CenturyLink Business

IMPLEMENTATION GUIDE

CenturyLink Cloud
Security Overview

IMPLEMENTATION GUIDE

CenturyLink Cloud Security Overview

Abstract

CenturyLink Cloud is entrusted with hosting many sensitive, business-critical systems for clients that include some of the world's largest corporations. This guide describes how CenturyLink Cloud manages security for its clients. It starts by reviewing CenturyLink's "Shared Responsibility Model" for security. The guide then outlines CenturyLink Cloud security features, processes and best practices used to secure the cloud platform and its data and explains the role of customer and provider for managed services. It goes into detail on change and incident management, data and storage segregation, cage protection, personnel policies, access controls, network security, replication, and disaster recovery.

CenturyLink is entrusted with managing the information assets of some of the world's largest corporations. This is not a responsibility we take lightly. Our commitment to security for our clients' data and systems is central to almost everything we do in our business. This guide outlines how we approach securing client information assets hosted in a multi-tenant environment. While not exhaustive, this guide was created to answer the most frequent high-level questions that our clients have about CenturyLink's security policies and procedures for its public cloud.

CenturyLink operates on a "Shared Responsibility Model" that delineates CenturyLink's obligation to secure physical and virtual environments and the customers' obligation to secure their applications and unique instances with tools that we and our partners provide. The client's security roles and responsibilities will vary based on service type. For instance, CenturyLink's responsibilities will be different in a Platform-as-a-Service (PaaS) scenario versus Infrastructure-as-a-Service (IaaS).

Overall, CenturyLink takes a "defense in depth" approach to securing customer environments, securing physical equipment, cloud resources, and customer data. In addition, an extensive permissions system, that extends to the group and individual VM levels, ensures only authorized users can access and alter systems. We've worked with leading IT auditing firms to ensure our systems are ready to support most global organizations:

- **Account Security** – We provide customers with role-based access to their cloud environments. Users access the Control Portal with a username and password, or by Single Sign On (SSO) through Security Assertion Markup Language (SAML). Actions performed by users through the Control Portal — such as provisioning servers, adding public IP addresses and powering-on a server — are logged and auditable. These logs are retained for at least 90 days, and customers can view access logs on an entity-by-entity basis.
- **Network Security** – CenturyLink Cloud establishes a robust digital perimeter around the client's cloud environment. Access to customer servers can only be done via a certificate-based VPN connection, IPSec tunnel, or Direct Connect unless specific public ports have been explicitly opened up by the customer. Customers can extend to two-factor authentication via LDAP (Microsoft Active Directory or OpenLDAP on Linux) for additional security where needed.
- **Intrusion Detection** – Data center Intrusion Detection System (IDS) and Intrusion Detection and Protection System (IDP) attack detection and prevention features screen incoming and outgoing traffic for potential attacks.
- **SOC 2 Audited Controls** – CenturyLink Cloud has demonstrated audited compliance for SOC 2 Type 2 in the areas of security and availability.
- **Physical and Personnel Security** – Each CenturyLink Cloud data center is housed within private, caged enclosures. Entry to the data center premises requires an electronic proximity key card. Data center facilities are staffed 24/7 and monitored by cameras. All staff receive thorough background checks. An electronic proximity card control portal, biometric scan, and onsite data center personnel provide additional security inside the facility. Only CenturyLink authorized staff are allowed access to the private cage enclosure. All access is logged in the ticketing system.

CenturyLink Security At-A-Glance

Physical Security

- Physical security controls with SOC 1
- All access is logged

Logical

- Logical security policies and processes with SOC 2 – built around IT best practices
- Backend Server and Operating System hardening
- Managed carrier class firewalls
- Intrusion Prevention services included
- Dedicated VLANs/IP addresses
- Nessus vulnerability scanning available
- 24/7 monitoring and incident management

Account

- Role-based access – authentication and authorization permissions set explicitly
- Username/password or SAML sign on
- Many actions logged and auditable

CenturyLink Cloud Shared Security Model

CenturyLink operates on a "Shared Responsibility" model for security. The shared responsibility model delineates CenturyLink's obligation to secure the underlying infrastructure as well as the customers' obligation to secure their own virtual servers, applications, and systems with tools that we and our partners provide. We commit to security roles and responsibilities that are within our ability to manage, while the client commits to security areas that are within the client's control.

