

Special Report

# Tech tools for small business

By Network World Editors

Sponsored By:



Gateway



Produced By:

NetworkWorld  
[www.nwfusion.com](http://www.nwfusion.com)

*Times are changing. The largest technology companies are starting to pay attention to small- and mid-sized businesses and the technology itself is becoming easier to digest and leverage.*

*This Special Report examines the shifting technology landscape and some of the most promising new tools, including wireless and the all important question of how to secure the airwaves, voice/data convergence and how this fits into the new wireless environments, and finally, advances in network management (including a resource list of tools ideal for the small shop).*

## Table of Contents

- Downturn offers silver lining for smaller IT buyers .....3**
- VoIP unwired: Voice and wireless Ethernet might seem an odd mix, but for mobile workers or hard-to-wire areas, it can be the perfect combo. ....5**
- Plugging wireless security holes: New standard could drive hot spot, academic installations. ....7**
- Pick your management weapon: software or hardware? .....9**
- The price is right for these management tools .....11**

## Downturn offers silver lining for smaller IT buyers

BY JAMES NICCOLAI AND STACY COWLEY  
IDG NEWS SERVICE, 11/25/02

With sales to large customers in a tailspin, suppliers of enterprise software products have stepped up their efforts to target midsize customers as a way of boosting revenue in the tough economic times.

Estimates vary, but preliminary figures from IDC suggest that despite the lagging economy overall sales of IT products to small and mid-sized businesses (SMBs) will grow 4% this year, eclipsing growth in sales to larger customers. By 2004, annual growth could hit 8%, with SMBs accounting for close to a third of all IT spending, said Ray Boggs, vice president for small business and home office research with IDC.

In the U.S., SMBs spent \$135 billion on IT purchases last year, comprising 30% of total IT spending in the country, according to New York research firm AMI Partners. In specific software niches such as customer relationship management and enterprise resource planning applications, the number of SMBs making purchases is doubling annually, said Andy Bose, AMI CEO.

Many smaller businesses are just now becoming comfortable with the Web, spying opportunities to use technology as a way of boosting efficiency and becoming more competitive, Bose said. Having sat on the sidelines during the Internet's first period of rapid growth, many are now taking their businesses on the Internet, using it to connect with customers and suppliers.

"Using the Web to gain competitive advantage and as a productivity tool is just now starting to be embraced in a broader perspective by smaller businesses," said Mark Ouellette, vice president for worldwide SMB sales and marketing with IBM's software group, which is among those more aggressively targeting smaller customers.

Spying the trend, SAP, PeopleSoft, Oracle, Vignette, Sun and a raft of others have also been tuning and rebuilding products in a bid to tap the growth among SMBs, generally defined as companies with up to 1,000 employees. Many vendors acknowledge that the shift in focus has come at least partly because larger customers are not spending so much.

Sun said it plans to make a "substantial" investment this year to reach more smaller customers through its iForce initiative. The effort involves partnering with an array of independent software vendors and channel partners who build systems that make use of Sun's hardware and software.

"Overall spending and server spending is growing faster right now in the midmarket than in the enterprise, and absolutely that has caught our eye," said Cheryl Kelly, director of marketing at Sun's iForce program.

Meanwhile, IBM is rolling out a family of middleware products for midsize customers under the Express brand. It started with its software for building portals, added its application server and will soon release an Express version of its DB2 database. Like Sun, it too is strengthening ties with the wide network of ISVs that it relies on to develop applications for the midmarket.

In June of 2002 Novell launched NetMail XE, a low-cost version of its e-mail software that it hopes will compete with Microsoft Exchange. Vignette recently rolled out suites of its content management applications specifically for the midmarket. The list goes on.

But midsize customers have unique needs, and it's far from clear that these and other offerings will fit them as well as vendors claim, analysts said. SMBs have smaller IT staffs and avoid the expensive customization that's a routine part of large enterprise purchases. They are used to close relationships with local partners. And they run different IT platforms, generally favoring Microsoft's Windows over the Unix systems common at big businesses.

What's more, some vendors have done a poor job of tailoring their products to meet the needs of smaller customers, said Mika Krammer, a research director with Gartner who has written several papers on the topic.

"In some cases, (vendors are) simply stripping away some of the complexity and functionality and repositioning the product, and that has not been a successful strategy," Krammer said.

