NETOP®
RemoteControl
Secure Remote Management and Support

Netop

Three Fundamental Rules for Choosing the Best Remote Control Software

For almost 30 years, remote control software has made it possible for IT professionals to connect to laptops, desktops, servers and other devices to manage networks and provide support – saving time, money and resources. Yet in an evolving IT environment, the business requirements for remote control software are also changing. Today, a remote control solution must meet the needs of a heterogeneous workforce, deploy solutions across many users and provide extensive security. Indeed, the remote solution an organization chooses can have a big effect on its scalability, compatibility and security.

This paper examines the remote control software functionality that best serves organizations, helping IT professionals select a solution that increases productivity and customer satisfaction, enhances the flexibility of the IT organization, and improves the company's risk profile.

Three Fundamental Rules for Choosing the Best Remote Control Software

For almost 30 years, remote control software has made it possible for IT professionals to connect to laptops, desktops, servers and other devices to manage networks and provide support. The companies using the software have saved tremendous time, money and resources by eliminating the need for their IT staff to travel, reducing system down-time and improving IT efficiency.

Today businesses continue to use technology to streamline processes, cut costs, operate globally and support their increasingly mobile workforce. IT has become pervasive, and remote control software has transitioned from a "technical support tool" to an integral component of any IT infrastructure, as well as a key application for service desk teams. Organizations use it to assist customers, troubleshoot and maintain products from a distance. Bottom line, without remote control software, IT department budgets would run through the roof, system reliability would suffer and end-users would be dissatisfied.

With a clear business case and the power to make life easier, it is no wonder that remote control software is now a standard tool in many IT organizations. However, it is common for organizations to use three to four different remote control products to support an increasingly heterogeneous mix of operating systems, software applications, mobile or embedded devices, leading them to reconsider their remote control product portfolio. Juggling several different tools does not make things easier or more secure: each product needs its own firewall configuration; also, for industries where data leaks are a serious concern, regulatory and compliance pressures have created justified apprehension around the security of remote control applications.

Whether you want to consolidate your remote control solutions or simply learn more about the world of remote control, the number of options on the market can easily overwhelm. Be selective. A rock-solid solution should do the following:

- Provide comprehensive security that can be adjusted to meet the needs of IT professionals and their users, no matter how demanding the security environment
- Support a heterogeneous environment within the current IT framework
- Include a versatile, open architecture and centralized deployment, so the solution will be able to grow at the same pace as the business

EVALUATING REMOTE CONTROL SOFTWARE: THREE FUNDAMENTAL RULES

Given the thirty-year history of remote control software, there are now numerous solutions delivering the same basic features to satisfy the need for "remote control" – for example, 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) and traditional software-based solutions like Netop Remote Control.

When examining the functionality of a remote control product, bear in mind your needs. Do you want a solution to help a friend or connect to your home PC, or are

There are two sides to every remote control session: the side providing the support, and the side receiving it.

Remote control vendors use a variety of terms to describe these two sides. In this paper, we will use the following:

1.) SUPPORT REPRESENTATIVE: This is the service provider and the remote access solution he or she uses to connect to and support another device.

2.) TARGET DEVICE: This is the equipment being accessed, as well as the remote access software installed on it. Target Devices can range from an employee's laptop to unmanned devices like servers or ATMs.

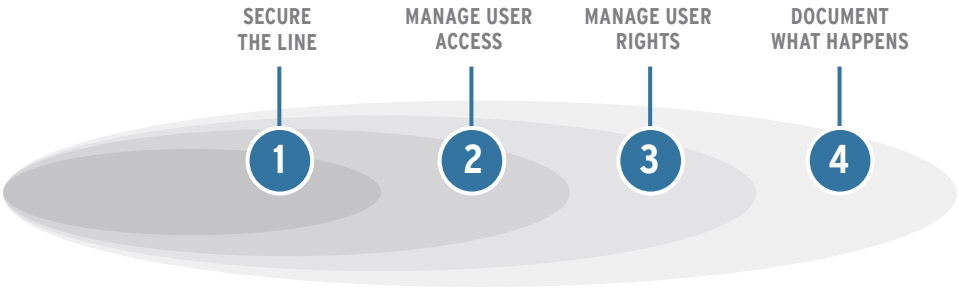
you running the service desk in a multinational company? If the latter, consider the key drivers for today's businesses – security, compatibility, and scalability – and look for one remote control solution that will completely meet your global needs

RULE 1 - PUT SECURITY FIRST

Remote control software offers invaluable benefits. At the same time, it can make your IT systems vulnerable to a variety of exploits: access through firewall ports opened for remote control, sniffing of passwords from an established remote control session, brute-force attacks on a password-protected Target Device, and so on. According to a recent Data Breach Investigations Report by Verizon, remote access services accounted for 88% of all hacking-related breaches.

