

# Asentria within the Service Provider Ecosystem

*With Asentria solutions, service providers can enable customers with reliable connectivity from any location*

Organizations today depend upon their networks to increase productivity and reduce network infrastructure and maintenance costs. Accordingly, these networks must be secure and perform reliably in order to accommodate geographically dispersed users. Unplanned remote site downtime due to equipment failure or adverse environmental conditions can severely impair network service. There is a growing need for diverse network services that are supported with cellular towers, microwave sites, broadband wireless towers and other remote facilities. Business customers are looking to service providers to support their remote computer and telephony rooms with customer premise equipment. In both cases, environmental conditions and power and equipment failures are major causes of unplanned network downtime. IT professionals responsible for providing high availability networks are becoming increasingly aware of the need to protect these vital, yet vulnerable remote sites.

## **Service Providers are Searching for the Holy Grail - OSS Solutions**

Operational support system (OSS) is a generic term used for a suite of programs that enable an enterprise to manage their business systems dealing with customers, supporting processes such as taking orders, processing bills, and collecting payments, as well as monitoring, analyzing and managing network systems. The term originally was applied to communications service providers, referring to a management system that controlled telephone and computer networks. The term has since been applied to the business world in general to mean a system that supports an organization's network operations. An OSS is critical to bridging front-office applications with back-office efficiencies, customer relationship management, differentiated IP services, rapid service delivery, and scalability. As networks evolve and expand, an OSS becomes essential to the delivery of high-margin services and



# Asentria within the Service Provider Ecosystem

---

profitability. The bottom line is customers will select service providers that save them the most time and money, while providing the best performance and customer care.

For many years, the leading telecommunications companies have been looking for interchangeable, interoperable, off-the-shelf business components to quickly integrate into their operations support system (OSS) solutions. These components include service activation, provisioning, quality of service, monitoring and management, billing, trouble ticketing, and other key elements. Carriers worldwide spend more than \$50 billion a year on OSS functions, with approximately \$4 billion going to network hardware vendors, and \$10 billion to independent software providers (ISVs). The remaining balance is spent internally. Yet, nearly half of the \$50 billion spent on OSS technology has been for custom-made solutions that were painful to install, not reusable, and expensive to maintain and support.

## Managing Customer Premise Equipment

Customer-premises equipment or customer-provided equipment (CPE) refers to any equipment and inside wiring located at a customer's premises and connected with a carrier's telecommunication channel(s) at the demarcation point. The demarcation point is a point established in a building or business complex that separates customer equipment from communications company equipment. CPE generally refers to telephones, DSL modems, cable modems, and set-top boxes for use with a service providers' service; also included are key phone systems and private branch exchanges (PBXs). Excluded from CPE are over-voltage protection equipment and pay telephones.

While the opportunity for managed CPE service growth has great promise, there are many challenges that service providers face. The new and varied technologies implemented at remote sites is usually more than just a traditional PBX voice system, and often exceeds the monitoring capabilities of traditional remote monitoring devices. Immediate

and secure access has never been more of a concern, yet many older monitoring devices lack the required security, are too complicated to set up, or report alarm conditions using proprietary communication methods. Furthermore, the demands for high system availability require monitoring and response that go beyond the simple, unintelligent monitoring that has traditionally been available.

## Monitoring Remote Equipment Sites

One of the greatest challenges to any service provider is the maintenance of continuous and economical service regardless of weather conditions and power irregularities. Remote equipment sites can include cellular towers, microwave sites, broadband wireless towers, TV and radio towers, and other remote facilities. Equipment in these sites can include a diverse set of devices such as microwave transceivers, cellular transceivers, WiMAX transceivers, broadcast transceivers, routers, servers, power supplies, batteries, generators, and much more. Physical elements can include doors and windows, security equipment such as cameras, temperature, water, fire, chemicals, and many other environmental conditions.

## Element Management Systems

An Element Management System (EMS) manages diverse network elements. Typically, the EMS monitors the functions and capabilities within each network element, but does not manage the traffic between different network elements in the network. To support management of the traffic between itself and other network elements, the EMS can communicate with higher-level Network Management Systems (NMS). A typical enterprise contains many different network elements. However, each device normally requires a vendor-specific element management system in order to effectively manage the network element. Therefore, multiple management stations may be polling network elements for the same information, and data collected by the different systems is stored in separate databases, creating undue administration overhead. The EMS provides the foundation to implement a telecommunications management layer that can plug into OSS architectures to

---

enable service providers to meet customer needs for rapid deployment of new services, as well as meeting stringent quality of service requirements.