Balancing simplicity with needed functionality can be the trickiest part of selecting IT systems, SMB customers say.

When Chad Pomeroy, CTO of health-care program provider Lumenos, began evaluating products in August to select a CRM system for his fledgling company's sales staff of around 30, he considered vendors with which the company already does

business, including Siebel Systems and Oracle. But he decided quickly that those vendors' CRM offerings were too complex for Lumenos' fairly basic sales needs.

"We just needed something that would run pretty much out of the box," he said. He chose Salesforce.com, which sells a CRM system that it hosts. Salesforce.com's subscription model helped win him over, he said: "There's no huge upfront investment. That's definitely something we appreciated."

While Lumenos, based in Alexandria, Va., has been quite happy in its dealings with Oracle and Siebel, he noted, "When dealing with any large company, being a smaller fish in their pond, you may not get the response you're looking for."

John Wade, president of multimedia materials provider Gung-Ho, in Incline Village, Nevada, feels the same way. His company picked ManagedOps.com, an application service provider in Bedford, New Hampshire, to host his Great Plains (a vendor now owned by Microsoft) ERP applications. The "boutique ASP," as he termed it, specializes in Windows and Great Plains environments, and is small enough that it gives him the attention he likes.

"I know the people there and I talk to them. I have my point of contact from sales, my IT has his point of contact for IT, and they've afforded us opportunities to talk to them along the way," he said.

But some in the midmarket need the features top-tier vendors are accustomed to providing. Tanning Research Laboratories, (which does business under the name of its top product, Hawaiian Tropic sunscreen) decided last year it needed a new e-business system to replace a patchwork of older programs running internally and at distributors it had recently acquired. The Ormond Beach, Florida, company has more than \$100 million in annual revenue and sells a product regulated by the U.S. Food and Drug Administration, which "adds a lot of complexity to the manufacturing process," said CFO Bill Jennings.

It considered software from vendors such as Great Plains, Jennings said, but those packages lacked the functionality Hawaiian Tropic needed. But when it solicited pitches from enterprise vendors touting versions of their products tailored for the midmarket, including Oracle, it couldn't elicit the reassurances it needed that its deployment would come in on time and on budget.

Hawaiian Tropic chose software from SAP, on which it went live in August 2002 after a seven-month installation. Sealing that decision was the sales pitch from Plaut Sigma Solutions, an SAP reseller that handled Hawaiian Tropic's deployment: "They proved it was a doable project. I never got that feeling from any of the others," Jennings said.

He was also drawn to SAP's pricing. While other vendors had complex cost structures based on the number of modules installed, SAP offered a flat, per-user licensing fee covering all the modules Hawaiian Tropic wanted to use.

But customers should be wary of lasting commitment from the biggest vendors, according to Gartner's Krammer. Some are acting opportunistically, she said, looking to shore up revenue until the economy recovers. Returns tend to be lower from midsize customers, and some vendors may find it hard to justify sustaining development and supporting commitments in the long run, she said.

"I project when the economy does pick up, a lot of these vendors will pull back. Fifty percent of them will be getting out as quickly as they got in and reverting to their bread-and-butter enterprise customers," she predicted.

It's too early to tell which vendors are serious about the mid-market and doing a good job of creating tailored products, said analyst Jim Shepherd, a research fellow with AMR Research Inc., in Boston.

**Leadership.  
Innovation. Performance.**

**Celebrate 30 Years of Ethernet**

1973 30 YEARS of Ethernet 2003

3COM Possible made practical™

**You Could WIN! Click Now to Enter**

[3COM](#)

"If you're an SAP or Oracle or PeopleSoft, you have a reputation for having built sales channels and support programs for very large companies. You have to convince people that you also know how to serve very small companies," he said. "Clearly, you have to be able to say, 'We have a different product for you, designed for your needs and capabilities.' They really aren't there yet."

The new products do present opportunities for midsize companies, in part because declining sales have forced vendors to lower prices, but customers need to be cautious, Krammer said. They should choose a vendor that has been in the mid-market for more than just a few months, pick one that offers products tailored to specific vertical industries and look closely at customer references, she said. Otherwise, smaller customers may find they've bitten off more than they can chew.

