

Invasion of the Data Snatchers

A Puma Technology White Paper

April, 1999



Contents

KEEPING ENTERPRISE DATA IN ITS PLACE.....	1
THE EVOLUTION OF THE PROBLEM.....	1
Mobile Device Infiltration of the Enterprise.....	1
Booming Sales of Mobile Devices.....	2

An Explosion of Diverse Devices..... 2

MOVING TOWARD AN ENTERPRISE SOLUTION..... 2

Characteristics of the Ideal Solution..... 2

 Connect Anywhere..... 3

 Support Mixed Devices..... 3

 Allow Customized Content..... 3

 Integrate Wired & Wireless Networks..... 4

 Deliver Centralized Management..... 4

 Implement Layered Security..... 4

 Provide more than just Synchronization..... 5

 Emphasize Performance & Scalability..... 5

 Support Industry Standards..... 6

MAKING THE TRANSITION: INTELLISYNC GOLD..... 7

Major Features..... 7

THE IDEAL SOLUTION: INTELLISYNC ANYWHERE..... 7

Major Features..... 8

An Emphasis on Performance & Scalability..... 8

 Performance..... 8

 Scalability..... 8

Providing more than just Synchronization..... 8

CONCLUSION..... 9

Keeping Enterprise Data in its Place

Enterprises are on the verge of losing control of their data. The threat isn't from sheer volume of data, or from industrial espionage, although both those things can be problems. Instead, the threat comes from all those cute little mobile devices that were little more than toys a few years ago. Personal Digital Assistants, cell phones, and pagers can all increase personal and corporate productivity. But these small devices can also compromise corporate data. Left uncontrolled, they can become miniature repositories of corporate information comfortably tucked in the insecure pockets of individuals.

So, what's changed over these last few years to turn these innocuous devices into a looming threat? Until recently, small devices tended to be used as standalone tools for improving individual productivity. Instead of carrying a paper calendar, for example, a person could carry an electronic organizer or palmtop computer that was smaller yet served the same purpose. Most small devices produced before 1996 were primarily a convenient way to store personal information. Limited in memory, and difficult to program, these devices rarely held more than a small amount of personal data.

In 1996 the first mobile data snatcher was born. That was when Palm Computing—now part of 3Com—introduced the first device in what was to become the PalmPilot family. This device sported three compelling benefits that made it stand out from its predecessors. The first benefit was its extreme ease of use, which made it the productivity tool of choice for millions of users. The second benefit was its built-in connectivity, which made it easy to synchronize data between the device and a PC. The third benefit was the availability of excellent tools for creating new PalmPilot applications, including connectivity components for adding synchronization to those applications.

The PalmPilot charted the way for a new class of connected organizers. Such devices immediately began filtering into the enterprise, oftentimes masked as individual purchases that quietly appeared on expense reports. Despite the promise of these exciting devices, their built-in connectivity features make them serious risks to the integrity of enterprise data.

The threat these data snatchers pose demands action. Mobile devices are no longer limited to holding only simple personal information like addresses and schedules. They can now send and receive email messages, messages that may contain sensitive information. New utilities and toolkits extend the capabilities of the devices, allowing them to synchronize with any number of enterprise applications and databases. It's now quite possible for users to compromise enterprise data without even knowing it.

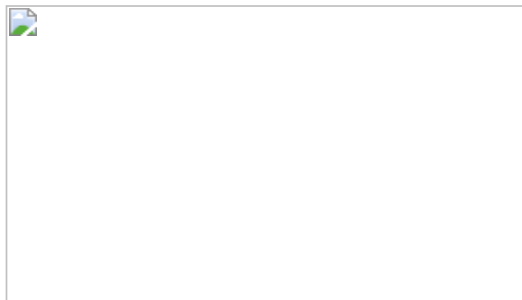
For companies that believe corporate data is a corporate asset, this situation is unacceptable. Some steps must be taken to prevent the "data chaos" that the unmanaged use of small devices can cause in the enterprise. Mobile devices are too valuable to ban outright. The challenge is to maximize and even extend the productivity benefits of these devices while minimizing the risks they pose for enterprise data.

It's time for a new breed of tools—tools that let an enterprise manage the ever-increasing number of mobile devices connected to its networks. Called *Mobility Management Tools*, these powerful applications can manage data snatching mobile devices, returning control of enterprise data to the company.

