

Top Technologies

By Michael Healey

PITY THE REMOTE OFFICE.

Long on promises and short on technology support, workers at satellite sites often don't even have an IT person to beat up on when their Citrix sessions tank. Worse, they have a serious image problem: 57% of respondents to a recent reader survey cite remote employees as the biggest threat to their organizations among all users. That's unfortunate, because the trend toward geographically dispersed workplaces is growing as gas prices edge ever higher and companies seek alternatives to maintaining expensive centralized headquarters.

On the IT side, supporting remote offices has always been a challenge, whether they house 10 users or 1,000. Every network, no matter how small, requires care in architecture, security, failover, and performance planning. One poorly designed and unmanaged remote site can bring everyone down. Case in point: In a high-tech version of *Lord Of The Flies*, a single site for a distributed national trade show booth manufacturer spun out of control, eventually crippling the entire network. For years the remote site, based in the Midwest, had made ad hoc

As the drive to better support remote sites gains momentum, you need to separate helpful tech from roadblocks

changes to its network, disabling antivirus software, adding hubs and switches, and loading applications at will. Then, it complained about slow remote access to the home office and demanded more bandwidth. Somehow, this anarchy tribe managed to convince the CIO to give it a direct pipe—without additional virus protection—to help its “speed” problems.

As a result, the law-abiding central office was soon crawling with viruses and malware.

“It was the worse infestation I had seen in 20 years,” says the lead engineer brought in to clean up the mess. “It cost them a fortune, yet they’re still moving slowly to clean up the Midwest. They’re claiming it’s not them!”

And because vendors often lump satellite offices in

with the remote worker craze when pitching products, CIOs can have a difficult time separating helpful technologies from the IT equivalent of the Abdominizer. When word of this article got out, we were deluged with pitches for an amazing mix of innovative offerings, bad ideas, and good old vaporware.

Needless to say, most didn’t make our list of technologies that can make for more efficient remote office management. But we will discuss IP telephony, server and desktop virtualization, WAN optimization, unified threat management devices, and instant messaging from the perspective of what a main office may promise, and what a good remote IT team should point out as pitfalls. We’ll also discuss two technologies, Apple

Remote Wi-Fi: Do It Right

IF REMOTE USERS AS A GROUP keep security teams awake at night, remote users on wireless networks are the nightmare scenario. But it doesn’t have to be that way—secure WLANs are possible at remote sites, you just need a little specialized know-how.

Promise: With devices including laptops, PDAs, and smartphones providing seamlessly integrated wireless functionality, secure, on-demand Wi-Fi is fast becoming more necessity than luxury. Throw up an access point as an extension to the wired network and instant employee gratification is assured. “We have wireless now,” is what they’ll say.

That’s the theory, anyway.

Reality Check: In contrast to corporate headquarters where the brass walks the halls and wireless access is typically superb, the best most remote sites can hope for are a few autonomous APs slapped up by a visiting IT team as an afterthought during a server upgrade. The system may work, but it likely won’t work well. Impromptu deployments done to get the wireless monkey off IT’s back can backfire because these “solutions” are rarely well thought out, lack a cohesive design, are difficult to support, and are cheap, both literally and figuratively. To make matters worse, the more employees using the system, the slower access

becomes. In the best possible scenario, a single one-radio AP will service one person at about 20 Mbps throughput, two people at 10 Mbps each, and so on.

And, with a lack of on-site IT support, wireless can seem like a mystery technology to local users. Maybe you get interference with the neighboring business’ APs or from a poorly shielded microwave oven. Simple autonomous APs often lack the intelligence to identify sources of RF interference, and forget doing anything about it, such as switching to a less-congested frequency. Client configuration problems and old wireless drivers can confound users with the result being, “Hers works but mine doesn’t!”

One alternative, doing nothing, is worse because employees often will take matters into their own hands. A single unauthorized AP can leave the local wired network—and the corporate WAN to which it connects—wide open to exploitation. Since IT considers the remote site a Wi-Fi-free zone, who knows when the rogue will be detected.