*The IDG News Service is a Network World affiliate.*

## VoIP unwired

*Voice and wireless Ethernet might seem an odd mix, but for mobile workers or hard-to-wire areas, it can be the perfect combo.*

**BY PHIL HOCHMUTH**  
**NETWORK WORLD, 07/28/03**

Converged voice/data network projects can be tough, especially if you can't use any wires. That's what Mike Burns, a systems integrator, discovered when a client asked him to provide voice and data services to a gold-mining operation in the middle of a Laotian jungle. Burns faced a sticky situation - literally.

"The ground was mostly mud, so we couldn't bury any cables, and there were no poles where we could hang wire," says Burns, who is president of Nationwide Computer Systems, an ISP and integration firm in Fort Lauderdale, Fla. The solution would obviously be a wireless one: Burns used 802.11b gear to connect 50 IP phones, PCs, a router and satellite dish for the mining camp. The camp, which stretches over a two-mile area, consists of 20 structures for operations, living quarters and offices.

Wireless Ethernet certainly isn't the first infrastructure that experts recommend for carrying voice over IP (VoIP), but Burns and other users are finding 802.11 works fine for their IP telephony requirements. The combination of the technologies is proving useful for keeping mobile employees, such as hospi-

tal workers, in touch or for linking IP phones in areas where Category 5 cabling is hard to run.

Voice quality can be a major issue because Wi-Fi LANs are slow at 11M bit/sec, and in most cases, a shared medium, likened to 10Base-T hubs. The IEEE is creating standards to increase security and quality of service (QoS) on Wi-Fi - such as 802.11i and 802.11e - but widespread adoption of those technologies is still at least a year away.

While some users say IP voice quality is fine over Wi-Fi, others have adopted proprietary QoS features supplied by Wi-Fi and wireless IP phone makers to make sure of that. At the mining camp, where voice and data contend for Wi-Fi connections, Burns relies on router-based QoS.

Burns built a wireless VoIP network using an AltiGen Communications AltiServ IP PBX, Polycom IP phones, Lucent Wi-Fi access points - lashed to trees, Cisco hubs and a router, which connects to satellite equipment for outside communications. Hubs and Wi-Fi routers in the camp buildings connect the IP phones and connect to PCs for e-mail and mining data analysis. (More than a dozen gas generators power the network gear.)

Connecting the mining camp to the outside world was easy, Burns says. A satellite dish syncs up to a fiber connection in Germany, which ultimately runs to Nationwide's ISP point of presence in Florida. The hard part, he says, was connecting telephones down on the jungle floor for calls between buildings - or huts, as Burns calls them.

"There was no way we could have deployed a traditional PBX in this environment," he says.

"It was pretty out there," Burns says of the network, which is still operating. "I've thought about that project a lot, and there was no other way we could have done it."

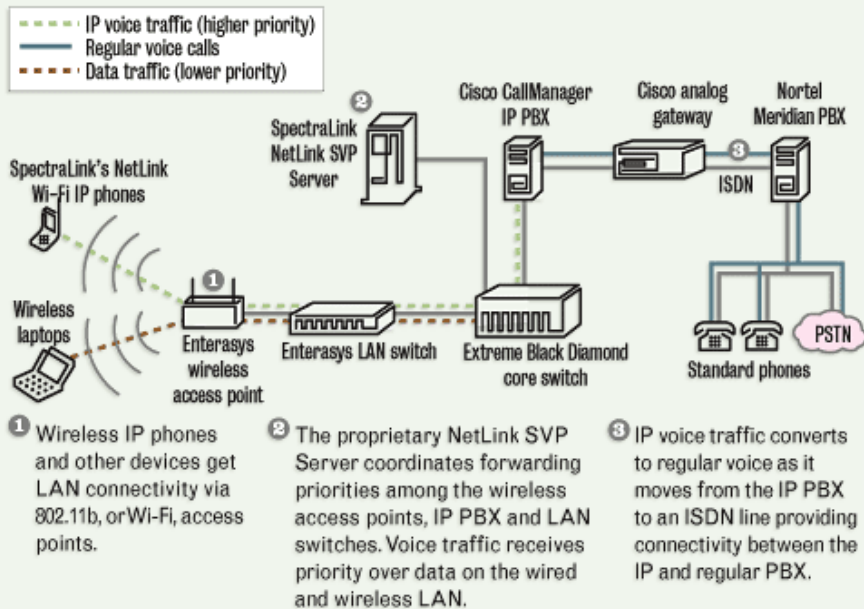
## Wi-Fi and VoIP

At Mercy Medical Center in Roseburg, Ore., IT Director Nancy Laney could have given nurses regular phones or new pagers, but opted for wireless VoIP devices instead. The hospital uses wireless VoIP communications badge appliances from Vocera Communications.

