

Case Studies

Top 3 US Drugstore Chain

Problem: Become PCI compliant, without reconfiguring the network, to avoid mounting fines

- \$50,000 monthly fine for not being PCI compliant which was about to be \$100,000 monthly fine
- no audit trail or ability to match controls to specific users

Results: Immediately PCI compliant; ROI within three months

- leveraged existing technology infrastructure investment and removed the need to replace costly POS systems
- provided a complete identity-based audit trail and proof of controls
- centralized management improving operational efficiency



Top 3 US Bank

Problem: Provide secure access to thousands of remote vendors and suppliers

- no containment of users to authorized resources
- IT resource intensive, cumbersome and ineffective access controls
- no audit trail or ability to match controls to specific users

Results: A unified, easy to manage appliance

- thousands of business critical 3rd parties now granted secure, controlled access
- increased operational efficiency with a single solution
- provided an audit trail for internal security requirements and external compliance mandates



“What is so special about you --- ‘containment, containment, containment.’”

VP Remote Access, Top 5 Financial Institution

Case Studies

Department of Homeland Security

Problem: Consolidate & grant secure access to 21 geographically dispersed data centers

- centralize access control across agencies with distinct missions
- ensure contained and auditable access
- meet federal compliance requirements (FDCC)



Results: Control over privileged users and critical infrastructure and assets

- tight control over who gets access to what, when and for how long
- contain users from the 21 sites to authorized systems only
- audit quality logging for compliance

“With Xceedium GateKeeper we have an all-in-one solution for these higher risk users which gives us the peace of mind that we are meeting our objectives to safeguard our network and the sensitive information it contains.”

Security Expert, Department of Homeland Security

Bert Fish Medical Center

Problem: Provide hospital personnel, physicians and 3rd-party vendors HIPAA compliant access to critical systems and devices

- work within a limited budget
- need to ensure segregation of duties once access was granted
- no audit trail or ability to match controls to specific users



Results: Automated, cost-effective HIPAA compliance

- tens of thousands in annual cost savings to hospital
- purpose-built, easy-to-manage solution versus previous IPsec VPN
- secure access to diverse groups inside and outside the hospital

“The granular control over user access minimizes the threat of data being destroyed or tampered with and helps us automate HIPAA compliance cost-effectively.”

Arch Beard, Information Security Officer, Bert Fish Medical Center