splunk>

CASE STUDY

# Children's Discovery Museum of San Jose Adopts Splunk 'Operational Idea Factory'


## Executive summary

With more than 150 interactive exhibits and programs, Children's Discovery Museum of San Jose (CDM) is one of the largest museums of its kind in the nation. Since its inception, CDM has welcomed millions of visitors and has offered new exhibits each year that respond to children's diverse educational needs. As a nonprofit, CDM faced challenges running its IT and security operations with limited staff and budget. Since deploying Splunk Enterprise, CDM has seen benefits including:

- Increasing protection from fraud and malicious security threats
- Reducing spam by 98 percent
- Saving thousands of dollars annually

## Why Splunk

Nonprofit organizations face many of the same challenges as their private sector peers. Within CDM, the IT department has broad responsibilities, managing everything from firewall and public web servers to its voice network and storage area network (SAN). Beyond that, security—especially messaging security—including guarding against unsolicited and fraudulent email, are critical priorities. Cybercriminals test vulnerabilities and are willing to attack any organization, even a children's museum.

CDM's IT Department has had to juggle all of these challenges with a limited staff of only four people: three technicians and a business manager. By partnering with Splunk4Good, which helps governments and nonprofits at all levels showcase the power of data, CDM is maximizing its budget and staff and can focus on its mission — instilling creativity, curiosity and lifelong learning in children. Speaking to CDM's adoption of Splunk Enterprise, Gregg Daly, visiting principal engineer, says, "I liked that you didn't have to be a database expert. I was able to collect, process and visualize data because of the intuitiveness of Splunk. We went from 0 to 100 with little external help."

### Industry

- Nonprofit

### Splunk Use Cases

- Security and fraud
- IT operations

### Challenges

- Limited resources and budget, typical of nonprofit organizations
- Lacked a solution that could provide holistic visibility into IT and security operations
- Concerned about security and fraud

### Business Impact

- Protecting from fraud and malicious security threats safeguards the museum's assets
- Reducing time to solve problems from hours to minutes maximizes staff productivity
- Eliminating underperforming systems saves thousands of dollars annually
- Reducing spam by 98 percent improves productivity and security

### Data Sources

- Syslogs
- Event logs
- Database transaction logs

### Splunk Products

- Splunk Enterprise

## Increased overall efficiency and 98 percent spam reduction

Over a six-month test install of Splunk Enterprise, CDM collected more than one billion event logs. While the volume is impressive, more important is the value CDM is getting out of those events. When a problem with a network, application or device occurs, there now is a single source for investigation. For instance, if there is an email server issue at a particular time, staff can do a time query in Splunk Enterprise. Asking very specific questions of Splunk software enables staff to solve problems in minutes instead of an hour required to diagnose a problem in the past.

Another daily diagnostic issue at CDM concerns physical disks in the SAN. CDM IT staff now get reports about issues with the SAN, such as which drive failed and how many spare drives are on hand. Using Splunk software is much more efficient; staff can knock out problems that used to take hours in less than 10 minutes.

As CDM began to learn more about how Splunk Enterprise processed and stored data, it began to experiment. The museum had a significant spam problem, and by looking at expressions and functions inside of Splunk software, it was able to reduce spam by about 98 percent after only a couple of weeks.

## Immediate operational visibility adds business value

Now that CDM has implemented Splunk Enterprise, IT staff can show management and the board of directors the business value of the software. Dashboards and alerts provide important visibility into IT and security operations. As an example, when someone tries to log in through the VPN gateway with the wrong password, staff members receive alerts and can act immediately. Splunk software has enabled CDM to identify the networks from which bad actors send traffic, what types of headers these bad actors will insert into the messages and more.

**"The donation from Splunk4Good is making our staff more efficient. We can now confidently tell the executive director 'we don't need more budget or more staff. We found a solution that has made us work better.'"**

**Gregg Daly**
**Visiting Principal Engineer**
Children's Discovery Museum of San Jose

"The donation from Splunk4Good is making our staff more efficient," Daly says. "We can now confidently tell the executive director 'we don't need more budget or more staff. We found a solution that has made us work better.'"

## "Splunk is an operational idea factory"

CDM has identified several other opportunities for quick savings as a result of its Splunk implementation. The museum eliminated front-end security filters for email and other services that had high error rates and weren't performing well. The museum made that discovery after its second week using Splunk software, and it will save several thousand dollars annually moving forward.

"Splunk is an operational idea factory in that you have the ability to think through a problem, ask questions related to that problem, and start building a workflow pretty much all at the same time," Daly concludes. "That is pretty dynamic in my book. I have very rarely run into a system where you can take parts of different types of information and build those into an information chain and experience a workflow."