### **The Market Need for Remote Site Management**

With each passing year, more and more strategic and sensitive network equipment is being deployed remotely. Service provider remote infrastructure for cell tower sites is expected to increase from 134,995 in 2007 to 169,166 in 2011, according to GeoResults, Inc. Alexander Resources predicts that by 2010 the worldwide WiMAX market will reach \$3.5 billion. This growth will be driven by new equipment from a growing list of hardware suppliers, and an increasing number of WiMAX trials and deployments. Multimedia Research Group forecasts IPTV services will reach 36.9 million subscribers in 2009, up from an estimated 3.7 million subscribers in 2005. Subscriber revenues will grow from \$880 million in 2005 to \$9.9 billion by 2009, and research firm IDC reports that the costs to support customers skyrocketed from \$41 billion in 2003 to \$58 billion in 2006, while during this same time period customer satisfaction declined from 75% to 73.5%. The difficulties in supporting customers are caused by many factors, including the increased rate of new service offerings, and the complexity of new converged services.

### **Asentria EMS solutions**

Service providers can enable customers with reliable connectivity from any location. Customers can rely on network services that are delivered with maximum uptime, IT personnel gain a dramatic improvement in quickly resolving remote site equipment and environmental problems, and organizations reduce their overall remote site infrastructure and maintenance costs. Over 10,000 organizations and service providers worldwide rely upon Asentria as the leader in remote site monitoring - ensuring secure, proactive monitoring that can make the difference between an inconsequential event and critical downtime.

By helping companies avoid failures from poorly performing equipment that threaten end-user service expectations, Asentria helps network administrators to better control and predict the performance of their remote site infrastructure. Our products are designed to provide a new level of protection by shielding end-users from remote site equipment failure, and enabling administrators with optimized alert response times due to equipment failure, inconsistent equipment operation and environmental conditions. Any one of these elements can cause end-users to experience service problems.

The challenge that today's service providers face is that there is more pressure than ever to keep their remote equipment up and running, as customers continue to demand higher levels of reliable service. Businesses are under increasing pressure to fix problems more quickly, and competitive cost pressures continue to mount. Thus, there is a growing need for remote site management solutions that can help service providers monitor, access, and control all of the equipment that they have based in remote or understaffed locations; be it remote communication towers, on-site security systems, transmitters, power sources, etc.

Asentria, the market leader in remote site monitoring and telemanagement, offers comprehensive solutions for remotely monitoring, accessing, and controlling equipment in remote locations. At the service provider NOC everything may look just fine in the call center. However, customers of managed CPE services are complaining that they can't access the network. So where is the problem? Unfortunately, the network management system at the NOC has limited or no visibility into the many vital remote equipment sites that extend and deliver network services to consumers, and the remotely managed CPE service for business customers.

# Asentria within the Service Provider Ecosystem

The ability to monitor, access, control and collect data to deliver a reliable end-to-end network experience has helped make Asentria the leader in remote site monitoring and telemanagement solutions. With Asentria’s unique position within the network, service providers are no longer blind to what is happening in remote equipment sites, and no longer have to wonder about the customer experience. They can have complete remote site visibility brought to their desktops.

This will not be accomplished through more devices, more complexity or more single capability solutions. The solution is found at the critical juncture where remote equipment sites link distributed networks and connect to the centralized network management system - where all the remote monitoring, access, control, and security are required, and are integrated within a cohesive platform.

Asentria EMS solutions plug into OSS solutions for remote equipment provisioning, monitoring, maintenance and support operations. Asentria enables service providers to monitor, manage, and update equipment in cellular towers, microwave sites, broadband wireless towers, and other remote facilities in support of network services, as well as for managing equipment located at remote customer offices. Customers can rely upon telecommunications services that are delivered with maximum uptime, IT personnel gain a dramatic improvement in quickly resolving remote equipment and environmental problems, and organizations reduce their overall remote site infrastructure and maintenance costs

Asentria’s EMS solution delivers a unifying management platform that enables service providers to simplify their ability to securely connect into remote customer sites to monitor and manage equipment. We deliver a single point of management through which remote administrators can monitor, access, and control SNMP-enabled or non-SNMP/non-networked equipment, monitor environmental conditions such as temperature and humidity, and manage related devices such as fans and security sensors. Asentria’s EMS consists of two primary components:

1. TeleBoss, a family of Telecom Site Controllers that reside at the customer premise to securely access, monitor, control, and collect data from PBXs, other telecommunications infrastructure and environmental conditions; and SiteBoss, a family of Remote Site Controllers that are located in remote equipment sites such as cellular towers, microwave sites, broadband wireless towers, TV and radio towers, and other remote facilities.
2. SitePath, a secure administration portal that provides a centralized management platform for the network operations center (NOC) to monitor TeleBoss and SiteBoss Controllers, and the managed equipment behind them. Together, TeleBoss, SiteBoss and SitePath work in combination to monitor and manage the health of vital telecommunications infrastructure.

