PanTerra

PanTerra Unified Cloud Service HIPAA Compliance

White Paper Series

The FutureProof Cloud
Built for Business

PanTerra Networks
4655 Old Ironsides Dr, Suite 300
Santa Clara, CA 95054
800.805.0558
www.panterranetworks.com

Unified Cloud Services
Communications
Collaborations
File Sync & Share
Business Analytics

PANTERRA'S UNIFIED CLOUD SERVICE & HIPAA COMPLIANCE

Executive Summary

The passing of HIPAA and the HITECH Omnibus acts in the US has ushered in new stringent requirements for any company handling Patient Health Information (PHI). This includes cloud service providers that store or support the transmission of PHI data. Many cloud providers, such as hosted VoIP providers, are not equipped or capable of supporting these new requirements. Covered Entities (CEs) may not know, but even hosted VoIP providers may fall under these new security requirements if they store voicemails, call recordings or patient faxes in their cloud. In addition, even those cloud providers that claim to be HIPAA compliant may not be providing an end-to-end compliant solution if they are not delivering fully secure (VPN/MPLS) bandwidth and authentication-controlled end device management.

PanTerra delivers an end-to-end fully compliant HIPAA/HITECH Omnibus solution, not only securing its service and data centers, but also delivering secure connectivity and full end device authentication control. PanTerra's end-to-end solution includes:

Full HIPAA/HITECH Omnibus Compliant Services – PanTerra has implemented all necessary administrative, technical, physical and organizational requirements to be HIPAA/HITECH compliant for all its cloud services.

SmartBand MPLS Secure Connectivity – PanTerra offers an IP-VPN secure bandwidth solution in addition to in-transit encryption to ensure complete security when transmitting ePHI data from a CEs location to PanTerra's data centers.

Security Protection Extended to End Devices – PanTerra implements full Multi-Factor Authentication (MFA) for all end devices as required by HIPAA.

Downstream BA Agreements – PanTerra has secured all necessary downstream BA Agreements with sub-contractors and 3rd party vendors.

PanTerra is fully committed to delivering a secure end-to-end cloud service solution for those enterprises that want to be compliant with HIPAA/HITECH. With PanTerra, your outsourced IT services and PHI content are safe and secure. See how PanTerra can be your HIPAA/HITECH compliant unified cloud service provider today.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

What is HIPAA and HITECH Omnibus?

HIPAA or the Health Insurance Portability and Accountability Act, was passed by the US congress in 1996 with the primary goal to make it easier for people to acquire and retain their health insurance, protect and secure protected health information (PHI) and help the healthcare industry control administrative costs. Covered Entities (CE) are those entities that actually provide the treatment, payment and operations in healthcare, while Business Associates (BA) are entities that have access to PHI and provides a supporting role to a CE. Examples of CEs can include hospitals, clinics, medical groups, healthcare professionals and consultants. Examples of BAs can include a 3rd party billing company, a cloud storage company, a patient record keeping company or even a cloud communications company.

When a cloud provider uses 3rd party technology (such as BroadSoft), service *outage times will increase* due to the inherent communications and procedural latencies between companies.

Both CEs and BAs must be HIPAA compliant with all HIPAA security and privacy guidelines, rules and regulations when dealing with PHI content. Additionally, a BA entity must maintain HIPAA compliance (thru a downstream Business Associate Agreement) with any subcontractors or outsourced entities that have contact with PHI content.

HITECH Omnibus, or the Health Information Technology for Economic and Clinical Health, was passed into law in 2009 to promote the adoption and meaningful use of health information technology and, specifically, electronic health records (EHR). HITECH stipulates specific HIPAA security and privacy rules and penalties that BAs must comply with and works in conjunction with HIPAA to ensure the privacy and security of PHI within CE and BA entities.

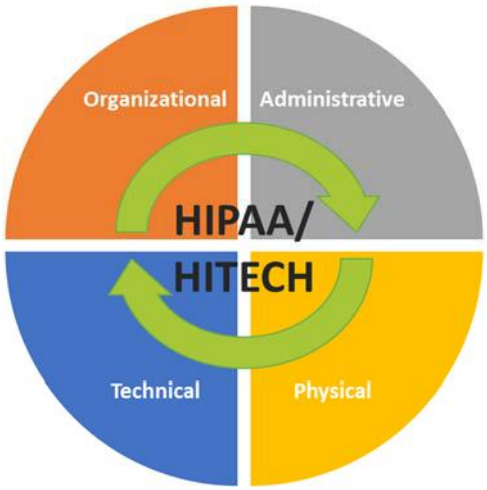
HIPAA/HITECH and Cloud Service Providers

Cloud service providers may be a Business Associate (BA) if they handle electronic PHI (ePHI). As such, the cloud provider would be subject to all the rules, regulations and guidelines of a BAA under the HIPAA and HITECH acts. Furthermore, and subcontractor or other downstream entity that the cloud provider engages that has access to ePHI would also be a BA and be subject to a downstream BAA between them and the cloud service provider.

Cloud service providers must meet and maintain stringent security and privacy standards in order to be HIPAA/HITECH compliant. However, that's only part of an end-to-end HIPAA/HITECH compliant cloud solution.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Examples of ePHI content can include patient records, scanned patient medical images, emails, voicemails, faxes and even phone call recordings. Indeed, HIPAA and HITECH place stringent security and privacy rules and guidelines on cloud service providers that many fail to meet. These rules cover four areas including administrative, physical, technical and organizational.



Let's take a look at each area:

Administrative – BAs must implement security management processes and procedures to prevent, detect, contain and correct security violations of ePHI data. They must have an identified security officer and must have ePHI access management procedures in place. BAs must also have ongoing security awareness training, incident and contingency plans and periodic security evaluation.

