



Business Continuity & Security

This document describes the security implementations for the VirtualRoof.com customer base. This description will be broken into several distinct categories: Physical location, Hardware, Software/OS, Network, and Data Security.

Our security policy is intended to protect the integrity of VirtualRoof.com Corporate software and data, the customer's software and data, and the integrity of our data processing network and processing resources. Our goal is to mitigate the risks and losses associated with security threats and physical disasters at VirtualRoof.com to IT Hardware and Software systems, Corporate and Customer data, and network access and resources.

PHYSICAL LOCATION.

All hardware resources are housed at our co-location facility in Bellingham, Washington. This facility is under the management and control of Fiber Cloud, Inc. The following is a description of the facilities with a list of features they support.

Data Center Specifications

The Data Center is located at 851 Coho Way, Bellingham, WA 98225

The FiberCloud data center is built to exceed the most stringent requirements necessary to guarantee Internet operations. Unlike other enormous, impersonal facilities, FiberCloud is designed as an elite, service-oriented facility with the in-house expertise to provide a refreshingly different approach to co-location.

Fiber Cloud is located in a 48,000 ft² office center with 24-hour security. IP based closed circuit video surveillance throughout the building with 5-day backup. Computer controlled access keys for all building entries, logged and retrievable, and instantly programmable for enabling and disabling access. Retinal eye scanning is required for access to data center Controlled Access Area. Video and alarms are monitored for intrusion or tampering. The Controlled Access Area contains fully enclosed cabinets with locked front and back doors. The 5,000 sq. ft. data center is protected by strict personnel access policies. Access to the controlled access area is available on a 24x7x365 basis for authorized users. All security systems are on full SLA with redundant backups. Fire Suppression FM200 dry chemical fire detection and suppression system and FM200 sensors installed throughout data center floor and ceiling. Features of the system include early action, dry pipe, and zone only sprinkler system. The controlled access area where the equipment racks are located is a clean room with dust filtering systems and it is a pollution free environment. The data center has redundant power & backup power is controlled with an automatic transfer switch. The Liebert 3-phase UPS system (300 KVA) provides constantly conditioned power to the data center. The Diesel generator backup (750 KW) is regularly maintained, tested and load-banked. A guaranteed fuel supply agreement is in place for the generator. Environmental Controls

consist of redundant 25-ton Liebert environmental cooling systems with zone temperature control. Room temperature is maintained at a consistent range of 55-70°F and humidity at 40-60%. The flooring is a Static-free raised floor and sub-floor. The data center provides customer work & equipment staging areas with tools, phones, and Internet connections. Complete full service support and modern conference room facilities with Internet access, projector, and refreshments are also available. All cabinets within the data center are Secure Cabinets with seismic bracing to the floor and ceiling they have lockable front and back vented doors with solid sides and a wire management cableway. Each cabinet has a dedicated 20 amp circuit and 16-outlet power strip, dual top-mounted fans. Standard dimension is 84" x 24" x 36".

This facility is a "Class A" data center designed, installed and maintained by collocation experts which provides a superior environment for hosting applications for VirtualRoof.com and Qwest . It has been built to Seismic Zone 3 standards and is located in a lower risk seismic zone independent of Seattle or Vancouver fault zones. It is independent of major metropolitan target areas for man-made disasters.

HARDWARE.

All components are located in secured racks. The Hardware we use consists of redundant, name brand servers and components. VirtualRoof.com uses Dell, Compaq, HP, Intel, or IBM servers depending on price and availability. All components are configured for redundant operation and spare components are available on site for critical components. The hardware components are broken up into several broad categories.

Terminal Servers.

Terminal servers provide the virtual desktop services for our customers. They all have mirrored hot swappable drives which the Operating System software. They may also host some application software depending on application requirements. These servers are configured to run in a load-balanced group. There is always a spare server available to provide backup support for the terminal server load-balanced farm. The switchover to the redundant server is automatic upon failure only impacting the sessions of people on the failed server. We try to limit the number of sessions per server to 50 or 60. Access to customer data is provided to the terminal servers via network shares from the application and file servers.

Application Servers.

Application servers provide support and access to application data and back end application services. The application servers are always set up in a clustered environment. This cluster is designed to be expandable as customer growth dictates. They all have mirrored hot swappable drives upon which the Operating System software and the application software is installed. Upon system failure the backup in the cluster assumes the duties of the failed server. Impact to uses of the application is dependent on whether or not the software is designed to run in a clustered environment. Most Microsoft enterprise applications are designed to run in this environment. These servers all have direct access via fiber connection to the Storage Area Network (SAN).

