

PaeTec Communications Increases Security and Reduces Administrative Overhead with DirectControl



"The time it has saved in both setting up and removing user accounts has made DirectControl worthwhile."

- Ted Sanfilippo, Manager of Network Engineering

PAETEC

Communications, Inc., provides integrated communications services, including local and long distance voice, data and Internet, software applications, network integration, and managed services. PAETEC currently supports medium-sized and large businesses, colleges and universities, hospitals, hotels, governmental organizations, financial markets, and affinity groups within its 29-market service area. The company is based in Fairport, N.Y.

> 1000 Employees

Environment:

- 50 UNIX Solaris & Linux Red Hat
- 30 in-house admin/users

Challenge: Increase Security and Reduce Costs

PaeTec has a commitment to first-rate customer service at all levels, and to ensure that quality experience, it has grown its IT infrastructure to provide ISP and hosting capabilities for its customers.

As new systems were added, it became too cumbersome to add unique accounts for each of the administrators; so in order to streamline deployment PaeTec system administrators would occasionally share accounts and root passwords. This practice benefited customers by getting systems up fast and ensuring that a cadre of qualified people was managing all aspects of the environment. But when an administrator would leave the company, it became disruptive for the remaining organization. They had to touch every system to be sure that they removed all of the administrator's accounts from each system. It could take three hours in order to be positive they had discovered and removed all accounts. And all the root passwords would have to be changed (and relearned).

The system depended on the integrity of its administrators to protect information, and though that trust has remained intact, PaeTec looked for a way to increase their security without adding time-consuming overhead.

Cost Savings: Leverage Active Directory and DirectControl

They wanted to centralize user name and access control and decided that Centrify DirectControl would meet their needs. By installing DirectControl on each of the 50 servers, they have been able to centralize all of the administrators' UNIX/Linux user accounts within Active Directory. Now, when an administrator leaves the company they can eliminate all of the accounts in 30 seconds—confident that all access has ended—without disrupting the other users. As new systems are added, authorizations can be granted in Active Directory so that the first time an administrator logs into a new system with DirectControl installed, they are authenticated through AD and a home directory is created for them on the new system.

“The time it has saved in both setting up and removing user accounts has made DirectControl worthwhile,” said Ted Sanfilippo, Manager of Network Engineering. “Now we can log all access on all systems in a central place.”