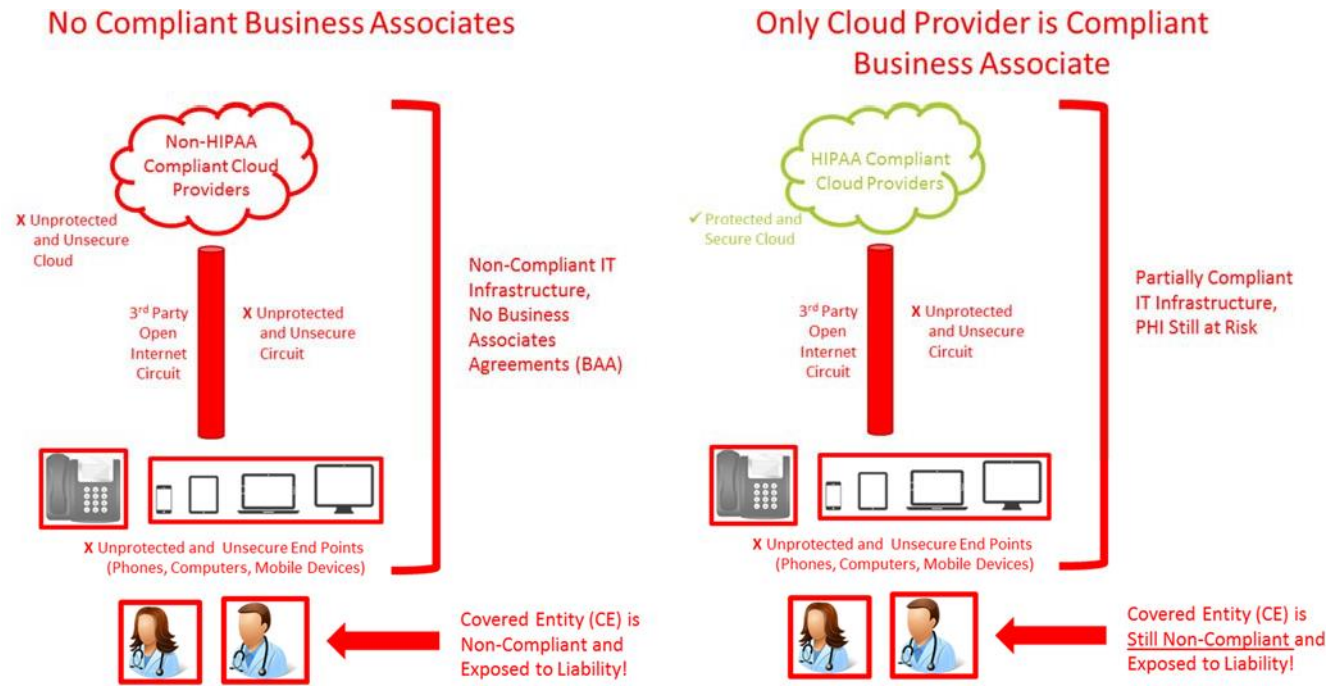
Physical – BAs must implement physical access control to all data centers housing ePHI data as well as any end point devices (workstations, mobile devices, IP phones) that access any ePHI data.

Technical – BAs must implement access control mechanisms to control access to ePHI data. User authentication, access logging and auditing of ePHI data access is also required. Finally, transmission security for any ePHI data transmitted to and from the cloud must be provided.

Organizational – BAs must implement any additional procedures and policies to ensure compliance with all HIPAA security rules. All security documentation should be in written/electronic form.

Cloud providers must not only implement the necessary HIPAA/HITECH rule and regulations themselves, but they must get any sub-contractors or third-party providers that will have access to ePHI data to also follow HIPAA/HITECH rules governing BAs. The cloud provider must have signed BAAs from each sub-contractor/3rd party in order to be compliant themselves. They will be required to sign a BAA with the CE guaranteeing compliance.

HOWEVER, obtaining a BAA from the cloud provider does not completely cover the CE, as some cloud providers would lead you to believe! From the CE's point of view, all components in the chain must be compliant in order to be fully compliant with HIPAA/HITECH. The cloud provider is one component (albeit a large component) in the chain. The access point and connectivity to the data center represents the other components that are involved in the end-to-end cloud solution.



All three components, the cloud service provider (and data center), the connectivity circuit and the end point devices (where ePHI is accessed) must be HIPAA/HITECH compliant in order for the CE to be fully compliant and secure. If for example, the end point device is not authenticated, then ePHI data accessed from that end point may be compromised. This violates the physical security rules of HIPAA. Most communications cloud service providers do not authenticate end point devices. In addition, many cloud service providers do not provide connectivity bandwidth, thus forcing the CE to acquire bandwidth from a 3rd party. The CE would then have to get a BAA from that downstream 3rd party provider as well.

If you are using or contemplating on using a cloud service provider and have ePHI data, make sure to ask your cloud provider the following questions:

- Is the cloud service provider HIPAA and HITECH Omnibus compliant?
- Is the cloud service provider willing to sign a BA Agreement?
- Does the cloud service provider have downstream BAAs with all sub-contractors that have access to ePHI data?
- Does the cloud service provider deliver an end-to-end solution for HIPAA compliance, including not just your cloud service, but connectivity and end point device authentication security?

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

PanTerra HIPAA Compliance – An End-to-End Solution

Delivering a HIPAA/HITECH compliant solution requires significant commitment and diligence from a cloud service provider. PanTerra is 100% committed to delivering an end-to-end HIPAA/HITECH compliant solution that not only covers the cloud service, but the end devices and connectivity components as well. This end-to-end single vendor secure solution is unique in the industry.

Enhanced HIPAA Level Security Features

HIPAA/HITECH security for cloud services is critical and cloud service providers can either follow the industry or lead it. PanTerra leads by being both technology and service provider. Utilizing the most advanced cloud security technologies available, PanTerra integrates enhanced security into their unified cloud services to protect and secure ePHI content and communications across the enterprise. Interoperability features with existing security systems and environments also means that you can be confident PanTerra's services will fit into your existing security environment.

PanTerra's HIPAA/HITECH security enhancements include:

- ✓ **Multi-Factor Authentication (MFA) on ALL devices** - Includes desktops, mobile devices and IP Phones. This meets HIPAA's workstation authentication requirement and virtually eliminates VoIP phone hacking, which can compromise ePHI security and cost companies thousands of dollars! Additional MFA administrative tools are also provided including IP range white and black listing and administration MFA request approval.

- ✓ **Single Sign On (SSO) authentication** - Allows single secure sign on to PanTerra services through industry standard SAML 2.0 providers including active directory, OneLogin and Okta.
- ✓ **Full encryption in-transit and at-rest** - All content and communications transmitted from PanTerra's data centers to customer locations is fully encrypted both in-transit (default RC4-128 encryption) and at-rest (256-bit AES encryption) within the data centers.
- ✓ **Downstream BAA compliance** - PanTerra supports full HIPAA compliance for all communications and content and has obtained BAAs with downstream sub-contractors and 3rd