The Evolution of the Problem

Mobile computing began years ago with the introduction of the first portable computers. The widespread acceptance of notebook computers in recent years was Phase I of the evolution of mobile computing. In this *PC Connectivity* phase, it became clear that notebook computers could deliver real value to the enterprise, particularly when they had some level of access to corporate data.

Attempts to further reduce the size and cost of mobile devices brought about Phase II. This *Personal Mobility* phase culminated in the successful development and deployment of connected organizers such as the PalmPilot. You can best characterize this phase as enabling synchronization of personal information between the mobile device and a locally connected PC (typically communicating over serial cable or infrared media).



Phase III of the evolution is imminent. This phase, the *Enterprise Mobility* phase, is a response to three major factors:

- Mobile device infiltration of the enterprise
- Booming sales of mobile devices
- An explosion of diverse devices

Mobile Device Infiltration of the Enterprise

Mobile devices have infiltrated virtually every company. They have almost certainly infiltrated **your** company. A large percentage of the 4 million plus mobile devices sold in 1998 were purchased by individuals for business purposes. Mobile devices are probably connecting to applications near you right now, synchronizing with data on a desktop PC or with an enterprise application somewhere on the network.

Two facts make the mass infiltration of mobile devices unstoppable. First, they can probably increase individual productivity. Who in the enterprise can argue against that? Second, mobile devices are very affordable. With devices typically priced well under \$500, it doesn't take much of a productivity increase to justify buying a mobile device for just about any professional worker in the organization.

The best strategy for the future is to **manage** mobile devices coming into the enterprise, rather than trying to **prevent** their deployment.

Booming Sales of Mobile Devices

The growth of the mobile device market is accelerating rapidly. Dataquest reports that some 3.9 million handheld units were sold worldwide in 1998. This represents a 61.4 percent increase over volumes reported in 1997. And more devices sold means more devices to infiltrate the enterprise.

But this is only the tip of the iceberg. These numbers fail to capture the real magnitude of the threat because they don't address the real data snatcher growth areas—two-way pagers and data phones.

An Explosion of Diverse Devices

Half a billion years ago, during the Cambrian explosion, multi-cellular life appeared, and promptly filled all available environmental niches in a frantic burst of evolution and diversification. Today's mobile device market resembles the world at the beginning of the Cambrian period. The wild success of the PalmPilot proved the concept, and now developers are scrambling to add data capabilities to every kind of small device. Two-way pagers now support to do lists and address books. Cell phones are going even further, with some phones incorporating the complete functionality of a PalmPilot into their handsets.

It makes no sense to standardize on one or a few devices. While limiting the choices of employees is one way to control the glut of small devices in the enterprise, this "solution" will ultimately fail.

Since small devices typically fill relatively narrow and specific niches, they will rarely displace general-purpose computers. They will be companions to personal computers. Multi-function mobile devices, on the other hand, will tend to be more expensive than specialized mobile devices, while less functional than general-purpose computers. For maximum productivity, users will need to be able to use the device that best matches their specific needs.

But the proliferation of devices will make it even harder to manage them. Dataquest reports that 1998 mobile phone sales exceeded 162 million units worldwide. And the leading phone makers are working to incorporate data handling ability into the next generation of phones. For example, Nokia, Motorola, and Ericsson all plan to introduce *data phones* in 1999. Many of those phones will be able to synchronize with your enterprise data. Add the number of new data phones to that of two-way pagers and standard mobile devices, and the number of potential data snatching devices in the world could increase 100-fold over the next few years.

The inevitable conclusion is that enterprises will need to deploy and manage a range of devices to support a variety of usage models. In some cases, a Personal Digital Assistant (PDA) may be the best choice of device, while in other cases a two-way pager or data phone might be more appropriate. Some devices will be optimized for sending and receiving wireless email, while others will be optimized for two-way synchronization of onboard data. Similarly, data phones may be optimized to support the combination of voice and personal data, while Web phones work best to facilitate Internet and intranet access. When it comes to small devices, one size definitely does not fit all.

Moving Toward an Enterprise Solution

The goal for the enterprise is to reap maximum benefit from the deployment of mobile devices, all the while retaining control over the distribution of corporate data. The resulting solution must be cost-effective, manageable and yet sufficiently flexible to address the varied needs of end-users.

A related challenge for the enterprise is to choose a solution that can evolve with the changing spectrum of small devices and the changing needs of small device users. Many solutions exist that are limited to a specific device, a particular network, and a particular application. Given the rapid evolution of the small device market, the ability to absorb new devices, applications, networks, and industry standards will be a critical factor in the long-term viability of any enterprise connectivity solution.

