db kay +associates

DB Kay & Associates – Virtual Support Networks – White Paper

Virtual Support Networks

Ten Tips for Delivering Managed Services to On-Site Systems

David Kay

Principal

DB Kay & Associates

April 2005

- *Multiple contacts to resolve*
- *Expensive field service*
- *Significant downtime*
- *Customer dissatisfaction*

Before Virtual Support Networks

The operations manager gets a flashing icon at the top of his queue. He glances over, looks at the customer site, and winces. It's another problem with the guest registration system at a small hotel in rural China.

The hotel chain is a big customer, but some of their remote locations appear designed to stretch the limits of his support capabilities. Sighing, he dispatches the incident to the support center.

Sure enough, as he expected, the technician isn't able to do anything. Phone problems, language challenges, and lack of technical expertise on site conspire to foil attempts to fix problems with anything as simple as a phone call. Yet, complete service is what the company sold the hotel chain, and complete service is what they'll deliver.

Mentally tallying the cost of another truck roll, the operations manager dispatches a partner's field service technician to the remote location and hopes he'll get there before the local hotel property complains to Corporate…

- *Closed at first contact*
- *Cost effective*
- *Shorter time to relief*
- *Customer satisfaction and loyalty*

With Virtual Support Networks

The operations manager gets a flashing icon at the top of his queue. He glances over, looks at the customer site, and shakes his head. It's another problem with the guest registration system at a small hotel in rural China. Downtime for systems like this can be costly, so he feels good his remote support team will be on it right away.

He dispatches the incident to his remote team which has recently been equipped with virtual support network (VSN) technology. This a system that allows them direct, secure access to customer systems anywhere in the world—even in places where internet access is slow and spotty, through a dial-up line or wireless.

A few minutes later, the operations manager notices the case has been closed. Curious, he opens up the incident and sees that the technician was able to easily reset a configuration file that had been corrupted, likely because someone working at the registration desk had installed something they shouldn't have. Smiling wryly, the manager remembers when a little problem like that would have likely turned into a truck roll! What a waste that was.

Pleased, the manager goes back to reading the company newsletter. The company just had its best quarter ever, fueled by repeat business from loyal customers. The CEO is quoted as saying their difference is the quality of the service they deliver. The operations manager agrees.

Executive Summary

*"Managed services in North America are the **key data service trend going forward.**"*
– Charles R. Carr and Eric Goodness, Gartner

The business of taking care of remote hardware and software has never been bigger:

- Managed systems and services for retail, point of sale, hospitality, and other distributed operations are a hot growth area.
- Enterprise help desks manage an increasingly dispersed array of hardware and software.
- Enterprise software providers are moving to managed services and other value added support offerings to preserve margins in the face of increasing price pressure.

Gartner estimates that managed services will grow at a CAGR of nearly 36 percent from 2001 to 2006.

These opportunities are being driven by CIOs' need to manage cost and risk carefully. With research showing that 47% of IT spending going to total cost of support and maintenance (TCSM), outsourcing system management to specialists makes sense for the buyer. But where does it leave the provider?

Field service visits are very expensive, costing at least a hundred dollars for even the simplest issue, and much more for complex resolutions. Managed service providers wisely avoid "truck rolls" and field service calls if possible. But how?

A new class of technology that we call Virtual Support Networks, exemplified by WebEx SMARTtech, has arrived to fill exactly this need. Virtual Support Networks allow service providers to securely, scalably, and cost-effectively manage distributed installations around the world.

But technology alone isn't enough: providers need to know the most effective ways to take advantage of this new technology to deliver added value to customers. In late 2004 and early 2005, DB Kay & Associates conducted a market survey to uncover the best practices for deploying Virtual Support Networks. Briefly, we learned the following principles, described in detail in this paper:

- **Make it easy for your customers**
- **Be secure**
- **The internet isn't perfect; deal with it**
- **Set customer expectations**
- **Be prepared for hard questions**
- **Measure effectiveness**
- **Create a dedicated team**
- **Back it up with remote access**
- **Keep good records**
- **Pick the right technology partner**

By following these principles, the practice leaders we interviewed were able to lower cost, shorten time to resolution, and increase customer satisfaction. We're confident other organizations can, too. We welcome your feedback and experiences at VSN@dbkay.com.

