

StarTech.com 



Take Control: *Secure Remote Management Using Server Remote Control*

"It's important that you choose a solution that allows you to maximize the benefits of remote access while clearly safeguarding your network."

Exclusive Distribution for
Benelux:

Compatible Distribution
Koninginneweg 129
1211 AP Hilversum
The Netherlands

T. +31 (0)35 628 14 14
F. +31 (0)35 624 04 40
E. info@compatible.nl
W. www.compatible.nl

Executive Summary

KVM Control-over-IP products offer powerful benefits to the enterprise and service providers. While the ability to use existing network infrastructure to streamline resource management makes sense, you must be able to demonstrate to yourself and others that every link in your network is fully secure, including the management tools you choose to use.

StarTech.com Server Remote Control products offer industry-leading security based on standardized protocols and encryption for unmatched transparency.

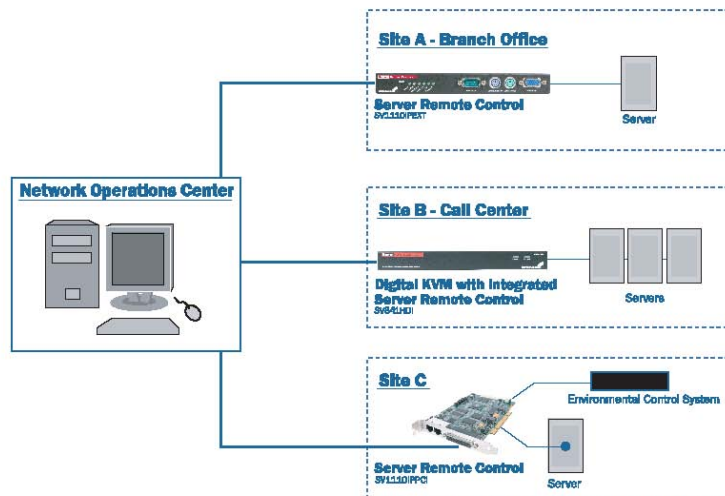
Unlike many competitors, Server Remote Control uses no proprietary client software or protocols, meaning you can verify the safety of your network and its data using standard tools for complete peace of mind. Features are important: security is everything.

Introduction

Manage more. Spend less. Make it secure. These three directives have come to define the role of the modern network administrator. Centralized administration of distant offices through a central support center is the norm. Increased convergence means that your "data" network also hosts voice, facility management, and myriad other applications. Technology and information managers are under increasing pressure to deliver cost-effective solutions to satisfy business demands and technical requirements. Trumping all these competing expectations is the need to meet increasingly stringent business-driven and regulatory demands for bulletproof security.

KVM Control-over-IP technology plays a key role in streamlining the remote management process. StarTech.com's exclusive line of Server Remote Control products and accessories deliver everything you need to develop cost-effective management solutions. From a central point of operation--and with nothing more complicated than a networked computer with a Web browser--you can monitor, configure, and interact with computers and other equipment over any network that supports the IP protocol without

the need for expensive client software licenses and extensive reconfiguration.



Your return on investment with Server Remote Control is clear: fewer costly on-site visits to distant offices, reduced IT staffing requirements and equipment downtime, improved end-user productivity, and more efficient use of technical support resources. Since these products are hardware-based, you have BIOS-level control over the equipment you monitor, allowing you to watch the startup process, change CMOS settings, and react to system prompts in real time. There is no client software necessary, so even “hung” computers and equipment can be monitored and, in many cases, restarted remotely.

Server Remote Control can help you manage more computers and devices, in more places, while you contain costs: this document outlines how it can also keep you secure. Network security has two primary elements: the management practices you develop for your systems (user rights, logging) and the features of the software and hardware (anti-virus software, spam filters, firewalls) you use to build your network. StarTech.com’s Server Remote Control line integrates easily into your existing security best practices while offering transparent, provable encryption and security features that blend seamlessly into virtually any network infrastructure.

Security Management made Easy

RADIUS Authentication Support

For networks that use RADIUS servers, the Server Remote Control product line can seamlessly access your existing system for user authentication.