A third challenge is to get from where you are today to the ideal solution, in the manner most practical and appropriate for your organization.

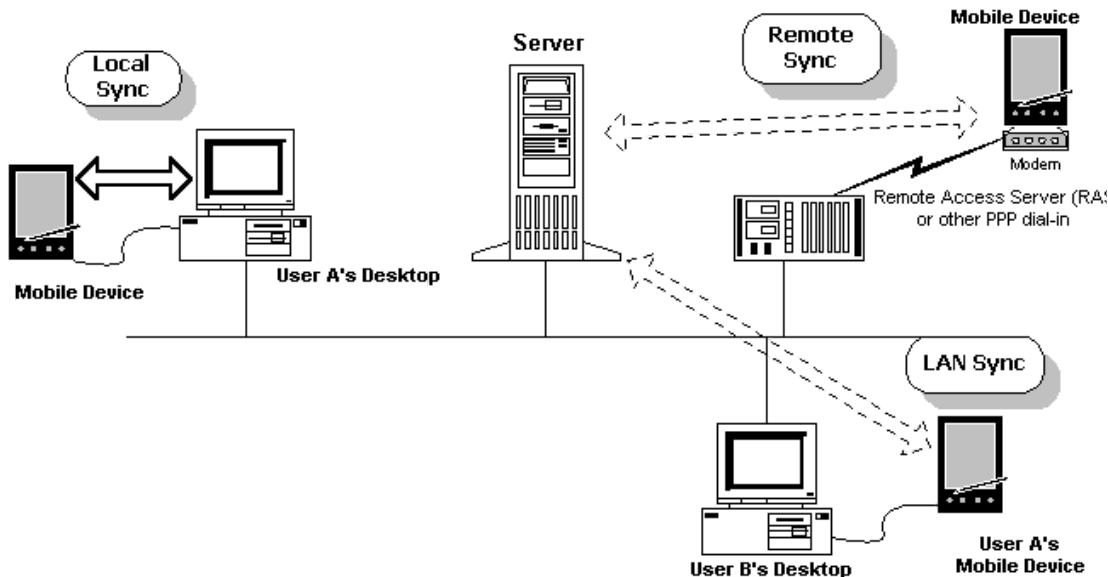
Characteristics of the Ideal Solution

The ideal enterprise solution will deliver many capabilities. The most important of these capabilities are addressed in the next several sections. The ideal solution will:

- Connect anywhere
- Support mixed devices
- Allow customized content
- Integrate wired & wireless networks
- Deliver centralized management
- Implement layered security
- Provide more than just synchronization
- Emphasize performance & scalability
- Support industry standards

Connect Anywhere

The primary usage model for mobile devices still requires a PC. This is because most devices synchronize their data using a serial cable or device cradle attached to the PC. While this model may have been adequate during the *Personal Mobility* phase of mobile computing, it clearly won't meet the requirements of the *Enterprise Mobility* phase.



A complete enterprise solution must support three distinct connection models:

- **Direct Connection.** If authorized, end users should be able to synchronize data residing locally on their PCs by connecting their small devices to individual personal computers as they do today. Security concerns may limit the use of this connection model in some enterprises.
- **Local Area Network.** When working in the office, users must be able to exchange data between their small device and server applications accessible through the local area network. This can be accomplished by using any PC connected to the LAN as a gateway to the network, or by using an Ethernet cradle that provides direct access to the LAN.
- **Wide Area Network.** When out of the office, users must be able to exchange data with the small device over a wide area network. The simplest case is to allow small devices to dial into a modem pool at the enterprise, and after authentication, exchange data with a server application. A more advanced approach might involve connecting over a wireless network to deliver a notification message to a data phone.

Support Mixed Devices

Small devices are evolving at a furious pace. As a result, the small device market will be a “moving target” for years to come. Nothing guarantees that the devices that dominate the market today will prevail in the next phase of the mobile computing evolution. Furthermore, the small device market is split into multiple device categories, each having their own strengths, weaknesses and usage models. This leads us to these rhymed conclusions:

- **One device will not suffice.** Mandating that one and only one small device will be supported for all enterprise users is doomed to failure. The approach cannot easily absorb innovations, and blatantly denies end users solutions optimized for their personal usage model.
- **Solution without dilution.** The enterprise must select a connectivity solution that capably supports today’s dominant devices, but remains flexible enough to embrace the small devices of tomorrow. Connected organizers, data phones, two-way pagers, or some device not yet invented, the solution must support them all.
- **Manage to prevent damage.** Since multiple devices and device types must coexist, the enterprise will need *Mobility Management Tools* to effectively manage the complexity. Without a standard set of tools for managing small devices and their associated data, chaos will reign.