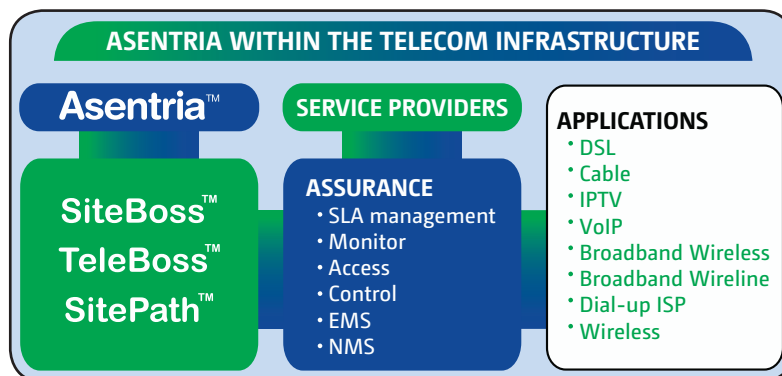


Figure 1. Asentria supports service provider customer applications

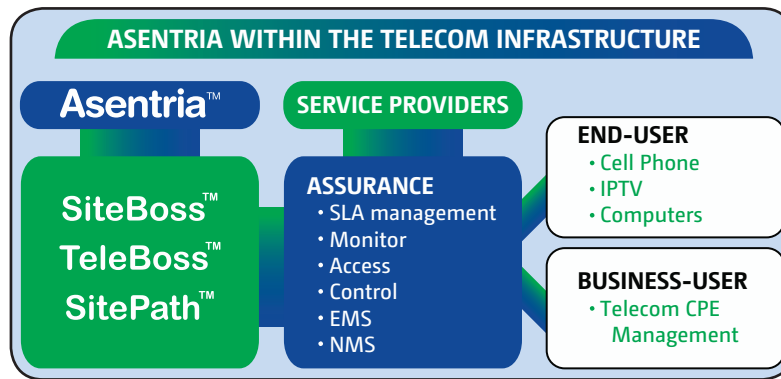


Figure 2. Asentria supports service provider customer applications

Asentria’s SitePath administration portal, TeleBoss, and SiteBoss Controllers create a standard process and user interface for network operators wherever they may be located. This simplifies training costs, and provides faster deployment of next generation managed services that require secure, flexible, and efficient network operations.

### TeleBoss™ – Telecom Site Controllers

The TeleBoss Series of Telecom Site Controllers address the monitoring challenges presented by this new generation of remote voice and data systems. The TeleBoss product line provides powerful, flexible, and cost-effective choices for PBX Vendors, Call Accounting Service Bureaus, Managed Service Providers and enterprise managers who need to securely monitor, access, control, and collect data from their voice and data infrastructure located within remote customer premises.

The TeleBoss product line meets these new challenges through a series of low-end to high-end stand-alone monitoring hardware devices that can be deployed at the remote sites where monitoring and management is required. The TeleBoss Controllers are scalable and economical, easy to setup and use, provide a variety of secure options for in-band and out-of-band remote access, and offer a powerful set of versatile and intelligent monitoring and control features that allow you to immediately detect and

react to potential threats at your remote sites in order to prevent downtime.

### SiteBoss™ – Remote Site Controllers

The SiteBoss Series is a powerful solution for service providers and enterprises that need to monitor, access, control, and collect data from communication infrastructure located in remote sites. The SiteBoss Series of remote site monitoring controllers are an affordable solution to help you avoid costly remote facility downtime. Many of the factors that impact the health of your network infrastructure, such as environmental conditions and legacy equipment alarms, remain dangerously outside the scope of your network management system (NMS). The SiteBoss Series enables you to easily integrate these elements into your NMS, and helps you prevent unexpected, undiagnosed downtime from non-networked, non-SNMP devices and environmental conditions, by monitoring threatening conditions before they damage or destroy your mission-critical equipment.

