



Server Security Services

Improve overall server security controls and align your security policies with business objectives. This three-step engagement provides a thorough review of current server policies and procedures against security best practices. Based on the audit findings, Stratus develops a remediation plan and implements a new design that optimizes server security and eases ongoing management.

Key Steps and Deliverables

■ Server vulnerability audit

- Stratus thoroughly reviews system security issues:
 - system policies
 - operating system security including vulnerabilities in OS and drivers
 - patch management procedures
 - malware protection
 - service permission policies and procedures
 - auditing policies
- To obtain a comprehensive server security picture, we also review account security issues:
 - password policies
 - authorizations and permissions
 - inbound and outbound policies and procedures
 - communication
 - encryption

■ Server security design

- Stratus availability advisors develop a remediation plan based on assessment findings, best practices and business needs to ensure minimum vulnerability and maximum availability.

■ Server security design implementation

- Stratus will execute the new server security design including configuration, testing and integration of the solution. Throughout the integration Stratus provides onsite support to ensure minimal disruption of the production environment. Stratus audit and design services are required pre-requisites for implementation.
- Two staff members will receive a security knowledge transfer. If in-house expertise is not available Stratus can provide ongoing server optimization and management.

Benefits

■ Protect Information

Unauthorized access to customer, employee and business data can cause operational and financial ruin. Improved security controls can virtually eliminate these attacks.

■ Balance security and protection against costs

Corporations cannot afford to assume their servers are secure. To protect the integrity and availability of business-critical information, it is imperative to periodically audit server security policies and procedures against current best practices.

■ Reduce system vulnerability and the risk of data loss

An intuitive, scalable solution for compliance management reduces the overhead associated with meeting today's strict regulatory standards. A well-designed solution can also help you control and lower ongoing compliance costs.

Duration

Based on number of servers: up to 26 hours for less than 20 servers



Risk
Avoidance



Cost
Avoidance



Optimize Service
Quality



Improve
Productivity