Allow Customized Content

In the early years of *Personal Mobility*, small devices mainly held addresses, schedules, short notes, and task lists. More recently, some devices have added a level of support for electronic mail and Web access. As we move toward the *Enterprise Mobility* phase, solutions will need to address a broad range of applications. An acceptable solution must support the following applications:

- **PIM.** As before, some small devices will continue to hold personal information like contacts, schedule, notes, and task lists. This means synchronization support for popular PIM applications on the PC and/or enterprise server will be required.
- **Messaging.** Increasingly, small devices exchange data with enterprise messaging and group scheduling systems. Support for messaging systems make it possible for small devices to synchronize electronic mail messages with the enterprise server.
- **Web.** The ubiquity of the Web makes it a highly compelling platform for online and offline browsing with small devices. Using a microbrowser on the device, it should be possible to dynamically access data residing on either the Internet or the corporate intranet.
- **Custom.** The connectivity solution must be extensible, and support the addition of commercial (like ERP) and custom applications that may be mission-critical. The enterprise should have the tools to extend the connectivity solution without external assistance, thereby avoiding “lock-in” to a single supplier. These tools should include a Rapid Application Development (RAD) tool for creating device-side applications, and a Software Development Kit (SDK) for adding custom backend applications.

Integrate Wired & Wireless Networks

In addition to coping with a variety of small devices, the connectivity solution will also need to support multiple communication networks over time. Right now, connected organizers typically dial into an enterprise server using a wireline modem. But this will change as data phones and two-way pagers (both wireless devices) infiltrate the enterprise. Even connected organizers are starting to go wireless.

A comprehensive solution must support several wireless media for short-distance connectivity. *IrDA* (infrared) and *Bluetooth* (short-range radio) are examples of wireless technology that will continue to be used to exchange data between nearby devices. Over wide area networks, a two-way paging device like the RIM *Blackberry* would likely use a wireless data network like *Mobitex* (operated by BellSouth Wireless Data). Likewise, a data phone from Nokia would operate over a network like *GSM*, which is a circuit switched cellular network.

The inevitable conclusion is that any connectivity solution targeting the enterprise must support a large and changing list of wired and wireless networks. The solution should permit new network “modules” to be added as needed, without disrupting existing services. Given the performance and cost sensitivity of wireless networks, the connectivity solution must support wireless data transfer efficiently. In particular, the protocols used to exchange data between the small device and an enterprise server must be defined with narrow bandwidth communication in mind.

Deliver Centralized Management

During the *Personal Mobility* years, connectivity to small devices was controlled from an individual PC. The enterprise needs a new breed of “mobility management tools,” tools that orchestrate and regulate the deployment of small devices in the corporate setting. These tools must be independent of any device, application, or network while supporting any combination of them. In addition, the tools must reside on an administrator-controlled server rather than on an individual PC.

Central management of small devices requires the system administrator to control a set of mobile services. The mobility management tools must address the following features and services:

- **Users.** The tools must allow central management of user accounts. Devices must be assigned to a valid user account before they can exchange enterprise data. All synchronization or data access requires authentication. The tools must also support multiple devices of varying types for each registered user. Furthermore, it should be possible to define “groups” of users to make it easier to assign access and security privileges for an entire group rather than one user at a time.
- **Access Control.** Once a user account exists, the administrator must be able to define the data the user has access to from each assigned device. At least three levels of access control are needed. One level determines the applications and databases the user has access to. Another level defines the read, write, change privileges for each selected application or database. In the final level, the administrator defines the items the user can work with in each application or database. For example, a user may only have rights to access data for the Central Region in the Sales database.
- **Security.** The tools must enable the administrator to assign (possibly varying) levels of security to all users, specific groups, or selected users. Security typically involves features like authentication, encryption, compression, and digital certificates. For certain applications, the enterprise may require that both client and server certificates be used. In other cases, simpler encryption and compression techniques may be sufficient. The mobility management tools must allow the administrator to make these security choices, not the connectivity solution.
- **Inventory.** The mobility management tools should permit the administrator to maintain a small device inventory (who has what device), and also to keep track of the applications installed on each device. In addition, the administrator

should be able to define inventory rules that get enforced at connection time. For example, it should be possible for the administrator to specify that a device can only hold certain applications. The tools should check for compliance at administrator-defined intervals and report any violations.

