windstream®
smart solutions. personalized service.

Security and the Cloud: What You Need to Know

Cloud computing, in the form of Infrastructure as a Service (IaaS), provides a wide variety of benefits, including improved economics, higher efficiency and greater agility. Yet concerns involving security have prevented some organizations from moving ahead with cloud adoption. While security is an essential consideration for every IT environment, it is important to understand that cloud environments — both public and private — offer appropriate levels of security for a breadth of applications.

In order to gain comfort with cloud security it is helpful to understand that Cloud Service Providers (CSPs) and cloud customers both have a role to play.

CSPs — generally handle physical data center security and are also involved in network and data security.

Cloud Customers — typically manage their own user access, passwords and encryption keys, often by taking advantage of services offered by the cloud provider.

Security and the Cloud Service Provider

Let's take a closer look at some of the security capabilities often delivered by CSPs:

- **Physical Security** – CSPs are responsible for maintaining onsite security, which often includes staffed security checkpoints, electronic and/or biometric access mechanisms and emergency procedures for events such as fires or tornados. Supporting multiple customers within a single data center makes protecting their assets from physical damage or intrusion a top priority.
- **Network Security** – CSPs are also responsible for maintaining a secure network environment for data and other traffic. They provide perimeter firewalls, intrusion detection systems, network monitoring and Denial of Service (DoS) protection — all to ensure the highest degree of network defense.
- **Data Privacy** – Privacy is also a top concern for CSPs and their customers. Multi-factor authentication techniques — where multiple forms of credentials are required, such as login name, password and a code received on a separate device — are used to help prevent unauthorized access to resources. CSPs may also offer support for encryption of data and secure channels for data transfer and data backup.

It is important to understand that cloud environments — both public and private — offer appropriate levels of security for a breadth of applications.

windstream®
smart solutions. personalized service.

IP Security and the Cloud Customer

Cloud users also have a significant role to play in cloud security. In order to ensure security within cloud environments, they must follow similar security practices as they do with systems and applications hosted in their own on-premises data centers. For example, they must follow basic security protocols such as establishing strong passwords and updating them periodically. They should also take advantage of the security options offered by the CSP, including application-specific firewall settings.

Shared Responsibility

Together, CSPs and their customers provide the necessary security for applications and data. At the same time, some CSPs make security easier and more flexible than others. Providers such as Windstream can offer hosted private clouds, which allow customers to take more control over security configurations in order to meet specialized requirements or regulations.

> Make sure to choose a provider that delivers reliable security within the core IT environment and one that provides compatibility with your security requirements.

They also provide hybrid clouds, which combine the greater security control of a private cloud with the economic benefits of a public cloud, allowing customers to utilize scale-out environments and applications without worrying that their data will be compromised.

Managed Services can also be an added benefit, allowing service providers to take on some of the security responsibilities that have previously been handled on the customer's end, such as data encryption, firewall protection and intrusion detection. Service providers rigorously test their own security measures to make sure their environments are safe, which can further reduce the costs of establishing and maintaining security onsite.

Choosing a Cloud Service Provider

To choose the right CSP you must first look at what security options are available to you as a customer. Make sure to choose a provider that delivers reliable security within the core IT environment and one that provides compatibility with your security requirements. Providers should also allow you to manage elements of your own security and customize your service to meet your unique security needs. This is important for meeting regulatory compliance and security requirements that may be specific to your field or industry.

At the same time, consider a service provider that offers Managed Security Services to further improve security effectiveness. It is also important to understand what infrastructure components your service provider implements. Each type of device — from servers and storage, to routers and switches — carries its own device-specific security capabilities, and enterprise-class devices often further enhance your overall security.

Handling private data or running secure applications in the cloud may seem risky at first. However, it is possible to establish the right level of security for a broad array of applications. Be sure to look for a trusted advisor who understands the shared responsibilities of cloud security and enables users to achieve their desired level of security. Then choose a provider, such as Windstream, that delivers secure core services built on enterprise-class IT infrastructure and that also provides Managed Services to further enhance your security.

PUBLIC CLOUD SECURITY

WINDSTREAM HOSTED SOLUTIONS

Cloud computing presents a number of unique benefits as compared to traditional or virtualized IT environments. Cloud computing shifts capital expenses (CAPEX) to operational expenses (OPEX) and introduces a new level of speed, flexibility and scale to the IT organization. These benefits help overcome challenges faced by IT organizations, including rapidly changing technology, budget constraints and time-to-market pressures. While cloud services can yield a number of advantages, this new model for computing also raises a few new questions.