The silver lining is that well-running wireless systems configured with a few essential features can provide adequate service to remote offices. Vendors such as Aruba Networks, Motorola (Symbol), and Cisco offer small versions of their controller-based lightweight Wi-Fi systems



\$499 million

Worldwide wireless LAN equipment revenue in 1Q '08; up 1% from the previous quarter as companies hold steady with investments.

Data: Infonetics

that are well suited to remote offices and can become extensions of the enterprise WLAN. This helps ensure that remote WLANs adhere to a company’s wireless security policy that defines controls such as authentication, role-based access privileges, and encryption. Further, extensions to enterprise wireless architectures may enhance performance through smarter channel agility and increase visibility by adding the ability to spot and report rogues. It’s even possible to have some of these features without a controller.

See much more on deploying WLANs to remote sites in our Wireless Everywhere Special Report, at informationweek.com/1188/report_wlan.htm.

—GRANT MOERSCHERL

Grant Moerschler is co-founder of technology consultancy WaveGard; contact him at infoweek@wavegard.com.

Macs and Vista PCs, best left to the consumer market.

And no, leaving software as a service and cloud computing off the list isn't an oversight—we're focusing on what IT can control to ensure that business runs smoothly at all locations, no matter where your applications reside.

SERVER VIRTUALIZATION

Promise: It's hard to find an enterprise that hasn't begun virtualizing the main data center, but should folks in the field follow suit? Short answer: All but the smallest sites should consider it. Even though few remote offices are dealing with the server sprawl and utility overload that drove big data centers virtual machine crazy, they face other challenges that virtualization can address, mainly around performance, backup, and disaster recovery. Moreover, virtualization software from VMware and Citrix continues to become less pricey, and Microsoft's Hyper-V is likely to apply further downward pressure.

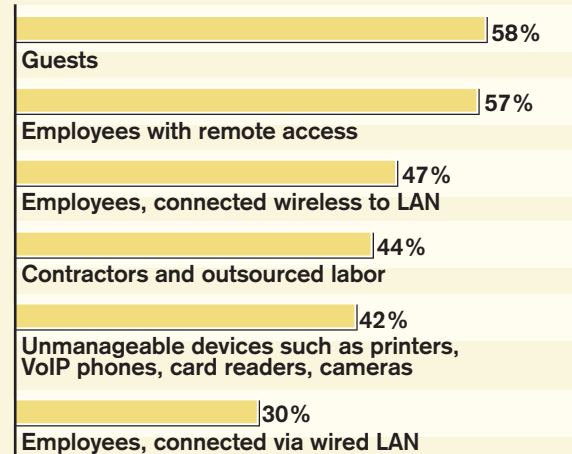
An "office in a box" can be built economically, leveraging two or three host servers configured with a small storage area network capable of supporting five to 20 servers in the future, depending on configuration. Companies won't necessarily spend for the additional software and equipment required to get higher-level virtualization features such as automatic failover and high-availability, but branches never had these before, and so likely won't miss them. Even with only basic virtualization in place, benefits will include better failover, improved utilization, and faster deployments. Future upgrades will be less time-consuming as well.

And the travel budget should see some relief from those emergency visits to rebuild servers. One client, the IT director of a national facilities management firm, summarizes the disaster-recovery plan for boxes that crash at the company's 100-plus remote offices thusly: backup tapes and plane tickets. The company is looking to pilot a virtualized "office in a box" for remote support and disaster recovery.

Reality Check: Most sites have closets housing a few 1U servers that, for a variety of reasons, can't be centralized, whether because of bandwidth constraints or support restrictions. The return on investment is definitely there to virtualize these mission-critical boxes, but HQ must not bank on the same boost it got when it started virtualizing the main data center. Also, remember the main concern for the remote office: support. The rapid growth of all virtualization platforms, especially VMware, has created a shortage of IT pros with engineering and troubleshooting skills. It's a short-term problem, but make sure in-house IT staff has VM expertise or has found someone who can jump in.

