secure Agent®
*Secure Enterprise Solutions*

# Product Overview



# The IDG 9074® Remote Access Controller™

**SecureAgent Software**
2448 E. 81st St, Ste 2000
Tulsa OK 74137-4271 USA
Tel: 918.971.1600
Fax: 918.971.1623

# Security requirements for open systems

## Access—the root of the problem

In support of business objectives, today's IT environment is an increasingly heterogeneous mix of hosts, servers, and operating systems, which can cause problems for IT systems administrators.

For mainframes, administrators need access at the system level, while for UNIX® and Linux® systems, they need root access. A person with root access has total control of the system—both unintended mistakes and deliberate maliciousness can cause catastrophic interruptions in system availability and business continuity (or even survival), therefore, such access is not to be granted lightly.

The concerns inherent in granting root access on UNIX and Linux systems are magnified as the computers are distributed geographically (for example, a production data center in one location and the associated disaster recovery site in another) or as the number of systems increases.

Granting root access to a particular user transfers control of that system from the central security administrator to a wider and, therefore, more vulnerable user environment, putting the entire enterprise at risk.

Increasingly valuable data and a corresponding growth in data intrusions have forced network security professionals to reevaluate the practice. An overall shift toward securing access to corporate data and systems sharpens the focus on this critical issue.

As a result, the standard practice of providing root access based solely on operational requirements is coming under increasing scrutiny. Its vulnerabilities have recently been questioned by internal security auditors and by external regulatory agencies.

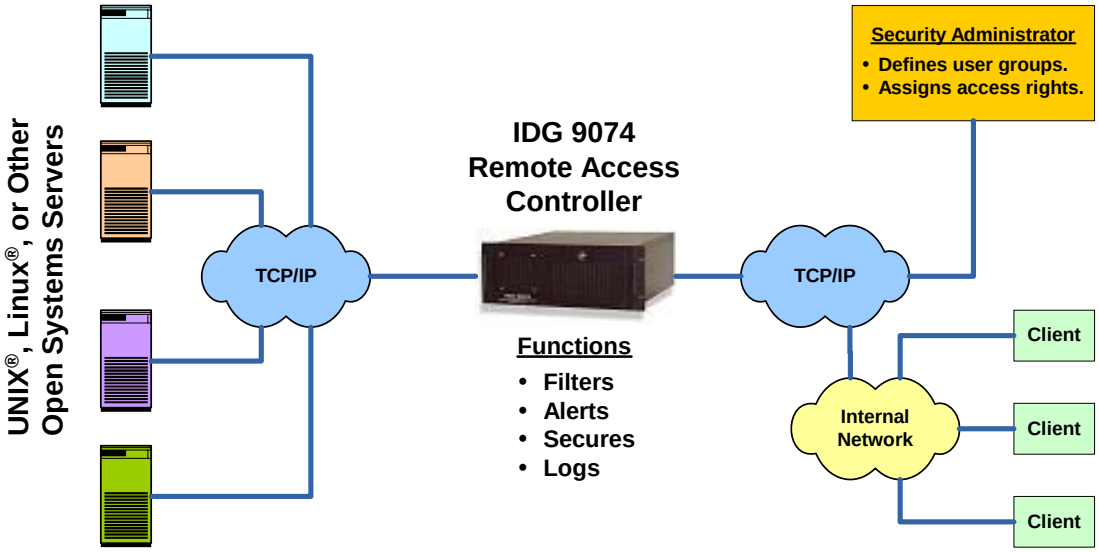
Out of many discussions with COOs, CIOs and Security Officers, the following requirements for open system servers emerged:

- Secure access to root level with a user ID and password known only to the authorized individual; that is, no blanket access with a global password
- Audit logs for root-level access and activity
- Role-based access controls (RBAC), so a user only can access a server based on his or her job function
- Central administration of all access controls and for all locations, including backup, disaster recovery, and archive sites—so administrative tasks only have to be done once
- Issue alerts if attacks are detected or a defined number of unaccepted accesses are counted
- Encryption of the entire data transfer to ensure security

## Problem solved—IDG 9074® Remote Access Controller™

Now such requirements (and many other functions) are integrated in the IDG 9074® Remote Access Controller.™

The figure below shows a typical installation.