The Virtual Support Network at Work

The Challenge of Delivering Managed Services

"Our analysts handle something like ten cases a day. ***They generally need to connect 100% of the time.*** *Since these have been escalated to level 3, we're trying to troubleshoot on-site, because it's hard to reproduce in our labs."*

– Director, Tier Three Support, Managed Systems Provider

Simply providing remote support is hard. Working with on-site customer staff can be frustrating as call-backs proliferate. Diagnostic and repair tasks that would be easy in-person are often time-consuming and error-prone when done remotely, through a customer. Remote support is many times harder than the "good old days" of field service, when on-site technicians kept temperamental mainframes running with ongoing intervention. Still, at least there's an on-site person working on the problem.

Not so with managed services. Customers pay a premium for support tasks to simply go away, especially in environments like retail locations, restaurants, conference rooms, and kiosks where trained staff aren't available. In these environments, the managed service provider must go it alone.

Technology for remote access to computer systems is broadly available, but fails to meet the specific needs of managed service providers, especially for

- Security over the Internet
- Performance over the Internet
- Unattended operation
- Trust

Until very recently, managed service providers with on-premise hardware or software had Hobson's choice—for many customer issues, they had to rely on the field service team as a first resort.

Moving from Lights-Out to World-Wide

*"****In the old days,*** *we would have needed to jump through two or three PCs, connecting from a laptop in Asia Pacific."*

– Director, Tier Three Support, Managed Systems Provider

Standard remote management technology (like VNC or pcAnywhere) is designed for local area network access inside the data center. Relying on the network for security, it's not secure when used outside of the firewall, nor is it architected for the Internet. On the other hand, Internet remote access tools and services require a customer on the other end. Neither solves the problem of providing managed services. Looking at the history of these technologies, it's not surprising that they don't.

Remote management technology came from IT server management. Technicians running racks of PC-based servers in a lights-out facility needed a way to log in and manage them without leaving their desks. As a result, a series of utilities were developed to allow one computer's screen to be displayed in a window on another computer, the most widely adopted of which are pcAnywhere and VNC.

Organizations supporting products remotely immediately started using these applications to see what their customers were seeing. While they did help, they did so in a way that wasn't scalable, efficient, or secure. This is because these products were designed to be used inside a single local area network (LAN)—from an IT staff member's PC to a server. This architecture resulted in serious issues when used for support:

1. ***Customer-side footprint.*** Applications like pcAnywhere require customers to install software on their systems to allow the TSR to connect.
2. ***Performance requirements.*** Being designed to work over a high-speed LAN, legacy systems require levels of bandwidth and connection reliability that the Internet rarely provides.
3. ***Holes in the firewall.*** Being designed to work on a closed connection, these systems communicate over proprietary ports that aren't generally open in security- conscious networks. As a result, these legacy remote access solutions require holes in the firewall.

For all of these drawbacks, old-school remote access technology has the advantage that it doesn't expect or require a user at the computer being managed.

New Internet-based solutions have overcome these issues (see our 2004 white paper "Show, Don't Tell: Remote Support Best Practices and Benefits.") But they haven't done the job for managed service providers, either. They were engineered to enable remote support staff and client-side staff to work together to solve support issues. They require someone at the other end to log in, initiate the connection, monitor activities, and grant or deny access for specific tasks.