As more businesses migrate IT services to the cloud, security is becoming a significant consideration for choosing a Cloud Service Provider (CSP). Businesses want cloud security that is comparable to what they receive from their own in-house IT services. They also demand cloud security that accounts for the complexities of virtualized, multi-tenant data center environments. Without these capabilities, businesses may not be able to take advantage of cloud computing and its associated benefits.

Customers need a trusted provider such as Windstream Hosted Solutions that can provide the security they need while delivering the scale, flexibility and speed that is unique to cloud computing. Yet, before deploying their applications to a cloud environment, customers want to understand public cloud security and gain assurance that their security demands are being met. This document responds to such security concerns and outlines how Windstream Hosted Solutions maintains a high level of security within its cloud solutions.

windstream®
smart solutions. personalized service.

OVERVIEW

In order to provide the greatest flexibility and choice, Windstream offers its customers several different cloud solutions:

- **Private Cloud** — Dedicated physical equipment is used to deliver Private Cloud infrastructure, including firewalls, switches, servers and storage. The resources within each Private Cloud are accessible only to a single customer organization and reside securely within Windstream Data Centers. Customers may manage their private cloud directly or engage Windstream to manage it on their behalf. Security can be designed and customized to meet the unique requirements of each customer.
- **Public Cloud** — A secure multi-tenant infrastructure, used by a variety of customers at the same time, is the basis for Windstream's Public Cloud offering. Customers get their own Virtual Machines (VM), which securely isolate applications and data from other tenants. Public Cloud users do not have access to, and cannot manage or control the underlying physical infrastructure. Customers may only access their own guest operating systems – including applications running there – and the virtual storage attached to their VMs. Windstream Public Cloud environments physically reside within secure Windstream Data Centers.
- **Hybrid Cloud** — The Windstream Hybrid Cloud offering provides secure, direct, low-latency network connectivity between the Windstream Public Cloud and a customer's colocation servers, and/or dedicated Windstream infrastructure – including network, server and/or storage – residing within the same Windstream Data Center or offsite at a customer premises or third-party facility utilizing private line connectivity such as MPLS. The public and private infrastructures remain unique entities but support data and application portability. The Windstream Hybrid Cloud solution allows customers to leverage the flexibility and cost savings of a public cloud, while allowing for the customizable security offered by a dedicated physical infrastructure.

Customers who have specialized security requirements or who want direct control over security often choose a Windstream Private Cloud. This lets them design and implement their own security processes using hardware of their choosing. With a Windstream Private Cloud, customers can also, for example, match the security architecture from their own on-premises environments.

Those seeking the flexibility, scale and economics of a public cloud often choose the Windstream Public Cloud, designed to provide robust security based upon industry standards and best practices.

For the best of both worlds, many customers select a Windstream Hybrid Cloud. With both public and private cloud environments, customers can deploy applications in the cloud that is most suited to their unique needs. At the same time, the hybrid environment supports secure communication between applications in different clouds.

In order to help businesses meet security requirements and get the most out of the Windstream Public Cloud, the remainder of this technical document discusses the overall approach to security used in the Windstream Public Cloud. If your business requires a more in-depth evaluation of Windstream security, please contact your Windstream representative for a confidential discussion.

WINDSTREAM PUBLIC CLOUD

As a leader in the Infrastructure as a Service (IaaS) industry, Windstream is currently on its third-generation cloud platform. The Windstream Public Cloud uses a consistent "Pod" design in each secure data center. This gives customers the flexibility and agility to address requirements originating from the business, applications and external regulations. Cloud Pods leverage a variety of advanced security capabilities to meet the requirements of tenant resources and their applications.

Windstream Cloud Pods are built using a secure reference architecture, emphasizing physical and logical compartmentalization, based upon best-of-breed technologies in compute, network and storage from

industry-leading vendors such as EMC, NetApp and Cisco. Each Cloud Pod is built upon a multi-tenant, Software Defined Network (SDN) architecture using VMware-based hardened Type 1 hypervisors and best practices from proven reference designs. Cloud Pods are scanned for vulnerabilities before and after moving to production and are continuously monitored 24 x 7 by our expert staff.

ACCESS CONTROL SYSTEMS

All internal and core systems are accessed using secure authentication methods with individual user IDs and passwords. Automatic disconnects of sessions are enabled for remote-access technologies after specified periods of inactivity. The privileges of Windstream personnel are compartmentalized based upon job roles and management approval, and enforced with corresponding access control lists. Network credentials are separated from cloud-based credentials to mitigate global elevated access.