Nurses wear the gadgets, about the size of TV remotes, around their necks with lanyards or pinned to their shirts. To reach someone, a nurse presses a button on the badge and scrolls through names in the system, then presses another but-

## Wi-Fi VoIP: Behind the curtain at one medical center

University of Southern California University Hospital uses QoS technology on a Wi-Fi gateway and at the LAN switch to ensure wireless IP voice calls get priority as they cross the LAN.



ton to talk. The voice signal travels to the recipient over the hospital's Wi-Fi infrastructure.

Mercy Medical installed 10 Cisco Wi-Fi endpoints throughout the facility to support the Vocera infrastructure, which replaces an outdated pager system, Laney says. Wireless VoIP lets nurses contact each other faster and more efficiently than previous pager systems or with telephones, she adds.

"We were going to install a wireless infrastructure anyway, so we just accelerated that project" when deciding to use the Vocera devices, Laney says. "After a 30-day trial, our nursing staff was hooked. We've had technology rollouts that met some resistance, but this is not one of them."

A Windows server running Vocera's management software and user database controls the Wi-Fi VoIP network on the back end. The software lets administrators add and remove users from the system and customize individual calling features. They can track users on the system using an open source MySQL database. The hospital uses interactive voice response (IVR) software from Nuance, processing voice-activated commands.

During emergency situations when nurses don't have time to scroll through names, they can use the IVR feature by voice

prompt. Speaking a person's name, the name of a group or for all nurses on a certain team will initiate the call.


Users also can find where someone is through the Vocera system. They say "find" and the name of the person, and the IVR software responds with the location of the requested user. To make this possible, Laney has assigned all the Wi-Fi access points in the hospital a name based on their location, such as "Emergency," "OR" or "Cafeteria" and entered them into the Vocera database. The hospital even is attaching Vocera badges to frequently used pieces of equipment, such as EKG machines or defibrillators so nurses can find these devices quickly, Laney says.

Mercy Medical has plans to give nurses wireless tablet PCs, so the Wi-Fi infrastructure will soon be carrying data, too, Laney says. Because the Cisco access points can support the prioritization of voice traffic, Laney says she does not anticipate bandwidth-contention issues.

The Vocera system is slightly more expensive than the pager system it replaced, but Laney says she expects the hospital to save money ultimately because it is giving wireless VoIP access to other groups, such as doctors, maintenance workers and cleaning staff. These employees had used pager systems or walkie-talkies.



### The Gateway IT Playbook

Free resource for technology professionals



- Latest IDG research
- White papers
- Searchable information
- Regular updates

> [Visit ITplaybook.com](http://ITplaybook.com)

[Gateway](http://Gateway.com)

Similarly, at University of Southern California University Hospital (USCUH) in Los Angeles, nurses and doctors now stay in touch via 802.11b-based NetLink IP phones from SpectraLink. A total of 273 wireless IP handsets are in use at the hospital. Wireless IP phones are now a single source of communication for all staff, and replace a mix of communication methods used in the past such as nurse call

buttons, a public address paging system and cordless telephones - which were inefficient, says Anthony Kellogg, project manager for USCUH.

The wireless VoIP decision came after two separate infrastructure projects USCUH undertook last year. In the first, the hospital built a Wi-Fi network using Enterasys Networks gear to support mobile devices, such as laptops.

traffic converts to regular voice as it moves from the CallManager to an ISDN line, connecting that IP PBX to the Nortel Meridian PBX.

While adoption of wireless LANs isn't expected to outpace wired networks anytime soon, and land lines for voice are still king in most organizations, users willing to push the IT envelope are finding that Wi-Fi VoIP is more than just the combination of two industry-chic acronyms.

## Plugging wireless security holes

*New standard could drive hot spot, academic installations.*

BY JIM GEIER  
NETWORK WORLD, 03/31/03

The wireless LAN industry's first crack at security - 802.11 Wired Equivalent Privacy - has been discredited and rightly so. WEP is so easy to break that it's like having a plastic lock on your office door.