Implement Layered Security

A connectivity solution targeting the enterprise needs to support multiple administrator-specified layers of security. The solution must address the three major objectives of any security system: *authentication*, *data confidentiality*, and *data integrity*.

Numerous technologies support these objectives, each with its own costs and benefits. The connectivity solutions will have to support some or all of the security mechanisms outlined below to satisfy enterprise requirements:

- **Message Digest Functions.** Message digest functions (also called *hash functions*) distill information into a single large number. These are most frequently used to create digital signatures and encryption keys, although the functions themselves are not used in encryption and decryption operations. Examples include MD5 (Message Digest #5) and SHA-1 (Security Hash Algorithm).
- **Symmetric Key Algorithms.** Used in encryption and decryption operations, symmetric key algorithms use the same key to both encrypt and decrypt the message. These are typically designed to be very fast, but require that both parties first securely exchange the encryption key. Examples include DES (Data Encryption Standard) and RC5 (by RSA Data Security).
- **Public Key Algorithms.** Public key cryptography is based on number theory. These algorithms use one key to encrypt the message and another key to decrypt it. This avoids the need to exchange the encryption key between parties, but tends to be slower than symmetric key algorithms. Examples of public key algorithms include Diffie-Hellman and DSS (Digital Signature Standard).
- **Digital Certificates.** Digital certificates are used to securely identify (or authenticate) either party involved in the communication. They serve the same purpose as the picture ID you must present at the airport counter. A *Certificate Authority*, which either can be internal or external to the enterprise, must formally issue the digital certificates.

Internet standards in the form of SSL (*Secure Sockets Layer*) and TLS (*Transport Security Layer*) encompass several of the advanced security layers needed to support the enterprise. However, these standard protocols are not necessarily available across the range of networks used with small devices.

Provide more than just Synchronization

Synchronization, first introduced with PalmPilot connected organizers, rapidly became a pivotal feature built into most small devices. The PalmPilot led the way by implementing a simple yet highly effective model for synchronizing application databases. The presence of unique identifiers in every PalmPilot record and the ability to track database changes are examples of simple features that made it possible for the PalmPilot to synchronize its data quickly and seamlessly.

As the *Enterprise Mobility* phase arrives, synchronization remains an essential feature for the enterprise. The ability to synchronize information quickly and reliably between small devices and enterprise applications must be a primary characteristic of any connectivity solution. Advanced features such as the handling of conflicting changes and the application of filtering rules to control data distribution will be crucial in an enterprise setting, where thousands of users may be affected by the solution.

Despite the importance of synchronization, the enterprise will need more than just synchronization to support its overall connectivity requirements in the future. Connectivity solutions must address these additional functions and usage models:

- **Notification.** Notification involves sending time-sensitive messages to the small device without waiting for a batch synchronization operation. Two-way notification entails sending messages in the opposite direction as well. This usage model is particularly relevant to small devices connected over wireless networks, where an active connection is possible much of the time. Let's say that an enterprise configures meeting invitations to automatically go to employees who have been issued data phones. When a new meeting invitation arrives at the group scheduling application, it is immediately transmitted to the data phones over the wireless network. Once received by the device, the user can accept or reject the invitation, with that action triggering an automatic response to the group scheduler. If the user accepts the invitation, the meeting is added to the calendar on the data phone itself. Notification will be an essential feature of any connectivity solution supporting wireless devices in the future.
- **Browsing.** Certain classes of applications that require up-to-the-minute information or that may be infrequently accessed from small devices are not particularly well suited for either synchronization or notification. These applications are better supported using a browsing model, where a *microbrowser* (small-footprint browser application) is used to view data residing on the enterprise server. This solution is especially effective for viewing Web data (usually HTML documents) accessible on the Internet or the enterprise intranet. Let's assume that an enterprise keeps a Contracts

database somewhere on the intranet. If users need only infrequent access to this database, then viewing individual contracts on the device may be the best usage model when out of the office. It may also make sense to implement offline browsing, where the data is first brought down to the small device and stored for later viewing. This allows for reduced communication costs, since the user doesn't need to stay connected while actually viewing the document. Browsing is an unavoidable usage model that must be supported as part of any enterprise connectivity solution.

