



---

# Using Remote Access Management™ to Increase Security and Improve Efficiency in Data Centers

---

[a white paper from Minicom](#)

---

---

# Using Remote Access Management™ to Increase Security and Improve Efficiency in Data Centers

---

a white paper from Minicom

---

## Executive summary

In recent years, remote server access has become standard for corporate data centers however, many data centers have adopted remote access strategies gradually, on an ad-hoc basis, as technologies have evolved. As a result they are enjoying only partial benefits, and may have opened up unexpected security gaps. With an overall strategy—and a software solution for system-wide Remote Access Management, such as AccessIT® from Minicom, corporations can maximize the benefits, and minimize the risks of remote server access.

## The benefits of remote server access

Years ago, the idea of operating and maintaining data centers remotely, or with “lights out” in the server room, seemed radical. Now remote access management is standard procedure. Why? Because remote server access offers three compelling advantages:

### 1. Increased data security

Remote server access reduces the number of people who come into contact with critical data, and limits the number of servers that any individual has access to. With remote access, the data center can be locked tight and secured from unwanted, unattended visitors. This is a primary reason for the increase in popularity of Remote Access Management solutions in security-critical sectors of business and government.

### 2. Improved operational efficiency

With remote access, your IT staff don't have to be onsite, or even near the data center. Instead of physically driving over or walking into a server room, they can fix a problem from their computer screen. In today's economy, when IT departments can be understaffed and overworked, remote access means doing more with less.

### 3. Better cooling/power efficiency

Cooling costs are a major component of today's IT budgets, and airflow planning is critical to data center design. But one of the major causes of cooling inefficiency is the service staff who open doors and wander around the equipment racks, and who find chilled server rooms uncomfortable. Remote access allows server rooms to be isolated from physical human interaction, for reduced energy consumption and longer equipment life

## What is Remote Access?

➔ Simply put, remote access is the ability to log on to a network from a remote location for data centers, it means that IT personnel can connect to and control the equipment in their data center from a remote location, generally over the Internet.

---

➔ A Remote Access Management solution can dramatically cut the time needed to access and control servers and devices—increasing productivity, reducing downtime, and saving money.

---

## Remote access tools for data centers

For data centers and computer rooms, remote access tools fall into three general categories:

### 1. In-band software: RDP, VNC, SSH, Telnet

- RDP, or Remote Desktop Protocol, is a Microsoft proprietary protocol that allows a graphical view of a remote computer's desktop.
- VNC or Virtual Network Computing is similar to RDP, but for non-Windows computers. It provides graphical desktop views and control of remote computers.
- SSH or Secure Shell provides a secure channel for data sharing between remote computers.
- TELNET is a text-based network protocol for two-way network communication using a "virtual terminal" connection.

These and other in-band tools are reliable, low cost or free, and in popular use. The limitation is that they are "in-band"—they can only access computers that are working properly (the operating system is running). RDP, for example, can't view, let alone fix, a Windows server with the dreaded "blue screen of death".

### 2. Out-of-band solutions: KVM, ConsoleServer, PDU

To go beyond the limits of in-band software, a hardware device is required. These devices are commonly available at commodity prices:

- a KVM switch, (for keyboard-video-mouse) controls

multiple computers from a single desktop.

"KVM over IP" switches provide remote Access and control over multiple computers via the Internet.

- a console server (or a console access server, console management server, serial concentrator, or serial console server) provides remote serial access to network devices. It is, essentially, a KVM switch for networking equipment.
- a PDU, or power distribution unit, distributes electrical power to the servers and allows remote monitoring of power-related data such as temperature and amps used. Some IP PDUs are switchable, meaning that the power can be remotely controlled.

### 3. Service Processors

A Service Processor is a hardware device that is either plugged into a server or embedded on its motherboard. It allows access to the server's internal management processes; some of its features are similar to IP KVMs and PDUs. Service Processors are available from the various server manufacturers, e.g. iLO from HP, DRAC from Dell, RSA from IBM, and IPMI from Intel, which is more of an open protocol.

## Remote Access Management tools: maximizing the benefits, minimizing the risks

While remote access tools are in common use, they have often been adopted gradually, one at a time,



often supplied by the manufacturers of the data center's existing equipment. As a result, companies may be enjoying some gains, but they're not likely to be maximizing their benefits. And they may have actually created new security risks.

### What are the new security risks?

While remote server access can increase an organization's security, it can also create security gaps. Perhaps the most critical is in access management: the vast majority of organizations store their passwords, user names, IP addresses, server names and more in a single spreadsheet or homegrown database. This provides IT personnel with almost unrestricted access to security-critical data, even data that has no relevance to their tasks. Windows admins can see how to access Unix machines, network admins can see how to access servers etc. There is no benefit to this, and considerable security risk. All an employee, intern or consultant needs to do is download the spreadsheet to a flash drive, and they can carry a corporation's secrets out of the building.

