’s Hadoop technology in the Dell reference architecture, we can cost effectively store, scale, and analyze that information.”

“We expect the entire investment for this initiative to have about a one-year payback as we look to retire much more expensive storage solutions in our environment.”

Robert Scudiere, Director of Engineering, SecureWorks

## About Cloudera

Cloudera is revolutionizing enterprise data management by offering the first unified Platform for Big Data, an enterprise data hub built on Apache Hadoop. Cloudera offers enterprises one place to store, process and analyze all their data, empowering them to extend the value of existing investments while enabling fundamental new ways to derive value from their data. Only Cloudera offers everything needed on a journey to an enterprise data hub, including software for business critical data challenges such as storage, access, management, analysis, security and search. As the leading educator of Hadoop professionals, Cloudera has trained over 40,000 individuals worldwide. Over 1,400 partners and a seasoned professional services team help deliver greater time to value. Finally, only Cloudera provides proactive and predictive support to run an enterprise data hub with confidence. Leading organizations in every industry plus top public sector organizations globally run Cloudera in production. [www.cloudera.com](http://www.cloudera.com).

---

[cloudera.com](http://cloudera.com)

1-888-789-1488 or 1-650-362-0488

Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA

© 2015 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.

cloudera-casestudy-dell-secureworks-102