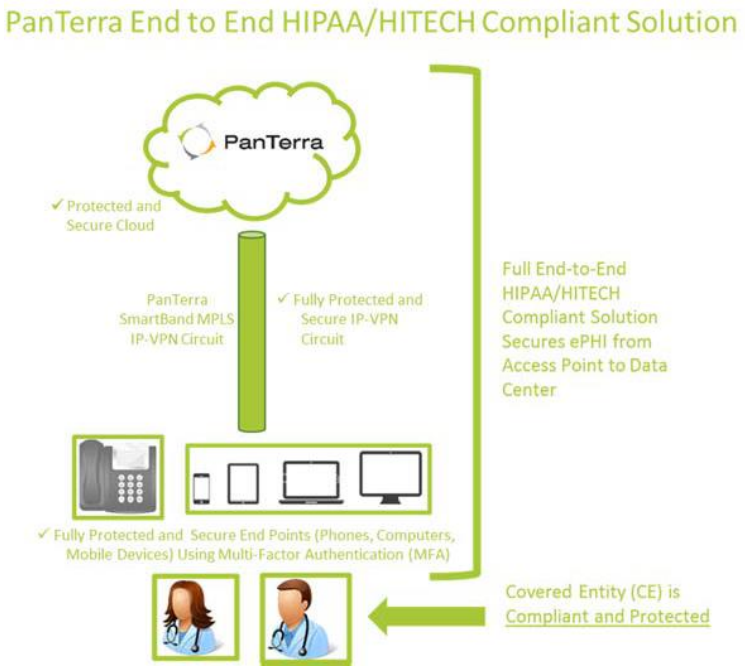
PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

party vendors.

- ✓ **SmartBand MPLS** - PanTerra offers its own managed IP-VPN secure, meshed MPLS network for maximum security and QoS. PanTerra's SmartBand MPLS is the most pervasive, cost effective way to ensure secure access to all enterprise locations as well as PanTerra cloud services.
- ✓ **Multiple Active Device Manager (MADM)** - Allows any user or admin to remotely lock out any device that might be stolen or lost.
- ✓ **Re-assign owner** - Allows admins to instantly re-assign SmartBox content to another user. This is useful when an employee is terminated.
- ✓ **Ultra-secure data centers** - Employing latest HIPAA compliant physical and cyber security technology, PanTerra's data centers are hardened to attacks including DOS, DDOS, unauthorized access, and viruses. Data center operations are constantly scanning and monitoring for cyber-attacks and continuously monitoring for new viruses and patching any at-risk software.
- ✓ **Security commitment** – PanTerra is 100% committed to security and has identified security personnel (security officer) to administer, manage, review and train PanTerra employees on an ongoing basis.

SmartBand MPLS – Secure Connectivity for an End-to-End Compliant HIPAA Solution

Securing the cloud data center is only part of a complete end-to-end HIPAA/HITECH compliant solution for the CE. CEs need to have a secure method for transmitting ePHI data from their locations to the cloud provider's data center. PanTerra performs application level encryption during transmission by default; however, application level security may not be sufficient for the CE. PanTerra offers, SmartBand MPLS, in these instances. SmartBand MPLS is a secure IP-VPN connection between the CE's locations and PanTerra's data centers to fully secure and protect ePHI data during transmission.



PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

With SmartBand MPLS and end device authentication, CEs can have the peace of mind that they have a full end-to-end HIPAA/HITECH compliant solution, fully owned and maintained by PanTerra.

Written BA Agreements

For those enterprises that require HIPAA/HITECH compliance, PanTerra has an end-to-end solution and will enter into a written BA Agreement (BAA) with the enterprise (CE). In addition, PanTerra has secured all necessary BAAs from any downstream sub-contractors or 3rd party vendors that may have access to ePHI data.

PanTerra Answers to the HIPAA/HITECH Questions

- ✓ **Is PanTerra HIPAA and HITECH Omnibus compliant?**

  Yes, PanTerra is HIPAA/HITECH Omnibus compliant with extensive security and privacy features that ensure your ePHI data is secure. PanTerra data centers implement the most stringent physical security measures and access controls while its unified cloud services implement extensive authentication, access control, logging and auditing features. Administrative and organizational policies and procedures along with responsible security personnel ensure that security is monitored, contingency plans reviewed, and all personnel receive training and are evaluated.

- ✓ **Does PanTerra have BA Agreements with all sub-contractors that have access to ePHI data?**

  Yes, PanTerra has written BA Agreements (BAA) with all relevant sub-contractors and 3rd party providers that have access to ePHI data.

- ✓ **Is PanTerra willing to sign a BA Agreement with the Covered Entity?**

  Yes, PanTerra will work with and sign a BA Agreement with the CE.

When a HIPAA compliant cloud provider doesn't offer secure broadband connectivity or authentication of end point devices, they are NOT delivering an end-to-end HIPAA compliant solution for the Covered Entity (CE).

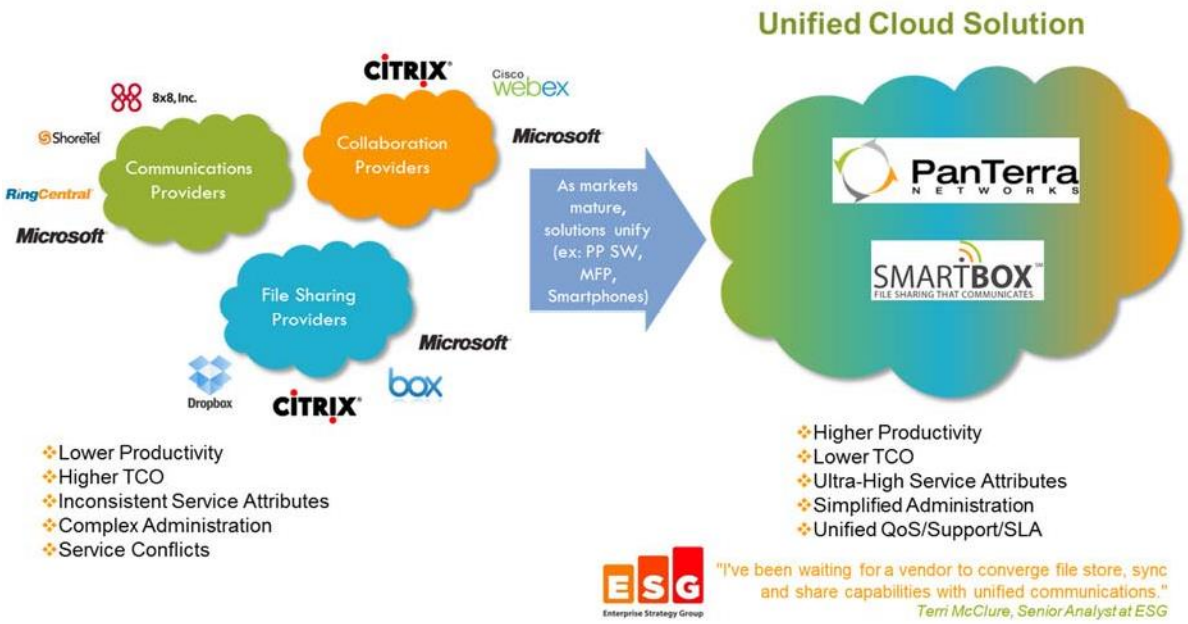
PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