Auditing of authentication and authorization is maintained and logged using a centralized Lightweight Directory Access Protocol (LDAP), Kerberos and Terminal Access Controller Access-Control System (TACACS) infrastructure. Kerberos is used to manage credentials securely (authentication) while LDAP is used for holding authoritative information about the accounts, such as the user's full name, user ID and what they're allowed to access (authorization). TACACS is a remote authentication protocol that is used to communicate with an authentication server commonly used in networking infrastructure. Logging and audit trails are unique, categorized and time stamped via a robust Network Time Protocol (NTP) infrastructure.

Customers define the Access Control Systems and policies that apply to their isolated environments. Windstream provides a suite of security and access control solutions, including a multifactor authentication service that can be incorporated into all the Windstream Cloud solutions.

DATA PRIVACY

Logical access to customer data is controlled by the cloud management platform and can only be accessed by the tenant who owns that data. Customer volumes are not directly accessible by tenants, and are managed only by the Windstream Operations team. Physical security for the data is provided by the Windstream Data Centers in which the storage is housed.

VM MOBILITY

Tenant VMs are not physically moved off premises unless the tenant specifically requests data replication. When customers require VM mobility, data is replicated using secure VRF (Virtual private network Routing and Forwarding). Customers have control over where and how their data is replicated.

DATA PERMANENCE

A common concern around data in public cloud environments is that even after a VM is deleted, copies of that VM may exist in snapshots or backups. While Windstream does use backup and snapshot technology to provide tenant data protection, this data is not directly accessible by tenants, and is managed only by the Windstream Operations team. The services to which a tenant subscribes determine the data retention policies around those snapshots or backups and when those copies ultimately are expunged. Unless otherwise contracted, the default retention period for these copies is 30 days.

NETWORK SECURITY

End-to-end network security is provided throughout the cloud environment in multiple layers, based upon a container model where network resources are abstracted and assigned as a group to each tenant virtual data center. Firewalls and virtual networks (including VPNs and VLANS) provide network compartmentalization between customer environments. Windstream staff use the cloud management platform to provision and control the network resources used by tenant VMs.

Cloud management networks and the Storage Area Network (SAN) are completely segregated and not accessible via routed IP addresses. Management Access Control Lists (ACLs) are also mapped to dedicated internal VLANs. The VLANs are separate from the

production cloud to maintain out-of-band management for availability and a zero-sized attack surface for heightened access to the cloud platform. All remote, out-of-band and internal access is encrypted.

APPLICATIONS AND SYSTEMS DEVELOPMENT SECURITY

Cloud systems and products are developed within a stringent Product Development Life Cycle (PDLC) process and meticulously documented by the Windstream Architecture and Systems Engineering groups. All systems are tested for redundancy, performance and security before being made available for customer use. The cloud management platform and associated databases are maintained and secured outside of the cloud service platform that hosts tenant VMs. The dedicated Virtual Management Cluster (VMC) hosting the cloud management platform is not accessible via the Internet. This extra layer of security is designed to eliminate heightened access levels directly from the Internet.

OPERATIONS SECURITY

Controls are maintained for operations personnel, hardware, systems, auditing and monitoring. This includes vendor access via badge, and multi-level authentication mechanisms for both physical and logical (device) security. Authorization is based upon evidence provided per position by management and information security personnel via role-based access and access control lists. Auditing of authentication and authorization is maintained and logged within a centralized LDAP (Kerberos) and TACACs infrastructure.

CHANGE CONTROL

Change control begins in the lab environment. Utilizing the same components as the production environment, all hardware and/or software changes to the production environments are first tested in the lab environment.

After changes are tested in the lab environment, Windstream Engineers create a Method of Procedure (MOP) detailing the steps to be performed in the change window. The MOP is subjected to peer and architectural review before being presented to the Windstream Hosted Solutions Change Control Board for approval. Once approval has been granted, the change is scheduled in accordance with our Service Level Agreement (SLA) and customers are notified of the upcoming change. In addition to procedural safeguards, the design philosophy is that no single change should require that the entire environment be taken down.

BUSINESS CONTINUITY (BC) AND DISASTER RECOVERY (DR) PLANNING

Redundancy and high availability is included throughout the cloud architecture. This includes replication technologies and backup platforms that allow for the use of the Windstream Disaster Recovery as a Service (DRaaS) platform. The Cloud Pods leverage backup platforms from companies such as VEEAM, EMC and NetApp. These platforms allow Windstream to offer backup, DR and replication technologies that mitigate data loss and inherently allow for business continuity via the cloud with multiple Cloud Pod locations. Cloud data is not physically moved off premises unless customers have specifically contracted for that service.