Although WEP can keep casual snoopers from accessing a wireless LAN, companies need and can do much better.

Effective wireless LAN security solutions, such as Cisco's Lightweight Extensible Authentication Protocol (LEAP), have been in use over the past year, but they provide limited interoperability. In most cases, client radio cards and access points must be from the same vendor, something that doesn't fare very well in public hot spots and many companies that don't enforce a standard desktop.

Late last year, the Wireless Fidelity (Wi-Fi) Alliance announced Wi-Fi Protected Access (WPA), a standards-based security mechanism that eliminates most 802.11 security issues.

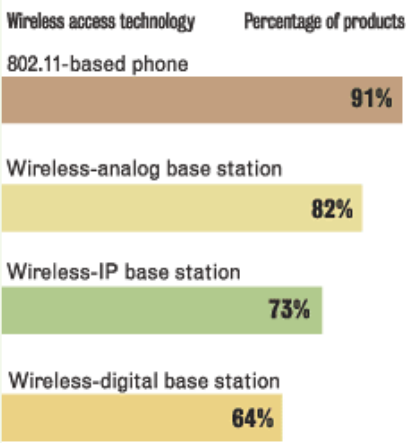
### WPA basics

WPA is based on the current state of the 802.11i standard, which is still under development. Ratification by the IEEE isn't expected until late this year. The Wi-Fi Alliance, realizing that the long wait is stalling the market, launched WPA, which is expected in vendor products this spring.

One advantage of WPA is that it enables the implementation of open wireless LAN security in public areas and universities. These hot spots and academic sites haven't been able to use basic WEP.

### Anticipating Wi-Fi VoIP

In a survey of 15 IP PBX vendors, making 22 IP-based telephony systems, Miercom found that most respondents' devices can handle calls from 802.11-compliant wireless phones.



### Calling CallManager

In the second project, the hospital installed a Cisco CallManager IP PBX to connect some remote facilities to a Nortel Meridian PBX over IP. USCUH brought those projects together when it chose to give the medical staff Wi-Fi phones. To ensure voice quality, the hospital relies on SpectraLink's NetLink SVP Server, which provides a proprietary QoS feature for giving voice calls priority over data. When the voice packets hit the wired network, they are placed into the first of eight priority queues on the Enterasys LAN switches.

CallManager - a redundant Windows server running Cisco's IP PBX software - routes all calls inside the USCUH. (The majority of the SpectraLink traffic is internal.) CallManager also provides call-control features, such as call forwarding, hold and dual-line support. While most VoIP calls are internal, SpectraLink phone users can place external calls, too. The VoIP

A key flaw in WEP is that its encryption keys are static rather than dynamic. That means to update the keys, an IT staffer has to visit each machine, which isn't feasible in an academic setting or even possible in a hot spot. The alternative is to leave the keys unchanged, which makes you vulnerable to hackers.

These public sites haven't been able to use the stronger proprietary mechanisms, such as LEAP, because of the interoperability issue.

But WPA provides effective key distribution and enables use across the often different vendor radio cards.

To ensure that WPA is taken seriously, the Wi-Fi Alliance has mandated that by year-end the security mechanism will be required for all new Wi-Fi certifications. It's likely that WPA also will become the default out-of-the-box configuration, which would help the majority of small office/ home office (SOHO) users. Older products will not need to comply, but vendors surely will supply applicable upgrades.

### How WPA works

WPA includes both the Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms, which together provide dynamic key encryption and mutual authentication for mobile clients. WPA thwarts hackers by periodically generating a unique encryption key for each client.

TKIP introduces new algorithms to WEP, which includes extended 48-bit initialization vectors and associated sequencing rules, per-packet key construction, key derivation and distribution function, and a message integrity code (referred to as "Michael").

In companies, WPA can interface with an authentication server, such as Remote Authentication Dial-In User Service, using 802.1x with EAP. The authentication server is a storehouse for user credentials. This function enables effective authentication control and integration into existing information systems.

WPA implementations in SOHOs, however, don't require an authentication server because of the ability to operate in "pre-shared key mode." Similar to WEP, a client's pre-shared key (often called a "pass phrase") must match the one stored in the access point. An access point uses the pass phrase for authentication. If the phrase matches, the client is given access to the wired side of the access point.

WPA fixes all known problems with WEP, except denial-of-service (DoS) attacks.