Figure 1 shows a simplified diagram of security responsibility sharing between CenturyLink and the client. At a high level, CenturyLink is responsible for security of the infrastructure, including the data center and network, and basic services of compute, storage, and network. The client is responsible for what it controls, such as the application software and data. The level of responsibility depends to some degree on the type of service in use. We discuss managed services on page 8.

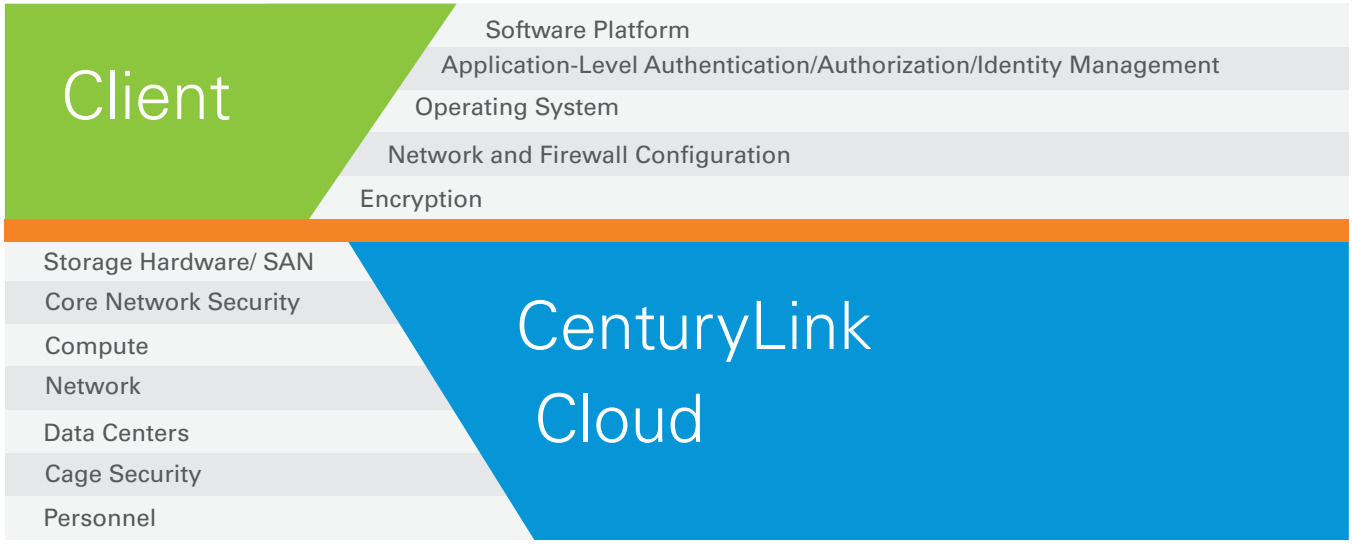

Figure 1 - Basic shared security responsibilities for CenturyLink and client

SECURITY RESPONSIBILITIES	PaaS		IaaS	
CenturyLink	• Infrastructure • Management platform • OS	• Database servers • Storage	• Infrastructure • Management platform	• Managed OSs • Managed Apps
Client	• Application • Secure Coding	• Application-Data interactions • End point security	• OS • Data • Application	• Secure Coding • Application-data interactions • End point security

Table 1

Table 1 shows — CenturyLink's security responsibilities are more extensive when the client uses the CenturyLink Cloud for Platform-as-a-Service (PaaS) versus Infrastructure-as-a-Service (IaaS). With IaaS, the client is undertaking a greater scope of IT activity on top of the cloud platform, so in that case the client has a greater share of security responsibility. With on-premise environments, the client assumes all responsibility.