COMPLIANCE

Businesses are under increasing pressure to adhere to numerous security compliance standards, including:

- **Payment Card Industry Digital Security Standard (PCI DSS)** – Applies to any company processing, transporting or storing credit card information
- **Government Mandated Privacy Acts (Massachusetts, California and Minnesota, with others to follow)** – Applies to anyone doing business in these states
- **Health Insurance Portability and Accountability Act (HIPAA)** – Applies to the healthcare vertical
- **Gramm-Leach-Bliley Act (GLBA)** – Applies to the financial vertical
- **Sarbanes-Oxley Act (SOX)** – Applies to public companies

Cloud service providers have an important role in compliance. Since the essential underlying focus of popular compliance standards today is on individual enterprise context, it's impossible for Windstream to provide "instant on" compliance. However, with our security consultation services, as well as the best practices that we've implemented internally and advise our customers to follow, Windstream has made it as easy as possible for customers from all verticals to meet and exceed the standards laid out for them by the various regulatory bodies. Each compliance standard is built around a foundation of concepts best outlined by the SANS Institute – the largest and most trusted source for IT, information security training, certification and research in the world – and mirrored by Windstream's business best practices.

They include:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers and Switches
5. Boundary Defense
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Windstream is actively taking advantage of the SSAE 16 SOC 1 type II auditing process to provide customers with the necessary information to inform their auditors and planners of compliance-friendly topologies and practices. An SSAE 16 audit is performed by a third party that reviews our security controls, then verifies that we are adhering to them by reviewing, auditing and scoring our performance.

Since Windstream customers are under a myriad of compliance standards, we developed controls based upon the best practices mentioned above and mapped our practices to PCI DSS and other compliance standards. Windstream is also PCI DSS certified. This way, we can present our SSAE 16 documentation to any customer who needs to prove that Windstream practices security standards that exceed the compliance standards to which they are being held. This approach makes the most sense for both Windstream and our customers.

Windstream has established a powerful set of security controls that enable compliance for customers seeking FISMA, HIPAA, PCI DSS and others. The company holds SSAE 16 Compliance in our Data Centers and colocation facilities and PCI DSS Compliance for our Cloud and IaaS Data Center facilities (physical controls). Windstream has Safe Harbor Certification and offers HIPAA Business Associate Agreements (BAA) for Healthcare industry customers. In addition, Windstream is running further assessments for compliance certifications for SOC 2, expanded PCI DSS and FISMA/FedRAMP in 2013, with expected compliancy in 2014 (Note: 2013 assessment work may drive changes to 2014 compliance targets).

LAWS, INVESTIGATIONS AND ETHICS

Windstream is a telecommunications company. It securely maintains Customer Proprietary Network Information (CPNI). Windstream protects its customers' privacy but may provide certain customer information to law enforcement and other government agencies when required by law to do so.

PHYSICAL SECURITY

Each Data Center with a Generation 3 Cloud Pod is encased within a shell made up of 12-inch thick, steel reinforced, insulated pre-cast concrete walls. An 18-inch multilayered roof that includes a 4-inch concrete slab provides a Level 1.5 seismic importance factor and enables it to withstand winds (including uplift) of up to 149mph (the equivalent of a Level 4 Hurricane). Cloud Pods are caged and locked with laser etched keys that must be signed out via an audit log and monitored via digital video.

Core physical security functions within each Data Center include the following:

- Multi-level authentication
- Biometric scanners and card readers
- Man trap
- Hardened security station
- Ballistic rated level III windows
- Ballistic shielding at the security station
- Digital security cameras with video recording
- Exterior security lighting

CONCLUSION

Security is important in every IT environment, from traditional on-premises data centers to multi-tenant public clouds. As businesses increasingly use public cloud computing, they have questions about cloud security. This paper has highlighted a number of important questions about cloud security and also outlined the security approaches used by Windstream's Public Cloud.

To ensure your security in the cloud, choose a CSP such as Windstream Hosted Solutions that offers a wide range of security coverage and employs best practices in security management. You should also take advantage of services like business continuity planning and disaster recovery to safeguard your data and mission-critical applications. A first-rate CSP should empower your organization to do more with the resources at hand while simplifying IT processes and assuring your security in the cloud.

Windstream offers multi-tier security at every layer of the IT stack, including physical security, to give customers complete security coverage. Our strict adherence to industry regulations also makes it easy for customers from all verticals to comply with the standards of various regulatory bodies.

Windstream is dedicated to end-to-end customer data security and we will work with you to meet your requirement. Windstream provides Cloud and Data Center Security Services, extensive Managed Security Services and private and secure MPLS circuits all focused on providing end-to-end information security.