- ✓ **Does PanTerra deliver an end-to-end secure solution for HIPAA compliance, including not just your cloud service, but connectivity and end point device authentication security?**

Yes, PanTerra is unique in the industry in offering fully secure IP-VPN connectivity and Multi- Factor Authentication (MFA) to fully secure end point devices in combination with their HIPAA/HITECH compliant unified cloud services, creating a completely HIPAA/HITECH compliant end-to-end solution for the CE. ***Only PanTerra can provide complete peace of mind for a CE moving their IT services to the cloud.***

Our Unique Unified Cloud Solution is *Unmatched in the Industry*

Today, enterprises are taking advantage of the benefits of a cloud solution as they migrate their IT services to the cloud. In fact, more and more enterprises are taking the next logical choice and moving multiple IT services to the cloud: communications, collaborations, file sync & share, and analytics are all services that benefit from a cloud implementation.



However, moving multiple IT services to the cloud can impose some new challenges and problems. Multiple administration portals, inter-service conflicts, inconsistent service attributes such as security and higher aggregate service costs are all real challenges that can result if multiple cloud service providers don't "play well together." And when they don't, resolving inter-service issues can be virtually impossible as the "finger pointing game" becomes a real scenario.

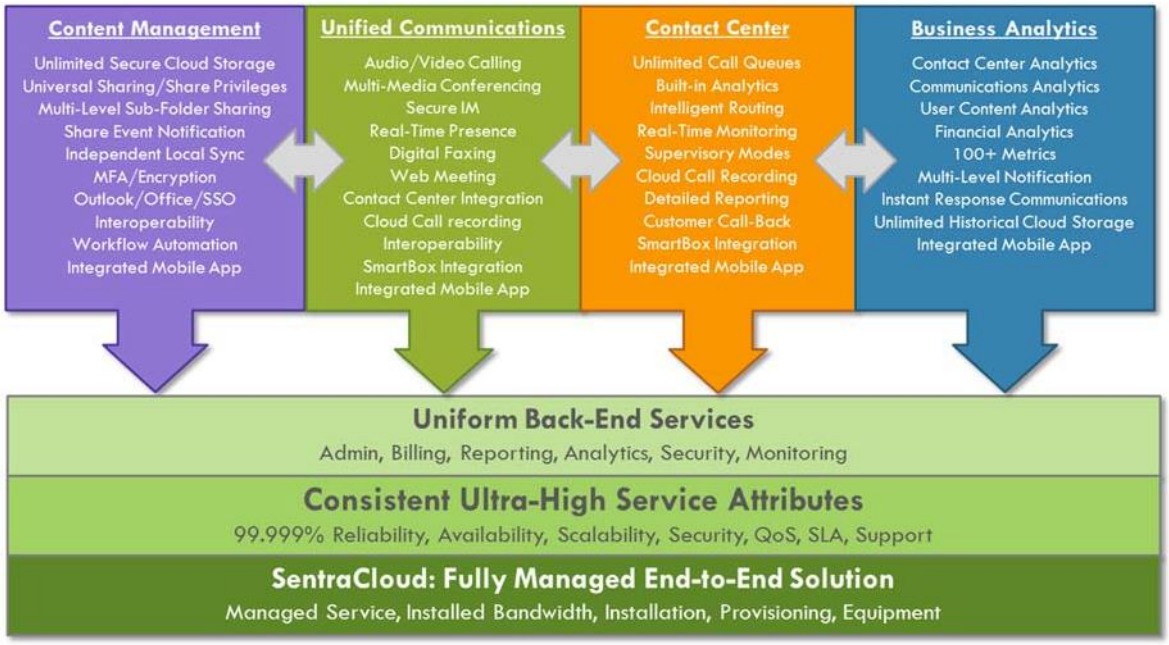
PanTerra's Unified Cloud Service Approach

PanTerra delivers a Unified Cloud Service solution that combines unified communications, collaborations, file sync & share and business analytics into a single fully customizable cloud solution. Enterprises can tailor each user within the company with the necessary features to match their role within the company. If their role changes, they can easily add or remove features instantly. Being 100% cloud deployed means that all services are consistently deployable anywhere in the world with the same service attributes.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Much like what Office did to personal productivity software, PanTerra's unified cloud solution does to the Cloud, delivering a unified experience, ease of use, higher productivity, lower cost and simplified management across multiple cloud services.

Without any dedicated on-premises hardware, PanTerra's service is FutureProof, essentially eliminating service obsolescence and making so called "rip and replace" strategies a thing of the past. As new technologies are made available to the industry, PanTerra can integrate them into the service and instantly deploy them to customers. The replacement of "heavy" client-side software programs, susceptible to virus injection and requiring complex version management, are replaced with browser-based clients that allow anywhere access to PanTerra services. Mobile apps provide an optimal interface for mobile devices, complementing desktop and IP phone access. Users can truly take their complete office environment with them including files, documents, calls, messages, and even web meetings.



Security is of paramount concern with cloud services and PanTerra adds significant security features above and beyond other cloud service providers. PanTerra data centers implement the most stringent physical as well as cyber security measures available to ensure security and continuous operations. PanTerra's enhanced security and privacy measures allow it to offer full HIPAA compliance. Along with its SmartBand MPLS offering, PanTerra offers the most secure end-to-end environment for those customers seeking HIPAA level security for their cloud services.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Hosted VoIP customers are susceptible to IP phone hacking which *can cost customers tens of thousands of dollars per attack.* PanTerra implements full Multi-Factor Authentication (MFA) on all mobile devices, desktops and IP phones, a first in the industry, virtually eliminating this type of attack.

PanTerra is the only provider to implement Multi-Factor Authentication on all desktops, mobile devices *and IP Phones*. With MFA, VoIP hackers cannot relay illegal VoIP minutes on your account by simply acquiring the IP phone credentials of one of your users. Indeed, VoIP phone hacking costs enterprises millions of dollars each year; but with PanTerra, VoIP phone hacking is virtually eliminated. In addition, PanTerra implements per user, per day, per country international charge limits so that in the event a hacker does gain access to a user's account, their potential cost damage is limited, much like how credit cards monitor and limit unusual transactions. PanTerra also implements full encryption in-transit and at-rest for content to ensure both security and privacy of cloud content. A Multiple Active Device Manager (MADM) feature monitors all active devices connected to the service and allows any user or administrator to lock out a device that might be stolen or lost. PanTerra's unified cloud service is the most secure end-to-end cloud solution in the market.

