

“...corporations may rest assured that their enterprise is secure, while their customers are being served.”



NSAi is an industry leader in ensuring best Security practices in the corporate enterprise. Our solutions seek to optimize risk management, balancing the cost of security solutions against the threats to your company's information. By providing security services for the whole business entity, NSAi's certified consultants will ensure a secure posture from the user-host level, to the critical services and beyond the network perimeter.

NSAi's Security services offer a proactive and secure environment where businesses can run operations at minimal or no risk.

By defining and enforcing a sound business-based security policy, corporations may rest assured that their enterprise is secure, while their customers are being served.

After a thorough assessment, NSAi's certified security engineers will recommend the necessary technical solutions to coordinate actual implementation with defined corporate policy. NSAi understands that some risk may be necessary for their clients to conduct business and makes all efforts to ensure utmost security with customer business as the key focus.

NSAi's world-class engineers conduct assessments to interpret the security posture of servers and network devices within a corporation's IT infrastructure. This provides vulnerability information and recommended solutions, which are crucial to the client whose data integrity is of utmost importance.

Crucial steps are taken throughout an NSAi security assessment. These steps include interpreting and enforcing corporate policies, analyzing the network infrastructure, identifying critical data and assets, and fortifying servers and network devices. These steps are followed up with timely and accurate reporting to ensure proactive responses to identified issues.

“Ensuring data integrity...”

Our security assessment customers gain invaluable insight into the security posture of their enterprise through eight categories of thorough analysis:

- Existing Security Design
 - Defined Corporate Policies – Enforcement
- Network Infrastructure
 - Perimeter, Internal LANs, Remote Access, VPN
- Components
 - Firewall(s), IDS, Encryption, Anti-virus
- Services
 - Applications and “external” business interaction
 - Web interface, Email
- Data Compartmentalization
 - DMZs, Collaboration Zones, (multiple levels of access / denial)
- Critical Assets
 - Servers
 - Ensuring data integrity through protection, uptime, and redundancy
- Management and Controls
 - Vulnerability detection, Protection, and Reporting
- Host Activity
 - Security practices among users and hosts
 - Patches, Critical updates, Identity enforcement

Businesses can make informed decisions based upon vulnerability assessments applied throughout their enterprise. We understand that security is an ongoing, reiterative practice that corporations need to continuously monitor and refine. Our engineers will recommend and implement an appropriate level of security defenses given your company's unique needs. NSAi offers complete security services, including security consulting and integration. In addition, training and technical support is available throughout this process, as well as follow-up support after solutions have been implemented. NSAi Security Engineers are certified and registered with the International Information Systems Security Certification Consortium (ISC2).



Network System Architects, Inc. (NSAi)

1550 Larimer St. Suite #222 Denver, CO 80202-1610 (303) 623-0035

<http://www.nsai.net>