Big LAN Threats

Percentage of respondents who say the following users pose a "high" or "somewhat high" threat to their LAN



Note: Percentages based on a rating of 4 or 5 on a five-point scale where 1 is "Low" and 5 is "High."
Data: InformationWeek Analytics Network Access Control Study of 471 business technology professionals

Another major challenge for any virtualized infrastructure is getting an overall picture of components on the WAN. This is an age-old issue; in traditional networks we dumped countless hours into management systems like HP OpenView or SolarWinds, only to get burned by an unmonitored function. The challenge is escalated in satellite offices because the addition of a hypervisor host, virtualized servers, and a remote office SAN bring additional layers of complexity to the mix. Management utilities from virtualization vendors such as VMware and Citrix do a nice job of monitoring the virtual environment, but they don't integrate with tools from storage or server vendors. Few remote IT staffs have the capability to understand how all these components can be monitored, or the time to do so.

DESKTOP VIRTUALIZATION

Promise: Desktop virtualization is generating a lot of buzz as the savior for the remote office, with early offerings from VMware, Citrix, and Sun holding the promise of addressing some of the core problems faced in Citrix/Terminal Server environments. The concept that each user can check out a desktop session with no more worries about application or hardware incompatibility is undeniably appealing.

IT can apply standard desktop management strategies, whether group policies, SMS, or the more advanced Altiris or ScriptLogic, to remote office desktops. You can even put your desktop support team in charge. But the

biggest benefit is being able to give employees wider options. The limitations and potential crashes that can be caused by one user in a Terminal Server session are all but eliminated once desktops are running as virtual machines managed by a host. IT also can give remote office users the ability to load their own software—heresy in the Citrix/Terminal Server camp.

If it delivers, desktop virtualization is the mother lode for IT in terms of user satisfaction. Hang out at a Terminal Server-centric remote office for a while and listen; there's real frustration with remote access limitations. Reboots and resets from Citrix can impact 5% to 15% of users on a regular basis, depending on applications. In addition, there is a draconian element implicit in the setup. Customizable desktops? Forget it.

Reality Check: Virtualized Windows XP sessions

eral, you can get 25% to 30% more clients on a Citrix/Terminal Server box compared with a VMware host running XP virtual machines. Before advocating for VDI, examine current application requirements. You're probably a great candidate if you've got heavy users of Microsoft Office that also need a few fat-client applications currently hosted on Citrix. If you can leverage the local client for Web browsing and media playing, you can avoid most limitations of remote desktop clients—including Citrix and RDP.

IP TELEPHONY

Promise: It's tough to get a definitive read on the percentage of corporate PBX systems that are IP-based, but the trend is clear. Infonetics Research predicts that the tipping point, when IP PBX shipments will outnumber

may be better than Terminal Server, but users are still dependent on a remote desktop client. And graphics performance and the ability to play media files have long been sore points for thin-client-centric applications.

These problems remain, but newer clients and systems at least address local device access, including USB and CD/DVD drives. VMware's Multimedia Redirection supports MPEG and Windows Media files but no QuickTime, and it's only for Windows XP. Graphic performance has definitely improved, but AutoCAD users still won't be able to go hog wild with graphics resolution.

You'll also need more server horsepower for a virtual desktop infrastructure vs. a Citrix or Terminal Server setup. Both require beefy hardware, but in gen-

TDM systems, will occur next year, and the firm expects the TDM segment of the enterprise telephony market to dip below the \$1 billion mark for the first time this year. IP-centric vendors, notably Cisco, quote higher numbers, while those with a mix of TDM and IP systems, such as Avaya, Mitel, and Nortel, take a more nuanced stance. In fact, these vendors are using the ability to start the migration path but keep legacy handsets and port them onto a new IP PBX as a major selling feature.