### SitePath™ – Secure Administration Portal

Asentria’s SitePath is a secure administration portal that provides on-screen visibility into remote customer networks to manage and control all monitored equipment and environmental conditions. Many of the problems found can be corrected remotely, thus avoiding costly physical site visits. When on-site service is required, technicians arrive with the information

# Asentria within the Service Provider Ecosystem

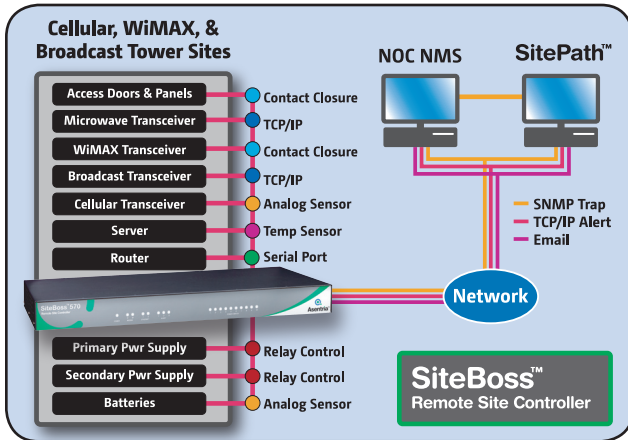


Figure 3 Asentria's SiteBoss monitoring a remote equipment cabinet

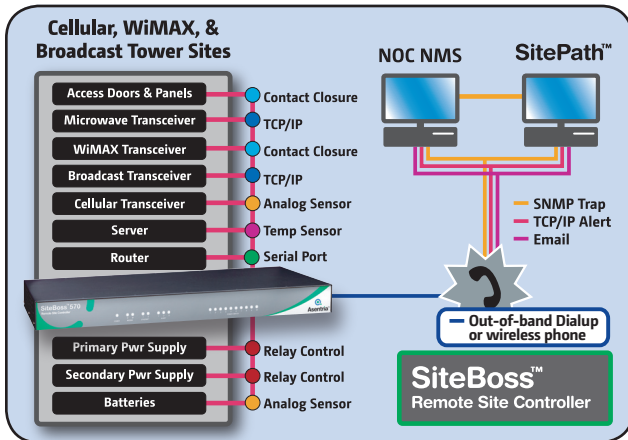


Figure 4 Asentria's SiteBoss delivers access and control to a remote equipment cabinet

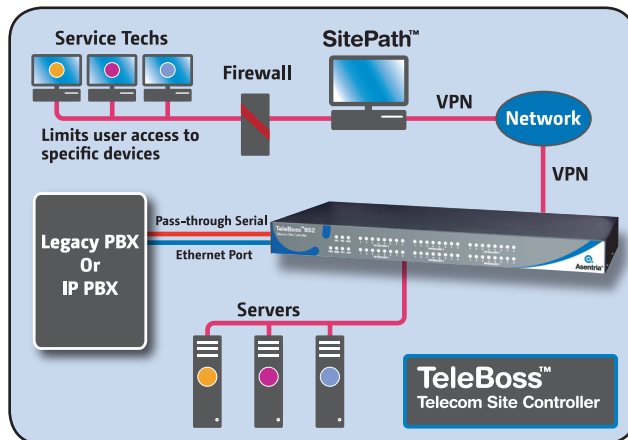


Figure 5 Asentria's solutions proactively monitoring serial alarm messages and SNMP traps from the PBX. VPN capabilities limit user access to specific devices within the network.

they need to take quick corrective action, reducing response time and maintenance costs.

The need to re-provision equipment to restore communications is a frequent occurrence, especially at remote locations that are often difficult to reach and costly to service. For service providers with remote cellular towers, microwave sites, broadband wireless towers and other remote facilities, maintaining reliable and highly available networks can be challenging. Traditional network management systems fall short because they only work in-band, or over the main microwave backhaul connection. If that connection goes down, that site goes down, and no management data will be collected or reported. NMS also lacks the control and automation capabilities to correct problems without manual intervention. A costly support technician must still be dispatched to solve the problem, which can take many hours or even days, depending on the location and availability of technical expertise. Traditional in-band software solutions are limited due to their dependence on the underlying network being up and available in order to function. By contrast, existing out-of-band technologies, such as terminal and console servers, provide local access via serial connectivity to networked devices. However, they lack robust management capabilities, such as automated maintenance and recovery.

## Remote Equipment Sites

Today, digital IP networks are king, with data, voice and video intertwined in virtually every enterprise and service provider infrastructure. For corporations, service providers and broadband ISPs, this means a host of network equipment sites often miles and sometimes hours away from the nearest qualified service personnel. However, with the number of broadband alternatives now proliferating in the market, a few service interruptions or reliability problems can cause customers to jump ship in droves. Yet, this same competition imposes cost constraints that demand cost-effective solutions to keep remote sites running smoothly with a minimum of "in-person"

service personnel or “truck rolls”. All of this has to occur while maintaining tighter security controls than ever before.