Back-end administration of PanTerra's unified cloud solution is also unified providing a single browser-based administration portal to manage all services. Common management tasks include user/team/group management, account level service management such as auto attendants, Call Center management, and advanced billing. Multi-select user capabilities make it easy to support larger enterprises and to make changes to a number of users quickly.

Advanced billing capabilities allow complete customization of billing statements and invoices to accommodate virtually any cost center structure a large enterprise might have. From a simple centralized single invoice structure to more complex per location invoicing or a hybrid of aggregate multiple location invoicing or multiple payment mode support, PanTerra's advanced billing capabilities provide ultimate flexibility to match an enterprise's existing cost structure. Separate multi-level billing statements and line-item cost splitting are also configurable.

SmartBand, PanTerra's own broadband solution, can be deployed as an open Internet connection or as a fully meshed, VPN secure, QoS enabled SmartBand MPLS connection. Both are fully deployed and managed by PanTerra.

As part of an end-to-end solution, PanTerra also optionally provides SmartBand circuits to connect customer locations to their cloud service. Customers can select from a broad range of speeds from T-1 to over 10 Gb/sec Ethernet over Copper (EoC). In addition, both Open Internet and MPLS connections are supported. SmartBand MPLS is available in over 85 markets to over 10 million business locations and

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

provides a fully meshed, VPN secure, multi-level QoS connection to PanTerra's cloud. SmartBand is the broadest connection offering available today.

Finally, PanTerra offers managed SmartBand connectivity, managed on-premises networking equipment and managed IP phones. With PanTerra, customers have a single point of ownership for their end-to-end cloud solution.

Access PanTerra's Unified Cloud Services Anywhere

A unified cloud solution can have a major impact on productivity for both IT staff and more importantly, every employee in the company. By significantly reducing or eliminating redundant or repetitive tasks that each employee has to perform on a daily basis to utilize the cloud services, a unified cloud solution allows more of each employee's time to be directed towards positively impacting revenue for the company. Take for example the amount of time a user wastes managing all the groups of contacts they use on a daily basis to collaborate with other employees or people outside of their company. Creating groups to do a web meeting or conference call or group IM. Adjusting groups when new people get involved. Now imagine doing that in 3 or 4 or 5 different cloud services: your file sharing service, then your web conferencing service, etc.… This wasted time adds up.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Company Size	Annual Revenue	Revenue/ Employee/Year	Avg Time Saved/Day by Eliminating Repetitive or Redundant Tasks	Potential $$ Increase in Annual Revenue	% Increase in Annual Revenue
100	$ 20M	$ 200,000	15 min	**$ 625,000**	**3.13%**
500	$ 200M	$ 400,000	20 min	**$ 8,333,333**	**4.17%**
1,000	$ 750M	$ 750,000	30 min	**$ 46,875,000**	**6.25%**

Impact Unified Cloud Services Solution has on Productivity and a Company's Revenue

Employees can waste an average of 15 to 30 minutes a day doing these kinds of redundant tasks instead of spending it on driving sales. The above table shows the positive impact on a company's revenue stream a unified cloud services solution can have. Conversely, implementing separate cloud services can decrease productivity and negatively impact sales and revenue.

PanTerra's unified cloud services solution includes:

Streams delivers leading edge unified communications capabilities to an enterprise maximizing productivity, eliminating upfront capital expenses and costly "rip & replace" obsolescence strategies, reducing on-going operating expenses, and simplifying administration and management.

Key Streams features include:

- ✓ Unlimited audio/video calling
- ✓ Intelligent follow-me/find-me call routing including call blasting and sequential routing
- ✓ Secure IM with real-time integrated presence
- ✓ Unlimited audio/video conferencing
- ✓ Unlimited deskshare and web meeting
- ✓ Cloud call recording
- ✓ Full contact management including Google, Yahoo, Outlook importing
- ✓ BLA/BLF, call parking, supervisory modes
- ✓ Digital Faxing
- ✓ Outlook, Salesforce, Office 365 plugins
- ✓ Unlimited ring groups, auto attendants
- ✓ Fully integrated with Streams Call Center
- ✓ Fully integrated with SmartBox file sync & share (communications content stored in SmartBox)
- ✓ Mobile app support

Streams Call Center delivers enterprise level Call Center capabilities significantly improving the customer experience while providing enhanced resource flexibility and supervisory monitoring and reporting tools. With built-in real-time analytics, enterprises can fine tune their businesses, maximizing customer satisfaction and top line revenue while optimizing agent resources and infrastructure costs.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Key Streams Call Center features include:

- ✓ Unlimited queues and minutes
- ✓ Built-in analytics with over 100+ customizable performance SLA/KPI metrics
- ✓ Intelligent routing including skills-based, round-robin, next available, longest idle and random
- ✓ Real-time live monitoring of all agents
- ✓ Supervisory modes including silent listen, whisper and barge-in
- ✓ Call-Back When First in Queue and Pull Caller Out of Queue
- ✓ Cloud call recording
- ✓ Real-time and scheduled detailed reporting
- ✓ Fully integrated with Streams PBX
- ✓ Fully integrated with SmartBox file sync & share
- ✓ Mobile app support

SmartBox is an enterprise File Sync & Share solution with built-in communications and collaboration features that allow users to maximize engagement with customers by sharing, communicating, and collaborating all in a single solution.

Key SmartBox features include:

- ✓ Unlimited secure cloud storage
- ✓ Multiple share privileges (viewer, editor, co-owner, owner)
- ✓ Share any file/folder at any level
- ✓ Communications content stored in same cloud (Voicemail, faxes, recordings, attachments)
- ✓ Unlimited independent local sync clients
- ✓ Unlimited file versioning and file locking
- ✓ Share event notifications
- ✓ Password protection and temporary sharing
- ✓ Trash bin and undelete
- ✓ Fully integrated Streams communications features
- ✓ Fully integrated contact management
- ✓ Mobile app support

Unified Business Analytics allows businesses to fine tune their businesses in real-time with over 100+ customizable SLA/KPI performance metrics. Provides a common analytics framework for communications, content and financial analytics.

Key Unified Business Analytics features include:

- ✓ 100+ customizable SLA/KPI performance metrics
- ✓ Real-time live analytics monitoring
- ✓ Ad hoc and scheduled analytics reports
- ✓ Multi-level, multi-user supervisory notifications
- ✓ Monitor analytics for any user within the account (not just Call Center agents)
- ✓ Instant corrective action capabilities thru unified communications features
- ✓ Fully integrated with Streams, Streams Call Center and SmartBox file sync & share
- ✓ Mobile app support

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

Our Cloud Infrastructure *Guarantees Ultra-High Service Attributes*

PanTerra's unified cloud solution is a 100% cloud solution delivered from a network of secure, hardened cloud data centers. These data centers provide multiple layers of both physical and cyber security to protect customer content and ensure reliable non-stop operation of the service. Redundant components at virtually every level ensure that no single point of failure, including a massive data center failure, can cause a service outage. This is critical when businesses consider migration to the cloud.

