



November 19, 2009

7 Must-Have Technologies

By Tommy Peterson

These IT practitioners agree that there are some products no IT shop can live without.

Professional though they are, IT managers are probably as susceptible to the allure of flashy technology as the next person, but the successful ones don't succumb to the temptation. Especially at small to midsize businesses with lean staffs and tight budgets, IT pros are focused on practicality, efficiency and supporting the business goals of their companies when they make technology decisions, according to IT Manager Brian Mintel of Frost-Arnett, a debt collection company in Nashville, Tenn.

"The way our companies look at technology is this: Do the things I do technologically keep us safe and secure and help us turn a profit?" says Mintel. "Some things sound good and look good, but if they don't keep the business running smoothly or do not help us long term to turn a profit, we have to analyze whether it's really worth the resources to fund."

The analysis of any technology has to include how easily it can be managed and how well it will scale to meet the needs of the business as it grows, says Ed Lundgren, systems administrator at Omnica, a medical technology development company in Irvine, Calif.

"My philosophy is to think big even as you make small decisions," says Lundgren, the only IT professional at Omnica. "You need technology that will help you maximize resources while you're small and give you the management capabilities you need as your business grows and gets more complex."

According to IT practitioners, here are seven essential categories of technology for small and midsize businesses, and their approaches to selecting products and services for their companies. Those approaches vary, but the need for essential technologies is a constant.

1. Managed Antispam/Antivirus

For Lundgren, choosing a managed system to block spam and viruses at Omnica was an easy decision. The networks of small companies need as much protection as those of large corporations, and lean IT resources require streamlined administration capabilities, he says.

"We have about 50 workstations that I actually deal with; but even with that small number of machines, I never considered anything but a centrally managed system," Lundgren says. "I like one point of contact and all the reporting and monitoring capabilities."

Lundgren installed Trend Micro Worry-Free Business Security software, which allows him to monitor the entire network on a single dashboard and produces minimal processing overhead, so there are few interruptions for those using the product.

In addition to blocking spam and viruses, the Trend Micro system monitors where users go on the Internet to protect Omnica from threats such as “drive-by downloads” from infected web pages, Lundgren says.

“The Trend Micro software does exactly what we want it to do unobtrusively, so people generally forget about it,” Lundgren says. “It gives me a great overview of what’s going on in the network all the time.”

Some IT managers, such as Mintel, use separate products for antivirus and antispyware. Frost-Arnett deploys CA’s eTrust software with a centralized threat management console for virus protection and uses WatchGuard technology to block spam, Mintel says.

Outsourcing antispyware and antivirus functions to a dedicated hosting service takes pressure off of his small IT staff, says Martin Szalay, IT director at Food Warming Equipment (FWE) in Crystal Lake, Ill. Regardless of the option it selects, a company should frequently reassess the strategy it uses to protect its network and IT assets, says Szalay.

“The threats change constantly, so nothing works great forever,” he says. “You have to be vigilant and constantly explore different options.”

2. Smartphones

Smartphones have quickly evolved from status symbols touted by C-level executives to essential tools for an increasingly mobile workforce.

Along with providing e-mail, smartphones offer Internet access to a growing number of the applications workers need to do their jobs efficiently from the road. IT managers are using smartphones not just to stay connected to the data center, but also for remote administration.

At Health Advocate, most of the salespeople rely on mobile access to e-mail over their smartphones, says Eric Weaver, vice president of information technology for the firm, which helps client companies and their employees navigate health-care and insurance issues.

“We support BlackBerrys and any other Windows handheld device,” says Weaver. “From a productivity standpoint, they’re important. From an IT standpoint, we’re monitoring systems all the time over them. It gives me the freedom to leave and still be in touch.”

Smartphones bear watching from a new-product development perspective, as the devices are increasingly used as a delivery platform for web-based applications, Weaver says. “Many people use smartphones as their only computing device — it’s their cheap computer, not their expensive phone,” Weaver says. “BlackBerrys in particular will increasingly be targets of new product development.”

Szalay at FWE works remotely via virtual network computing through his smartphone, he says. Most of the company’s sales, marketing and accounting staff use company-issued mobile phones, and requests for the smartphones come from all corners of the company. “Mobile computing is the future, so you have to have a strategy to support it,” he adds.

3. Remote Access Software

The potential for smartphones to deliver productivity tools in the future may be virtually unlimited, but most companies need a way for telecommuters, road warriors and remote offices to access applications now.

Health Advocate connects remote workers via a SonicWall VPN and Citrix Secure Gateway, which together ensure the safe transmission of applications and data, Weaver says.

“It’s important to have the ability to deploy workers at home or on the road,” he adds. “From my point of view in IT, that ability is also part of a business continuity plan.”

Frost-Arnett has a Multiprotocol Label Switching (MPLS) network connection between its four main offices for optimum data transmission, Mintel says. The company also deploys a WatchGuard VPN through which the remote sales force accesses sales management software that resides on office servers.

Grange Insurance uses Citrix XenApp, which delivers virtualized applications to mobile devices, says Jeff Sheen, lead enterprise architect at the Columbus, Ohio-based company. An added element of his remote access strategy is the deployment of NetMotion software to safeguard the work of employees on a Wi-Fi connection, he adds.

