

- **Strong Authentication** - Authentication provides assurance that the user/host requesting access is the entity it claims to be by requiring a name and password. USi also offers Strong Authentication to add another layer of authentication protection using one-time passwords such as physical tokens or private key/public key technologies like digital certificates and digital signatures.

- **Access Control** - Access control is the ability to limit access by user, host, and type of function.

"USi is at the forefront of the ASP service delivery model."

John Doe, VP of Operations, Client
Quote Example

USi implements access control to allow different users or hosts access to different capabilities, different amounts of information, or different types of information after they have authenticated themselves to the system.

- **Auditing/Logging** - Auditing/Logging provides information about use characteristics (including username, time of login and logout, commands, areas accessed, etc.) on each system. USi monitors this information in real time and stores it for research purposes. USi's Auditing/Logging procedures are in place and operational so that forensic information gathered from these systems can be admissible as evidence in court if required.
- **Operating System Hardening** - Operating System Hardening is configuring an operating system so that as many services and functions as possible are removed or disabled. USi implements Operating System Hardening to limit the number of potential avenues for an unauthorized attack. In addition, known "holes" or security vulnerabilities identified in security CERT (Computer Emergency Response Team) notifications and from other advisory organizations are patched in a hardened operating system. These precautions make it more difficult for hackers to access or disable a system.

- **Network Management** - Network Management is the 24x7x365 monitoring, troubleshooting, and support of a network. The USiView SM network management system is an innovative solution based on proven technology and a standard management approach to distributed environments. It consists of a unified method for providing configuration and change management; proactive monitoring of system-level events, processes, and thresholds; an event correlation facility that collects, processes, and responds to management event attacks, remote procedure attacks, service exploits, and unauthorized network traffic.

USi Total Security Architecture Delivers Total Security Solution

USi's combination of security expertise, architecture, and technology adds up to a total security solution for USi clients. USi's Total Security Solution includes:

- Highly qualified security experts and information security engineers led by a Vice President of Information Assurance
- Aggressive intrusion detection and vulnerability analysis program in conjunction with third-party assessments for validation
- Continuous 24x7x365 monitoring by experienced security personnel
- Ongoing operating system, application and database hardening, and tracking of vulnerabilities
- Use of proven, policy-based procedures along with the latest technologies to accurately track incidents, identify potential security breaches, and provide rapid, appropriate response

Together, USi's security features provide today's organizations with the capability to safely and reliably migrate their critical business applications to the web.