What managed service providers require is technology that combines the **scale and security of Internet-based remote access solutions** with the **unattended access features of IT remote access software.** We call this new class of technology the ***Virtual Support Network.***

The Virtual Support Network

"We started out with [a leading remote support solution,] but we were always waiting for something like SMARTtech, ***where we didn't need to have someone on the other end."***
– Director, Tier Three Support, Managed Systems Provider

The Virtual Private Network (VPN) extended the security of behind-the-firewall communications out to the distributed enterprise. Now people worldwide can connect into their intranet from their hotel rooms, customer locations, home offices, and partner facilities. They're distributed geographically and across the network, but they're directly integrated into their businesses.

Similarly, Virtual Support Networks allow managed service providers and IT organizations to support unattended, on-premise hardware and software as though they were there in person, even if they're ten thousand miles away and managing a computer connected to the internet through a low-speed dial-up line.

Virtual Support Networks (VSNs) are a second-generation of internet-based remote access technology. Like those solutions, VSNs are:

- ***Web-based.*** This means they communicate over standard secure web ports that are already open in the firewall.
- ***High-performance.*** They are not only faster over any kind of network but also more resilient to packet loss, temporary loss of connections, and the other realities of today's Internet.
- ***Secure.*** Using the same secure web protocols that drive billions of dollars of financial transactions VSNs are secure, permissions-based, and give granular control over the level of access the supported system provides.

These additional characteristics distinguish VSN technology further:

- ***Bulletproof security contracts.*** Without an on-site user to grant or deny each individual action, VSNs must allow customers to set, manage, and monitor specific policies about who can do what to their machines.
- ***Full control.*** When supported by the security contract, the remote user must be able to install software, reboot the system and immediately reconnect, log on as both a user and an administrator, and generally have the same access to the system as if he or she were in the same room.
- ***Total auditability.*** While auditing actions is important in any remote access scenario, it becomes especially important in an unattended scenario. This is even more true in the light of today's IT compliance and regulatory environment created by Sarbanes-Oxley, HIPAA, EU privacy regulations, and more.

The Business Case for Virtual Support Networks

*"**We get through a lot more calls remotely** than we would going out to visit customers!"*
– Director of Operations, IT Services Provider

The business case for the Virtual Support Network is simple: for organizations providing support to a stringent service level, VSNs reduce the number of costly field visits. The result is higher per-agent productivity, lower cost and higher margins, and (because of shorter resolution times) higher customer satisfaction and loyalty.

Reduced Support Costs

*"We're experiencing a big period of growth…I installed this technology primarily to **reduce the number of support visits.**"*
– Director of Operations, IT Services Provider

Support industry research shows that the cost of a single field visit costs a minimum of $100 to $150 dollars, even for the simplest issues. Not only that, but it takes time: time to dispatch busy technicians, time for them to become available, time for them to badge in, and time for them to get to and from the customer location. A field service technician who can resolve four issues in a day is considered productive, where their remote counterpart may be expected to resolve three or four issues in an hour.

The math is clear: managed support organizations must do as much work remotely as possible. With Virtual Support Network technology, a much greater percentage of incidents can be resolved remotely with no loss of close rates or customer success. The bottom line is lower support costs and higher margin for managed services. Remote support can even create the opportunity to package additional high-margin value-added services that are priced attractively to the customer.

Reduced Time to Resolution

*"**We saw a 50% reduction** in average close time in just a few months."*
– Customer Service Coordinator, Professional Services Software Company

In addition to being more cost effective, remote support (empowered by next-best-thing-to-being-there VSN technology) resolves issues much faster for customers—especially if the issues are complex. The field technician might not have the expertise to debug the issue without a great deal of back-and-forth with escalation engineers in the support center or the sustaining engineering organization. In contrast, with a VSN, all the experts can collaborate at first contact—even if they're in different locations.

The result is faster time to relief for the customer, faster time to close and lower backlog for the service provider.