Data Cluster Servers

These servers provide file services to terminal and application servers. These servers are always set up in a clustered environment. They all have mirrored hot swappable drives upon which the Operating System and software is installed. Upon system failure the backup in the cluster assumes the duties of the failed server. These servers all have direct access via fiber connection to the SAN. This cluster is designed to be expandable as customer growth dictates.

Storage Area Network.

The SAN consists of the following components. Multiple rack-mounted, disk arrays in a raid 5 configuration. All arrays have 2 fiber connections to the fiber array controller. All disk arrays have a hot spare. There is also several cold spares on site. The fiber array controller has a spare unit on site in case of failure. All customer Data is stored on these arrays. We also have a spare array available in case of a catastrophic failure of one of the production arrays. Some application software is also stored on the arrays.

Active Directory Domain Controllers.

We have 2 clustered AD domain controllers that provide support for internal DNS, DHCP, and Active directory services and data. This cluster is designed to be expandable as customer growth dictates. These servers all have mirrored hot swappable drives upon which the Operating System software, services, and AD databases are installed.

DNS Servers.

External DNS servers are all housed in separate physical locations and subnets to ensure redundancy and availability.

Data Backup Servers.

We have 2 clustered data backup servers that provide for nightly backup of customer data and applications that reside on servers and on the arrays. Each backup server can handle backup of the entire network. Each server backs up half of the network on a nightly basis. VirtualRoof.com has a fully documented and managed tape rotation system. This system provides for off site and on site tape rotation as dictated by the tape rotation system. This cluster is designed to be expandable as customer growth dictates. These servers all have mirrored hot swappable drives upon which the Operating System software, services, and tape backup software and DB's are installed. Each server is connected to external tape drive and library systems, which are highly expandable depending on data backup requirements

SOFTWARE/OS.

Operating Systems and services.

- Windows 2000 for all servers except for external DNS.
- Linux and Bind to support external DNS services.
- Citrix Metaframe
- vWorkspace by Quest Software

Application Software.

- Exchange 2000 for email services.
- MS Office for office applications.
- Acrobat Reader
- VirtualRoof.com Managed Virus Protection Software for A/V detection and prevention.
- Veritas Backup Exec and Comvault Galaxy for tape backup Systems.

NETWORK.

The network infrastructure consists of redundant 3com switching hubs for the internal private network and redundant HP switching hubs for the public network.

Public Network Segment.

The data center provides 2 fully redundant 100mbps connections to our meshed public switches. One cable is connected to each physical switch. There are 4 connected meshing ports on each switch to provide for transparent connectivity for the public network segment. The firewall's public interface is connected to the switches.

Private Network Segment.

The private network segment has half the servers connected to each switch. There is meshed connection between the 2 switches. The firewall's private interface is connected to the switches.

Data Center Network.

The data center network provides VirtualRoof.com with access to the Internet via there internal layer 2 switched network. FiberCloud provides us with fully redundant access via 2 OC3 circuits with separate fiber paths to the 2 locals providers. One OC3 is routed to AT&T Canada thus bypassing all the Seattle metropolitan internet traffic. The second OC3 is provided by Sprint Canada again bypassing the majority of the west coast internet traffic congestion in Seattle and San Jose. This provides VirtualRoof.com with a tremendous amount of Bandwidth and redundancy and excellent response time and extremely latency.

Data Security.

VirtualRoof.com controls access to customer data and applications by use of Active Directory (AD) Global Policies and NT file permissions.

AD policies are used to lock down customer virtual desktops to disallow access to server drives and operating system utilities. The intent is to provide customers with access to all the applications that they have subscribed to without allowing them access to any other utilities and applications.

Data access is controlled by NT file permissions and share access permissions. The only access to customer shares and data allowed is administrative access and the customer themselves.

Network Access to Servers and Data.

All file and application servers are not physically connected to the public network segment. The only access to the file and application servers is through the terminal servers.

Administrative access via the internet is provided via an VPN connection.

Access to the terminal servers from the internet is only available via the firewall connection to the private network segment.

Session Security and Control.

All access to terminal servers is by Authenticated, encrypted connection.

Metaframe is used to provide support for the virtual desktop. This provides the customer with a high level of security while working within their virtual desktop. The way Metaframe works is that all processing actually occurs on the terminal server and not at the client's desktop. The only data that is sent back and forth between the terminal server and the user desktop is screen, keyboard, printer, and mouse data. By default the data stream is compressed and encrypted. Optionally, we can require the vWorkspace/Citrix client to use 128-bit DES encryption. In addition, the only way to access your virtual desktop is by use of the vWorkspace/Citrix client and your correct logon id and password.