The IDG 9074 Remote Access Controller is an integrated hardware/software solution that supports customers' needs and smoothly integrates into their existing infrastructures.

In addition to a primary IDG 9074 Remote Access Controller, secondary Remote Access Controllers may be used as defined by customer requirements, access-load balancing, and to ensure redundancy (particularly at remote locations such as backup, archival, or disaster recovery sites).

### Features of the IDG 9074 Remote Access Controller

We designed the IDG 9074 Remote Access Controller to be transparent in use and with features that make configuration and maintenance quick and easy—and that provide state-of-the-art security, even for remote locations.

- Role-based access controls—Using the included GUI administration program, you can easily set up user groups and assign access privileges to them. Equally important, if group membership changes, you can easily add or remove users, and do so from a central location, avoiding the time and expense of travel to remote locations or dealing with individual user systems.
- SecureAgent Software's patented authentication logon protocol ensures only authorized users have access. Combined with role-based access controls, it assures that those who actually access a system should have access, even from remote locations. Our logon protocol helps prevent attacks not only by outsiders, but also

by negligent or malicious insiders. It is currently in use in many of the world's largest data centers.

- Encryption of all communications between the IDG 9074 Remote Access Controller and clients ensures security of the data stream. All data is transmitted using our industry-proven, advanced encryption technology, and our patented, centralized key-management strategy.
- Access and activity logs provide auditability. Unauthorized personnel cannot access log files, assuring proof of regulatory compliance.
- Easy-to-use GUI-based administration program means you can configure and maintain the IDG 9074 Remote Access Controller quickly and easily from one central location—even remotely, so in the event of problems, travel and downtime are minimized.
- Secure remote access means disaster recovery plans can be supported and maintained from any location.
- Our patent-pending Instant Replay feature presents a scrollable history window showing a keystroke-by-keystroke recall of a particular connection. As the associated console emulation updates itself, Instant Replay captures refreshed screens and saves them in memory. It helps reduce downtime—you can see what actually occurred, down to the keystroke level, and quickly take corrective action, even from remote locations. Instant Replay is also useful in training.
- Secure Telnet clients included at no additional charge. Connections can also be made through SSH or SSH2.
- Includes easy-to-use REXX programming language that allows quick automation of operating system command sequences without extensive prior programming experience.
- Provides security administrators with an "over-the shoulder" view of operators with root access without the operators' knowledge, allowing for real-time, proactive monitoring, even of multiple consoles simultaneously.
- The IDG 9074 Remote Access Controller is an "out-of-the-box" solution that installs quickly and does not require intensive training of security administrators.
- The IDG 9074 Remote Access Controller can connect to multiple UNIX servers. An alternate IDG 9074 can provide redundancy. The combination of a primary and alternate is far more affordable than other solutions priced on the basis of an entire server farm.

## About SecureAgent Software

SecureAgent Software has been helping customers protect and manage sensitive data for more than 20 years. Many of the largest companies across the United States and throughout Europe use SecureAgent products in mission-critical areas of their daily operations. The Company develops both software and hardware products that play an integral role in

secure remote console access, data backup and recovery, advanced automation, integrated tape management, and disaster recovery.

SecureAgent Software is a pioneer in the implementation of role-based access controls, and both commercial customers and the governmental sector use its products extensively to comply with evolving regulatory guidance.

Among the companies using SecureAgent Software products are three of the four largest US banks, two of the largest credit card processing companies, the nation's two largest communications companies, the world's largest stock exchange, the largest US airline, and the largest airline reservations companies in the US and Europe.

For additional information, please contact:

**SecureAgent Software**
2448 East 81st Street, Suite 2000
Tulsa, OK 74137-4271
Voice: 918.971.1600 Fax: 918.971.1623
Toll-free: 888-746-7735
www.secureagent.com