However, hardware redundancy is not the only important factor to consider when looking at a cloud service provider. In fact, there are seven key cloud attributes that are critical for any cloud service provider. The seven key attributes include:

1. **Reliability** – Reliability is the measurement of how often a service "fails." The inverse of this is Mean Time Between Failure (MTBF) which is the average uptime between failures of the service. The higher the MTBF the more reliable the service can be and the less likely the service will fail. With cloud services, there are many components to delivering the service including the local LAN and networking equipment, the last mile circuit, the backbone carrier and the data center with all its various components. Each one of these components has an MTBF and reliability number. Taken together, the reliability of the whole system can be less than the reliability of the least reliable component.

   PanTerra's unique ultra-reliable architecture and fully owned approach to its cloud service means that it can guarantee a minimum of 99.999% reliability for its service. With extensive expertise in building reliable business-class cloud networks, PanTerra has architected its cloud service to be ultra-reliable, maximizing MTBF for all components in the service and thus maximizing reliability, virtually eliminating service outages. When combined with our ultra-high level of availability (ability to recover from an outage instantly), business continuity for all its cloud services is maintained 24/7.

Software related outages, last-mile broadband circuits and on-premise disasters (power outages, non-redundant equipment failures, etc.) contribute more to cloud service outages than hardware failures at a cloud data center.

2. **Availability** – Availability goes hand in hand with reliability in determining how available the service is or conversely how long a service is unavailable. Availability is the inverse of how long a service is unavailable (outage time) when it does fail. Taken together with Reliability, these terms determine how often and how long a service will be "down" and unavailable which means your employees are "down" and non-productive. Both terms are important. You can have a service that is reliable (doesn't fail often), but has a low availability indicating that when the service does fail, it is "down" for long periods of time. Conversely you can have a service that recovers faster from an outage (higher availability) but has a lower reliability, i.e. it fails more often. In both cases, company impact and employee productivity can be significantly impacted.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

PanTerra has the highest level of availability (and reliability) in the industry and has historical metrics to prove it. Over the past 4 years, PanTerra has delivered a proven track record of over 99.999% availability for its services with no full-service outage lasting longer than a few minutes. This is not only due to its state-of-the-art hardware and software redundancy architecture, but also to its 24/7 operations monitoring team, QoS managed circuits, certified networking and end-point equipment and its business-based cloud DNA expertise and experience. PanTerra has more experience and expertise in delivering enterprise-class unified cloud services than any other vendor in the industry.

3. **Scalability** – One of the biggest advantages of cloud is the ability to scale service globally through the theoretical addition of new data centers. While this may sound easy, adding data centers and interconnecting them in such a way that service can be consistently accessible is not easy. Some cloud service providers that depend on 3rd party technology vendors to provide the service are challenged to deploy and maintain the same version of that technology across all data centers or be faced with inconsistent features or operations between each data center. This can be very counter-productive to a company that depends on service consistency.

PanTerra is both service provider and technology provider. PanTerra doesn't rely or depend on any 3rd party technology provider so it is better able to deliver globally consistent scalable services around the world. In addition, PanTerra's N+1 per service scaling architecture means that it can increase scale on any service, both within a particular data center or by adding additional data centers, ensuring optimal cost-effective scaling for each service.

4. **Security** – Cloud security has been a much talked about topic for many years. Extending the IT infrastructure outside of the physical confines of a corporate building can pose security challenges both physically as well as in cyberspace. Over the past couple of years, however, business cloud service providers have made tremendous progress in securing the cloud environment for enterprises to confidently migrate to the cloud. Key to ensuring a secure cloud service environment is working with a service provider that can provide end-to-end security from endpoints (IP phones, desktops and mobile devices) to secure broadband connections and secure cloud services themselves.

PanTerra delivers complete end-to-end enhanced security and privacy features that keep business communications and content maximally secure. With advanced features such as multi-factor authentication (MFA) on all endpoints (including IP phones), secure MPLS broadband connectivity, full encryption in-transit and at-rest for all user and communications content, mobile device remote management and multi-level administration, PanTerra's unified cloud services provides a robust and secure cloud environment for your enterprise.

5. **Quality of Service (QoS)** – Quality of Service is one of the most important cloud service attributes as it can negatively impact productivity for every employee in the company and it can occur instantaneously at any time without warning. Additionally, QoS may be impacted by external factors; more so in certain cloud service providers than others. As more IT services are moved to the cloud, inter-service QoS issues will also become a more frequent occurrence challenging even the best cloud service provider to be able to resolve. 3rd party circuits, networking equipment, data center bandwidth and scalable software architectures all play a role in determining QoS.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

PanTerra delivers the highest level of QoS by ensuring that every component in the solution has QoS and is monitored for QoS. PanTerra is the only cloud service provider to offer a fully owned approach with guaranteed QoS over open Internet and MPLS connectivity. In addition, PanTerra's unique multi-service management ensures QoS between PanTerra's cloud services; so real-time voice services always maintain highest priority. Only PanTerra can offer this inter-service QoS guarantee.

Quality of Service (QoS) depends on many factors including cloud service architecture, broadband bandwidth, transport control and on-premise network implementation. PanTerra delivers complete end-to-end QoS management through QoS managed cloud services, SmartBand MPLS circuits and on-premise managed networking equipment.

6. **Service Level Agreement (SLA)** – The SLA represents the actual legal "meat" behind all of the service attributes. It is how the cloud service provider stands behind their service and exactly what guaranteed service levels it will deliver the service at. The SLA should be reviewed for level and completeness in covering all seven service attributes listed here.

   PanTerra's SLA is the highest in the industry, guaranteeing availability, QoS and support levels to ensure your IT services are delivered at continuous peak performance and continuity. PanTerra has a historically proven track record in delivering enterprise-level cloud services to meet your enterprise's demanding needs.

