

2008 Democratic National Convention Committee, Inc.



Securing the Democratic Convention with Symantec Solutions

To safeguard a critical decision-making process, the 2008 Democratic National Convention Committee, Inc. (DNCC) turned to Symantec for a comprehensive set of information security solutions to support the IT infrastructure of its 2008 convention. Results included no significant disruptions from security incidents, multiple threats detected and blocked, and streamlined, automated helpdesk resolution of 720 incidents in the convention's four days.

Choosing under pressure

Who should hold what is arguably the most powerful job in the world?

In late August, 2008, 5,000 delegates descended on a convention center in Denver, Colorado for four days—watched by 15,000 media professionals from 130 countries. The delegates would nominate the Democratic Party's candidate for President of the United States.

This was the Democratic National Convention, and it was Brook Colangelo's job as CIO of the DNCC to provide the technology infrastructure that would make the event work.

Choosing the right technology providers was critical. Months earlier, Colangelo had created the Democratic convention's first-ever IT security advisory council. "I wanted to work with people who could help us actively think about what security products and services we should deploy, and what threats we should be most concerned about," he says. Based on input from advisory council members, the DNCC chose Symantec as the Official Information Security Software Provider of the 2008 Democratic National Convention.

At the convention, there was much to protect. "I chose Symantec because of its diverse products and services," Colangelo says. "I had worked with Symantec products before, but this was my first experience with Symantec's professional service teams—and they became essential to us."

A single view of the action

The team needed a single overview of the entire security infrastructure. It deployed Symantec™ Security Information Manager as a foundation for comprehensive incident response, helping the team identify, prioritize, respond to, and review incidents and threats. Symantec Security Information Manager comprehensively monitored all critical assets from firewalls, hosts, virtual private networks (VPNs), intrusion detection systems (IDS), directories, and applications.

ORGANIZATION PROFILE

A tradition since 1832, the Democratic National Convention (www.demconvention.com) is run by the Washington D.C.-based Democratic National Committee (www.democrats.org). With 300 employees, the 2008 Democratic National Convention Committee, Inc. (DNCC) was responsible for the planning and execution of the 2008 convention.

INDUSTRY

Government: Federal

SOLUTION

Security Management

Data Loss Prevention

Data Protection

“The Symantec team was fantastic. We need teammates who understand, dive in, and make sure it all works. And that’s exactly what I got from the Symantec team.”

Brook Colangelo

CIO

Democratic National Convention Committee, Inc.

Altiris Helpdesk Solution automated and streamlined the handling of 720 incidents in four days.

“Altiris Helpdesk Solution provided some of the best service and support we’ve seen, with real-time metrics that helped our incredibly diverse service desk address all issues as quickly as possible.”

Brook Colangelo
CIO

Democratic National Convention
Committee, Inc.

Symantec also provided local and remote security analysts who optimized the Security Information Manager and reviewed incident activity 24x7 throughout the convention.

As an example, the Symantec Security Information Manager monitored a denial of service attack directed at a border firewall, coming from multiple IP sources around the world. Based on information provided by the solution, the security staff decided to null route the IP address. The traffic stopped immediately, avoiding a potential outage.

Eye on bots

Symantec Security Information Manager gets automated updates from Symantec’s Global Intelligence Network, providing real-time information on the latest vulnerabilities and threats occurring across the rest of the world. The Security Information Manager correlates this data with events from the many local security devices it is monitoring, helping the team prioritize. Of strong interest at the convention was a particular remote bot net site. Four of the machines within the convention center seemed to want to call the site at a consistent time for two days in a row. The team decided to track these calls by writing a custom rule for the Security Information Manager that would generate an alert if activity increased, which would indicate the infection was spreading. It did not.

The Security Information Manager also monitored Symantec Endpoint Protection, which was installed on network servers and all endpoints managed by the convention. The solution detected and quashed several malicious code infections. “It was critical that we had the Endpoint Protection solution turned on,” notes Colangelo.

Symantec Data Loss Prevention discovered, monitored, and protected confidential data wherever it was stored or used at the convention. “We were able to get actionable information within 30 minutes of setting up Symantec Data Loss Prevention,” Colangelo observes.

SOLUTION AT A GLANCE

Key Challenges

- Minimize disruption from threats
- Locate and protect sensitive information
- Streamline and automate helpdesk response
- Enhance resilience from data loss or corruption

Solution

Centrally monitored, hardened network and information security with automated helpdesk

Symantec Products

- Symantec™ Security Information Manager
- Symantec™ Endpoint Protection
- Symantec™ Data Loss Prevention
- Altiris™ Helpdesk Solution
- Symantec Backup Exec™
- Symantec Backup Exec™ System Recovery Server Edition

Symantec Services

- Symantec Consulting Services

Technology Environment

- Applications: Custom voting application, Microsoft Exchange Server 2003, BlackBerry Enterprise Server
- Databases: Microsoft SQL Server 2005
- Server platform: 20 HP ProLiant DL380 servers running Microsoft Windows Server 2003
- Storage: HP StorageWorks EVA SAN

Business Results

- No significant disruptions from IT security incidents
- Multiple threats detected and blocked
- Faster helpdesk resolution vs. previous convention
- 720 incidents resolved by automated helpdesk within four days
- Successful data and server backups and fast, successful data recoveries

“We had users lose data, and with the Symantec solutions we were able to rapidly find it, secure it, and restore it.”

Brook Colangelo

CIO

Democratic National Convention
Committee, Inc.

Altiris wins friends

Altiris™ Helpdesk Solution, an automated incident management tool, tracked over 720 incidents, and all but five were closed. “Altiris Helpdesk Solution provided some of the best service and support we’ve seen, with real-time metrics that helped our incredibly diverse service desk address all issues as quickly as possible,” Colangelo says. “It delivered a much faster resolution and better user experience than we had with a simplistic email-based helpdesk at the 2004 convention.”

The IT team also used Symantec Backup Exec™ for disk-to-disk backup of a terabyte of information, and Symantec Backup Exec™ System Recovery to capture live images of the convention’s 20 servers, enabling them to be quickly restored if necessary. Notes Colangelo, “We had users lose data, and with the Symantec solutions we were able to rapidly find it, secure it, and restore it.”

Symantec teamwork

As history recorded, the convention was successful—and so was its information security architecture. “The Symantec team was fantastic,” Colangelo reports. “All of them had just an incredible level of commitment to the project. We went from 20 to 2,000 plus users in a matter of days. We can’t keep providing detailed, succinct requirements. We need teammates who understand, dive in, and make sure it all works. And that’s exactly what I got from the Symantec team.”