Increased Customer Satisfaction and Loyalty

"When we do upgrades, if there's an issue, often the customer doesn't even know about it because we've just taken care of it. With [a pre-VSN solution], the customer often had to do something to the machine because something hangs or something. ***This is a big customer satisfaction driver****. …'no news is good news' in support."*

– Manager, Technical Support, Managed Hospitality Systems Vendor

Managed service customers pay a premium for not having to think about support—for making downtime "somebody else's problem." And the services they're buying are often business-critical. So it's no surprise that they're impatient when having to wait for a technician.

Similarly, system maintenance is a necessary evil. While customers understand the role of maintenance in delivering the uptime they need, they'd prefer not to be involved in it.

By enabling effective remote support, VSNs provide more of what the customer is paying for: rapid resolutions and transparent maintenance. In many cases, problems are detected and resolved long before the customer knows there's a problem. Upgrades and maintenance are invisible. The whole messy reality of the technology is hidden from the customer, and they just reap the business benefits.

This model can have major impacts on satisfaction. But more importantly, from a business standpoint, it can be great for loyalty. Customers now see the managed service provider not a vendor who is always trying to justify their support contract on a cost-per-incident basis but as a trustworthy business partner who deserves to share in the benefits they enable.

Ten Tips for Getting the Most from Virtual Support Networks

Based on successful adoptions across the industry, we have identified the following ten best practices developed by the leading practitioners of VSNs.

Tip 1: Make It Easy For Your Customers

*"**We needed something that would install easily without any user interaction.** We didn't want to require someone to push 'next,' 'next,' to install something to give us access."*
– Manager, Technical Support, Managed Hospitality Systems Vendor

In his bestselling book The Agenda, business guru Michael Hammer advises companies to be "ETDBW:" easy to do business with. While grammatical purists may decry the terminal preposition, the underlying message couldn't resonate better in today's world, and especially in the world of managed services.

Leaders are making themselves easy for customers to do business with by:

1. ***Enabling true hands-off support and maintenance.*** On-site staff should not have to press the reboot button, install new versions of the software, or click "OK" to security requests. Remote access should be completely transparent.
2. ***Providing effective tools for administering and monitoring remote access.*** Permissions to access and modify systems should be very clearly granted and documented, and should be easy to revoke for any reason.
3. ***Working anywhere, anytime.*** Whether your customers' systems are peered to an Internet backbone or connected via slow dial-up line, remote access and management should just work.

Customers are paying for someone else to do the worrying for them. Making it easy for them to forget all about you makes for a very good memory at renewal time.

Tip 2: Be Secure

*"Because customers will demand smart-card access control or token-based methods that will be difficult to deploy, Managed Service Providers should consider offering alternative access-control mechanisms, such as **Secure Sockets Layer virtual private network technology.**"*
– Gartner

Managed service providers are trusted partners and the access they have to customer systems carries a significant burden of responsibility. As a result, leaders do everything in their power to make sure the ways that they remotely access systems is as secure as possible.

To assure security, managed service leaders do the following:

1. ***Avoid direct connections.*** There should be no direct connection between the remote system and the analyst's machine. This is important because a direct machine-to-machine connection is easier to hijack. The most secure solution is to have each machine initiate a session with a common set of network services in a physically and logically secure location, and to have those services intermediate interaction between the two machines. Obviously, a signal needs to get to the target machine since it's unattended, but the actual live connection should still go through a server network.
2. ***Use strong encryption.*** Encryption should be at last 128 bits for practical insurance against cracking. As mentioned in the Gartner quote above, a standard such as Secure Sockets Layer (SSL) should be used so that the protection afforded by the encryption is broadly understood.
3. ***Industry certifications.*** Enterprises should look to certifying bodies such as WebTrust (www.cpawebtrust.com) and SAS 70 (www.sas70.com) to ensure the solution has met high, objective standards for security.