Multiple Levels of User Authority

Separate administrator access allows you to segment those who can configure the Server Remote Control settings from those who have simple access as a remote user.

Built-in Firewall

Every Server Remote Control offers a configurable firewall feature that uses IP filtering to restrict the potential computers that can initiate a remote control session. If you choose to use the Server Remote Control through an existing proxy server or firewall, this feature can provide an additional layer of security.

SNMP Support

The Server Remote Control line supports the Simple Network Management Protocol (SNMP) so that administrators can include our products when viewing network details inside existing network management applications.

Plain Text Names

Administrators can assign a "plain English" name to each Server Remote Control unit that appears on the Welcome screen for easy management.

Fully Configurable IP Address

All Server Remote Control products can be configured with an administrator-defined static IP address (or via DHCP) depending on the existing network configuration.

Comprehensive System Event Logging

All local and remote login attempts and failures--down to IP-level detail--are recorded and can be viewed using the Web configuration interface or exported to a text file for additional analysis.

User-definable SSL Certificates

Administrators have the option to upload their own Secure Socket Layer (SSL) certificate to each Server Remote Control for a high degree of customization to your precise network configuration.

What's the best time to stop an attack? Before it starts.

Every point in your network that is open to external access is a potential opportunity for a hacker. You need to be absolutely sure that you can enjoy the benefits of a management solution without introducing unnecessary risk. That's why StarTech.com built comprehensive external security features into the design of our Server Remote Control line. Choose individual options to supplement your existing security strategy, or use them together to create your own solution.

Integrated, Configurable Firewall

All of our Server Remote Control products include a simple yet powerful firewall tool that allows you to restrict access to available ports using IP addresses or address ranges. Either as standalone protection or in tandem with your existing firewall or proxy, you can create a policy that is as inclusive or restrictive as you need to create a customized solution for your specific network.

VPN Support

External connections to a Server Remote Control can be tunneled through a VPN connection for an additional layer of security.

Separate Connectivity to your WAN and LAN

SV1110IPEXT and SV1110IPPCI models include separate Ethernet connections for WAN and LAN connectivity for more flexibility. You can choose to configure the connections separately so you can offer different services and access choices to internal and external users.

Fully Configurable TCP/IP Port Configuration

All services that are accessible by remote (VNC, HTTP, HTTPS, SSH, etc.) can be opened on custom ports or disabled if not used, reducing the opportunity for malicious external attacks. Want to use a non-standard port for VNC access? No problem. Want to disable HTTP access altogether? Easy. Only active services that you have configured appear during a port scan.

Dial-up Access

If you need the highest possible degree of security or you need to manage servers and equipment in a remote location that lacks high-speed infrastructure, Server Remote Control includes built-in support for an external modem. By attaching virtually any Hayes-compatible modem, you can dial into the Server Remote Control and create a private network connection. Remote images are converted to grayscale to maintain an impressive degree of responsiveness over varying phone line conditions.

Encryption that's Clear

Encryption is about two things: security and peace of mind. StarTech.com Server Remote Control uses the same level of encryption trusted by banks, insurance companies, and brokerage houses to protect online transactions.

Unlike many of our competitors, we offer you the comfort that comes from using standardized, open encryption methods that continue to withstand the scrutiny of the wider security community. This transparency is important to you for two reasons. First, you are not relying on a vendor to ensure that a closed, proprietary encryption method or connection protocol is secure and remains uncompromised.

If you're asked if your remote management platform is secure, do you want to respond with something more convincing than "The vendor says it is"? We would, and we think you probably do too. That brings us to StarTech.com security advantage number two: you can use standard tools to verify to yourself and others that StarTech.com Server Remote Control security and encryption is working the way we say, every time.

Complete 128-bit SSL Data Encryption

All of our products provide encryption for all data (keyboard, mouse, and video) passed between the Server Remote Control and the remote location. Many KVM control-over-IP products encrypt only keyboard and mouse activity.

Encryption is provided using strong (commerce grade) 128-bit SSL (Secure Socket Layer).

