@Remote Security Help Sheet

The @Remote device incorporates advanced network security technology designed to maintain a strong security posture.

The @Remote device is:

- Maintained as a dedicated device
- Disallows local users, reducing local and malicious code threats
- Installed in a secure LAN environment behind your clients corporate firewall
- Configured with an IP address that is non-Internet routable
- Configured to automatically send an e-mail notification to the Ricoh Central Server upon any configuration changes
- ISO 15408 Common Criteria Certified.

These security safeguards combined with simplicity of installation and configuration guidelines assure that the @Remote device will not pose significant threat to your client's network.

Although @Remote offers capability using two-way communication, the @Remote device located on the client network ALWAYS initiates the communication process behind their network firewall – similar to a PC contacting Microsoft to see if a Windows update is available. At no time does the Ricoh Centre server contact the client @Remote device.

The @Remote device is based on the Monta Vista Linux platform and the auto-discovery filter was developed to exclusively discover Ricoh devices and all network printers.

Q1) Is the data sent out over the internet secure?

Yes – because it is transmitted in SSL protocol, after both ends verify each other's identity, and only to the address specified at setup. Also for further security, the data itself is encrypted (encryption level is at 56-bit).

Q2) Local Threats?

There is very little opportunity for a local user to maliciously attack the @Remote gateway. The @Remote gateway is used solely to collect device information and does not require ANY local user to log onto the system for daily tasks. Because there is no local user access, local users are unable to identify any vulnerability in software components, escalate privileges, or read/modify information.

@Remote Security Help Sheet Cont.

Q3) Malicious Code Threat?

Successful Linux viruses are rare and basing the @Remote device on the Linux platform virtually mitigates virus threats in the @Remote device. This is accomplished by:

- The lack of everyday system users
- Files are not automatically executable under the Linux operating system
- Powerful Linux user security model
- Precise installation by trained personnel.

Q4) Remote Threats?

@Remote was designed so that it is not accessible from the internet and the @Remote device does not require direct access to the internet. This means that we can install the @Remote device in very secure locations behind corporate or departmental firewalls. Additionally major remote threats (including buffer overflow attacks, eavesdropping, and denial of service) have also been addressed.

Q5) ISO 15408 Certification?

ISO 15408 Certification (Also called “Common Criteria Certification”) is an internationally recognized certification for evaluating Information Technology security of network devices. This is the same certification as is required by the Department of Defense and intelligence community. It is critical for IT management to assure network integrity. Ricoh has obtained this certification for existing @Remote products.

Ricoh has received an EAL 3 certification, the highest level a COTS-platform (Commercial Off-the-Shelf) can achieve. Levels 1 - 4 certifications apply to technology designed for civilian applications. Levels 5 - 7 certifications apply to technology designed for military applications.

ISO International Organization for Standardization