The SiteBoss Series of Remote Site Controllers address each of these monitoring challenges facing today’s network architects and managers. The SiteBoss Series products help you detect and control remote site factors such as non-networked, non-SNMP devices and environmental conditions which otherwise remain dangerously outside the scope of your network management system (NMS), while providing security sufficient to satisfy even the most stringent requirements.

### **Secure Access to Remote Equipment Sites**

The SiteBoss Series brings remote site management into the 21st century by providing high bandwidth connectivity such as Ethernet, GSM, CDMA, EDGE cellular and/or an on-board ADSL interface to provide fast, reliable, cost-effective connectivity into your remote sites. However, in today’s world connectivity is a liability without corresponding security. The SiteBoss Series provides dialup security options such as modem callbacks and caller ID filtering, as well as SSH, SFTP, one-step VPN, and two-factor authentication options to provide secure point-to-point connection options. Through this connectivity, the SiteBoss facilitates pass-through sessions with connected serial devices as well as other devices on the same remote network via Remote Access and Routing. With Asentria’s SiteBoss products, service providers can offer new revenue generating services previously not possible because of security concerns or logistical difficulties.

### **Secure CPE Access and Control**

The ability to deliver secure remote access to customer premise equipment enables service providers to create new managed service offerings. Automating secure access and control can limit the technicians access to specific sites and explicit equipment.

### **Alarm Management**

Alarm management allows users to collect and organize alarms that are received. Administrators can manage new, open and closed alarms, prioritize alarms based on resolution response factors, and categorize alarms based on alarm process management criteria. Alarms can be sent to specific individuals, groups and departments.

### **Easy-to-Manage, Scalable Remote Managed Services**

The SiteBoss and TeleBoss product lines integrate with the Asentria SitePath Administration Portal to provide a unified single point of access and management of the TeleBoss Controllers deployed throughout the enterprise. When using the SitePath VPN Gateway, a secure point-to-point connection can be made between your service managers and the remote devices they are managing, without exposing any passwords or access information to mid-level staff. Once connectivity is initiated, the TeleBoss Controller automatically maintains a secure connection between your technician and the remote TeleBoss device. All routing and NAT traversal is transparently handled by TeleBoss, enabling easy and secure access and delivery of alarm information.

### **Asentria EMS Solution Benefits**

From a business standpoint, managed service providers, service bureaus, and network operators are under continuous pressure to optimize operational expenses and to improve profitability. Significant areas that can benefit from efficiency gains include network field operations, administration, maintenance and provisioning – reducing “truck rolls” for field technicians and ensuring maximum uptime for customers. Combining business requirements and new technical capabilities enables an integrated and unified remote site monitoring strategy.

## Planning and Design

- Easier vendor management with less capital investment for deploying remote site equipment.

## Implementation

- Faster, easier and error-free deployments with fully managed, plug-and-play provisioning.

## Maintenance

- Future-proof your network through Asentria's comprehensive EMS solution platform.

## Onsite Repair

- Reduce network downtime by ensuring timely repair or repair of non-operational equipment.

## Monitoring and Alerting

- Business-critical network reliability delivered through automated equipment and environmental monitoring, access, and control.

## Upgrades and Changes

- Minimize total cost of ownership and improve remote site recovery by maintaining accurate CPE records and automating firmware upgrades and configuration changes.

## Customer Support

- Lower operational costs and reduce downtime using purpose-built telecom CPE management solutions.

## Summary

The accelerated growth in the complexity and quantity of data and voice equipment at remote sites and branch offices has brought with it many new challenges that today's service providers must meet.

The new and varied technology implemented at remote sites is usually more than just a traditional PBX voice system, and often exceeds the monitoring capabilities of traditional remote monitoring devices. Immediate and secure access has never been more of a concern, yet many older monitoring devices lack the required security, or they are too complicated to set up.

For service providers with remote equipment sites that deliver network services, and managed service offerings for equipment located within customer offices, physical conditions and equipment failures are some of the major causes of unplanned network downtime. Service providers are becoming increasingly aware of the need to protect these vital, yet vulnerable sites. However, acquiring more devices, more complexity or more single capability solutions is not the answer. Bridging the gap between diverse remote equipment sites and the central NOC, by providing visibility through remote monitoring, access, control and security within a cohesive platform is required.

Asentria provides real-time visibility, secure access, and desktop control of remote equipment sites. Environmental extremes, equipment failures, and power loss threaten communication networks, yet many of these critical factors reside outside the scope of a centralized network management system. Asentria delivers a single unifying platform to enable remote equipment sites and network management to be simplified, consolidated, more reliable, and more cost-effective. With unified and improved remote site monitoring, access, and control, service providers are able to run their critical networks more efficiently, while lowering their operational costs.