SSH Tunneling

Server Remote Control products also support the use of SSH (Secure Shell) tunneling and encryption that routes all traffic between two locations over a specific, secure socket for a high degree of security.

VNC Protocol Support

We use the industry-standard VNC (Virtual Network Computing) protocol to compress the information between the Server Remote Control and remote connections. This allows users to have the flexibility of using the built-in Java VNC client or any of the publicly available standalone software packages. Since VNC uses a single TCP/IP socket connection, it is easy to completely encrypt all traffic using SSL or SSH.

User-Identifiable Security

The key strength of the encryption method used is displayed to every remote user through the Welcome window, presented at the time of login into the remote session interface, regardless of whether the session is initiated through the Java VNC client or a third party software package. This makes it highly unlikely that a remote user could initiate an unsecured remote session without being aware of the fact, allowing everyone to contribute to your system's overall security.

Shopping for a new Remote Management solution? Questions to ask:

1. Does this solution require proprietary software? Do we have to buy licenses?
2. What protocols does the product use? Are they industry-standard?
3. Can you show me how to prove the security and encryption work using standardized tools?
4. Who validates the security and encryption features of the product? Are they open to examination and testing in the public domain?
5. Does this product offer security and feature upgrades via user-downloadable firmware updates?
6. Will this product integrate into my existing network infrastructure? How configurable is it?

Conclusion

The benefits of an effective remote management platform are clear. It is important that you choose a solution that allows you to maximize the benefits of remote access while clearly safeguarding your network. Some manufacturers ask you to trust them; to take them at their word when they say their products are secure. We would rather earn your trust by proving our products do everything they say they do, and give you the tools to do it. StarTech.com knows administrators are accountable for the security of the varied systems they manage, and we believe that you are in the best position to evaluate the effectiveness of the security in our offerings.

In the Technical Reference, we will explain how you can use standard networking tools to verify the bulletproof security of the Server Remote Control product line. What to know more about our products? Contact StarTech.com or your preferred reseller for more information.

Server Remote Control: Products at a Glance

All of the products in our Server Remote Control line employ the security features outlined in this white paper. Which model makes the most sense for you depends on your needs and existing configuration; you can get to know a little more about our different models here. For comprehensive specifications, visit www.startech.com or contact your local StarTech.com reseller

Other Key Benefits

- BIOS-level access and control
- Virtual USB Drive Technology for file transfer (some models)
- Use any Java-enabled Web browser: no proprietary software or licenses required
- Cascadable using most brands of KVM switches
- Up to 4 remote users can access a Server Remote Control at a time
- IPMI and modem support included at no charge
- Ability to manage remote serial console devices and power switches

SV1110IPEXT

The external Server Remote Control unit allows BIOS level remote control of a target server or servers connected to a KVM switch over a TCP/IP network. Administrators can control, reset and reboot servers in a datacenter from a remote location and even watch the entire boot process remotely. Our unique Virtual Drive Technology allows the computers you are managing to access your files as though they were stored on the machine.

SV1110IPPCI

Looking for the power of Server Remote Control in an internal package? The SV1110IPPCI offers all the features of our external product, packed into a potent PCI card that works in virtually any server or other computer.

SV841HDI, SV1641HDI

Do you need to remotely manage more than one computer? Don't have an existing KVM switch? StarTech.com has the solution. This next generation of products are true digital KVMs housed in a compact, rackmount-friendly 1U chassis design. Available in 8 and 16 port versions, this product line reduces the clutter in your rack or cabinet by putting a Server Remote Control and a KVM into one product. Perfect for mixed environments, these digital KVMs can interface with PS/2 and USB-compatible computers across a wide variety of platforms.

Technical Reference

You can use the commands and methods listed here to test the validity of a Server Remote Control unit's security settings. The actual programs and commands may vary depending on the operating system and application programs you wish to use (the examples here are Linux-based), but the methodology is similar across all platforms.