So what does all this mean for branch offices? Plenty. Every major vendor offers an IP-based telecom system that lets remote sites become extensions of the main bank. Sure, the old TDM PBX systems did that, too. However, they typically required dedicated lines and fairly big boxes at both ends. In contrast, IP-based sys-

DIG DEEPER

STAY SAFE Virtualization is good for main and remote sites, but you need to deploy it safely. Learn how in this *InformationWeek Analytics Report*, free for a limited time at: securingvmware.informationweek.com

See all our Analytics at informationweekanalytics.com

tems add some crazy flexibility, like being able to take a single phone, connect it to the Internet, and have it become an extension. If you're willing to invest in a small, inexpensive PBX unit at the remote site, it could be programmed to take over all calls in the event of a disaster, routing extensions to cell phones or a smaller bank of numbers.

For those remote offices that have warehouses or production floors, you can take all telephony support back to the main site while providing branch employees with nice IP features, such as wireless phones that work in the office and softphones for laptops. The list of vendors that have fleshed out their remote-office IP PBX offerings is huge, a good sign of maturity. Take your pick—Alcatel, Avaya, Cisco, Mitel, NEC, and Nortel are all vying for this business.

Reality Check: Smaller sites can see major cost savings by removing all lines and linking their phone systems back to the main PBX. Offices with five to 10 phones can easily use the Internet to pass traffic if they

have a T1 or better, and average throughput needs. However, before pursuing this route, think about bandwidth impact and 911 emergencies. Linking your staff and customers via a

single extension system that supports transfers, conferences, and other PBX functionality is a big win in terms of productivity, and it will drive up your intersite call volume. Don't make the mistake of underestimating the potential bandwidth hit at both ends, particularly if you plan to use the Internet to handle traffic.

Moreover, it's amazing how many times we see folks lay out a plan to funnel all calls back to a main site and forget about emergency services. If a user dials 911 on an IP phone, that caller ID needs to show the local location of the user, not a routed call from the home office. One possible solution is to leave a few analog lines at the remote site. Or, a nonprofit in downtown Boston found an innovative way to link its offices while providing for emergencies. Because there was line of sight between the remote building and HQ, IT installed a wireless bridge between the two sites and created a central phone system, then added a small phone switch at the remote location with a few analog lines. The switch was programmed to route 911 calls through the local lines, giving critical location details to responders.

Another option is to provision DSL at the remote office. DSL Internet links typically include two local lines, which also helps shore up redundancy. Many remote offices have only one Internet connection, so as more applications are moved into the cloud or centralized at the home office, the single line to the Internet becomes a major risk point. Supplementing a main line (typically a T1) with a DSL, cable modem, Verizon FiOS, or business-class wireless bridge like those from Towerstream is a must for remote sites. These second-tier lines won't come with a service-level agreement like a T1 provider, but they're a great way to increase bandwidth and provide backup connections. You should be able to easily add them into your remote firewall if you've adopted one of the modern unified threat management devices (more on UTM below).

Beyond The Basics

» **Make sure you understand all applications in use locally.** Many remote sites have legacy apps that haven't been brought into headquarters. We've seen plans to consolidate apps in the main data center derailed when an important piece of software requires the local IT team's support or runs poorly over a WAN.

» **Bandwidth should always be top of mind.** Before deploying any technology to remote offices that will increase the WAN load, dig into the sites' traffic profiles. This includes pulling data from telcos and ISPs as well as monitoring traffic on your network.

» **Make individualized disaster plans for each site.** What will workers do if they lose their primary line or phone connectivity? How can employees work locally if the backup lines fail, too? Have a process for getting local data replicated after the outage is resolved.

» **Audit remote sites for local data silos.** Critical information often ends up stored on local servers or, worse, on local machines, because of convenience or ignorance.

» **Don't dictate from on high.** Bringing remote sites into the mix and listening to feedback and concerns will help focus priorities and set the foundation for collaborative technologies.

