Miracom Network Security Analysis

The All Important Question

As a network manager, government official, or business executive, your primary security concern is that an application that monitors printer and copier activity in no way provides any third-party with access to content. In other words, you don't want them to be able to see what is being printed, copied, or faxed, nor have the ability to alter the content in any way.

There are a number of standard security protocols now governing access to sensitive data. For example, the Health Information Portability and Accountability Act (HIPAA) was designed to protect access to an individual's healthcare information; the Sarbanes-Oxley Act of 2002 (SOX) was designed to protect the integrity of financial information supplied to the Security and Exchange Commission; and Federal Information Processing Standards (FIPS), a derivative of the Information Technology Management Reform Act and the Federal Information Security Management Act of 2002, is designed to maintain the security and privacy of sensitive information in Federal computer systems.

What do all of these security protocols have in common? **First**, they each provide penalties for destroying data, altering data, or having unauthorized access to data. In effect, they create an imperative to control access to data. And because a significant amount of data is now transmitted electronically from one device to another, organizations need to ensure that the devices themselves are secure, the network between devices is secure, and processes are in place for transmitting or transferring data between parties. **Second**, none of these security acts provide a direct technology imperative. In other words, they simply set standards and establish guidelines. The details of how these guidelines are to be met and the policies to support them are left to individual corporations or governmental departments to establish, regulate, review, and audit. There is no one all-encompassing legal or technical requirement.

So the most important question you can ask of Miracom *is* - does the application enable access to content being printed, stored, or transmitted from a workstation to a print device? The answer to this question is, no. Miracom does not have any capability to view print content. What Miracom sees is number, type, and location of print devices; number of pages printed; alerts, error codes, and tickets. We do not touch content at all, anywhere, at anytime. This is why our solution is so well-received by the IT community.

Solution Delivery is Everything

Miracom utilizes a hardware-based approach to solution delivery. Almost all of our competitors use either a server approach or a client-server approach, each of which creates extensive security vulnerabilities. The architect of our application was previously responsible for network security with GE Zurich, and subsequently designed the application to avoid most of the security weaknesses inherent in other product designs.

A client-server solution involves software on both the client workstations and a dedicated service on a server, while a server-based solution is a dedicated service which is almost always resident on the print server. The goal of these solutions is to read the information from the print job as it is received. In some equipment, this can actually happen on the print device itself. Another piece of software is often required to aggregate the information from all the print devices. This is the standard approach to remote print management in the industry today.

Miracom Network™, Ltd. • 100 N. Central Expressway, Suite 500 • Richardson, TX 75080
Phone: 214.292.2931 • FAX: 972.235.5271
www.miracomnetwork.com

We don't recommend this approach for the simple fact that software sitting on a work station or the print server, can provide someone with access to content. Couple this with the fact that they have network access, and you've got yourself a problem.

Additionally, it's important to note that the print server and the file server are often one and the same for many companies, so when the print server goes down so do the network drives. In other words, a crash or security violation can impact more than just print. So granting system-level access to your server or opening up large holes through your network firewalls can be dangerous.

By contrast, a hardware-based solution doesn't reside on your servers, but resides instead on a separate server either in an appliance or accessed through an appliance.

Although unable to provide user-based tracking, our application still enables you to allocate, distribute, and filter per-page costs by device, cost center, location, customer, and even by print device model. Again, we've chosen to sacrifice data at the individual user-layer in order to have a more security-centric solution.

The Architecture

Our Magic 1500 appliance collects data on print devices connected to the network, including maintenance parameter and printer diagnostics data, such as toner usage, printer duty cycle, maintenance alerts, page counts, cartridge yields, and over two dozen other data attributes. The appliance does not have access to content. The Magic 1500 is what automates the Miracom Solution.

The Magic 1500 is a rack mountable appliance that plugs into any Internet Ethernet port. Outbound communication occurs across HTTP/HTTPS which is configurable by the user. The appliance shapes the outbound bandwidth to the internet to a maximum of 56kbit/s. No external access is required.

The Magic 1500 does not have any open ports other than the web configuration page, used solely to configure the Magic 1500, which can also be done through the serial port. There are no inbound ports from the Internet that need to be opened for it to function. The only required inbound port into the customer network is UDP 161 (SNMP) to the print devices.

The Magic 1500 scans only the IP subnets or individual IP addresses you provide us. This allows you to define exactly what the Magic 1500 communicates with. Of course restricting SNMP access to only certain IP addresses or ranges would further ensure communication with only authorized devices.

Miracom Network™, Ltd. • 100 N. Central Expressway, Suite 500 • Richardson, TX 75080
Phone: 214.292.2931 • FAX: 972.235.5271
www.miracomnetwork.com