Potential DoS attacks are a significant risk for any application where loss of wireless LAN access affects life, profits or reputation. A hacker easily can bring down a WPA-protected network by sending at least two packets using the wrong key each second.

When this occurs, the access point assumes that a hacker is trying to gain access to the network. The access point shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Thus, a continuous string of unauthorized data can keep the network from operating indefinitely, which means you should have a back-up process ready for critical applications.

### Implementation considerations

WPA is primarily a solution for legacy equipment because you can install WPA via simple software upgrades to your Wi-Fi-certified access points. This enables effective security among clients having different radio cards, assuming the radio cards also implement WPA. Access points that implement WPA will support a mixed environment of client devices, ones implementing WPA and others that don't.

WPA will maintain forward compatibility with the 802.11i standard. The eventual 802.11i standard will include Advanced Encryption Standard (AES) as an option, which is stronger



**Business solutions that grow with your business.**

Get the essential technology you need at Dell Medium Business.

intel inside pentium 4

More Details

Easy as **DELL**

Dell

### Evolution of wireless LAN security

WEP goes the way of the dodo bird, WPA emerges as missing link to 802.11i

Name	Wired Equivalent Privacy	Wi-Fi Protected Access	802.11i or Wi-Fi Protected Access Version 2
Acronym	WEP	WPA	WPA2
A.K.A.	Won't Even Protect	Will Protect Alright	Will prove airtight
Features	Weak encryption keys based on RC4 algorithm (typically 40-bit keys).  Static keys that make easy targets for hackers	Same underlying RC4-based encryption as WEP  TKIP (temporal key integrity protocol) added so that keys are rotated and encryption is strengthened.	Strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes).  Adds two strong authentication features: wireless robust authentication protocol or WRAP; counter with cipher block chaining message authentication code protocol or CCMP.
Life span	1997-2003	2003-2004	2004-??????

than RC4. But an issue is that AES will likely require the replacement of a legacy access point because of the need for higher performing processors. As a result, 802.11i will be targeted for new equipment.

Is WPA an interim step or a long-lasting solution?

WPA can provide excellent security. The demand for compliance from the Wi-Fi Alliance assures users of plug-and-play security that has been a real roadblock to wireless LAN proliferation.

Customers should implement WPA through upgrades to existing equipment and should insist on it in new equipment. Because of new hardware requirements of 802.11i, WPA will likely be a security solution that lasts until you move to the next generation of hardware.

*Geier provides independent consulting services to companies developing and deploying wireless network solutions. He is the author of the book, Wireless LANs. He can be reached at jimgeier@wireless-nets.com.*

## Pick your management weapon: software or hardware?

BY DENISE DUBIE  
NETWORK WORLD, 06/30/03

Semiconductor company Smith & Associates is bent on getting a better handle on its network resources, recognizing that it just can't afford to keep adding servers every time LAN traffic spikes.

In exploring its options, the Houston company has determined that a different network management strategy was in order. But instead of taking the conventional path of swapping its old management software for new, the company is looking to replace its software with ... hardware.

"We need a product that offers some automation and doesn't require my staff to be in front of it 24-7," says Bob Ackerley, president and co-founder of the semiconductor maker. The company is leaning toward start-up Vieo, which released its multifunction management appliance into beta tests last week. The box would replace software from BMC Software and Peregrine Systems, which, while working as advertised, no

longer fit Smith & Associates' needs in managing about 22 Unix and Windows servers in its data center.

The debate over whether to manage networks via software or hardware - or some combination of the two - is an increasingly common one as IT budgets remain tight and a new breed of management appliances hits the market from a mix of newcomers and more established vendors such as Gold Wire, Oculan and SilverBack.

The products come with a host of management capabilities, including network discovery, fault management, security management and performance monitoring. While management software that runs on general-purpose hardware is tried-and-true, if often expensive and complicated, management appliances have the advantages of simplicity and aggressive pricing.

"Pricing is key to the management appliance model," says Glenn O'Donnell, research director at Meta Group. "Dedicated devices must be priced low enough to offer ROI within six months."

Appliances are in the \$1,000 to \$30,000 range, whereas management software installations can run into hundreds of thousands or even millions of dollars.

But lower prices often come fewer features and less scalability (Gold Wire's Formulator configuration management box, for example, maxes out at about 3,000 managed nodes). For this reason, appliances are seen by many as the purview of small to midsize companies with less-demanding IT needs.

