

Success Stories



Emergency Notification Service Provider Improves IT Accessibility, Security with Move

Dialogic Communications Corporation

An emergency notification company uses Raritan solutions to strengthen security and reduce mean-time-to-repair, even as it expands into remote and disaster-recovery data centers.

Dialogic Communications Corporation (DCC) is a leader in emergency notification solutions with a strong base in the nuclear power industry. DCC solutions alert critical personnel by phone, fax, pager, SMS and e-mail with user-defined, interactive messages in the event of user-defined conditions. These solutions are offered as turnkey packages or as hosted applications.

In addition to mission-critical notifications, other DCC services include applications like conference-call setup and administration. Here, the service dials out to preconfigured groups of participants at set times, or upon a group leader's request. DCC's platforms bridge the call and also keep logs of conference attendance. DCC also offers IVR (interactive voice response) applications that dial out, send notifications and receive touch-tone responses in turn; these logged responses confirm that the right personnel respond to emergencies. All applications require constant, frequent updates as clients' notification needs change.

DCC's clients have a choice of several hosting models, which include completely dedicated IVR/notification systems, shared systems, and those that are hosted by DCC, but are managed and maintained from the client site via the Internet. Depending on the customer, DCC also performs data management services as well.

IT Infrastructure

DCC's hosting business is now expanding and moving from one data center at their Franklin, Tenn., headquarters to a Sungard colocation facility 30 miles away, as well

The Challenges:

Moving to an off-site data center without incurring access delays, port blocking, security holes, or cost overruns.

Solution Components:

CommandCenter® Secure Gateway 2.2

Paragon® II KVM switches

Paragon II System Controller (P2-SC)

IP-Reach® KVM-over-IP gateways

Dominion® KX KVM-over-IP switches

as to a disaster recovery site hosted by AT&T, 1,500 miles away in Phoenix. Servers running office support applications will remain at Dialogic Communications headquarters, but the bulk of 120 hosting servers, 99 percent of them Wintel-based, are making the move.

Challenges

Bill Kirby, Manager of Hosting Center Operations at DCC, has primary responsibility for the center's infrastructure and support, maintaining regular access to servers for a staff of 12 administrators. He also provides access as needed for a team of developers. Kirby emphasized that he could not begin to make the move off-site until he was confident that real-time accessibility, security and mean-time-to-repair would not only not take a hit, but actually be improved as a result of the move.

"Sometimes customers have really short time frames for making system changes on the servers," says Kirby. "I needed to make sure that the new remote KVM solution would not impose any port blocking so that the actions of some of my staff would not affect others."

Success Stories - Dialogic Communications

He also needed to be sure he could provide both his system administrators and his customers with secure remote access to only those servers that they were authorized to access, and isolate them from other parts of his network.

And finally, he had to do this within a finite budget. Giving his staff remote access to configure and administer servers, he had to avoid excessive trips to the off-site facility. He had to manage the cost of the move, manage the use of space in the collocation cage, and avoid colo-site charges for simple operator assistance there - charges that can bite deep into the savings of colocation.

Inescapable security checkpoints

Back in February 2004, Kirby had chosen Raritan's Paragon II Cat5 KVM switches for the headquarters data center because the non-blocked architecture of the Cat5 analog switch provided always-available, instant access: "The Paragons just gave me the ability to insure that all of my people could get to any server at any time."

When it came time to plan and implement the move, Kirby purchased Raritan's CommandCenter Secure Gateway (CC-SG) and Paragon II System Controller (P2-SC). These additions allowed him to maintain his SLAs during the move and after, while the Paragon II switches provide the video performance and tight mouse synchronization that Kirby and his users need, CC-SG gives his users a centralized, inescapable security checkpoint. In addition, CC-SG provides Kirby with authentication, authorization, and accounting via integration with DCC's Active Directory servers, with failover to CC-SG's own internal authentication database.

Finally, CC-SG's logging is now an essential element of DCC's security policy. Kirby gets access logs from both his VPN server and CC-SG, "which really gives me a good paper trail. I know who, when and from where someone logged onto a server. And the logs aren't stored on the server, they're stored in CommandCenter Secure Gateway, so very few people can actually change them. It's a way to prove to customers that we can track what happens to their service, and that we take that very seriously."

"CC-SG was a must for us, for the Active Directory authentication piece, and the logging piece," says Kirby. "And the key thing that allowed me to move forward with this was the P2-SC." The Paragon II System Controller (P2-SC) is the intelligent interface that integrates his Paragon KVM switches under CC-SG control.

