



Network Security Services

Proactively address attacks on your IT network. Security plays a significant role in continuous availability by fending off attacks that can cripple your system and compromise compliance and auditing efforts. Create awareness and ensure security policies and procedures are implemented throughout your organization with a comprehensive service that is custom-designed to protect your network and data.

Key Steps and Deliverables

■ Network vulnerability audit

- Stratus audits your network, devices, servers and desktops during its Security Posture Assessment. This complete security snapshot of your network includes an:
 - internal assessment: a controlled network attack simulation is conducted yearly to gauge exposure
 - external assessment: a remote vulnerability scan is undertaken quarterly to quantify security risk associated with Internet-connected systems.
- Stratus delivers a detailed analysis of the simulated attacks. The report prioritizes vulnerabilities and includes appropriate remediation measures.

■ Network security policy review

- If you have a network design already in place, your current network security policies are assessed against industry best practices, including ISO 17799. You receive:
 - a collaborative review of your business strategy and related security goals, requirements and standards
 - identification and prioritization of security requirements including protocols, policy and feature improvements
 - network diagrams and sample configurations

■ Network security design

- Stratus creates a comprehensive network design optimized for scalability, redundancy and performance of all security components.

■ Network security design implementation

- Plans for testing, installation, configuration, integration and management are jointly developed with your IT team.
- The network staging plan includes physical and logical topography, configurations, test scripts and acceptance criteria. Onsite support is provided during the integration.
- We conduct a knowledge transfer for two staff members and provide recommendations for ongoing management and optimization.

Benefits

■ Prevent unauthorized access to vital information and systems

Ensuring security procedures and controls are in compliance eliminates the potential risks of data theft and system attacks.

■ Reduce costs and potential revenue losses

Adherence to compliance requirements reduces time and resources spent to audit the network and prevent losses due to a potential security breach.

■ Maintain business continuity

Protecting the network infrastructure from attacks ensures continuous availability and enables you to provide a higher level of service to users.

■ Ensure policy enforcement

Verifying and documenting network security policies and procedures demonstrates integrity of the network and the IT organization, enhances credibility and creates a culture of professionalism.

Duration

Initial internal assessment: 3 days

External assessment: 2 days (performed quarterly)



Risk
Avoidance



Cost
Avoidance



Optimize Service
Quality



Business Process
Optimization