### The solution: task-appropriate access

To improve corporate security, a Remote Access Management solution should limit servers and IT tools to task-appropriate access. Windows admins should be able to access Windows servers only. Depending on their tasks, one admin may only require RDP access to a server, but not power and KVM access.

A Remote Access Management solution should restrict administrators to a single IP address and username—the address of the Remote Access Management interface itself. To access the servers, the administrator should use a web browser, where they enter the IP and their username and password. The system should then restrict them to only what their status allows them to see.

Some Remote Access Management systems go further, with authentication against AD or the like. This allows the quick addition or deletion of approved users. With a spreadsheet or homegrown database, any change of users is a cumbersome manual process.

### Measuring operational efficiency: resolving critical issues faster

When a server goes down, business operations can be at risk. Resolution speed is what matters. And with a spreadsheet or custom database, speed is a problem: first, the IT admin is notified of the issue. Then they have to open the spreadsheet, locate the name of the server, and copy and paste its IP address and password and username info. This can require opening and closing browsers and applications—and dozens of mouse clicks and many minutes, before a device can be found and accessed.

Then, once the device is located they have to fix the problem. They may try an RDP solution and fail, and attempt a KVM fix—and the copy and paste process begins again. The downtime adds up. Over a typical

---

➔ when comparing Remote Access Management solutions, compare the complete costs of the deployment. The advantages are clear: you can maximize your security, increase operational efficiency and save on energy

---

shift, the wasted minutes can add up to wasted hours of valuable work time.

### **The solution: a minimum 6x faster server access and resolution**

Minicom compared the mouse-clicks taken by IT staff using RDP and a spreadsheet, to a web-based Remote Access Management dashboard. In the best-case “spreadsheet” situation, it took 37 clicks, simply to access a server. The Remote Access Management software cut the number of clicks to six. That was a “test case”—the real-world situation is far worse: generally, RDP is just the first line of attack. If the IT admin has to try KVM or iLO access and then a PDU, the number of clicks increases exponentially—and if there’s a copy-and-paste error along the way, downtime jumps drastically.

➔ **When a server goes down, business operations can be at risk. Resolution speed is what matters.**

### **Critical factors for deploying a Remote Access Management solution**

If a company decides to adopt a Remote Access Management solution, where do they begin? When comparing solutions and vendors, keep these “success factors” in mind:

#### **1. A centralized web-based dashboard**

For security and efficiency, the Remote Access Management system should centralize access to servers and devices in a single web-based dashboard, with a simple interface that enables one-click access to servers and devices, and restricts access to task-appropriate servers and tools.

#### **2. Device and manufacturer agnostic**

In today’s technology market, change is constant. To protect your investment, don’t choose a Remote Access Management solution that restricts your future equipment choices. You may have standardized on one vendor’s servers, but you don’t want to be locked out, should a better server come on the market. Choose a system based on open standards, with the capability to monitor and control all major vendors’ equipment.

#### **3. Supports in-band, out-of- band and Service Processor access**

Your IT staff may use nothing but RDP today, but as you’ve read, there are major advantages to out-of-band access. Be sure that the system you choose will allow your technical capabilities to grow, by allowing the monitoring and control of out-of-band devices, Service Processors, and whatever new devices may appear in the future.

#### **4. Accommodates existing equipment**

A Remote Access Management solution does not necessarily require a “forklift upgrade”. Most data



centers are equipped various models of servers, from several manufacturers. Similarly, their PDUs, KVMs and console servers have been acquired over time.

Some Remote Access Management systems require you to replace your older gear—servers, PDUs, KVMs and/or console servers—or to purchase costly licenses in order to use the tools you already have in place. Not only is this large-scale replacement costly and wasteful, it can cause massive disruption to a company's daily activities—for example, replacing PDUs could require a complete server shutdown, and likely a total interruption of business. And it's not necessary. Solutions are available that accommodate existing equipment and tools. While newer tools may add functionality, they can be brought online in phases, without the costs and disruption of wholesale replacement.

When comparing Remote Access Management solutions, compare the complete costs of the deployment. The advantages are clear: you can maximize your security, increase operational efficiency and save on energy. And with proper planning a selection, you can minimize the complications and costs of the deployment, and ensure that the benefits of Remote Access Management will continue into the future.

**➔ Most data centers are equipped various models of servers, from several manufacturers. Similarly, their PDUs, KVMs and console servers have been acquired over time.**

### **A proven solution: AccessIT® from Minicom**

AccessIT from Minicom was designed from the ground up to meet IT managers' mission-critical requirements for secure web-based, centralized remote access management.

AccessIT provides fast, secure, trouble-free access to every aspect of a data center's infrastructure, and streamlines access to remote access tools such as RDP and KVM. It supports all major manufacturers of KVM switches, PDUs and console servers, and supports the industry's leading in-band and out-of-band remote access services, including RDP, VNC, VMWare, SSH, Telnet, HP iLO, KVM IP, and any proprietary web-based or customized applications.



---

For complete details, and to read  
how major customers have deployed  
Minicom solutions,

---

visit [www.minicom.com](http://www.minicom.com)