

Genesis Hosting Solutions, LLC Data Center Security and Reliability Controls

Genesis Hosting Solutions' equipment is collocated at an XO Communications facility downtown Chicago, at 140 S. Dearborn St (the Marquette Building). XO Communications is a proven provider of telecommunications and networking services with over 900 central office collocations and a 1.3 million fiber-mile long-haul and metro-network. The facility where our equipment is collocated is a primary facility for XO's telecommunications network for downtown Chicago.

XO maintains high-quality controls to assure their facilities are secure. The following are controls XO has in-place specifically for the facility Genesis has collocated equipment:

Built and Constructed for Ensuring Physical Protection

The facility datacenter room has no exterior walls, doors, or windows. There is at least two concrete, steel re-enforced, walls between the room and the outside of the building.

Protection of Physical Grounds

To enter the facility, a person must present an ID to guards at the entrance and pass through multiple steel doors, unlocked by authorized proximity cards.

Security Systems

Multiple off-site video surveillance cameras are located throughout the facility. Power for this system is provided by the facility's redundant battery and generator backed-up power systems.

Cages, Cabinets, and Vaults

The facility has cages and cabinets. Every cabinet is locked with a combination lock to prevent unauthorized access. Genesis' cabinets are solely leased by Genesis and not shared with other XO customers. Surveillance cameras are located throughout the facility.

Uninterruptible Power

Two independent power legs are provided to each cabinet, each connected to an independent industrial Uninterruptible Power Supply (UPS) and generator. Our facility has multiple electrical feeds to two sides of the building from the same electrical carrier. In the past 11 years, since the facility opened, it has experienced a single power issue, which occurred on one power leg for 0.1 seconds due to a failed power transfer switch during the standard monthly generator test, where all power to the facility is transferred from commercial power to battery, to generator, back to battery, and finally back to commercial power.

Access to power systems is protected by multiple doors requiring XO staff proximity cards to gain access. Customers are never provided access to this equipment.

HVAC

Air conditioning and humidity controls are fully-redundant and monitored by XO at its NOC.

Authorized Personnel

Only authorized proximity card holders may enter the facility. Proximity cards must be purchased and registered by a authorized representative of a company collocating equipment at the facility. Visitors are normally not allowed.

The following are specific controls related to Genesis Hosting Solutions' infrastructure:

Network

Genesis maintains multiple connections to XO's network edge. XO's network maintains connections to over 45 peers, each with at least one 10Gbps connection. Our facility has over 880Gbps of connectivity to XO's network and its peers. Both Genesis' Ethernet, connected with BGP4, and fiber channel networks are fully-redundant with multiple switches and controllers, both at the server and SAN controllers and arrays.

Network Security

Network monitoring is provided based on the requirements of customers, including Intrusion Detection Systems, Intrusion Prevention Systems, and application-layer and basic firewalls. Foundry Networks' IronShield Security is used to provide granular control over every aspect of Layer 2 and Layer 3 traffic, including protecting against Denial of Service (DoS) attacks and rate limiting ICMP and TCP SYN packets, protecting networks against external or user-generated attacks, whether intentional or not.

Monitoring

Genesis uses Nimsoft's NimBUS for its Network Operations Center (NOC) to monitor all physical and virtual components within its network, as well as some customer networks. NimBUS is the fastest growing Enterprise service level monitoring system with many Fortune 500 customers. sFlow information is also gathered from our Foundry equipment to provide real-time wire-speed network monitoring. Reflex Systems' Virtual Network Security products are used to monitor and protect the virtual network edge within our virtualized infrastructure.

Physical Infrastructure

Genesis' physical infrastructure consists of only Enterprise-grade equipment from HP, IBM, APC, and Foundry Networks. This includes power distribution, Ethernet switches, fiber channel switches, servers, disk systems, and SAN controllers.

Virtualized Infrastructure Reliability

Genesis' main service is providing virtual infrastructure. All virtual infrastructure is designed for highly-available configurations where any physical component can fail and the virtual infrastructure will repair itself by using redundant components.

Virtualized Infrastructure Security

Our virtualization platform of choice is VMware's ESX server, used by every Fortune 500 company as well as 120,000 other companies, currently owning over 85% of the virtualization market. Customer virtual networks are separated by Layer 2 VLANs on our Ethernet switches. Storage segmentation is provided by the virtualization platform and/or fiber channel zoning within our fiber channel switches (similar to Layer 2 VLAN segmentation for Ethernet networks). Access to various virtual infrastructure components is provided by security within the virtualization platform.

Disk Systems

Disk storage is provided by our Storage Area Networks (SAN). Each SAN has redundant connections to multiple switches and to each server. Every SAN controller shelf has redundant controllers, redundant power supplies, and redundant connectivity to our switches. Fail-over tests are performed periodically to guarantee that we fail-over properly in the case of an emergency. Storage shelves are configured so an entire shelf can fail without affecting service.

Backup Systems

All backups are performed by esXpress, a disk to disk backup system. We maintain a separate SAN for backup storage in a RAID 1+0 configuration with multiple hot-spares. As with our SAN equipment, all equipment is redundant, including storage arrays, where an entire shelf can fail and the SAN will still function.

Initials _____