“NetMotion maintains the connection so you don’t lose applications and data, even if Wi-Fi is going in and out where you are,” Sheen says. “It smooths the transmission so there are no drop problems.”

Szalay relies on virtual network computing (VNC) and calls remote access a “lifesaver” as he moves about, both in and out of the data center. FWE uses various remote desktop, remote assist and web conferencing solutions as gateways to provide access to telecommuters and mobile employees.

4. Imaging Software

For saving time and data during a disaster, few technologies prove their worth as easily as imaging software, which pushes out a system snapshot for deployment on many PCs and workstations at once.

Grange Insurance uses Symantec’s Norton Ghost, VMware Workstation 6 and a variant of Windows PE to deploy consistent desktop images to 1,000 PCs in the company, Sheen says.

“We have a ready-to-deploy image for each of our three main profit centers, which are maintained via VMware Workstation 6,” he adds. “Then whenever we need to deploy a new PC, the image is there.”

As small companies grow, the potential benefits of using an imaging system increase as well, says Mintel, who has been experimenting with Acronis technology at Frost-Arnett.

“The bigger we get, the more time consuming it becomes to freshly load 40, 50 or 60 machines at one time,” he says. “With the software, you just create one template and the system re-images all our PCs.”

That point was recently driven home to Szalay, when he received a shipment of 50 new Hewlett-Packard PCs he had purchased for FWE.

“We just brought the new machines in, and Acronis saved me many hours of work,” Szalay says. “We use the software every day; it’s the coolest thing since sliced bread.”

FWE uses Acronis software to create image files of entire servers, which can be deployed as virtual machines on alternate hardware. Imaging is part of Szalay’s routine backup strategy.

“With Acronis, you don’t have to restore to the same computer; you can go to a new iteration and not lose anything,” he says. “The imaging we do with Acronis has also allowed us an easier transition to each VM. We don’t have to rebuild from scratch in a VM. In simple terms, we just image the existing server, Universal Restore into the VM, disconnect the old server hardware and go live on the VM.”

5. Server Backup

Server backup solutions come in many sizes, prices and levels of complexity, and the backup process often requires several steps.

Both Health Advocate and FWE rely on Symantec Veritas Backup Exec software for initial server backup, according to Weaver and Szalay, respectively. FWE also deploys a Quantum Autoloader automated tape library for its archival process, Szalay says. With two data centers, Health Advocate replicates data to its second site and also performs traditional backup to tape at night, says Weaver.

“Backup is so important to your operation,” Weaver says. “The technology also makes it easy, but you have to do a bunch of things, not just one, to make sure you don’t lose critical information.”

Although Lundgren deploys Backup Exec for imaging and backing up desktops at Omnica, he uses Baracuda’s Yosemite technology for primary server backup, then moves data to a tape library and finally uses offsite storage to safeguard the backups.

Grange Insurance backs up its servers first through IBM’s Tivoli Storage Manager, then to disk and on to a tape library, Sheen says. “We use that sequence for our mainframe and for all the 500-plus servers that we have,” he says, noting that Grange is definitely on the large end of the SMB category. “Here we’ve got the big technology sledgehammers because we need them.”

6. Storage: NAS and SAN

When Frost-Arnett recently installed a VoIP phone and call-recording system, Mintel knew he had to upgrade the company’s storage infrastructure.

“NAS [network attached storage] seemed like the right solution,” Mintel says. “We were looking for a midrange solution with scalability so we could add on later, and failover was important because we were connected to a RAID array.”

To meet its increased needs, Frost-Arnett has deployed a 4-terabyte Netgear ReadyNAS Pro appliance in its Nashville headquarters and is about to install an identical unit in its Campbellsville, Ky., office. Those units also store backup data from calls in the company’s Houston and Knoxville, Tenn., offices. Recorded calls are initially stored in SQL databases for 30 days, and then the data is transmitted to the NAS units,

but must continue to be readily available.

“We’re recording calls at five sites [the company maintains a small remote office in Memphis], and we need access to the calls 24x7,” Mintel says.

As their capacity and availability requirements grow, many SMBs use NAS as a first step into networked storage. If the growth of the company and those needs continue, investment in a storage area network (SAN) begins to be a consideration. Health Advocate, with ever-increasing volumes of sensitive data to store and access, maintains redundant data centers with an EMC SAN at each location, says Weaver.

7. UPS Devices

Uninterrupted power is necessary both to keep systems up and running and to preserve the integrity of the data in those systems. Protecting the IT infrastructure’s power supply from outages and spikes is about as fundamental a task as a technology can perform, says Health Advocate’s Weaver.

“It’s critically important to have clean power, which is what a UPS does,” he says. “We have APC UPS devices on the network, which protect our servers from short outages. That’s only a small part of the power protection picture. Right now with a fully loaded UPS, we can live for about 30 minutes, which is obviously not enough to sustain the business if something really bad happens. But it gives you a chance to shut down in an orderly way and protect your data.”

Even small companies with rigorous backup protocols need protection from surges and outages, says Mintel.

“We’re not so worried when the power goes out as long as there’s time to shut down the equipment,” he says. “We don’t have a data farm or even a data center, but everything has an APC or Tripp Lite UPS.”

www.biztechmagazine.com/article.asp?item_id=680