In a PaaS scenario, the customer and the provider have a more balanced share in the areas of responsibility related to securing the customer's critical information. The provider is responsible for things like the underlying operating system of that platform, its availability, and the software versions as well as configuring all that software sufficiently and securely. The customer is responsible for the applications they write, how the applications interact with data, and secure coding principles. The client is also responsible for authentication and authorization of users.

For the customers hosted in a multi-tenant environment operating on an IaaS basis, CenturyLink focuses on the security of the infrastructure and underlying platform. Our goal is to enable the customer to secure critical data and remain compliant with various regulatory regimens, such as those that cover personally identifying information (PII). The customer is responsible for overall security controls around their data, managing access, securing virtual machines (VMs), and the operating systems on those VMs — including patching and configuring it securely. The customer is responsible for securing their data, encryption-at-rest where needed. To that end, we have partners who specialize in encryption-at-rest solutions, such our ecosystem partner Vormetric.

Security and Managed Services
Security responsibilities are different for clients who use CenturyLink Cloud's Managed Services. CenturyLink is providing the managed operating systems or application, so we take on a greater role in securing the managed service. Specific security parameters vary depending on the service offering. Page 8 provides additional detail.

Securing the Platform

CenturyLink Cloud secures its platform through multiple sets of tasks and work streams. These include Secure Architecture, Change and Incident Management, Data Segregation, Physical Protection, and Personnel Practices. Each work area is distinct, but they overlap and form a defense-in-depth approach to security.

Secure Architecture

CenturyLink Cloud employs a thorough Secure Architecture Review process based on the SOC 2 Type 2 Audit Standard. SOC 2 Type 2 is designed to report on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy. Based on the AICPA Guide, the SOC 2 Type 2 audit covers oversight of the organization, vendor management, internal corporate governance and risk management processes, and regulatory oversight — if applicable. We focus specifically on the areas of security and availability.

For CenturyLink, the core of our security model comes from the concept of isolation. A new CenturyLink Cloud customer is set up in an isolated environment on our platform. By default, the new customer is in a secured, isolated Cloud environment with a "nothing open to the world" perspective. We ensure isolation in our multi-tenant environment by adhering to six internal principles:

1. Isolate tenants within their own network.
2. Do not allow tenants to see another tenant's network, data or metadata.
3. Encrypt data in transit.

4. Clean up deleted resources, e.g. reset and clear resources when a network or storage volume is released by one customer and another can use it.
5. Prevent "noisy neighbors" from affecting others.
6. Define and audit policies to ensure proper administration of shared environments.

CenturyLink uses work-based controls to isolate one customer from another as well as from the public network. We also take advantage of the capabilities of our virtualization platform to enforce isolation between customer environments at the hypervisor and storage layers. Other relevant isolation controls include:

- **Built-in Platform Isolation** – CenturyLink's IaaS customers can create sophisticated network topologies with one or more VLANs. We exercise VLAN isolation to make sure that data packets stay within the appropriate VLANs.
- **Account-Level Isolation** – We have implemented an account hierarchy structure that enforces isolation between accounts and sub-accounts. This can be changed depending on customer needs. Sub accounts are containers that can have unique users, permissions, billing procedures, networks, and even branding. The customer can choose to inherit various settings from a parent account (e.g. "share parent networks", governance limits) or treat them as completely independent resources. There is a fully-featured role-based access control system to allow customers to further allocate fine-grained access into their environments based on role.
- **Project-Specific VLANs** – We use separate VLANS to isolate servers within an account, providing users with remote access to cloud servers but only allowing a small subset of administrators to place the servers on the appropriate VLANs. This makes it possible to have project-specific VLANs where traffic is cleanly isolated from other networks in the account.
- **Multiple Data Centers** – CenturyLink Cloud is spread across the globe. Clients can set up sub-accounts and intentionally constrain users to a chosen set of data centers. This helps isolate accounts (and applications) to the geographies that work best for the client's business.
- **Avoiding Noisy Neighbors** – We always leave "headroom" on host machines and closely monitor usage to know when it's time to scale. We also use features in our hypervisor platform to protect against capacity and latency bursts in CPU and disk. Our storage subsystem is built to handle multi-tenancy and provide protection against I/O bursts. CenturyLink's network is designed to prevent any one tenant from overwhelming the firewalls, and our ample bandwidth ensures that network saturation is nearly impossible.