WAN OPTIMIZATION

Promise: The concept is straightforward: Stick an appliance on both sides of a WAN link and, voilà, faster traffic. No clients to load, no messing with the firewall (maybe). There are plenty of vendors to choose from: Blue Coat, Cisco, Citrix, F5, Juniper, Packeteer, and Riverbed have all been in this space for a while,

tweaking and refining their systems or buying up promising upstarts. And they've all moved toward creating platforms that support appliance-to-appliance optimization and support for "soft clients," letting you bundle WAN investment to give even home office workers some compression.

Reality Check: Test before you buy because performance is dependent on application load. In general, the bigger the individual packet size for an application, the better the optimizer will work. If you don't have a good sense of what traffic flows between your sites, we recommend getting an extended demo or try-and-buy. For example, if traffic between HQ and a remote office is mainly Citrix sessions, dropping \$50,000 on a compression appliance is probably not the best way to improve speed. The packets are small and typically don't

transfers, and Exchange. Worst bets: Citrix, Terminal Server, Telnet, VoIP (because compression should be done at the IP PBX), and GroupWise.

UTM APPLIANCES

Promise: If there's one thing that creates friction between headquarters and remote IT staffs, it's device proliferation. One router, one firewall, one antivirus box, one intrusion-prevention system, one SSL/VPN appliance, one content filter, and soon there's no room for a coffeepot.

Enter the UTM, or unified threat management, appliance. The concept has been growing and expanding over the years, arguably in response to the security needs of smaller businesses. A 20-person office has the same threats as a large enterprise; however, this

get enough boost from WAN optimization technologies.

A client company was all set to pull the trigger based on initial tests of passing graphics files. IT started down the slippery slope of creating an ROI calculation based on that initial compression. However, while the graphics transfers were a huge part of overall bandwidth, they represented only a small fraction of time during the day and a small number of users. The rest of the office used Citrix exclusively. They'd see a boost, but not the 50X performance jump that was in the cost justification for the CFO. The project went forward, but after setting the proper expectations; the purchase was justified for the graphics team, not for everyone.

Best bets for performance boosts that folks will notice: printing, SSL/HTTPS traffic, FTP, Windows file

market typically refused to purchase multiple single-function devices. In response, security vendors such as SonicWall and WatchGuard added functionality to their appliances while striving to improve performance. Others, like Fortinet and Astaro, built from scratch based on the UTM concept. Not to be left out, larger players, notably Check Point, Cisco, and Juniper, have either combined existing functions or introduced new products to add broader UTM features on one box. This competition has spawned a wealth of options for remote sites, while the UTM concept provides central office with added consistency and manageability.

Reality Check: Some UTM boxes may actually do too much, adding unneeded complexity. The key functionality remote sites need: basic firewall, gateway an-

IN DEPTH / REMOTE OFFICE SUPPORT

tivirus, intrusion prevention, content filtering, load balancing/failover, and site-to-site VPN. Nice-to-have features include inbound SSL/VPN, anti-spam, and client VPN access.

Push hard to get the right size device. Most vendors have product lines that can scale all the way up to the main office (imagine, a unified security design). Central IT could set the overall policy and design and give remote offices some level of control over which appliance is right for them.

INSTANT MESSAGING

Promise: As instant messaging use continues to grow within the corporate walls, some sites have seen a reduction in e-mail of 10% to 15% and faster response to questions. IT departments were often the first to

Communicator, the latest retooling of Microsoft's IM strategy. Redmond's previous IM attempts, notably Exchange 2000 Conference Server and Live Communication Server, have left many IT folks gun shy when it comes to Microsoft IM. Other possibilities for enterprise IM include software-as-a-service vendors like Near-Time and Google, as well as IP PBX vendors like Cisco and Mitel that combine their hardware and software into a unified approach.

Consumer IM systems such as MSN or AOL are free, but you get what you pay for. They generally don't provide enterprise-class control tools, such as access lists or logging, required by some compliance policies. AOL abandoned its enterprise IM service in 2004.