- **Querying.** The ability to query data residing on an enterprise server is especially important for supporting custom applications. This usage model is frequently called "query/response," meaning that the user issues a query that is sent from the small device to the enterprise server. The server application replies with a tailored response. Let's imagine that an enterprise maintains an automated inventory system to track office supplies. An application can then be installed on the small device to check the availability of any particular item. The user brings up a query form on the device and selects the inventory item from a list. The application then connects to the enterprise server, sends the query, receives a response containing the item quantity, then disconnects. This usage model is essential to support interactive client-server applications.
- **Installation.** For programmable devices, the connectivity solution must allow an administrator to remotely install new applications or upgrade pre-installed applications on the small device. The administrator must be able to request that new applications be downloaded to all users, select groups, or only specific individuals. Once installed, the application is automatically enabled to exchange its data with the enterprise server as allowed by the access privileges, and without requiring further user intervention. This is the only practical way to install custom applications developed by the enterprise. This avoids the need to recall devices from the field for installations.
- **Backup.** Experience has shown that small devices are easily lost or destroyed. When this happens, the contents of the device must be restored easily and without drama. For this reason, a remote backup and restore feature is a necessary feature of any enterprise connectivity solution. The administrator must be able to specify backup rules that get executed when the device is connected to the network. For example, it should be possible to specify that certain databases be copied to the server on a given schedule.

Emphasize Performance & Scalability

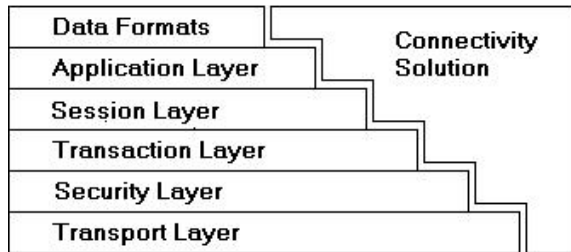
The performance of client-server applications inevitably involves some complex and interrelated factors. While there are no fixed or easy answers to questions surrounding performance, connectivity solutions for the enterprise must be "small device friendly." The architecture must account for the specific needs of small device users and the characteristics of the networks they use to communicate. The final proof of good performance lies in the responsiveness of the system to its end-users (latency), and the resource demands it imposes on the enterprise (cost).

Scalability is the ability to grow the solution over time to accommodate a growing number of users, devices, and services. Like performance, scalability must be designed into the core of the connectivity solution. These questions will help you evaluate performance and scalability features.

- How large is the client application that runs on the small device?
- What are the typical resource requirements on the server?
- What protocol is used to exchange data between the small device and server?
- What assumptions are made about the underlying communication network?
- Is a persistent connection required between the small device and server?
- What is the typical latency (time waiting) experienced by the end user?
- What's required to add support for a new device?
- What's involved in adding support for a new application?
- How many concurrent users can the server typically service?
- Can functions be spread across multiple hardware platforms?

Support Industry Standards

An enterprise connectivity solution must leverage reasonable de facto and formal industry standards to the extent possible, without compromising significant performance and functionality. Use of pre-existing standards gives the enterprise greater flexibility for the future, and reduces its dependency on vendor-specific interfaces. The following diagram depicts a layering of standards applicable to connectivity solutions targeting the enterprise.



The following list describes each layer, with one industry standard mentioned per layer to help clarify the type of interface in question. Many more standards than the ones identified here exist at each level. The reader is advised to refer to the many available Internet Engineering Task Force (IETF is the body responsible for Internet standards) specifications for more information on relevant standards.

- **Data Formats.** The data format layer includes standards that specify the representation of data for certain types of applications. In the context of connectivity solutions, data format standards encode the data exchanged between small devices and the enterprise. An example of a data format standard is *iCalendar*, which is an Internet standard for representing events and tasks.
- **Application Layer.** The application layer consists of standards that promote consistent interfaces to specific application categories. As the need for interoperability grows, the number of application types covered by these standards likewise grows. An example of an application layer standard is *Infrared Mobile Communications* (IrMC), which is an industry standard that facilitates synchronization of personal data among telecommunication devices connected over short distances.
- **Session Layer.** The session layer defines standards that govern the way connections are established between the small device and an enterprise server (in our case). It usually defines the negotiations that must precede a connection, and the “envelope” used to carry the data. A popular example of a session layer protocol is *Hypertext Transfer Protocol* (HTTP), which defines both the negotiation and envelope used for sending *Hypertext Markup Language* (HTML) documents.
- **Transaction Layer.** The transaction layer contains standards that specify the lower-level mechanisms for sending messages or transactions over a network. For our purposes, these messages are transferred between the small device and the enterprise server. A predominant Internet standard that falls in this category is the *Transmission Control Protocol* (TCP), which defines how packets are sent over the network as a stream of data.
- **Security Layer.** The security layer consists of protocols that ensure secure transmission over the network. These standards focus on data integrity, privacy, and authentication. An example of an Internet security standard is the *Transport Layer Security* (TLS is also known as SSL), which applies public key cryptography for securing transactions sent over the network.
- **Transport Layer.** The transport layer standards specify the low-level interfaces to the network itself. Each network type has its own set of interfaces. An example of a transport layer standard is the *Infrared Data Association* (IrDA) standards that govern the physical and logical transfer of data between devices equipped with infrared transceivers.

