phoenixNAP®
GLOBAL IT SERVICES

Server Security Checklist

Secure Connections

□ Use SSH for secure remote access.
□ Change the default SSH port from 22 to a higher, non-standard port.

SSH Key Authentication

□ Implement SSH key pairs instead of passwords for authentication.
□ Store private keys securely and do not share them.

Secure File Transfer Protocol (FTPS)

□ Use FTPS for encrypted file transfers.
□ Encrypt files before transfer for additional security.

SSL Certificates

□ Install SSL certificates to secure web administration areas.
□ Ensure all web traffic uses HTTPS.

Private and Virtual Private Networks

□ Implement VPNs for secure remote access.
□ Use private networks for internal server communication.

Login Attempt Monitoring

□ Use intrusion prevention software.
□ Monitor and limit login attempts.

User Access Management

□ Disable root account SSH login.
□ Create limited user accounts to restrict user access based on roles and responsibilities.

Firewall Configuration

□ Install and configure a firewall to manage incoming and outgoing traffic.
□ Regularly review firewall rules and access controls.

Password Policies

□ Enforce strong password policies (length, complexity).
□ Implement two-factor authentication.

Software Updates

□ Regularly update all software to patch known vulnerabilities.
□ Test updates in a staging environment before deploying in production.

Remove Unnecessary Services

□ Disable or uninstall non-essential services to reduce the attack surface.

Data Backup

□ Perform regular backups of critical data.
□ Store backups offsite and test them regularly.

Hide Server Information

□ Adjust HTTP headers to hide software versions and system details.
□ Modify error messages to avoid revealing system info to unauthorized users.

Intrusion Detection Systems

□ Use an IDS to monitor and alert to suspicious activities.

Service and File Auditing

□ Regularly audit files and services for unauthorized changes.
□ Implement file integrity monitoring systems.

Multi-Server and Virtual Environments

□ Use dedicated servers or virtual environments to isolate different applications and services.

Security Audits

□ Conduct regular security audits to identify and address vulnerabilities.
□ Review and update security policies and practices based on audit findings.

Employee Training

□ Train employees in security best practices and threat awareness.
□ Revise and improve security procedures based on the outcomes of simulations and real incidents.

AI and Machine Learning

□ Integrate AI and ML tools into your security infrastructure to enhance threat detection capabilities.