CASE STUDY

Clark County School District

CCSD
CLARK COUNTY
SCHOOL DISTRICT

The Customer: The sixth-largest school district in the United States, Clark County has more than 315,000 students, 36,000 staff and 357 schools.

The Challenge: Replace an aging BIND solution that was consuming too much staff time and tying IT experts up with mundane tasks, and protect an increasingly open network from security threats

The solution:
• Infoblox appliances
• DNS and DHCP
• DNS Firewall with DNSSEC

The results:
• Seamless installation
• Less burden on key IT staff
• Protection against DNS- exploiting security attacks

The Customer

This is how Superintendent Pat Skorkowsky describes the Clark County School District's approach to technology:

"As society and the needs of our students change, we must be prepared to meet students where they are and assist them with navigating the rapidly changing world in which they live. In fact, we must go a step further, preparing them to succeed today with tomorrow's tools. A key component is accepting and utilizing technology in the classroom and at home."

As a result of this philosophy, the Clark County School District has been recognized as one of the top 10 districts in the country for digital collaboration.

The Challenge

Key players in making the vision a reality are Chris Squatritto and his Technical Resources group. According to Squatritto, his team's goal is to "blanket the district with the high-quality technology services that the students need in order to learn."

"That's a moving target in education, especially now," says Squatritto. "Today it's Internet access, mobile devices, and Wi-Fi. Tomorrow it will be even more technology to help individualize learning. And we have to do this in a time when funding is tighter than ever and enrollment is at an all-time high."

One obstacle to hitting that target was the district's 15-year-old BIND system, which didn't give the IT staff the agility and efficiency it needs. One problem was that Squatritto was one of the only two people who knew the BIND system well, and his time is required for more strategic work than managing Domain Name System (DNS) records. He wasn't the only one who was putting too much effort into mundane tasks. The BIND system required a lot of manual processes that kept other members to the Technical Resources group tied up.

The Solution

Squatritto decided to replace the BIND system with Infoblox DNS and DHCP management tools because of Infoblox leadership in DNS management and because of the solution's extensive automation. "Infoblox is a respected player in the DNS space," he says, "and an Infoblox solution would allow us to automate the process and make it as simple as possible." This would save time and, as a bonus, eventually allow Squatritto to delegate some of the work to other groups.

Squatritto also implemented Infoblox DNS Firewall—which prevents DNS-exploiting malware from launching distributed denial of service (DDoS) attacks or ex-filtrating sensitive information—along with the Infoblox solution for automating Domain Name System Security Extensions (DNSSEC), an important industry specification for adding security to DNS.

"I'm a proponent of multiple layers of security," he says. "Nothing catches everything. You need multiple defenses for incoming and outgoing email, end points, firewalls, and so forth. So DNS Firewall is an important layer of protection. Infoblox is ahead of the game on DNS vulnerability, so it makes sense to use their solution for that particular layer of safety and security."

The Result

Squatritto engaged Infoblox Professional Services to help with the rollout, and the installation went quickly, partly because his team is well-versed in DNS. "There were a couple of hiccups around the way the Infoblox solution handles records," he says, "but once we worked them out, it makes a lot more sense than the way BIND handles them."

With the Infoblox DNS solution in place, it is much easier for Squatritto's group to edit and maintain records. They have better visibility into DNS status and processes. And strategic initiatives no longer have to wait while key staff—including Squatritto—perform mundane tasks, because less experienced staffers can be easily trained. Eventually, Squatritto says, he will take advantage of Infoblox's granular role-based access control to delegate this work outside the Technical Resources group.

He is also satisfied with the security part of the solution. "Infoblox DNS Firewall isn't designed to prevent bugs from coming in," he says, "and we have had a couple. But what it does is prevent the bugs from calling out to communicate with command-and-control servers. This is automatic, so we don't have to have a full-time person monitoring the DNS queue."

Currently, Infoblox is running DNS for the entire district, for both internal and external clients.

"I like Infoblox for DHCP and DNS," he says. "and I do see the advantage from a management perspective of having the whole district on one IPAM system."

For more information, please contact your Infoblox representative or visit www.infoblox.com