The main point to remember is that enterprise connectivity solutions must deliberately support germane standards at all these levels. For example, there are efforts underway to standardize on a synchronization protocol to be used for communicating with any small device over either wired or wireless networks. Once approved, synchronization solution providers should implement this standard to avoid the proliferation of incompatible small device synchronization standards.

Making the Transition: Intellisync Gold

It's clear that there is an ideal enterprise solution to the problem of data-snatching small devices. But there's still the issue of getting there from whatever state your organization is in now. Perhaps a step-by-step transition is in order.

The most logical first step in the transition is to get some control over the way small devices interact with your networks. Without such control, you have no hope of defending your enterprise data. Asserting control means setting a carefully chosen synchronization standard.

Remember that a range of small devices and applications are likely already in use in your enterprise. To minimize the disruption caused by choosing a standard, you need one that supports the most common small devices and synchronizes with the most popular applications.

The standard you choose should also offer some sort of migration path to the ideal enterprise solution.

And it wouldn't hurt if the standard was part of an award-winning family of advanced synchronization products. The standard you need is Intellisync® Gold from Puma Technology®, Inc.

Intellisync Gold is Puma's all-in-one site license solution to data synchronization. Intellisync Gold supports small devices based on the Palm Computing Platform and Microsoft Windows CE. On the application side, Intellisync Gold supports popular PC applications like Microsoft Outlook 97/98, Lotus Notes and Organizer, and Novell GroupWise.

Major Features

The following list details benefits that Intellisync Gold provides as the transitional step from where you are now to the ideal enterprise solution:

- **Superior Synchronization.** Intellisync Gold gives you the latest versions of the award-winning Intellisync for Palm Computing Platform and Intellisync for Windows CE, so you know you have the best synchronization available from Puma Technology, Inc.
- **Simple Licensing.** You license Intellisync Gold on a "per seat" basis. You don't need to worry about how many users of each particular device or application your company has. Simply license Intellisync Gold for the number of users you have, and you're on your way. If users change devices or applications, you're covered. And as the number of users increases, so does your volume discount.
- **One Interface across the Organization.** Since all Intellisync products are designed with a common user interface, you won't have to support a different interface for every device.
- **Premier Subscription Service.** The Intellisync Gold Premier Subscription Service protects your investment with a year of upgrades.

The Ideal Solution: Intellisync Anywhere

Intellisync Anywhere[™] is an enterprise connectivity solution from Puma Technology, Inc. But it is more than just a product. Intellisync Anywhere is the base technology for all future enterprise products from Puma. As this product family evolves, we intend for it to meet all of the criteria for an enterprise connectivity solution described earlier in this paper.

The first member of the Intellisync Anywhere product family, *Intellisync[™] Anywhere for Microsoft Exchange*, exhibits many of the features described in this white paper. For example, it enables local, LAN, and remote connections from small devices. It supports communication over infrared, serial port, dial-up networking, the Internet, and any wireless network supporting the Internet Protocol (IP).

Intellisync Anywhere supports a variety of small devices, including the PalmPilot Connected Organizers and devices powered by Windows CE from Microsoft. It simultaneously synchronizes personal information and messaging data with the small device. It provides central management of user accounts, server settings, and synchronization configurations. Intellisync Anywhere also uses industry-standard security algorithms like SHA-1 and RC5 to implement symmetric key encryption, and leverages important industry standards like TCP.