Change and Incident Management

CenturyLink has established change and incident management processes. The goals are to ensure that all changes to the production infrastructure are properly planned, tested, and approved. Change management processes are audited. Our incident management program is designed around a quick response to customer tickets and incidents, regular communication about status of incidents on our platform, and quick resolution to incidents.

Change Management

Our Change Management Process is designed to provide an orderly method in which changes to the IT environment are requested and approved prior to installation or implementation. This covers any and all changes to the hardware, software or applications. This process also includes modifications, additions or changes to the LAN/WAN, network or server hardware and software, and any other environmental shutdowns (electrical). The process is put into action for any change that might affect one or all of the environments CenturyLink Cloud relies on to conduct normal business operations. The purpose is to ensure that all elements are in place, all parties are notified in advance, and the schedule for implementation is coordinated with all other activities within the organization. It also includes any events that may alter the normal operating procedures. All changes require a technically qualified engineer other than the person implementing the change review and approve the change. Changes are recorded and tracked in a master change management calendar, and all changes that may impact customers are required to meet the notification timelines published in the SLA on our public website.

Incident Management

CenturyLink's Incident Management program is designed around three principals: Quick response, frequent communications, and swift resolution. Our Ticket Prioritization Matrix explains the process in detail. Given that incidents tend to vary, there is some flexibility built into the response though the CenturyLink Cloud team adheres to the following general steps when handling a security incident:

- **Collection** - The goal of this phase is to ensure all requests and incidents that require human attention are collected into a single system that enables requests and incidents to be triaged and then assigned for completion. Inputs include webforms, email, chat, phone, monitoring alerts, and social media. A ticket is created for all requests and incidents using the ticketing system.

- **Incident Management Steps** - Once a ticket is created, the next step in the process is to determine if the new ticket is related to an existing incident for the same customer or for other customers. Once it has been determined this is a new incident and not connected to an existing one, the incident needs to be classified and prioritized properly to drive resolution and communication activities.
  - Classification and Prioritization, e.g. Normal, Urgent, High
  - Triage
  - Notification, e.g. CSO, CTO, Legal
  - Service Restoration

Data Segregation

How data is segregated in a shared environment?

CenturyLink enforces data segregation in its environment using the VMWare hypervisor. We allocate customers' data on VMWare's Virtual Machine File System (VMFS), in virtual disk files (VMDK) files. VMWare enforces permission on the VMDK files so that the only file visible to the virtual machine is one to which the customer has directed the VMWare software to grant permission. CenturyLink's automation enforces a policy wherein when a customer creates a new virtual machine, that virtual machine creates its own dedicated disks. They are not shared. The CenturyLink Cloud Control Portal does not have any ability to share or create a shared file between multiple VMs. We can have thousands of customers, each with VMs, on a shared data store. Each machine will only see the disk files that have been assigned to it, and the disk files can be seen by no other machine on the platform. While this also means that customers cannot grant shared access from different VMs to the same SAN, we believe this security model is in the best interest of our customers long term.

Physical Protection

CenturyLink's Cloud nodes are hosted in 13 data centers around the world. All of our data centers are governed by security standards for the protection of our cloud environment within those data centers. Those security standards include an isolated and protected cage that is dedicated to the CenturyLink Cloud equipment and is secured separate from the other customers in that given data center or facility. For instance, a CenturyLink Colocation customer cannot gain physical access to the CenturyLink Cloud's cages. CenturyLink data center have security cameras, and 24/7 alarms at the physical data center layer. We maintain tight control over our lists of authorized users, who can access facilities, and who can authorize work in, or authorize vendors into our cage.