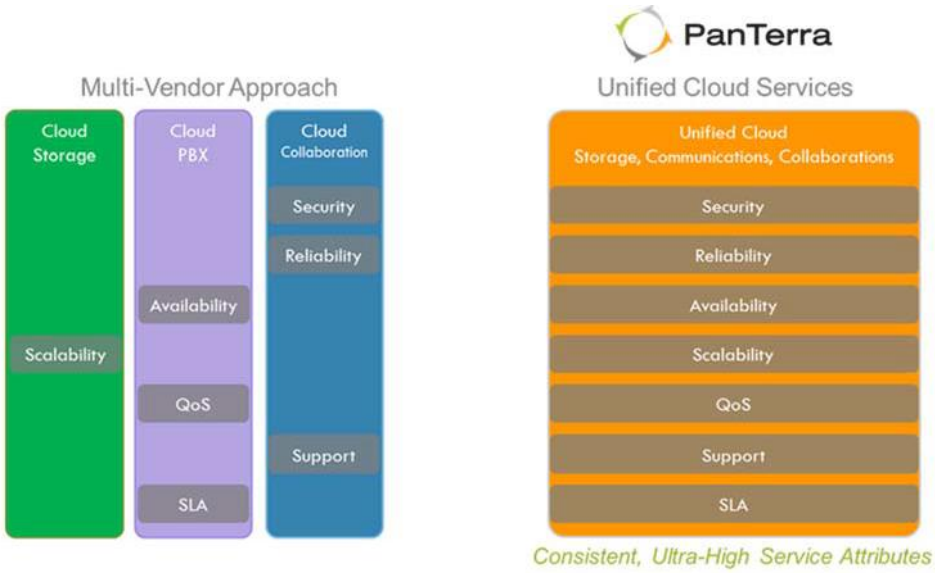
7. **Support** – Support is key when outsourcing your business-critical IT services to a cloud service provider. When an issue arises, getting fast and accurate support can have a major impact on your bottom line. Understanding the support escalation process is critical to resolving issues in a timely manner.

   PanTerra delivers the most comprehensive and responsive support in the industry. With multi-media access to support including a 30 second live IM support option, PanTerra guarantees a response to a customer issue within 30 seconds! And PanTerra's "100% ownership" philosophy guarantees that you will not be "passed" to another vendor even if the problem is with a 3rd party vendor. PanTerra will be involved until the issue is completely resolved.

Considering these seven service attributes for a single cloud service is challenging enough, but when considering migration of several IT services to the cloud, these seven key service attributes can be virtually impossible to manage and maintain if each cloud service is provided from different cloud providers. Imagine migrating your PBX to one cloud provider, your collaboration to another provider and your file sync and share to another service provider. Each cloud service provider will have different or varying levels of each of these seven service attributes. Even more troubling is that one cloud vendor's solution may negatively impact a service attribute from another cloud service provider. For example, unloading gigabytes of files to the file sharing cloud might cause QoS issues with your voice or video calls

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

if they happen at the same time. These kinds of inter-service QoS are virtually impossible to debug and resolve when multiple providers are involved.



PanTerra's Ultra-High Service Attributes are Consistently Delivered Across All Services

With PanTerra's unified cloud services solution, all cloud services are delivered from a single secure cloud. This ensures consistent cloud service attributes across all services.

Moving multiple IT services to multiple separate cloud service providers can have disastrous results due to inter-service resource conflict. Imagine trying to run a web meeting from one service while another service tries to sync 100 GB of content to local desktops.

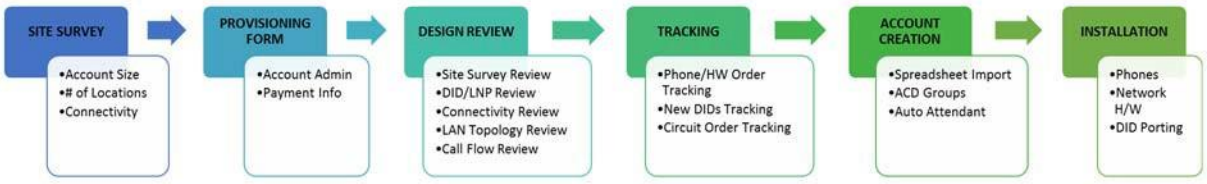
In addition, inter-service QoS impact is eliminated since PanTerra controls and manages all the services in parallel, prioritizing real-time critical services over non-real-time services. Finally, PanTerra's unified cloud services approach significantly reduces ongoing operating costs since there is only a single ultra-reliable cloud infrastructure as opposed to the costs associated with multiple separate clouds infrastructures.

Our "Hands-On" On-Boarding Process *Doesn't Leave You in the Dark*

Selecting a cloud service provider should not just be about the features and service itself. There are many more factors to consider when selecting a cloud provider. One of the most important and often overlooked critical areas is the on-boarding process that the service provider uses both for the initial deployment as well as new incremental deployments which most likely will occur over the course of time. New locations need to be provisioned, an existing location may move to a new location or some existing locations may require changes.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

It is critical to engage a cloud service provider that is going to truly be hands-on during the on-boarding process. Communications within a large organization are complex and require careful planning and review to match end user and corporate requirements to the networking environment. Auto attendant setups, ring groups, analytics, Call Center agent configurations, and call routing plans are just some of the configurations that go into setting up cloud communications.



PanTerra's "Hands-On" Design Review Methodology Maximizes Successful Cloud Migration

PanTerra takes a complete "hands-on" approach to the on-boarding process, providing all the necessary human resources to make the migration to the cloud as easy and painless as possible. A multi-step design review methodology is employed involving the customer, PanTerra and optionally the 3rd party IT vendor. Current networking environments and equipment are reviewed for acceptable compliance, telephone numbers are mapped out, circuits are optionally ordered and tracked, LNP porting is ordered, auto attendants and ring groups are created and if necessary, new networking equipment and/or IP phones are ordered.

PanTerra on-boarding is an "all hands-on deck" philosophy versus "here, you do it and here's our web knowledge-base if you have problems."

During each and every step, PanTerra manages, coordinates and tracks the on-boarding process to make sure everything goes smoothly during the migration. And if a new location is added or an existing location needs to be moved, PanTerra resources are available to make that transition as smooth as possible as well.

