Insiders' Guide to Evaluating Remote Control Software

Three Fundamental Rules for Choosing the Best

ABSTRACT:

With a clear business case and a promise to make life easier, it is no wonder many organizations have been quick to adopt remote control software. However, in today's computing environment, IT professionals must address business requirements that focus on protecting the security of networks, meeting the needs of a heterogeneous workforce, and deploying solutions across many users. The type of remote control software an organization chooses to implement can have a strong affect on its ability to deliver in the areas of scalability, compatibility, and particularly security.

This paper examines the remote control software functionality that best serves organizations that need a highly secure tool that crosses all platforms and devices and is completely scalable in any environment. It will help IT professionals select a remote control solution that increases productivity and customer satisfaction, as well as enhances the flexibility of the IT organization and improves the company's risk profile.

Insiders' Guide to Evaluating Remote Control Software

Three Fundamental Rules for Choosing the Best

Introduction

For almost 30 years, remote control software has allowed IT professionals to connect to desktops and servers to manage networks and provide support. Companies taking advantage of remote control technology have saved tremendous amounts of time, money, and resources by eliminating the need for IT staff to travel, reducing system down time, and improving the efficiency of the IT organization.

As businesses continue to look to technology to help streamline processes, cut costs, operate globally, and create mobile workforces, remote control software has transitioned from a "technical support tool" into an integral part of any IT infrastructure and a key application for customer service, manufacturers and the mobile workforce. As IT becomes pervasive, organizations are looking to remote control software to assist customers, trouble-shoot and maintain products from a distance. Bottom line, without remote control software, IT department budgets would grow exponentially, system reliability would suffer, and end users would be dissatisfied.

With a clear business case and a promise to make life easier, it is no wonder many IT organizations have been quick to adopt remote control software. You will often find that organizations are using three to four different remote control products in order to support an increasingly heterogeneous mix of operating systems, software applications, PDAs, mobile phones or embedded devices.

Many organizations are now reconsidering their remote control product portfolio as they realize that juggling several different tools does not necessarily make life easier or more secure as each product needs its own firewall configuration. And, regulatory and compliance pressures in certain industries where data leakage is a serious concern has created new apprehension regarding the security of remote control applications.

Whether you are looking to consolidate your remote control solutions or are new to the world of remote control, the number of remote control products on the market will easily overwhelm you. It is easy to get confused, but to find a solution that is rock-solid and future-proof look for a solution that

- Provides comprehensive security that can be adjusted to meet the needs of IT professionals and their users, no matter how demanding the security environment;
- Supports a heterogeneous environment within the current IT framework; and
- Has a versatile and open architecture and centralized deployment, ensuring that the solution can grow at the same pace as the business

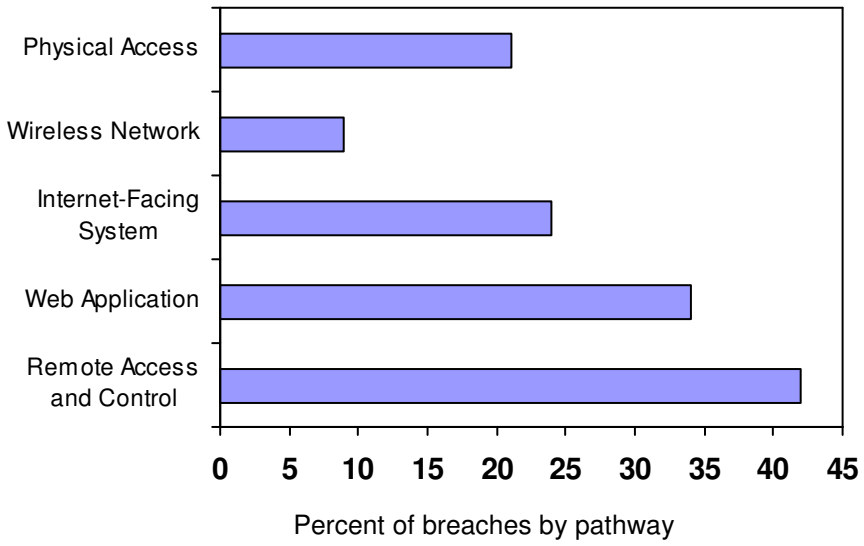
Evaluating Remote Control Software: Three Fundamental Rules

Given the long history of remote control software, it is no wonder that there are numerous solutions delivering the same set of basic features to satisfy the need for “remote control.” These options include open-source flavors of VNC (virtual network computing), built-in tools (e.g. Windows Remote Assistance or SSH in Unix variants), web-based services (e.g. gotomypc.com) and traditional software-based solutions like Netop Remote Control.