SSL and VNC

1. Download from a public site the source code for a VNC client and an SSL tunneling program. We recommend, but do not require, TightVNC (www.tightvnc.com) and STunnel (www.stunnel.org). You will also need OpenSSL to do the actual encryption (www.openssl.org).
2. Examine the source code to these packages and compile them, if desired. Once you've done this, you can verify that STunnel, for example, can be used to access an on-line bank and that it indeed implements the SSL standard.
3. With our product at IP address 10.0.0.1 (in these examples), perform this command to connect without encryption:

```
vncviewer -bgr233 10.0.0.1
```

Note the "Welcome" window on initial connection shows that you are connected with no encryption. You have verified that we implement the standard VNC protocol and are compatible with this open-source VNC client.

4. Using STunnel, create an SSL tunnel between your machine and the test machine's encrypted VNC socket. By default, VNC runs on port 5900 and our SSL-wrapped version of VNC runs on port 15900 (all port numbers can be changed or disabled in our product). Here is a configuration file to setup the tunnel (for STunnel 4.0 and later):

```
client = yes
socket = r:TCP_NODELAY=1
ciphers = DES-CBC3-SHA:
[vnc]
accept = localhost:5900
connect = 10.0.0.1:15900
```

For demonstration purposes this configuration file limits the encryption choices to a single encryption type. SSL protocol supports many different combinations of algorithms for encryption and message authentication.

5. Use the tunnel to connect to our product:

```
vncviewer -bgr233 localhost
```

You will see the level of encryption listed on the "Welcome" window. This will be described by the Server Remote Control as "DES-CBC3-SHA (168-bit key)" which is exactly the algorithm specified in the STunnel configuration file.

6. You have now personally proven that our product uses the encryption it says it does.

SSH

You may repeat the same experiment using SSH. The correct OpenSSH commands are available in the on-line help page of the Server Remote Control. Those on-line examples will have the correct IP addresses and port numbers in place for your network, but here is a general example of the command to use (typed on a single line):

```
ssh -f -p 22 -l <TargetUser> -L 15900:127.0.0.1:5900  
<TargetIP>  
sleep 60 vncviewer -bgr233 127.0.0.1::15900
```

Limiting Open Ports

All Server Remote Control products offer remote services that are fully configurable by TCP port. You can also elect to disable ports for services that your users will not access, a good strategy for preventing external attacks.

You can verify that we have implemented this feature using "port scanner" software, such as nmap (<http://www.insecure.org/nmap/>). Here is the nmap command that will scan and report open ports on a single machine.

```
nmap -sT -p -15900 10.0.0.1
```

When that command is used against an SV1110IPEXT Server Remote Control LAN port (which by default has all services enabled) we get this output:

```
Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)  
Interesting ports on ebox2-LAN (10.0.0.1):  
(The 15895 ports scanned but not shown below are in state:  
closed)  
Port State Service  
22/tcp open ssh  
80/tcp open http  
443/tcp open https  
5900/tcp open vnc  
15900/tcp open unknown  
Nmap run completed - 1 IP address (1 host up) scanned in 4  
seconds
```

If the same command is used against the WAN port of that product (which already uses restrictive security by default), only SSH is open. All other access will be denied.

```
Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Interesting ports on ebox2-WAN (10.1.0.1):
(The 15899 ports scanned but not shown below are in state:
closed)
Port State Service
22/tcp open  ssh
Nmap run completed - 1 IP address (1 host up) scanned in 4
seconds
```

Acknowledgements

We wish to acknowledge and thank Peter D. Gray and Daryl Hunt for the creation and preparation of this document

About StarTech.com

StarTech.com is "The Professionals' Source for Hard-to-Find Computer Parts". Since 1985, we have been providing IT professionals with the quality products they need to complete their solutions. We offer an unmatched selection of computer parts, cables, server management solutions and A/V products and serve a worldwide market through our locations in the United States, Canada, the United Kingdom and Taiwan. Visit www.startech.com for complete information about all our products and to access exclusive interactive tools such as the Parts Finder and the KVM Planner. StarTech.com makes it easy to complete almost any IT solution. Find out for yourself why our products lead the industry in performance, support, and value.