Tip 3: The Internet Isn't Perfect. Deal With It

*"[The old solution] was inefficient over low bandwidth connections such as ISDN. It would often drop the connection or freeze… **[our VSN] works well in low bandwidth—really great."***

*"We're moving to a world of chaotic networks. **[Our VSN] is architected for chaos."***
– Manager, Escalation Team, Business Intelligence Software Company

*"These are very experienced and expensive people, so **wasting their time on connectivity wasn't the right thing to do."***
– Director, Tier Three Support, Managed Systems Provider

On an engineer's whiteboard, the Internet looks like a pretty well organized place: Internet Protocol (IP) packets whiz from machine to machine regardless of the underlying physical transport mechanism.

Those of us who have tried to download large email attachments from hotel rooms or stream video from overseas servers know better.

While poor performance may be invisible to your customers, it will directly interfere with your analysts' ability to do their work, and as a result will hinder the adoption of VSN technology. No expert likes sitting around waiting for a screen refresh.

Make sure your VSN works well when deployed wherever your customers may be. Test it specifically through dial-ups, satellite, ISDN, WiFi, and other less-than-perfect connections.

If you're using a hosted service, make sure that they have Internet access points that are logically close to your customers worldwide. If you're hosting the service yourself, make sure your IT organization can support these local points of presence.

Tip 4: Set Customer Expectations

*"**Customers ask for it by name.** 'Can't you WebEx? We don't have much time.'"*
– Director, Support

The effectiveness of Virtual Support Networks can be its own trap, raising the expectations of customers beyond a level that's needed or mutually profitable. And, by getting attached with the technology, users can drive its use in cases when it's less appropriate, much as patients ask their doctors to prescribe antibiotics for the common cold. The inappropriate use of powerful technology can get in the way of its effectiveness in cases when it is the right tool.

Leaders manage—and exceed—customer expectations using a combination of techniques:

- ***Define clear SLAs.*** Whether providing a managed service or supporting unattended technology from the IT help desk, leaders define service level agreements that clearly specify the actions (and in some cases, the outcomes) of support in specific circumstances. An SLA is not just a way of enforcing a contract; it's a tool for facilitating conversations about value with the customer.
- ***Keep communicating with the customer.*** Make sure the customer knows when VNSs are mutually beneficial—and when a brief telephone conversation will accomplish the same thing more quickly. While a VSN is an outstanding way to get access to a machine, it doesn't help at all understanding the customer's situation, plans, or state of mind.
- ***Define clear policies internally for using remote support and VSNs.*** If your support team is clear about when the VSN should and should not be used, they'll be able to manage customers who immediately demand remote connectivity. This is especially true when the service is value-add, but not fully managed.

Tip 5: Be Prepared For Hard Questions

"There were initially customers who were concerned about security, but we've worn them down with facts and logic, answering their queries confidently. ***Every customer has been convinced."***

– Manager, Technical Support, Managed Service Provider

Customers who are giving you remote, unsupervised access into mission-critical applications and systems are going to ask difficult questions. They'll come from both the business and the IT side, and will increasingly focus on their own regulatory compliance issues. The most challenging will come from companies in the healthcare industry based on the stringent nature of HIPAA regulations, but all sectors are affected by compliance.

Customer-facing staff need materials—whether scripts, bullet points, FAQs, or a knowledge base article—to help them explain the benefits to customers and overcome likely concerns about security, privacy, and changes in the resolution process. They should be coached to answer customer questions based on their needs and interests ("we'll take less of your time") and not their own ("I don't have to drive all the way out to your facility anymore.")

Questions to cover include "will I be able to see what you did?" "can you take files from my machine?" "can you put viruses on my machine?" "will your software stay on my machine and monitor my actions?" "is this spyware?" and "does this cause a breach in our firewall?"

Customers need to understand that remote support is an option, not a requirement, and that their security contract will grant rights only for certain pre-defined activities.