Appliance vendors configure the processing power in their boxes to work specifically with their management software. They claim this helps avoid the sort of CPU meltdown general-purpose servers are vulnerable to when trying to juggle events, alerts and non-management applications.

"The big advantage of the packaged system is you get a bounded, plug-and-play solution. It removes the necessity of the staff having to do all of the run-of-the-mill management tasks," says Rich Ptak, principal of consulting firm Ptak Associates.

Still, appliances make up a fairly small chunk of the overall management product market - 10%, according to consulting firm Enterprise Management Associates (EMA). This number includes earlier management appliances, such as packet shapers, that tend to focus on one task.

"Software can be more flexible and easier to integrate with other applications, and frankly, there are fewer ways to slice and dice scalability with an appliance," says Dennis Drogseth, an EMA vice president.

Chris Holbert, director of IT at North American Scientific in Chatsworth, Calif., uses Computer Associates' Unicenter software to manage his LAN, WAN and remote offices. Using software for management gives him flexibility, scalability and integration features that he says he's doubtful an appliance could match. He also says he feels more in control of his management strategy by deploying software that can be tweaked and upgraded on the fly.

"An appliance is a black box. You have to depend on the vendor to upgrade and service the box, and while it may be easier to manage because it only does certain things, it's an immobile, permanent fixture," he says.

Jim Sherer disagrees. It takes too much effort to get software working, says Sherer, director of ASP Operations at ADP Dealer Services in Hoffman Estates, Ill. He prefers appliances.

"Putting an appliance in is 10 times easier than having to come up with a solution to integrate," he says.

Sherer recently began working with Gold Wire's Formulator, a configuration and change management appliance. The start-up embedded its proprietary software in a high-availability box and built in integration with popular software and equipment to ensure its product will work in a heterogeneous network.

Sherer uses the tool to address a specific need.

"I can put this appliance anywhere in the network, and its purpose is to manage security," he adds.

Ross McKenzie is considering both management software and appliances to augment the network and system management strategy at Johns Hopkins Bloomberg School of Public Health, in Baltimore, Md. With freeware such as Multi Router Traffic Grapher and proprietary management applications such as CiscoWorks in place, McKenzie's staff is looking to branch out and implement a comprehensive framework to manage the network that supports 5,000 end users.

Kevin Stone, senior network administrator at the school, has his doubts about the price and people skills required with software, and says he has equal doubts about the performance and scalability of hardware.

"Software would require we dedicate a person to understand a complex package, and we usually can't dedicate people to know one product inside and out. You get issues with employee turnover," he says. "An appliance is simpler to set up, but you may need two or three to do the work of one software application, and then you can't customize it too much anyway."

The team at Johns Hopkins might opt to mix and match, which is what industry experts recommend at this point. Newer vendors emerging with appliances won't take much business away from management heavyweights such as IBM and HP because the start-ups have yet to prove their equipment works. But they will get some nibbles, thanks to their low entry prices and fast deployments, which can give results sooner than roll-out cycles with complex software applications, analysts say.

### Hardware vs. software

New management appliances give companies an alternative to management software.

#### Why an appliance?

**Price:** These devices are priced starting at around \$1,000, whereas software point products start at about \$10,000, and management platforms can get into the millions of dollars when professional services costs are factored in.

**Simplicity:** The self-contained boxes require little IT oversight, making them ideal for companies or sites with minimal IT personnel.

**Performance:** Appliance vendors pre-package their management software on high-availability hardware optimized to run the software.

#### Why software?

**Scalability:** One platform can be extended to support thousands of endpoints through the use of agents and third-party programs.

**Flexibility:** Software programs are extensible and work together with other vendors' products to support a range of applications from fault management to security monitoring.

**Reliability:** Whereas appliances are being sold by newcomers such as Gold Wire and Vieo, management software comes from established companies such as Computer Associates, HP and IBM.

"Appliance packaging should be considered as an option, but not a replacement to software," EMA's Drogseth says. "There are trade-offs for both. The simplicity of an appliance vs. the flexibility and adaptability of software."

## The price is right for these management tools

BY DENISE DUBIE  
NETWORK WORLD, 03/31/03

Smaller IT budgets don't necessarily translate into fewer projects or less work for network executives and managers. The opposite is often true, as network staffs are forced to work around not having the latest commercial tools.