When examining remote control functionality you should consider your need. Are you looking for a solution to help a friend, connect to your home PC or running the service desk in a multinational company? If you are gravitating towards the latter, you would want to consider the key drivers for today’s businesses when selecting a remote control software solution that will completely meet your global needs- security, compatibility, and scalability.

RULE # 1 - PUT SECURITY FIRST

Remote control software offers many benefits but potentially it makes your IT systems vulnerable to different exploits, e.g. access through firewall ports opened for remote control, sniffing of passwords from an established remote control session, brute force attacks on password protected Hosts, etc. A recent report by the Verizon Business RISK Team reported that, “in over 40 percent of breaches investigated, an attacker gained unauthorized access to the victim via one of the many types of remote access and control software.”

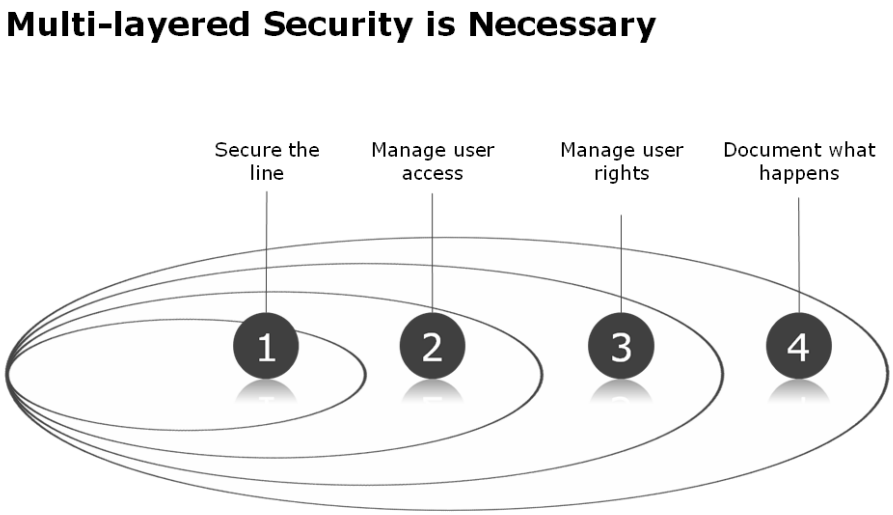


Source: Verizon Business RISK Team 2008 Data Breach Investigations Report

Does that mean that all remote control software is inherently a big security risk and you should avoid using it? No, the benefits greatly outweigh the potential risk and there are measures you can take to minimize the risk, such as changing the default ports, using role-based access profiles, etc. That is why you should put security first.

A four-layered security model for remote control software

To continue to play an integral part in any IT infrastructure, a remote control solution must protect information and prevent unauthorized access using multi-layered security as shown in the following figure.



There are two sides to every remote control session: the side providing the support, and the side receiving the support. Remote control vendors use a variety of terms to describe these two sides. For consistency sake in this paper, we will use "Guest" to describe the provider and "Host" to describe the receiver.

Securing the line

Establishing a connection between the Guest and the Host involves network traffic and thus the potential risk that an intruder can sniff the packet information and eavesdrop on your remote control session. Obviously, the risk is greater when using a connection over the Internet than on your LAN. This security risk is heightened when access is granted through third party servers. In this scenario, an outside company stores your log-in information, traffic and logging data, giving them the control to access and manipulate your confidential information and putting you at further risk for outside attacks to the provider's systems. Accessing the Host through the Internet does have its advantages – you don't have to reconfigure firewalls, routers or proxies, making it easier to provide support for employees outside your network, home users and mobile employees. So, to ensure that security is not compromised for flexibility, look for a solution that allows you to provide Internet-based remote access through your own servers. This way you are in control of the security and your own data.

Either way the best thing is to look for market leading 256-bit AES encryption and dynamic key exchange using the Diffie-Hellman method with key lengths up to 2048 bits.

Although encryption is often the first thing you think of when talking about security, it is actually just the first step in setting up a professional secure remote control solution. You also need to manage how users of remote control connect to each other and what users are allowed to do once connected. Finally, it is important to be able to document what happened during a remote control session.

Manage user access

A remote control session begins when the Guest sends an invitation to the Host asking for permission to establish a connection. Once the Host accepts the invitation, the remote session is initiated. It is important that the Host has certain criteria for accepting incoming invitations, otherwise any rogue invitation would allow an intruder easy access to your network. Managing user access is setting the criteria on which the Host should accept an invitation.