Personnel Practices

CenturyLink includes personnel policies and practices into its overall security program. The company emphasizes the reliability of the personnel we hire and who have access to the platform. We have rigorous screening and interview processes that make sure that we only hire highly qualified and trained candidates who are experts in the technical area for which they're being hired. The hiring process includes industry standard background checks, looking for any issues that contradict our standards for employee conduct. These include criminal background checks.

Our onboarding process includes training in all of our security policies and procedures as well as training in our Change and Incident Management procedures. Our onboarding also includes supervised training and knowledge transfer prior to individuals being given access to production systems. Ongoing training follows at regular intervals, including refresher courses on our security policies and procedures. They receive training on updates or changes, policies and procedures and ongoing technical training as the technology that we use changes over time. Policies are vigorously enforced through Human Resources.

Network Security

CenturyLink Cloud's network security starts with our commercial-grade, clustered, highly available firewall. With this, we can do stateful packet inspection. We have implemented intrusion prevention screens to block well-known web-based attacks. With our "isolated by default" model, each customer account is given their own VLAN. That VLAN by default has no connectivity to anything other than through a standard VPN server, a default VPN server that is provisioned for each account. This is the only way a customer can access its virtual machines by default.

Security Advisory Services

CenturyLink has extensive security consulting services available for clients. We can work with customers on the development of secure architecture and controls to ensure compliance with various regulatory schemes. We have the ability to create a customized, robust security framework for cloud, colocation, network and managed hosting services.

We provide load balancing, either on a shared load balancer service or through a dedicated load balancer appliance if the customer needs more sophisticated configurations. Customers have the ability to open and assign public IPs to their virtual machines and specify open ports as needed for their business and use of the platform. VMs are isolated on the network. For instance, when a customer creates virtual machines in four different data centers, by default they are all isolated from each other. They can't communicate with each other. The customer has the ability to create firewall rules that will allow those different VLANs to communicate with each other, if they choose. The customer can create powerful network isolation architectures that can include a DMZ if one is required.

Our recommended practice is that the client should never assign a public IP address or open a port unless they have a specific need to do so. They should never expose SSH or RDP protocols to the public network because these are common attack vectors. We allow them to do it, but we strongly recommend they do not take this course of action. If there is business reason that they need to have SSH or RDP exposed to the public network, then they should use our source IP limitation feature, which will restrict traffic to those ports from specifically authorized external IP addresses.

Platform Security Features/Capabilities

The CenturyLink Cloud platform is built for performance, reliability, and security. Our IaaS platform offers on-demand provisioning of high-performing virtual machines with any combination of operating system, storage, and memory. VMs can be extensively customized for myriad workloads and security/compliance requirements. Virtual servers rely on fully redundant enterprise-class hardware connected through private high-speed virtual LANs. The customer is able to deploy to data centers around the globe. Each security-audited data center contains "Nodes" that are engineered to include fully redundant enterprise-class hardware from front-end firewalls to storage.

Deep Content Inspection

CenturyLink Cloud does not offer deep content inspection from its built-in IDS/IDP platform. Clients looking for in depth deep content inspection should contact a CenturyLink Cloud sales resource to review add-on security products.

Intrusion Detection and Prevention

CenturyLink's Data Center Intrusion Prevention System (IPS) attack prevention feature screens incoming and outgoing traffic for potential attacks. This protection is available data center-wide, and is enabled by default for all cloud customer instances. The IPS feature is a standard feature of our edge firewall product. The CenturyLink Cloud platform uses "screens" to look for specific and common attack traffic.

If a specific attack or event is detected, CenturyLink offers numerous, flexible remediation activities. They vary depending on the source, target, number of customers affected and type of exploit. CenturyLink Cloud resources will work closely with our customers to take appropriate steps to resolve these events in a timely manner. This includes, but is not limited to, isolating a specific Virtual Machine to blocking IP addresses of attack sources.

Identity and Access Management

CenturyLink Cloud provides sophisticated Identity and Access Management features. These include granular Role-Based Security settings. Role-based access control (RBAC) is designed to make it possible for certain common customer roles, such as Account Administrator or DNS Manager, to have access to preset admin functions. For example, a Billing Manager will only see billing information, not configuration settings for VMs. See Appendix for an excerpt from our Role Permissions Matrix.