One way network staffs are coping is by using freeware, available on the Internet or from commercial product vendors willing to give away software in hopes of enticing customers to buy products later. We informally polled readers to get their recommendations, listed here in no particular order.

### Aida32

Aida32 should be in every network administrator's toolbox. Or so says Herb Read, network technician at International Solutions, an insurance industry investor and consultant in St. Petersburg, Fla.

"Aida32 provides direct and rapid access to a server's Event Viewer, User Manager, live lists of [Dynamic Link Libraries], open files, services in use and other hidden tools that even the operating system does not provide," Read says. "It's the greatest administration tool to maintain desktops and servers."

Developed, upgraded and maintained by Unlimited Possibilities in Budapest, Hungary, Aida32 works specifically on Win32 platforms and can be used to perform diagnostics and benchmarking. The software extracts data from servers and PCs, and lets network managers gather statistics on the health and status of machines. Also, Aida32 can be used to perform network audits and remotely access managed devices from any workstation.

Aida32 resides on a server, and network managers can use a built-in Java client or any standard terminal emulator to manage other servers and desktops.

### Network Probe

Network Probe is a protocol analyzer designed to provide a real-time view of network traffic. Developed by ObjectPlanet of Oslo, Norway, the application works much like products from companies such as Agilent Technologies or Fluke Networks.

The software can track and isolate traffic problems and congestion on network lines. It monitors conversations between hosts and applications, and shows network managers from and to where the network traffic is traveling.

Java-based server software is installed on a dedicated server and collects network traffic statistics. The client software can run on a Java-enabled Web browser such as Internet Explorer, Netscape, Opera, Mozilla and Safari. Now in Version 0.4, the server software supports Windows NT/2000/XP, Linux, FreeBSD and Solaris operating systems.

"It's pretty cool and quick to learn for a network protocol analyzer," says Eric Zatko, security and telecommunications analyst at a county government agency in Ohio.

### Cflowd and Flowscan

Jim Kirby, senior network engineer/architect at Wells Dairy in Le Mars, Iowa, says cflowd and flowscan, "two very interesting freebies" from Cooperative Association for Internet Data Analysis, help him collect and monitor NetFlow data from Cisco routers.

Cflowd collects and correlates data from NetFlow, a part of Cisco's IOS that collects and measures data as it enters router or switch interfaces. The data can be used to monitor key applications, including accounting, billing and network planning, for corporate or service provider customers. The current release of cflowd includes collection, storage and basic analysis modules.

Flowscan works with cflowd to report on IP flow data exported by Cisco routers and connected by cflowd. Consisting of Perl scripts and modules, flowscan includes a flow collection engine (cflowd), a high-performance database and a visualization tool. It generates graph images that provide a continuous view of the network border traffic.

### Kismet

Kirby also recommends Kismet, a network sniffer with a twist - it can spot unauthorized wireless access points.

Unlike a standard sniffer, Kismet can identify and separate wireless use on the IP network. Kirby also uses a freeware sniffer dubbed Ethereal to watch traffic and decode packets on his Ethernet network.

Kismet works with any 802.11b wireless card that can report raw wireless packets, including wireless cards from Cisco, D-Link Systems and Linksys (which Cisco is acquiring).

### Conserver

Kirby also takes advantage of Conserver, freeware that helps network managers monitor servers via their serial ports - which lets them be accessed even if the IP network was down.

Conserver is an application that lets multiple users simultaneously watch a serial console. Connecting via the serial port lets network managers get health and status updates from the machine without relying entirely on the network connection. The software resides on a server and communicates with the serial cards and ports on the server to check availability when IP connections are down. Conserver lets users take write-access of a console (one at a time).

"By putting one of these in every communications closet and applying strong security to the private Ethernet, we have created an excellent out-of-band management network, which keeps us from needing to visit every rack unless we're physically moving equipment," Kirby says.

Conserver logs all serial traffic so network managers can review why something crashed, look at changes (if made on the console), or tie the console logs into a monitoring system.

"We can watch the console output as a router or switch reboots, or restore a device that came up in a bad state, so Conserver is almost necessary for disaster-recovery reasons," Kirby adds.

---

© 2003 Network World, Inc. All rights reserved.



[Request Reprint](#)

[Request a reprint of this report.](#)