



Small Group Link

Security

User Permissions

There are three primary permission levels: Admin, Leader, Member. You can choose whether to give leaders and members access to the site. Leaders can only view information on their own groups not the groups of other leaders. Members can only view their own information.

Group Search

The search placed on your site only allows members to view the group name and information describing the group. They are able to map their closest groups, but cannot view address, phone, e-mail of the leaders. All of that information is kept private.

Infrastructure

Security starts at the data center and includes traditional locks, access controls and biometric surveillance systems. Robust fire suppression, HVAC, power feeds, hot-swappable servers and routers are available in the event of an outage. Background checks and certifications ensure the integrity of all personnel.

Network

Our hosting environment's 100% Cisco Powered Network, built on hardened routers and audited by Cisco, ensure maximum security protection. Our network incorporates a patented Intrusion Detection System to protect against external threats.

Firewalls are managed by security specialists and deployed in a 'private IP' space, while servers and routers are segregated in Virtual Local Area Networks (VLAN). Network security features also include multi-level privileges, OS lockdowns, centralized authentication and device change logs.

Applications

The security regimen also addresses the inherent vulnerabilities of applications, including enterprise databases, Microsoft IIS, Apache, Linux, mail services, FTP servers, DNS and streaming media. We implement firewalls and deactivate non-essential features to further protect applications.

Security Patching

By constantly updating security systems, we ensure optimum protection. Our hosting team monitors and addresses emerging threats, and quickly processes and applies new security patches.

Threat Analysis

Our hosting environment employs advanced technologies to identify and address security weaknesses in Web-oriented servers, applications and activities. We constantly examine all firewalls, load-balancers, SSL accelerators and switches, as well as external developments, for any potential security events.

Forensics

Should a security event occur, we can conduct a comprehensive post-incident examination designed to reduce the risk of future threats. By documenting dollar losses, if any, we can help justify the involvement of the FBI or other law enforcement agencies.

Reliability

Multiple levels of redundancy ensure 100% availability of your mission-critical data. A minimum of RAID 5 is built into each configuration with available hot standby hard drives, redundant power supplies, processors, HBAs, and network switches. The storage solutions have been carefully engineered to ensure no single point of failure exists.

Backup

All information is backed up on a daily basis to ensure data integrity in the event of an outage or data loss.