Reality Check: What if you bypass free services, invest in corporate IM, and no one uses it? Will the com-

adopt IM, with remote offices becoming early benefactors of smoother communication, quick updates, and a reduction in e-mail chains. A medical instrumentation company in Boston, for example, deployed an enterprise-class IM system for the IT team. The goal was to facilitate better communication within the department. Remote IT staffers were added after the fact to address complaints about multiple voice-mail messages.

The project quickly expanded to engineering, production, and sales. The company got to 100% IM adoption within one year through a grassroots movement.

For an IM client the site, an IBM Lotus Notes shop, used Lotus Sametime, which has very nice integration with Notes. The company recently moved to Exchange but kept Sametime, not willing to switch to Office

pany embrace IM, or will people simply see it as an annoyance and set their systems to perpetually "busy"? To know the answer, understand the culture at branch offices.

Then there's the Big Brother angle. If you think "IT is watching us" conspiracy theories are rampant at the corporate headquarters, head out to the field some day. Add any IM product with logging turned on—mandated for many companies—and folks get even more paranoid.

Finally, there's the specter of lost productivity. Unless you've blocked all the variants of IM, some users are already doing personal messaging. Once you sanction IM for corporate use, expect a flood of requests for gateway services to outside providers like

IN DEPTH / REMOTE OFFICE SUPPORT

AOL. It's a brave new world, and not everyone knows the rules. One senior executive told us he didn't think having an IM chat open all day with his daughter was the same waste of organizational resources as if he were calling her 20 times a day. How did I know they were IMing? He was constantly looking at his machine and typing back during our conversation.

DON'T GO THERE

As always, there are technologies to avoid, and we'll address two specifically: Apple Macs and Microsoft Windows Vista. Let's face it: Many IT staffers and C-level folks now have Macs at home. Engineers love 'em. They can run Mac OS, Windows, and even VMware all on the coolest-looking laptop since the Epson HX-20 (Google that). Apple's market share, while still

SharePoint or Outlook Web access, Safari or Firefox users won't get the full functionality.

» Unix chops. Just because engineers like Macs, that doesn't mean they know how to fix them. Don't forget, at the core of this nice-looking laptop is a BSD Unix kernel that takes some real skills to troubleshoot.

» Desktop management tools. Every network needs to have some level of desktop management, from asset tracking to desktop policies to patching and control. If you're Windows-centric, throw out most of your desktop management tools and strategies once you support Macs. You can integrate them into Active Directory, but your Group Policies won't run. The closest you'll get to a mixed-platform system is Altiris, and that's limited to inventory and software delivery.

As for Vista, this is one area where both headquar-

relatively miniscule, is growing, according to most analysts. At first glance, Macs seem to make sense in the remote office because the promise (at least in the commercial) is that Macs are easier to use.

That's what can bite you. Now, before you flame us, we like Macs. That said, they have major problems in a corporate environment, especially in an office that may not have sophisticated users. The issues:

» Limited support for Microsoft applications. Yes, it matters. Office for the Mac is good, but it's not the same client as Exchange. The connections and layout are different and don't offer the same functionality.

» No Internet Explorer. This matters less than in the past in terms of Internet delivery of many applications, but for using Microsoft-centric apps such as

ters and remote offices agree: Most will stick with XP for now, thanks. We recently reviewed the plans and licensing for our larger clients with enterprise agreements with Microsoft. Less than 3% run Vista in any significant capacity, and very few have begun developing formal rollout plans. The reasons include hefty hardware requirements and existing investments in XP equipment and skill sets; the difficulty of making custom applications work on Vista; and the extensive user retraining required, a problem exacerbated with multiple remote office sites.

Michael Healey is the CTO at GreenPages Technology Solutions. He has more than 20 years of experience in technology and software integration. Reach him at michael.healey@greenpages.com.