Leading VSN users also provide white papers and detailed security information on their web site or customer extranet to help technical people at customer sites evaluate the security of the VSN. Ideally, this is backed up with internal expertise and, as a last resort, a conference call with the vendor. Vendors should provide customers with a template white paper that can be customized and branded for the specifics of the implementation.

Tip 6: Measure Effectiveness

"On typical highly complex cases we deal with, we can move from 2 or 2 ½ hours to about 35 minutes…at today's run rate of 1200 sessions per month, this translates to an annual savings of nearly $600,000 and an ***ROI in excess of 700%.****"*

– Manager, Support Center Tools, Enterprise Software Company

Most support organizations need to build an ROI and business case to justify the purchase of technology, but then fail to follow up to see what the business impact actually is. This is a mistake: without measuring effectiveness, it's hard to validate the original assumptions, and it's hard to identify areas for improving the return. Additionally, since there is an ongoing cost component to most VSN solutions (either internal for software or paid as a service fee for hosted solutions), this cost needs to be justified as well.

Leaders track:

1. In what percentage of incidents remote support is used
2. What the alternatives would have been to the virtual support network in these incidents (e.g., 50% would have required an on-site visit; 40% would have required a customer call-back, 10% would have required an additional escalation)
3. What the cost of a VSN incident is, and what the cost of the alternative is. Most companies look to marginal cost—that is, the cost that would have been saved by not doing the last incident in this way—rather than allocating all the fixed cost equally across all incidents.

With this data, a very simple spreadsheet model can show the financial benefit of the VSN.

One other point to keep in mind: if you're casting the benefit of VSN in pure apples-to-apples cost savings, you need to be prepared for management to take you up on the offer, which will mean layoffs or consolidations. Most organizations focus on (a) the ability to handle new support demand without scaling headcount and (b) the ability to create new value-added offerings to drive margins.

Tip 7: Create a Dedicated Team

*"**We created a remote support team.** These are dedicated staff, Tier 1 through Tier 3."*
– Director of Operations, IT Services Provider

As with any other effort, specialization has its benefits. And the leaders we spoke with have all taken the initiative to create a dedicated team that's focused on using the VSN. This makes them expert in the tool as well as the resolution processes that are most effective. And, if a particular type of incident pops up all of a sudden, for example, related to an OS upgrade or a virus, this team can quickly document and share best practices for dealing with it.

Tip 8: Back It Up with Remote Access

*"**We also use [Internet-based remote access]** if we need to connect to a particular computer on someone's desktop—if, for example, Mary in reservations can't print."*
– Director, Tier Three Support, Managed Systems Provider

Virtual Support Networks are an excellent hammer—but that doesn't mean that all your support problems are nails.

VSNs are ideal for unattended machines: kiosks, conference rooms, and servers. They're also good for machines without a dedicated owner, like point of sale terminals. They are not, however, appropriate for machines that are actually "owned" by someone. Dedicated users would rightly resent and feel uncomfortable about others having transparent access to their machines, no matter how legitimate the business purpose.

In the case of user-dedicated machines, back up the VSN with Internet-based remote access. In particular, select a solution that provides fine-grain opt-in privacy, so users need only grant those rights which make sense for their support needs, whether it's view but not drive, access to specific applications, or logins to specific user accounts.

Tip 9: Keep Good Records

*"**We always enable auditing,** as much to cover ourselves if something malicious happens as to help the customer."*
– Director of Operations, IT Services Provider

All public enterprises have a regulatory requirement to manage their IT resources, and all businesses have a right to know what actions their service providers are taking. This is especially true in today's hostile security environment, in which a single badly managed technology asset could compromise the security of the entire enterprise network.

Clean audit trails are a must-have for managed service providers. Unfortunately, these are often easier said than done.

Files that are transferred and executed, or scripts that are run, can be logged in an audit trail conventionally. But many of the actions taken over a VSN work through a graphical user interface, for which a simple audit trail won't suffice: "mouse moved to 125, 765, double clicked, moved to…" isn't helpful.

