

Security and Privacy Statement

Sedna Globe Inc. respects and protects your privacy. Sedna Globe Inc. will never sell, trade or rent your personal information to other individuals or companies. The information that you provide is used only to provide phone service. No Sedna Globe Inc. customers may connect, or contract with an outside vendor to connect, any VoIP device to Sedna Globe Inc.'s Voice networks without the prior review and approval of Sedna Globe Inc.

Sedna Globe Inc. recognizes your concern for security, and will use reasonable efforts to establish secure connections with you and to limit access to information containing personal information to authorized personnel only.

Sedna Globe provides Voice-over Internet Protocol (VoIP) telephone services based on a SIP voice-over-packet network design. SIP deployments in a VoIP network are exposed to a variety of network security threats and attacks. If SIP is deployed in an Internet environment, it can be hostile. Usually attacks made in the Internet environment are not traceable. The type of attacks include, but are not limited to, Traffic Capture attacks, Bootp attacks, Phone-based vulnerabilities, Management Interface attacks, Denial of Service attacks, VoIP SPAM, Viruses, TFTP, False Caller ID, Interception, Eavesdropping, Wiretapping and Spoofing.

The consequences of these attacks are listening or recording of phone calls, injecting content into phone calls, spoofing caller ID, crashing phones, denying phone service and spamming voice call.

The factors involved in the security of VoIP telephone services includes the types of End Points deployed, the services and servers used in the IP telephony solution, the trust level of users who have access to the VoIP infrastructure, the degree of access to your VoIP network from the public network, Internet, or other untrusted networks, and gateways or interfaces to the PSTN, and to other networks.

Data Center Security:

Physical access to Sedna Globe Inc. collocation equipment is not permitted without the prior approval of Sedna Globe Inc. Sedna Globe Inc. is hosted in a secure server environment with 24/7 security monitoring and other advanced technology, including fingerprint based access, to prevent interference or access from outside intruders.

Web Portal – Management Interface Security:

Sedna Globe Inc. utilizes some of the most advanced technology for Internet security available today. When you access our website portal using Microsoft Internet Explorer versions 6.0 or higher, Secure Socket Layer (SSL) technology protects your information using both server authentication and data encryption, ensuring that your data is safe, secure, and available only to registered users in your organization.

Sedna Globe Inc. provides subscribers with a unique user name and password that must be entered each time the subscriber logs on. Sedna Globe Inc. issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user. Sedna Globe Inc. does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

End Point Security:

Access to Sedna Globe Inc. provided equipment (VoIP devices, routers, etc.) is not permitted without the prior approval of Sedna Globe Inc. Sedna Globe Inc.'s End Point authentication allows all VoIP phones to register with the call controllers using SSL authentication before being allowed to make a call. The authentication can protect against spoofing and TFTP attacks.

Data and Voice Segmentation:

Sedna Globe Inc. divides the network; typically into a voice and data segment. Segmenting the network helps protect it from the next viruses that affect one of the networks. It also protects the voice packets from being sniffed by unauthorized persons and helps enforce Quality of Service (QoS) standards.

Network Monitoring:

Sedna Globe Inc. monitors the traffic flow and analyses reports which helps to take proper action. Sedna Globe Inc.'s network analysis tool classifies packets according to flows, where each flow is defined by different characteristics. These characteristics provide data to create a baseline profile of normal traffic patterns. By producing detailed accounting of traffic flows, Sedna Globe Inc. identifies deviations from typical traffic patterns, an early sign of potential DoS attacks.

Server Redundancy and Firewall:

Sedna Globe Inc. architecture is very flexible. All components of our architecture communicate with other components using IP networking and run on different machines, with redundancy, failover, and load balancing. The system can also be easily expanded; typically server machines can be added at any point, without affecting service, to handle more capacity.

Sedna Globe Inc. services are protected by firewall on a server level. It allows Sedna Globe Inc. to restrict unauthorized VoIP protocols from entering via the Internet gateway or the internal network. Sedna Globe Inc.'s firewall also protect against intrusions such as denial-of-service, interception and TFTP attacks.

Authentication:

The VoIP devices are provisioned during initial setup. Once the setup is complete, the IP of the device is stored in a secure database. All the calls from the End Point from that point onwards will first be filtered using the database information.

Patch management:

Any new patch upgrade will be pushed down to the VoIP device via internet when the device is not in use.

Email:

Sedna Globe Inc.'s voicemail are send via email. The server only supports outgoing emails. By supporting only outgoing emails, Sedna Globe Inc. does not allow any type of potentially harmful incoming emails to their existing voice network.

Soft-phones:

Sedna Globe Inc. does not provide PC based IP phones due to security vulnerabilities. Sedna Globe Inc. is in the design phase of secure soft phone. Sedna Globe Inc. does not support third party soft-phones.

Long Distance Control:

Sedna Globe Inc. validates long distance calls by making sure the customer has enough funds on their account to make calls. No customer is provided with unlimited long distance credit. Also, Sedna Globe Inc. provides pin based long distance calling for businesses who wants to restrict their employees from calling overseas. This control allows Sedna Globe Inc. to identify activities like toll-fraud and unauthorized long distance calls.

VPN Solution:

Sedna Globe Inc. will provide VPN based connectivity to selected clients. A VPN based connectivity will secure VoIP traffic over a wide area. With a VPN client at the remote site, all communications to the remote VPN gateway, is encrypted through a tunnel.

Security Assessment:

Sedna Globe Inc. is currently evaluating multiple security assessment companies. Sedna Globe Inc. will utilize one of the companies to identify certain vulnerabilities and measure the risk of our infrastructure within the next twelve months. The result of the evaluation will be posted on our website (www.sednaglobe.com).

Note: As the adoption rate of VoIP increases, so will the technology's security issues. An increasing number of hackers will attempt to infiltrate VoIP based devices and protocols and gain access to VoIP infrastructure to steal data or disrupt the service. While Sedna Globe Inc. will use every reasonable endeavor to ensure the integrity and security of our service, we do not guarantee that the service will be free from hackers or any security vulnerabilities, and we shall be under no liability for any loss or damage caused.