Distributed Denial of Service Mitigation

windstream® Hosted Solutions

IMPERVA®

The Windstream Difference

We believe that understanding your business, not just your technology, is key to creating hosting solutions that keep your applications and business up and running. More than just taking pride in what we do, we understand what's at stake for our clients and their business. That's why we're personally invested in building hosted solutions that help businesses succeed.

Automated Mitigation of the Largest and Smartest DDoS Attacks

Windstream's Distributed Denial of Service (DDoS) mitigation service secures websites against the largest and smartest DDoS attacks. Large attacks use a high volume of packets targeted at Layer 3 network and Layer 4 transport level protocols. Volume attacks overwhelm network bandwidth, routers and firewalls. Smart attacks focus on Layer 7, the application layer, looking for vulnerabilities in databases, scripting and web servers. Our DDoS mitigation service is built with industry leader Imperva to not only defeat these attacks, but to do so automatically, without requiring intervention and without interrupting your customers' service.

Scalable High-Capacity Network to Handle Volume-Based Attacks

As DDoS attacks continue to grow, mitigation requires a robust high-capacity scrubbing network. We use a global network of highly-scalable scrubbing centers which intercept volumetric attacks near the point of origin—far from your network. Keeping attacks at a distance ensures your network is unaffected and desired customer traffic reaches your hosts.

Intelligent Multi-Layer Protection

Carrier-grade edge routers filter out IP protocol attacks, such as DNS amplification and Martian packets. Global, high-powered scrubbing clusters manage real-time DDoS traffic profiling and blocking. Web application firewalls (WAF) process HTTP sessions and use intelligent traffic profiling and bot detection technology to accurately weed out malicious web traffic. This multi-layer approach is continuously updated with the latest detection and defense techniques to provide world-class results.

Advanced Bot Protection

Visitor identification technology differentiates legitimate website visitors (e.g. humans, search engines, etc.) from automated or malicious clients. This capability is critical with respect to application layer (Layer 7) attacks, where the DDoS requests look like legitimate visitors.

Transparent Mitigation

Windstream protects your site not only from complete denial of service, but also from disruptions related to DDoS attacks, mitigation false-positives and more. We offer transparent mitigation with less than 0.01% false positives, and without degrading the normal user experience in any way.

Automatic Detection and Triggering

Windstream delivers "always on" DDoS mitigation, which is well-equipped to handle "hit and run" attacks. This type of attack can wreak havoc with solutions that need to be manually turned on and off on every burst. Always on means automatic detection and activation whenever and for however long an attack persists.

Fast, Easy Onboarding—DNS-Based Routing

DDoS protection can be enabled without the need for hardware, software, integration or web application code changes. Customers can be added to this service simply by changing their website's DNS setting. This effortless deployment allows customers to be protected in a matter of minutes while maintaining their existing hosted environment and application infrastructure.

Protect your website from all types of DDoS attacks:

- TCP SYN+ACK
- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK + PSH
- TCP Fragment
- UDP
- ICMP
- IGMP
- HTTP Flood
- Brute Force
- Connection Flood
- Slowloris
- Spoofing
- DNS flood
- Mixed SYN + UDP or ICMP + UDP flood
- Ping of Death
- Smurf
- Reflected ICMP and UDP
- Teardrop
- Zero-day DDoS attacks
- Attacks targeting Apache, Windows or OpenBSD vulnerabilities
- And more...

World-Class Support by DDoS and Security Experts

With all the advantages of our network-based, always-on solution, it's hard to believe it gets even better, but it does. Our security experts stay ahead of attackers by profiling new attacks and adding new filters to stop them, so the service is getting better all the time. Windstream's DDoS mitigation service is another example of how we provide smart solutions and personalized service to keep your business up and running. Together, we win.

Why Windstream's DDoS Mitigation Service?

- Powerful backbone across globally distributed data centers
- Specialized support for massive SYN flood and DNS amplification attacks
- Advanced algorithms which mitigate sophisticated application layer attacks
- Dedicated 24 x 7 NOC for enterprise-grade uptime
- Always on, automatic DDoS attack detection and mitigation
- Zero business disruption
- Activated by simple DNS change—no hardware or software installation
- Constantly improved by our partner Imperva, a world leader in data center security

smart solutions. personalized service.

DATA
VOICE
NETWORK
CLOUD

Find out how we can make the cloud work for you—and your bottom line.
Contact your Windstream Representative, or visit **windstreambusiness.com/hosted**

14343 | 6.14