In the case of actions taken through the desktop or GUI of a computer system the audit trail needs to include a complete session record of the activities and displays. This needs to be maintained so that customers have secure access to it, but others don't. Also, the identities of the authenticated users taking the actions must be stored as well.

Good audit trails and session recordings will simplify compliance, increase confidence, simplify debugging, and cover you should questions arise about support practices.

Tip 10: Pick the Right Technology Partner

*"**When we started looking at a replacement solution,** we needed something that handled the three issues we had with our current technology: scalability, bandwidth and performance, and the need for a direct network connection…and we needed a system we can start without a person."*

– Manager, Technical Support, Managed Hospitality Systems Vendor

Most of the practices described in the previous nine tips require some technology support, as well as people and process management. After reviewing them, make sure that your business requirements capture the points that are most important to your organization. These will typically include:

1. Certified security and security architecture
2. Breadth of functionality for unattended operation
3. Auditing and session recording functionality
4. Performance over the Internet, including low-bandwidth and unreliable links
5. Effective management tools and reporting

An additional consideration is whether to select a software solution or a hosted solution. Software solutions are appealing from a control standpoint, but their total cost of ownership can be surprisingly high, given the challenges involved in creating a worldwide network that supports VSN functionality. The following table summarizes some of the trade-offs between hosted and licensed solutions:

Software Solutions	Hosted Solutions
Control	Global, highly available network
Ability to be integrated	Low starting costs
Cost predictability (vendor, not TCO)	Ability to scale to demand spikes

Conclusions

*"**My people, they all love it**. Not just them, but also in the development center, when we have to pass an issue along. They were the ones who pushed me to do it."*
– Director, Tier Three Support, Managed Systems Provider

Managed service providers, and support organizations that are reaching up the value chain with offerings that increasingly provide managed service, are hitting the sweet spot of market demand right now. But without good technology and processes, they will not be successful in scaling their businesses profitably.

A key enabler of successful, scalable managed services is the ability to support an unattended system securely and efficiently, across whatever network infrastructure exists. Virtual Support Network technology, combined with the proven practices documented in this paper, has generated significant return on investment for the leaders who participated in this industry study. This ROI is coupled with increased customer satisfaction and loyalty, creating a win-win.

By following the best practices outline in this paper, and selecting a VSN partner after considering the requirements we've outlined, we predict your enterprise will experience these benefits, too.

Acknowledgements: WebEx and Its Customers

DB Kay & Associates gratefully acknowledges the financial support and customer contacts provided by WebEx for this white paper and the market research that led to it. WebEx is a leading provider of the current generation of internet-based remote access solutions, and their SMARTtech product is a leader in Virtual Support Network technology.

We recommend that service and support organizations that are considering VSNs for all the reasons discussed in this paper consider the WebEx SMARTtech solution. For more information on WebEx for Support, visit

http://www.webex.com/solutions/online-support-solutions.html

We would also like to thank the following WebEx customers who, among others, participated in the research that led to this white paper:

- Agilent Technologies
- Cognos
- Ericsson
- Epicor
- InfoGenesis
- Lawson
- Medtronic
- Micros
- Wind2 Software Inc.

About DB Kay & Associates

DB Kay & Associates is a consultancy that focuses on high-leverage initiatives for service and support, including knowledge management, self-service, collaboration, and remote access.

DB Kay provides

- assessments
- training
- technology selection
- adoption consulting services

for market-leading support organizations and the vendors who serve them.

David Kay, principal of DB Kay & Associates, has been a leader in applying technology to knowledge-intensive business processes like customer support since 1984. He has been certified by the Help Desk Institute (HDI) as a trainer for Knowledge-Centered Support, and is a frequent speaker and contributor for the Service and Support Professionals Association (SSPA.) Kay holds a patent covering the use of next-generation technology in customer support, and has been recognized as a Customer Service Innovator by the Consortium for Service Innovation.