Remote control products differ on what criteria you can enforce, some use only passwords, others need user acceptance, which is not good for servers. The best solutions will offer you multiple access criteria including:

- **MAC/IP address check.** The host will only accept connections from Guest addresses that appear in a predefined MAC/IP list. This provides a base level security, but IP addresses can be forged, so this criteria should never be used as a stand-alone alternative to security.
- **Closed user group** assign specific serial numbers for all Guests and Hosts, enabling only matching serial numbers to connect. Guest modules with any other serial number are rejected. This helps provide best in class security, but there are other elements to consider in a multi-leveled secure system.
- **Authentication.** Any remote control application should be able to integrate with the current authentication scheme that is deployed across your network - whether it is a Windows Domain, LDAP server, or RSA SecurID server. Integrating with the existing authentication scheme provides a secure method for the Guest to identify itself to the Host.
- **Callback.** A feature where the Host calls back to Guest can be used with a modem, ISDN, or TCP. The callback feature forces the Guest user to be at a specific location, introducing another obstacle to prevent intruders. This is especially important in industries where many systems are connected through modems, such as retail stores, banks, and gas stations.
- **User-controlled access.** When you use user-controlled access, a pop up window will ask the Host user whether he wants to accept an incoming Guest request before the remote control session is established. This a typical set-up feature in help desk environments where it adds a good amount of security, however, it is not practical for remote administration of servers or desktops, remote system rollouts or remote updates.

Now a remote control session is established, we can turn to another import aspect of remote control security; what the Guest user is allowed to do on the Host computer.

Manage user rights

Once connected a Guest can perform various tasks on the remote computer, reboot, edit registry, delete files, copy files, print, chat with the user, etc. Exactly what the Guest can do varies widely among remote control products, however, more important is the degree to which you can specify various access roles. The importance of this is highlighted in the aforementioned Verizon report. According to the study, an account intended for use by external consultants to remotely administer systems was compromised by an external entity and used to illegitimately access enterprise information assets.

Different remote control users need different access profiles. You would probably want to look at being able to limit functionality like locking the keyboard and mouse, executing commands (delete, copy files), running programs, managing services, entering command prompt, editing registry, etc.

A final caveat on managing user access rights - a number of high-end remote control products will allow you to manage user access rights, but look for a solution with central management. A centrally managed user access rights solution will enable you to change the settings for thousands of computers without having to configure each Host individually. This also provides more flexibility in administering user rights, as authorizations can be changed “on the fly” as a further level of protection.

Document what happened

Documentation is the final frontier of a solid secure remote control system. With extensive logging and video recording of sessions, you will know exactly what happened and when. Did the help desk employee delete that important sales file while assisting the sales clerk with his Internet connection? Who remotely accessed the confidential medical records Saturday night? These are questions you would want to be able to answer.

Data leaks not only potentially expose customers’ personal information and confidential company information, but open the company up to significant financial penalties, even jail time, for failure to meet security standards outlined in regulations such as HIPAA, Sarbanes-Oxley, the Freedom of Information Act, and the International Financial Reporting Standards. That is why you should pay special attention to the documentation feature of a remote control product. This is often an overlooked feature, but is vital to ensuring compliance to these regulations. Session recording is another vital component, as you can trace the actions of each Guest on each Host.

RULE #2 – ENSURE CROSS-PLATFORM COMPATIBILITY

With Microsoft's prominent position in today's IT environment, it is all too easy to think that you just need a remote control product that runs on Windows. What Windows you might ask, as it comes in many varieties for desktops, servers, mobile devices and embedded systems, including Vista (32 and 64-bits), XP, 2000, NT, ME, 98, 95, MS-DOS, Server 2003, 2008, CE, XP embedded, Mobile 5 and 6? Many remote control products only cater to the latest versions of Windows for desktops or servers, but in many enterprises, you will find customized applications running on old Windows platforms. And, increasingly you need to support smart phones and embedded devices.

The truth is that few enterprises are 100 percent Microsoft only. You will find Linux servers, Macs in the marketing department and in the financial sector you might easily encounter OS/2. Add the complexity of several local area networks and the need for support over the Internet, and it is not unusual to find IT departments and service providers having to switch between two, three, even 10 different remote control tools to cover daily maintenance and support tasks. As a result, rather than create efficiencies and streamline the IT environment, remote control begins to contribute to the myriad software products that need support and maintenance.