To gain the benefits of remote control without the danger, you must take measures to minimize your risks – for example, changing the default ports, using role-based access profiles and more. In other words, put security first.

A Multi-layered Approach to Remote Access Security



Secure The Line

Establishing a connection between a Service Representative and a Target Device involves network traffic; thus, an intruder could potentially eavesdrop on your remote control session. Obviously, the risk is greater when using an Internet connection than it is on your LAN. It is greater still when access is granted through third-party servers. In this scenario, an outside company stores your login, traffic and logging data, and could potentially access or manipulate your confidential information. It also puts you at risk for outside attacks on the provider's systems.

However, granting access through the Internet does have its advantages. Because you don't have to reconfigure firewalls, routers or proxies, it is easier to provide support for home users, employees outside your network or mobile employees.

To avoid compromising security for flexibility, choose a solution that lets you provide Internet-based remote access through your own servers. This way, you are in control of your own data and the security. Look for market-leading 256-bit AES encryption and dynamic key exchange using the Diffie-Hellman method, with key lengths up to 2048 bits.

That said, encryption is just the first step to security. You also need to manage how users connect to each other and what they are allowed to do once connected. Finally, you need the ability to document what happened during a remote control session.

Manage User Access

A remote control session begins when the Service Representative sends an invitation to the Target Device asking for permission to establish a connection. Once the Target Device accepts, the remote session is initiated.

The Target Device must impose certain criteria for accepting incoming invitations; otherwise any rogue invitation could allow an intruder access to your network. Managing user access means setting the criteria on which the Target Device should accept an invitation.

Remote control products differ in what criteria you can enforce. Some use only passwords; others require user acceptance. The best solutions offer multiple access criteria, including:

- **MAC/IP ADDRESS CHECK.** The Target Device will only accept invitations from a Service Representative whose address appears in a predefined MAC/IP list. This sets a base level security. However, because IP addresses can be forged, this criteria should never be used as a stand-alone security alternative.
- **CLOSED USER GROUP.** Assign serial numbers to all Service Representatives and Target Devices where only matching numbers may connect. A Service Representative module with any other serial number would be rejected. This is a step toward best-in-class security.
- **AUTHENTICATION.** Any remote control application should be able to integrate with the authentication scheme currently deployed across your network – whether this is a Windows Domain, LDAP server, or RSA SecurID server. Integrating with the existing authentication scheme provides a secure method for the Service Representative to identify itself to the Target Device.
- **CALLBACK.** The Target Device can call the Service Representative using a modem, ISDN or TCP. Callback forces the Service Representative to be at a specific location, 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.** With this feature, a pop-up window appears on the Target Device asking the end-user whether they want to accept an incoming request from the Service Representative; a remote control session cannot be established until they accept. A typical set-up feature in service desk environments, this is an effective security measure. However, it is not practical for remote administration of servers or desktops, remote system rollouts or remote updates.

Once a remote control session is established, we can turn to the next important aspect of remote control security: what the Service Representative is allowed to do on the Target Device.

Manage User Rights

Once connected, a Service Representative can perform various tasks on the Target Device: reboot, edit registry, delete files, copy files, print, chat with the user and so on. What the Service Representative can do varies widely among remote control products; more important is the degree to which you can specify access roles.

Different remote control users need different access profiles. You should be able to define user functionality as needed: lock the keyboard and mouse, execute certain commands (delete, copy files), run programs, manage services, enter command prompt, edit registry, etc.

Recognize too that while some high-end remote control products will allow you to manage user access rights, not all provide centralized management. With a centrally managed user access rights solution, you can change the settings for thousands of computers without having to configure each Target Device individually. This provides greater flexibility in administering user rights, as authorizations can be changed "on the fly" when a need arises, 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 for sessions, you can know exactly what happened, when. Did the service desk employee delete that important sales file while assisting the sales clerk with his Internet connection? Who remotely accessed the confidential medical records on Saturday night? These are questions you would want to be able to answer.

A data leak may not only expose your customers' personal details or confidential company information; it can also open you up to significant financial penalties – even jail time – for failure to meet security standards such as HIPAA, Sarbanes-Oxley, the Freedom of Information Act and the International Financial Reporting Standards. For this reason, pay special attention to the documentation functionality of a remote control product. Though often overlooked, this feature is vital to ensuring regulatory compliance.

RULE 2 - ENSURE CROSS-PLATFORM COMPATIBILITY

Given Microsoft's prominent position in today's IT environment, it is tempting to think you need only a remote control product that runs on Windows.