No open firewall ports

The combination of Paragon, P2-SC and CC-SG gives Kirby the bulletproof security he was looking for. "We can tighten the perimeter around the network, and the only access in and out is through the CommandCenter Secure Gateway," says Kirby. "We don't have to have ports open on the firewall for pcAnywhere or any other type of remote desktop software. For extra precaution, however, Kirby has his users VPN onto the network before they can reach DCC's CommandCenter: "You can't access our CommandCenter from the outside world," he says.

In addition, Kirby adds a third layer of security by putting CC-SG and IP-Reach and each customer system in a separate VLAN. This is possible because all KVM communications are maintained "out of band." So when authorized users VPN into the network, the only devices they see are the CommandCenter Secure Gateway and the IP-Reach. They can only access the servers via KVM console; they have no direct access to them, limiting the possibility of spreading malicious code from a compromised workstation to the Hosting Center environment.

Paragon's analog architecture provides yet a fourth layer of security. "Whenever you go from Paragon back to the servers, there's no way you can hack that connection. You can't get to the other boxes from the Paragon, so it secures up my network really nicely. It's just totally safe and secure. And I like that."

Since the initial installation, Kirby has added a Dominion KX KVM-over-IP switch at the corporate site. This KVM switch controls servers that are installed on an isolated network segment for security reasons. This group of servers is used by his support staff to access and maintain DCC application servers that are not physically hosted at

one of DCC's hosting facilities. The Dominion KX switch itself is connected to a network segment that is visible to, and therefore accessed through, CC-SG.

Kirby is now considering Dominion SX serial console servers, to be able to shut down another avenue into the network: the Telnet and SSH sessions that admins now use to manage switches, routers, and other serial devices. The Dominion SX will incorporate those sessions, but will provide one secure point of control to manage up to 48 serial servers and other IT devices.

CommandCenter Secure Gateway also simplifies DCC's security measures by reducing the number of IP addresses administrators need to remember. "You used to have to carry a list of all the IP addresses of all the servers, all the passwords and user names. That's a security problem right there, because if someone gets their hands on that list, they have everything," says Kirby.

"This way, there's just one IP address you have to know along with just one user name and one password, and because it's integrated with Active Directory, maintenance is simplified. Every server you want to get to is listed right there in the CommandCenter Secure Gateway. We can even shorten our password change policy without adversely impacting my support staff, because there's just one password to remember. It's helped me in a lot of ways."

Self-sufficiency in colo sites

Kirby needed to be sure that incident response times would not increase when he moved the data center off-site, and he knew that software-only remote management solutions wouldn't serve the purpose. Paragon II's non-blocked architecture gave him some assurance, since any administrator would be able to access any server at any time. The KVM switches' BIOS-level access was also very important. Kirby: "If a system is acting up, it's kind of scary to reboot that server when you can't see what's happening throughout the complete boot cycle. When a server comes back up, the information in the BIOS post screen can often tell you what the problem is. Seeing

our system in all of its states - not just after it's up and running through a PC Anywhere screen - gave us the necessary comfort level we needed to perform our remote maintenance."

BIOS-level access also gives Kirby the self-sufficiency he needs to make changes and repairs immediately, and not have to wait until the staff at the colocation facility can fit it into their queue. This is in sharp contrast to their disaster recovery site in Arizona, where they have not yet deployed the Raritan solution and are using Windows Terminal Services and pcAnywhere to remotely manage the servers.

"The colocation facility has on-site support that we call if we need a button pushed or something physically done to the servers. Every time Terminal Services or pcAnywhere stop working, we've got to call them to go out there and troubleshoot our remote management software problems. More than once we have had to stop our troubleshooting efforts while we wait for remote hands to fix a hung terminal session. That is a problem." Kirby looks forward to extending the Raritan solution to the Arizona disaster recovery site.

Kirby also agrees that CC-SG's single sign-on and consolidated interface gets his admins "to the scene" more quickly. "There's a URL you hit, you enter your user name and password, and bang, you're in. All of the devices in your infrastructure are available to you. My group is very broadly deployed. All of us need to see everything. We can sort by name or application, and get to the device we need in certain areas so much quicker."

