**Engedi's Secure Remote Management™ Technology: Multiple Paths, Encrypted Data for Secure Management Access and Communication**

*Secure Remote Management for IT Sectors of Government, Financial, Health, Telecom and Retail and for SCADA Systems*

**August 2, 2009**

**RICHMOND, VA –** New software is working to eliminate downtime and bolster security for network administrators managing the remote infrastructure of telecommunications networks or SCADA systems. The patented Secure Remote Management technology is designed for commercial and government IT organizations. Engedi's Secure Remote Management software can be embedded into all types of network devices and telecom equipment to provide multiple management communication paths to the device or appliance. Use of this technology ensures high availability – a crucial component for eliminating costs associated with remote site visits – and offers encrypted data transmission and centralized server password queries for more secure access control.

SRM technology manages and protects the flow of critical network management communications required to operate remotely located network infrastructure devices or control system equipment. While many administrators repurpose devices and create ad hoc solutions to obtain this capability, Engedi's patented SRM technology is designed specifically to provide secure management access control and communication.

"SRM is used in distributed networks to increase management security and reduce operation costs. Its use in a network or control system enables secure management access and communication," said Engedi co-founder and CEO Craig Palmore. "The patented solution is crucial for a wide variety of markets, including telecom networks, and electric, water and oil and gas providers who use Supervisory Control and Data Acquisition (SCADA) systems. The technology caters directly to the needs of the US Departments of Defense and Homeland Security by protecting the network infrastructure and making it easier for management personnel to communicate with and manage the remotely located devices and appliances that make up the network or control system."

Engedi's SRM technology enables the secure flow of all management data using both a primary or a back-up communication path, and it employs centralized authorization services to quickly limit access to any device without the need for long lists of passwords for remotely located devices.

**Multiple Paths: High Availability to Increase Network Uptime**

Corporations that rely upon their networks for the transfer of mission critical and revenue generating data must have solutions that quickly and securely restore networks when problems arise.

Downtime is extremely costly for financial, health, telecom and retail organizations that must have reliable networks and the means to maintain them – regardless of location – to ensure a continuous flow of data. Likewise, government and military networks require infrastructure security and efficiency in operations to extend resources to support the warfighter.

When the primary communication path to network devices is broken, islands of the network could develop, stopping communications internally until the primary data path is restored. While management data transmission occurs using the primary, in-band communication path 95 percent of the time, the SRM approach utilizes an independent back-up communication path to carry management data when the primary in-band path is down or unavailable, thereby greatly increasing availability and reducing time spent traveling to off-site, remote locations for maintenance.

**Encryption and Central Authentication for Total Access Control**

Engedi's SRM technology authenticates through central authentication servers at the Network Operations Center (NOC) during the use of the primary, in-band or the back-up out-of-band communication path. There is no telnet access or password access directly to an SRM enabled device that bypasses NOC authentication. The methods used by several competing products create local passwords that are rarely updated and often

facilitate security vulnerabilities because those access accounts become widely known and are rarely updated.

In the case of administrators who have left the organization, the SRM process allows system administrators to quickly and easily restrict or block remote access by the former employee to avoid security vulnerabilities. With the SRM technology embedded in network devices, administrator access to the network infrastructure can be closed quickly by removing the administrator's authorization at the centralized authentication servers at the NOC.

No matter what language, SRM transmits all communications, including timestamps, management logs and system logs, delivering the data in encrypted form across both the primary or, if needed, the backup communication path.

For more information about Secure Remote Management technology, please visit www.engedi.net.

**About Engedi**

Based in Virginia, Engedi delivers patented and patent-pending security solutions for network infrastructure management, SCADA systems, sensor and surveillance networks, and network appliances and devices. The company's Key2 Technology™ brand encompasses Key2 Secure Remote Management (SRM)™ and Key2 Control (K2t)™ multi-party authorization solutions.

For more information, please visit: www.engedi.net or contact Andrea Lawn, SS|PR, 609-750-9111