Case Study

Thin Client Solution Energizes NNSA's Cyber Security Measures

With responsibility for the Department of Energy's (DOE) classified networks, the National Nuclear Security Administration (NNSA) is vigilant in the application of cyber protection measures.

The use of classified removable electronic media (CREM) to store information presented a persistent security challenge to NNSA. When a federal mandate for increased cyber security was issued, DOE's chief information officer, in partnership with the NNSA, proposed conducting a thorough evaluation of commercially available thin client (diskless) technology to determine its viability in reducing either the intentional or unintentional mishandling of classified information. The agency's objective was to design and implement a diskless technology solution that would permit desktop IT functions to be performed without risk.

With diskless technology, there is no writeable disk space; data resides on a server in a controlled data center instead of a PC or desktop. A stateless boot device, used to connect a monitor, mouse, and keyboard to the network, provides access to the servers and Internet. Users must be logged in to access the data, and when they log out, the data is automatically stored on the server. Because the boot device does not have an imbedded operating system or internal storage, there are no operating system images to maintain and data cannot be transferred to the thin client. Additionally, USB ports are disabled in the BIOS, ensuring that data cannot be removed or tampered with.

Easy Integration Into Existing Infrastructure

Initially, NNSA engaged Energy Enterprise Solutions (EES) through its sub-contractor GTSI, a systems integrator and long-time partner, as the systems aggregator and integrator of the pilot CREM program. GTSI subject matter experts worked closely with NNSA's director of the newly formed CREM initiative to assess NNSA's needs.

Leading an in-depth review of commercially available products, GTSI evaluated hardware, software, power, cooling, and network components from multiple vendors. The selection of products, including those from Ardence, Cisco, Citrix, Clear Cube, Decru, Dell, HP, NetApp, LG, RSA, and Symbio, among several others, ensured that the recommended diskless technology solution met NNSA's requirements for security, reliability, deployability, certifiability, interoperability, and scalability.

Of primary importance to GTSI was how easily the components could be integrated into existing NNSA back-end infrastructure and their ability to meet specifications for:

- Transparent deployment and integration with NAS, DAS, IP-SAN, FC-SAN, and tape
- Wire speed encryption of data at rest for stored data protection
- Strong access controls, authentication, and tamper-proof auditing
- No application/database changes or downtime
- Native support for NFS, CIFS, iSCSI, Fibre Channel, and SCSI
- Operating system agnostic, no software agents required
- Secure, enterprise-wide, and lifetime key management

GTSI worked with NNSA and other vendors to develop a pilot diskless architecture that provided extended multi-functionality and allowed NNSA to add or decrease layers of security according to mission requirements.

DOE's Improved State of Security

After the pilot program was successfully completed, GTSI worked with NNSA to deploy the first production version of the architecture, and then continued to implement this turnkey, stateless thin client solution at other DOE and NNSA facilities, with full authority to operate in classified environments. As the DOE's partners of choice, EES and GTSI coordinated the efforts of 15 vendors and kept the program on schedule. Two GTSI team members received DOE's Award of Excellence for Outstanding Achievement.

The DOE NNSA diskless project was completed on time and within budget.

For more information contact GTSI Corp. at 800.999.GTSI or visit GTSI.com