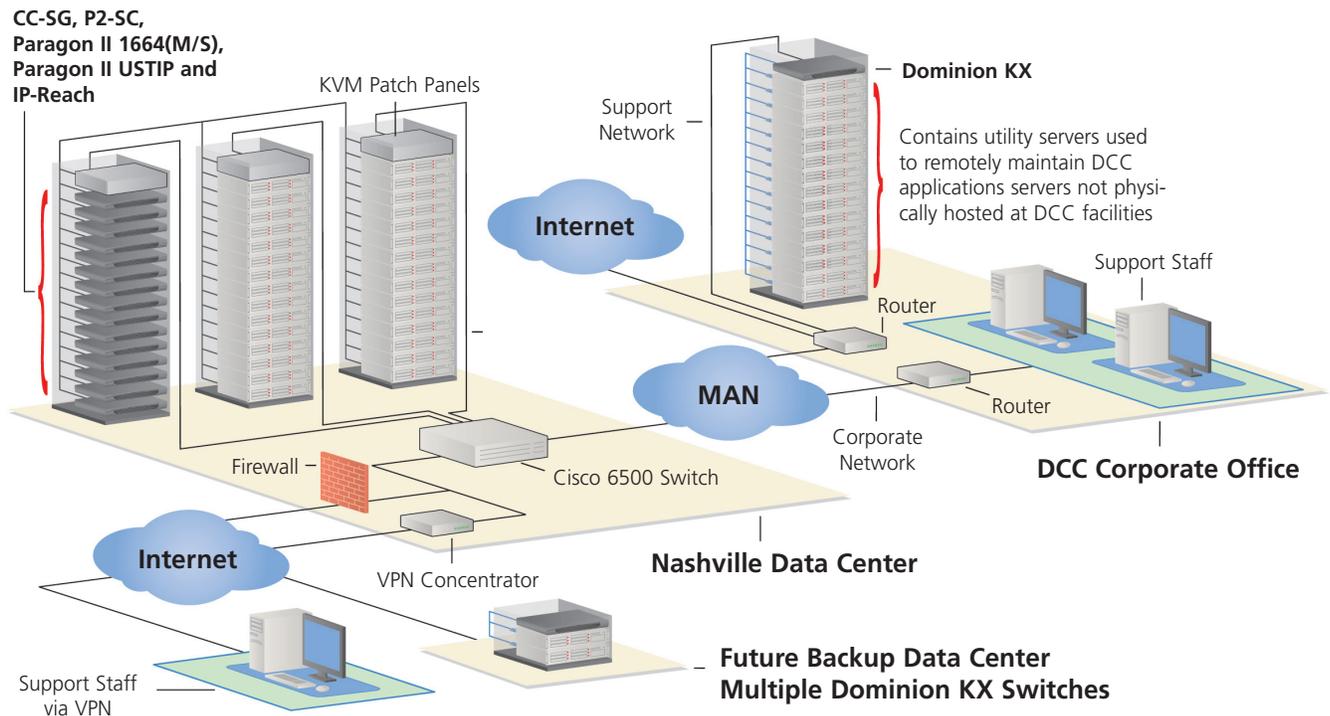
He can also get to either of his two sites: "That was the piece that CommandCenter Secure Gateway bought me. It gave me the single sign-on, and the ability to manage multiple data centers from a single interface." Another major benefit: collaboration between multiple people actively working on a single problem at the same time using the PC Share functionality. "We had three people collaborating on the same problem last night, which is something we couldn't do with pcAnywhere or Terminal Services."

Success Stories - Dialogic Communications

Saving Operational Costs

Secure, remote management of both sites will obviously save DCC time and money on travel. It also costs money to use on-site help at the collocation and disaster recovery sites, which Kirby saves now at Sungard and expects to save when Raritan's KVM solutions get installed in his Phoenix site. He is now looking at adding Raritan's remote power control (RPC), as well as Dominion SX secure serial console servers. The remote power control, which is integrated into the CommandCenter interface, will eliminate his need to call for on-site hands to reboot servers. (SX, as noted, will end his need to open ports for Telnet and SSH.)

Finally, asked if Raritan's equipment has been important in helping him move efficiently, Kirby goes quite a bit farther: "I don't think the move to the remote data center would have been possible without it. The data center's about 30 miles from where we are right now. If I didn't have this capability, I don't think I would have been as willing to buy on to collocating all of our systems."



Raritan is a leading supplier of solutions for managing IT infrastructure equipment and the mission-critical applications and services that run on it. Raritan was founded in 1985, and since then has been making products that are used to manage IT infrastructures at more than 50,000 network data centers, computer test labs and multi-workstation environments around the world. From the small business to the enterprise, Raritan's complete line of compatible and scalable IT management solutions offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to simplify the management of data center equipment, applications and services, while improving operational productivity. More information on the company is available at Raritan.com.

© 2006 Raritan, Inc. All rights reserved. Raritan, CommandCenter, Paragon and Dominion are registered trademarks of Raritan, Inc. in the United States and/or other countries. All others are trademarks of their respective owners.