Every time an incident cannot be solved using a remote control tool, a help desk service person will need to make a desk-side visit or spend hours in the server room . You incur extra cost, lose efficiency in the IT department and increase user/server down time. Thus, it makes business sense to consolidate on one remote control solution that can reach across plenty of operating systems, devices, LANs and the Internet. Furthermore, you save time and resources in training new employees or just finding the right tool for a particular issue.

RULE # 3 - IT'S GOT TO BE FLEXIBLE AND SCALABLE

A medical center in New Mexico employed 1,400 people across the state, and when end users needed technical support, they were required to make an appointment rather than get immediate assistance, sometimes waiting days until help arrived. Support was not the only issue. When performing maintenance or system upgrades on the hospital's 1,000 computers, it took months and thousands of hours to complete the job.

For organizations with issues like the New Mexico hospital, making an investment in remote control software can help solve a number of IT-related problems. However, to work across wide-spread organizations, hundreds or thousands of computers, LANs, the Internet and through different firewalls and routers, it is important that the remote control application is flexible and scalable.

Look for features that help manage scalability and provide flexibility for both Guests and Hosts, including:

- **Central installation and deployment capabilities** that provide for an easy, network-wide roll out of the remote control to Host computers with help of deployment and installation utilities.
- **Centralized security management.** A scalable remote control solution relies heavily on a centralized security management system allowing administrators to easily administer authentication rules, user groups and their associated access rights without having to visit each Host computer.
- **On demand remote control which** gives you the flexibility to support computers without a Host installed. With an on-demand solution, a user needing help will be asked to install a small executable, either by clicking on an icon on a web site or through email. Once installed, the executable will allow a temporary remote control session.
- **Flexible connectivity** with an Internet-based connection service where the Guest and the Host need only send out traffic through the firewalls to the connection service in order to initiate a remote control session. This gives the freedom to connect easily to any Host anywhere and, as outbound traffic is normally allowed through the firewalls, you do not need to make any changes to the firewall configuration. For security purposes, it is best not to rely on third party servers with access to your login and traffic information.
- **Support for the Intel vPro,** a set of features built-into the chipset providing additional flexibility. With a vPro supported remote control solution administrators can remote access computers before the operating system is loaded or even if no operating system is available. A computer can be remotely powered on/off to get into the BIOS settings or install an operating system from an image located on the Guest computer.
- **Scalable telephone book** that allows Guests to organize, share and customize connections giving easy access to all hosts no matter where they are or how many there are.
- **Reliable, future-proof technology** that comes from a provider with extensive experience in the development of remote control solutions.

Conclusion

Remote control software is an exceptional tool for IT departments, as well as employees in the organization, because it provides faster resolution to computer-related problems, brings efficiencies to system maintenance, and generally leads to higher levels of operational stability and reliability. Yet because of the changing IT environment including the increased need for high levels of security, the heterogeneous state of most enterprises IT architecture, and growth in the number of end users, business requirements for remote control software are changing.

In considering the purchase or consolidation of remote control software, IT departments now need one secure tool that crosses all platforms and devices and is completely scalable in any environment. More importantly, the remote control software must have the highest encryption, role-based access and rights management, and logging and session recording to protect the organization from data leakage and security breaches.

With careful research and attention to features that represent the best in remote control technology, IT departments can select an application that stretches the limits of remote control and not only increases productivity and customer satisfaction, but enhances the flexibility of the IT organization and improves the company's risk profile.

About Netop Remote Control

Netop Remote Control is the complete remote control solution for professional users. It offers everything you need for the service and support of computers and networks: from the completion of complex remote maintenance and file transfer, through remote user support to network-wide software and hardware inventory administration. All of this comes under a single, intuitive interface, perfectly protected by encrypted connections, sophisticated authentication and comprehensive rights management.

About Netop

Formerly known as Danware A/S, Netop Solutions A/S develops and markets software solutions that enable swift, secure and seamless transfer of screens, sound and data between two or more computers. The company has three business areas: Netop Desktop Management, Netop Education and Netop Live. The core Desktop Management product, Netop Remote Control, enables remote control of one or more computers. The Netop Education business consists of Netop School and Vision software solutions for computer-based classroom teaching. Netop Live consists of modern solutions for unified communication and collaboration and includes products like Web, video and audio conferencing; secure chat; one-button click to talk; and desktop and file sharing. Netop has subsidiaries in the United States, the United Kingdom, Germany, China and Switzerland, and the Netop solutions are sold in more than 80 countries. Netop Solutions A/S shares are listed on the Copenhagen Stock Exchange and are part of the SmallCap+ index. For further information, please see http://www.netop.com.