Our 24/7 Customer Satisfaction Commitment is to *"Go the Extra Mile"*

Enterprises depend on their IT services 24 x 7. They are mission-critical to the enterprise and when there is an issue, getting resolution as quickly as possible is paramount. There are four key aspects to determining customer satisfaction with a cloud service:

- ✓ **Customer Support Access/Availability** – How accessible and available is the provider's customer support? Are there multiple ways to contact support? Is there live phone support 24 x 7?
- ✓ **Ownership** – Does the cloud provider take ownership of all issues or do they forward issues to 3rd party vendors?
- ✓ **Resolution Time** – Does the cloud provider own the technology so they can affect resolution

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

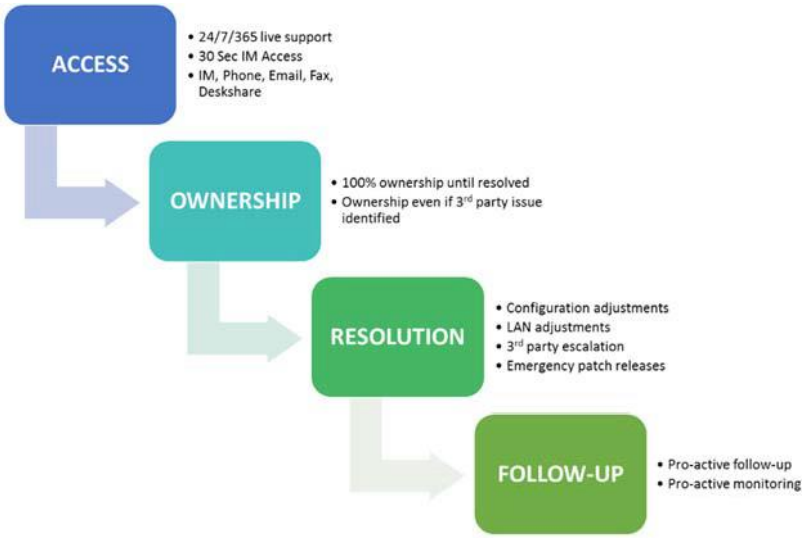
faster? Do they have a formal escalation process?

- ✓ **Follow-Up** – Does the cloud provider follow-up in a timely manner? Is there pro-active follow-up?

PanTerra is dedicated to 100% customer satisfaction and delivers on each and every one of the key aspects above, going the extra mile for our customers.

Often, time-to-resolution is more about minimizing the number of vendors involved and maximizing single vendor ownership. PanTerra takes 100% ownership of all support issues, regardless of the source.

With live 24 x 7 customer support to instant 30 second response time for IM support, businesses get immediate access to the support they need when an issue arises. And PanTerra takes 100% ownership of the issue, regardless of whether the issue is with PanTerra, a broadband carrier, some 3rd party networking equipment or any other remote entity. PanTerra will never push a customer off. Being both the service and technology provider also allows PanTerra to resolve service issues in a more expedient manner since support personnel have direct access to the engineering developers.



PanTerra Takes Ownership of All Issues from Start to Finish

With PanTerra customer satisfaction starts the minute you become a customer and never stops being our number one priority.

We are 100% Committed to *Your Enterprise's Success*

In today's competitive fast-moving business world, you need a cloud partner that is 100% focused on your enterprise's success. With our mission-critical business DNA, PanTerra delivers that 100% focus with a proven holistic approach that includes not just the cloud service itself but all the necessary pieces of the

solution to guarantee peace of mind that your IT services will deliver leading edge features with ultra-reliable and secure operations, backed by world-class enterprise level support.

Select the Ultra-Secure Unified Business Cloud from PanTerra

Migrating to the cloud has incredible benefits and PanTerra can get your enterprise into the cloud faster, more reliably and secure than anyone else on the planet. Contact PanTerra (800.805.0558) directly or a PanTerra partner today and get a free live demo and see how your enterprise can immediately benefit from PanTerra's Unified Cloud Services.

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054
Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763
www.panterranetworks.com | info@panterranetworks.com

PANTERRA UNIFIED CLOUD SERVICES

Streams – Unified Communications

Streams increases business productivity, customer satisfaction and ultimately improves top line revenue while dramatically reducing infrastructure expenses.

Comprehensive Unified Communications - unlimited business-class calling, powerful call routing, secure instant messaging and real-time presence

Professional Call Features - auto attendants, ring groups, BLA/BLF, music on hold, call recording, after hours and holiday routing, failover rules

Group Collaborations - includes audio/video conference, IM Conference, web meetings, desk sharing and file sharing

Unified Cloud Communications (UCC) Panel - the hub for all your communication interactions

Call Center Service - call queuing, call selection, call back recording, supervisor controls, statistics, and reporting

Mobile Device Support - includes Android and iOS mobile apps that bring all UCC desktop features to mobile devices

Streams - Call Center

Streams' integrated Call Center solution delivers more productive interaction with customers with advanced monitoring, reporting and analytics built-in.

Unlimited Minutes and Queues - unlimited minutes and Call Center queues per account with sophisticated overflow management

Intelligent Routing - routing based on agent skills, round robin, next available, idle time, random, least active or ring all agents

Supervisory Modes - silent listen, whisper or barge-in to any agent or user in the account

Cloud Call Recording - static, random or on-the-fly recording stored in the cloud

Real-Time Live Monitor - monitor any or all agents on Desktop, mobile device or wall monitor

Advanced Reporting - detail triggered, ad hoc or scheduled reports

Analytics Built-in - monitor and trigger on 100+ customizable SLA/KPI performance metrics

PBX Integration - fully integrated with PanTerra's Streams solution

SmartBox – File Sync & Share

SmartBox is the ultimate in secure file store, share and sync functionality with unified communications features built right in. Share a file and get instant notification when it's viewed, make a quick call or set up a web or video meeting or simply send a secure IM.

Unlimited Secure Cloud Storage - secure cloud storage with multi-factor authentication, single sign on support and full encryption in-transit and at-rest

Simple, Secure File Sync & Share - includes link and user sharing, sub-folder sharing, pwd protection, temporary sharing, file versioning, share notifications and multiple share privileges

Mobile Device Support - includes Android and iOS SmartBox apps

Communications Content in Same Cloud - see and share all your communications content (VMs, faxes, call recordings) just like any other file

Unified Communications and Collaboration Features Built-in - instant audio/video calls, IM, conduct conferences or conduct online web meetings with any number of people

Unified Business Analytics

Unified Business Analytics provides a common framework for tuning a business's performance in real-time based on over 100+ customizable SLA/KPI metrics.

100+ SLA/KPI Customizable Metrics - including queue lengths, talk times, missed calls, handled calls, idle time, etc.…

Instant Corrective Action - take instant corrective action through integrated communications when a specific KPI/SLAs are exceeded

Live Real-Time Analytics Monitoring - monitor users and queues in real-time and see when specific KPI/SLAs are exceeded

Advanced Reporting - detail triggered, ad hoc or scheduled reports delivered to multiple supervisors or viewable in browser

Analytics on Any User - monitor any user in the account, not just Call Center agents

Mobile Device Support - monitor analytics and receive detailed reports in real-time on any desktop or mobile device

Call Us for a Demo Today
800.805.0558

PanTerra Networks, Inc.
4655 Old Ironsides Drive, Suite 300
Santa Clara, CA 95054

Toll Free: +1 800.805.0558
Direct: +1 408.702.2200
Fax: +1 408.625.3763

www.panterranetworks.com | info@panterranetworks.com