Forward-Thinking County Government Enhances IT Security and Manageability

Company: Fulton County, State of Georgia
Web Site: www.co.fulton.ga.us
Customer Size: 5,000 employees
Country or Region: United States
Industry: Government

Company Profile

Through a workforce of 5,000 people in agencies, airports, fire stations, police stations, courts, and libraries, Fulton County serves nearly one million people in northwest Georgia.

Software and Services

- Windows Server® 2008
- Windows Vista®
- Windows® XP Professional SP3
- Microsoft® System Center Operations Manager 2007
- Microsoft System Center Configuration Manager 2007

Hardware

- HP ProLiant DL340 servers
- Dual-Core Intel Xeon processors

For more information about other Microsoft customer successes, please visit:
www.microsoft.com/casestudies

"We have reduced help-desk calls from an average of 20 per day for a user group of similar size down to just 5 per day—a 75 percent improvement."

Robert E. Taylor, CIO/Director of Information Technology, Fulton County

The Fulton County IT department is responsible for thousands of computers across dozens of government departments. Having faced network disruptions in the past due to noncompliant computers, the county needed a new security solution. In response, it is deploying Windows Server® 2008 to take advantage of Network Access Protection (NAP). After an initial deployment, help-desk call volume decreased by 75 percent, for a projected annual savings of more than U.S.$150,000 in maintenance costs.

Business Needs

The government of Fulton County serves a population of nearly one million in northwest Georgia. Its IT department supports 5,000 employees in 400 buildings, dozens of agencies, airports, fire stations, police stations, courts, public-health clinics, and libraries. Its mixed IT infrastructure includes mainframes, clustered servers, workstations, desktop computers, multiple operating systems, dozens of vertical applications, and a sophisticated network encompassing multiple topologies and protocols.

For Fulton County IT executives, such an infrastructure poses major challenges in terms of security and standards compliance. IT security was complicated by the sensitive nature of public-health and court documents, and was especially difficult within the libraries, whose 600-plus Internet-facing computers were vulnerable to outside attack. Even with a desktop firewall enabled, the county needed greater protection, as evidenced by virus attacks in 2003 spread via county-owned mobile computers.

"The Blaster virus brought the network to its knees," according to Robert E. Taylor, CIO/Director of Information Technology, Fulton County. "For four days nobody could get any work done, including jail

administrators, who were unable to book or release prisoners. This led to a serious PR situation and the threat of a major lawsuit."

Standards compliance was also a problem because Fulton County relied on a paper policy. "Standards enforcement and policy compliance were practically impossible without tying them into the larger administration of systems," Taylor explains.

Solution

Fulton County IT executives researched a more effective way to enforce client security and compliance policies, and found the Network Access Protection (NAP) solution. They saw that with NAP, administrators could tackle three vital challenges: One, they could customize health policies to validate computers' health before allowing them to access the network. Two, they could automatically update policy-compliant computers. Three, they could confine noncompliant computers to a restricted network until they become compliant.

Once they decided to investigate a NAP solution, Fulton County IT executives needed to evaluate the technologies that can be used to enforce NAP. They started by evaluating NAP with Dynamic Host Configuration Protocol (DHCP)–based enforcement, because they were using a DHCP server to manage their IP addresses. But DHCP enforcement did not meet the security requirements of the network because of the possible use of static IP addressing, which can bypass a DHCP deployment. They also evaluated 802.1X-based enforcement, but decided against it as well.

Then they evaluated NAP with IPsec enforcement, a solution that is built into the

Windows Server® 2008 operating system. They liked the support of IPsec for isolation of problematic clients and for encryption that is compliant with HIPAA regulations. Fulton County decided to deploy NAP to all clients on its IT infrastructure. To support NAP, the County is deploying Windows Server 2008 on its servers, and the Windows Vista® or Windows® XP SP3 operating systems on desktop and notebook computers.

As part of the project, Taylor and his team developed and deployed a Domain Isolation solution that put all clients into a single logical network domain. Next, they deployed Windows Server 2008 and Windows Vista to a test bed of three servers and 300 client systems, respectively. Taylor and his colleagues intend to deploy Windows Server 2008 to all the county's 200 servers by the second quarter of fiscal year 2009. They also will deploy Windows XP SP3, to the 90 percent of clients that run Windows XP SP3.

To help enforce security updates on the Windows XP SP3 clients, they will use Microsoft® System Center Operations Manager 2007 management packs and System Center Configuration Manager 2007 reporting tools. As Taylor says, "We anticipate that System Center Configuration Manager will help us implement NAP very smoothly."

Benefits

After six months of the test deployment of NAP, Windows Server 2008, and Windows Vista, Taylor and his colleagues have observed an improvement in security standards compliance, an easier approach to standards enforcement, and an increase in system uptime that helps to maintain their focus on business deliverables.

Stability up, help-desk calls down. Among client users, stability is noticeably higher, with fewer problems caused by malware attacks. "We have reduced help-desk calls from an average of 20 per day for a user group of similar size down to just 5 per day—a 75 percent improvement," says Taylor.

Automated compliance. Instead of the cumbersome, paper-based policy of the past, Fulton County is using NAP to enforce standards, policy, and system-health compliance. As a result, the county has been able to reassign two full-time maintenance staff members to new technology initiatives, resulting in IT maintenance cost avoidance of U.S.$157,000 annually.

Real-time reporting. The county will further automate compliance with the reporting tools in System Center Operations Manager 2007, which will be built on top of the NAP platform. "Using System Center Operations Manager 2007 reporting tools, we will know immediately whether a client is in compliance," Taylor says. "This will help us save money and improve the level of service we can offer to users and citizens."

A powerful and agile platform. For Taylor and his team, the impressive gains of the NAP test deployment mark the start of something much, much bigger. "With Windows Server 2008 and the integrated System Center technologies, we will achieve a more integrated, manageable, and available infrastructure," Taylor says. "This will bring us not only cost-control and productivity advantages, but also the agility necessary for building innovative solutions, such as a countywide migration to VoIP that is already underway."

Microsoft