Interoperability by Design at Microsoft
Customer Solution Case Study

Software Firm Eases Compliance, Improves Security by Linking Heterogeneous Systems

Customer: Centrify
Web Site: www.centrify.com
Country or Region: United States
Industry: Professional services--IT services

Customer Profile
Centrify's auditing, access control, and identity management software solutions centrally secure heterogeneous systems, Web applications, databases, and storage systems using Active Directory®.

Software and Services
- Windows Server® 2003 Enterprise Edition
- Technologies
  - Active Directory®

For more information about the Interop Vendor Alliance, please visit:
www.interopvendoralliance.org

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

> "Centrify allows customers to move toward a secure, connected computing environment in a cost-effective manner by elegantly extending a technology they already have—Active Directory."
>
> Tom Kemp, President and Chief Executive Officer, Centrify

Today's businesses face new regulatory pressures to integrate and centrally manage heterogeneous computer systems. Centrify is a leading security software vendor that uses Active Directory® as the core of its auditing, access control, and identity management software solutions. With Centrify solutions, companies are able to centrally manage diverse systems, comply with data security regulations, and increase staff efficiency.

Business Needs

Many businesses today use a wide variety of technology solutions, including Windows®, UNIX, Linux, and Mac operating systems; Microsoft® SQL Server™, Oracle, and DB2 databases; Microsoft, Apache, and WebSphere Web applications; and a variety of storage solutions. IT management needs multiple specialists to integrate and manage such environments, and users have to remember multiple user names and passwords.

"Heterogeneous environments can be inefficient for both IT departments and users," explains Tom Kemp, President and Chief Executive Officer of Centrify, a Mountain View, California–based company that makes interoperability solutions. "IT staffs invest huge sums integrating and managing heterogeneous environments and supporting users. And employees spend a huge amount of time every day logging in and out of different applications, which is an inconvenience and a drain on productivity."

However, the biggest challenge to companies with heterogeneous environments is a host of new federal and industry regulations, such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry's Data Security Standard, which require that businesses audit access to systems, applications, and data. "There's huge pressure for organizations to figure out

interop VENDOR ALLIANCE

how to audit their diverse IT environments to meet regulatory deadlines," Kemp says.

Closely related to the difficulty of auditing heterogeneous environments is the difficulty of securing them. Users tend to write their multiple passwords on notes that they stick to their computer monitors, or to forget them. Employees who leave the company sometimes still retain access to key systems, because it is difficult for the IT staff to keep tabs on the myriad islands of identity.

Solution

Kemp and others founded Centrify in 2004, to create software solutions that make a heterogeneous environment look, feel, and act as if it were a homogeneous environment from an auditing, access control, and identity management perspective. "Achieving this goal with proprietary technology would take years to develop and deploy and cost bundles of money," Kemp says. "Instead, we allow customers to move toward a secure, connected computing environment in a cost-effective manner by elegantly extending a Microsoft technology they already have—Active Directory."

Organizations can use Active Directory®, an essential component of the Windows Server® 2003 operating system, to centrally manage and share information about network resources and users and to act as the central authority for network security. Centrify chose the Microsoft directory service as the foundation of its interoperability solution because of its feature-rich design, its support for both the Lightweight Directory Access Protocol (LDAP) and Kerberos security standards, and its significant installed base.

"By building our products on top of Active Directory, we're able to deliver a solution that's easy to evaluate and deploy," Kemp says. "Using our software, customers are able to integrate hundreds of heterogeneous systems, typically in a week or two. Accomplishing the same thing with proprietary solutions would take months."

Using Centrify DirectControl, organizations can secure UNIX, Linux, and Mac operating system computers using the same authentication services deployed for their Windows® environments—and allow those users to participate in an Active Directory domain. The Centrify DirectAudit suite complements DirectControl by delivering auditing, logging, and real-time monitoring of user activity on non-Microsoft systems.

In 2006, Centrify joined the Interop Vendor Alliance, a community of software and hardware vendors working together to enhance interoperability with Microsoft systems. "Participating in the Interop Vendor Alliance with other vendors helps us respond to our mutual customers' needs and make it straightforward for customers to see the many ways that the vendor community can help them manage a heterogeneous environment," says Kemp.

Benefits

By deploying Centrify's Active Directory–based products, customers of all sizes across many industries have met an array of regulatory requirements, improved the security of their data, and boosted the productivity and efficiency of their staffs. Centrify products offer:

- **Easier regulatory compliance.** One publicly traded company uses DirectControl to bridge "islands of identity" across Windows, Sun, UNIX, Linux, and other systems. "When the SOX auditors looked at the access controls to this company's systems, they were well covered with Centrify," Kemp says. "They could print a DirectControl report showing which individuals had access to each system and when."

- **Improved security.** Another customer, in financial services, had to make sure its environment was highly secure to safeguard confidential financial transactions. The company used DirectControl to simultaneously simplify and tighten access to business applications, and DirectAudit to monitor user access to those systems. "This customer replaced lots of manual auditing processes with automated reports, which saved time and money," Kemp says.

- **Increased user and IT efficiency.** Another customer used to have six people spending dozens of hours each week on server administration; one person now completes the work in seconds using DirectControl. Yet another customer, a startup with limited resources, wanted to efficiently manage a data center that contained 700 Linux and Windows-based server computers. Every time an employee left the company, an administrator had to log on to each server to disable the employee's access. This customer was able to save three-quarters of an employee per year in personnel costs by using DirectControl. "This customer saved a great deal of administrative and password reset time," Kemp says. "This is time they're now able to devote to setting up new business systems."

This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Document published June 2007