Major Features

The following list details some ways in which Intellisync Anywhere matches the ideal enterprise connectivity solution described in this paper:

- **Connect Anywhere.** Intellisync Anywhere can connect with small devices over a direct connection, Local Area Network, or Wide Area Network. This combination satisfies the enterprise requirement to permit users to "connect anywhere."
- **Support Mixed Devices.** Intellisync Anywhere is designed to be independent of any particular device or type, with each product capable of embedding support for a combination of devices. This addresses the need to support a mixture of small devices within the same connectivity solution.
- **Integrate Wired & Wireless Networks.** Intellisync Anywhere is independent of the underlying network, and uses an application layer protocol that operates efficiently over wired and wireless networks.
- **Implement Layered Security.** Future versions of Intellisync Anywhere will support advanced levels of security through a partnership with an established security vendor. To meet the needs of enterprises looking for the best possible security, Intellisync Anywhere will support public key cryptography.
- **Support Industry Standards.** Wherever possible, Intellisync Anywhere leverages pre-existing industry standards. All levels use industry standard interfaces to reduce the need for proprietary Puma interfaces. Once a standard synchronization protocol exists, Puma will rapidly move to embed that protocol in Intellisync Anywhere. Additionally, Puma is involved in standardization efforts in *IrDA*, *IrMC*, *Bluetooth* and *WAP* (partial list). We have also joined with

AvantGo to support *MAL* (Mobile Application Link), an open source code initiative to standardize small device synchronization. As each of these standardization efforts bears fruit, we will integrate it into Intellisync Anywhere.

An Emphasis on Performance & Scalability

Intellisync Anywhere is designed with scalability and performance in mind. The solution can support a growing number of concurrent users, eventually spanning multiple enterprise servers. The architecture incorporates a number of pervasive performance and scalability features which make it easier to support a growing number of concurrent users over time. In addition, the solution supports plugging in new devices, applications, and networks as required, without impacting the core server components. These factors make Intellisync Anywhere highly scalable, eliminating the need for multiple point solutions.

Performance

One of the underlying premises of the Intellisync Anywhere product family is that everything should be “fast sync” enabled. Fast sync is an important element of the architecture, designed to minimize the connection time needed to complete data exchanges between the small device and server. In the background, the server accumulates changes on behalf of configured users, awaiting a connection request. Once the small device connects to the network, the device and the server exchange only items that have changed. After the device disconnects, the server application applies the device-side changes to the application database. This approach eliminates performance variances attributable to the server-based application, and minimizes connection time for the mobile user (resulting in a reduced cost of ownership).

In addition to adopting a fast sync model, Intellisync Anywhere implements a highly efficient synchronization protocol that optimizes communication between the small device and enterprise server.

Scalability

Intellisync Anywhere is designed to include a *Messaging Layer*, which is the “piping” that facilitates communication among all components of the product. In principle, the Messaging Layer provides a simple and secure way for programs to send and receive data, without having to worry about the complex differences between platform operating systems and networks. As messaging is a connectionless paradigm, the Messaging Layer model allows the administrator to add new wired and wireless networks over time.

The use of a Messaging Layer has a major impact on the scalability of the resulting solution. For example, the messaging paradigm allows any of the server components to reside on the same machine, on different machines at the same location, or on machines in totally different locations. Given this flexibility, system administrators are able to influence the distribution of work across multiple servers over time.

Providing more than just Synchronization

Enterprise mobility will eventually involve much more than data synchronization. Puma plans to offer a progression of products and features in the Intellisync Anywhere family that will address the enterprise needs for:

- Notification
- Browsing
- Querying
- Installation
- Backup

Conclusion

Like something out of a science fiction movie, a vast swarm of small devices is encroaching on the enterprise world. These data-snatching mobile gizmos are coming your way, whether you like it or not. Combining enticing features, low prices, and ever-improving wireless networking capabilities, small devices have become irresistible productivity enhancers for enterprise employees. But nothing this good comes without a price. By making enterprise data mobile, these devices shatter existing methods for defending this key enterprise resource.

The key challenge small devices pose for the enterprise is maximizing their ability to improve productivity, while minimizing the data security risk they pose. To succeed in the Enterprise Mobility era characterized by the ubiquity of these small devices, your enterprise needs to deploy mobility management tools.

Mobility management tools will make possible connectivity solutions that are capable of managing the wild diversity of small devices that are just now appearing. These solutions will provide centralized management over users and their small devices, as well as the applications and data the users need access to. The solutions will be server-based, and extensible, allowing administrators to plug in any number of devices, applications, and wired or wireless networks to meet the enterprise's changing needs. The best solutions will also support varied usage models, including incremental synchronization, notification, browsing, and querying.

Puma Technology has long been the leader in advanced synchronization solutions for the mobile market. With its new Intellisync Anywhere family, we offer you a solution designed, from the ground up, to meet demanding enterprise needs. With an extensible architecture, support for local, LAN, and remote connectivity, advanced security, optimized performance, and scalability, the Intellisync Anywhere product family is the best solution for empowering the mobile enterprise.