However, even if that were the case, Windows comes in many shapes: desktops, servers, mobile devices and embedded systems: Windows 8, Windows 7, 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 cater only to the latest versions of desktops or servers, yet in most enterprises, you will find customized applications running on older platforms as well. Then there are smartphones and embedded devices, which must be supported as well. There are Linux servers, Macs and even OS/2.

Though perhaps the case a decade ago, today few enterprises are 100% Microsoft.

Once you add the complexity of several LANs and support over the Internet, it is not unusual to find IT departments and service providers switching among two, three or more remote control tools to cover daily maintenance and support tasks. At that point, remote control becomes another one of the myriad software products that need support and maintenance – rather than creating efficiencies and streamlining the IT environment, as it was meant to do.

It makes business sense to consolidate on one remote control solution that can reach across multiple operating systems, devices, LANs and the Internet. Not only does this ensure you'll have access where you need it; it also saves time and

resources in training new employees, or just finding the right tool for a particular issue as efficiently as possible.

RULE 3 – MAKE IT FLEXIBLE AND SCALABLE

A medical center in New Mexico employed 1,400 people across the state. When end users needed technical support, they had to make an appointment, 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, investing in remote control software can help solve a number of IT-related problems.

However, in order to work across widespread organizations, hundreds or thousands of computers, LANs, the Internet and firewalls and routers, the remote control application must be flexible and scalable.

Look for features to manage scalability and provide flexibility for both the Service Representative and the Target Device, including:

- **CENTRAL INSTALLATION AND DEPLOYMENT CAPABILITIES** that offer an easy, network-wide rollout of the remote control solution to all Target Devices, with help of deployment and installation utilities.
- **CENTRALIZED SECURITY MANAGEMENT.** A scalable remote control solution depends on a centralized security management system that lets administrators easily administer authentication rules, user groups and their associated access rights without having to physically visit each Target Device.
- **ON-DEMAND REMOTE CONTROL** that gives you the flexibility to support computers without pre-installed software on the Target Device. With an on-demand solution, a user needing help will be asked to install a small executable, by clicking an icon on a website or in an email. Once installed, the executable will allow a temporary remote control session.
- **FLEXIBLE CONNECTIVITY** with an Internet-based connection service, where the Service Representative and Target Device only need to send traffic through firewalls to the connection service to initiate a remote control session. This provides the freedom to connect easily to any Target Device, anywhere, and because outbound traffic is normally allowed through the firewalls, you do not need to change the firewall configuration.
- **SUPPORT FOR THE INTEL VPRO,** a set of features built into the chipset that provides additional flexibility. With a vPro-supported remote control solution, administrators can access computers before the operating system is loaded, or even if no operating system is available. A computer can be remotely powered on or off to get into the BIOS settings or install an operating system from an image located on the Service Representative's computer.
- **SCALABLE TELEPHONE BOOK** that allows support representatives to organize, share and customize connections, providing easy access to all target devices, 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 excellent tool for IT departments and employees: it provides faster resolution to computer-related problems, brings efficiencies to system maintenance and generally results in higher levels of operational stability. Yet due to a changing IT environment – including a greater need for intensive security, the heterogeneous state of an enterprise's IT architecture, and a growth in the number of end users – the business requirements for remote control software are also changing.

When considering the purchase or consolidation of remote control software, today's IT departments need one secure tool with features that represent the best in remote control technology: a tool that crosses all platforms and devices, and is completely scalable in any environment. Most importantly, to protect the organization from security breaches, it must have the highest encryption available, role-based access and rights management, and logging and session-recording functionality.

With careful research and attention, IT departments can select an application that stretches the limits of remote control, not only increasing productivity and customer satisfaction, but enhancing the flexibility of the IT organization itself and improving the company's risk profile.

ABOUT NETOP REMOTE CONTROL

Netop Remote Control is a complete remote control solution for enterprise environments. 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. It includes this in a single, intuitive interface, intensively protected by encrypted connections, sophisticated authentication and comprehensive rights management.

ABOUT NETOP

Netop develops and sells market leading software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers. The company has two business areas: Customer Service and Education.

Used by half of the Fortune 100, Netop's customer service solutions, including secure remote access and live chat, help businesses provide better customer service, reduce support costs and meet security and compliance standards. In Education, Netop is the world leader in classroom management software, helping teachers in 75 countries make teaching with technology easier and more effective.

Headquartered in Denmark, Netop has offices in the United States, Great Britain, China, Romania and Switzerland. The company sells its solutions to public and private clients in more than 80 countries. Netop Solutions A/S shares are listed on the Copenhagen Stock Exchange OMX.

Read more at: www.netop.com.