The CenturyLink Cloud Control Portal can be configured to do single-sign-on against the customer's existing identity infrastructure using Security Assertion Markup Language (SAML) 2.0. SAML lets the customer leverage their existing identity management processes and tools and mechanisms. This allows the customer to implement whatever multi-factor authentication or enhanced authentication schemes that they need to control access to the Control Portal. For example, the CenturyLink portal can authenticate against Microsoft Active Directory Federation Services (ADFS), Oracle Identity Manager, Microsoft Forefront Identity Manager, and so forth. The Control Portal is used to manage the customer's Cloud environment, create/modify/delete machines, change the firewall, connectivity, and so forth.

Data Replication and Backups

CenturyLink has a disaster recovery program known as Safehaven from Data Gardens. Safehaven for CenturyLink Cloud is a solution that offers protection for production workloads in a cost effective, low investment model. SafeHaven for CenturyLink Cloud protects both at the level of virtual IT infrastructure (VMs and data volumes) and at the level of active business processes. Customer benefits include:

- Enterprise-class disaster recovery with recovery at the site, group, or resource level
- Live VM migration back-and-forth to the Cloud Provider
- Configurable RPO with no data loss for most failure scenarios
- RTOs in minutes
- Automatic failure detection and reporting
- Live recovery audits Disaster Recovery is a complex topic area and that there are many protection strategies to achieve the desired results. We created this service offering in response to customer feedback as yet another option for our customers to protect their production IT environments.

We also recognize this solution is not a panacea for DR; rather it's a solution oriented tool that may help you service certain production workloads in a cost effective, low investment model. And for those workloads that require a different protection technique we have the depth of resources to help you realize your goals.

Additional CenturyLink Security Features and Services

In addition to the security features and services provided in CenturyLink Cloud, CenturyLink offers many others that go beyond the basic platform capabilities. Some of these services require consultation and customization by CenturyLink. In other cases, CenturyLink makes it possible for the customer to install and configure specialized security software or add third party security services to their accounts.

Security Aspects of Managed Platform Services

CenturyLink gives customers the option of ordering managed operating system and application services. For example, the customer can have CenturyLink set up and manage Windows Server running IIS or Active Directory, RedHat Linux machines running Apache Tomcat, Cloudera, and so forth. With these managed services come certain built-in security features and various security options.

CenturyLink managed services are run on the same secure CenturyLink Cloud infrastructure that is used for all customer cloud instances. We also secure our managed Operating Systems with industry-standard (McAfee) anti-virus protection, regular virus and malware signature updates. Managed Operating Systems come with basic OS-level hardening, such as closed ports, to mitigate risk. Support is available for all critical and vendor-recommended patches, though the customer must request patching based on their specific corporate policies. This includes keeping the system current with all patches and "hot fixes" to help prevent security compromises or operational reliability issues. CenturyLink ensures that only OS vendor-recommended patches are installed.

Managed Services are set up for uniform baseline security using a "blueprint" that configures the OS and application with CenturyLink's standard security policies. We employ a shared domain controller to authorize customer administrators. With this approach, a customer administrator cannot access any managed services product except their own. Only CenturyLink staff can access multiple customer managed service instances.

Managed Security Service

CenturyLink's Managed Security Service reduces the costs and complexities associated with comprehensive threat protection and Internet security by providing flexible, around-the-clock protection against known and unknown Internet threats. Managed Security Service provides comprehensive threat protection, options for malware mitigation, Web filtering, spam filtering, access control, and VPN support. As a managed security service provider, we offer 24/7 monitoring, management, and support-including easy visibility into service information through an online self-service portal. Services include:

- Service Configuration and Implementation
- Service Support
- Fault Management and Escalation
- Managed Security Service offers 2 levels of service:
  - Managed Firewall: Firewall policy between network and the Internet, plus IPSec VPN support.
  - Comprehensive: Managed Firewall features, plus email defense and URL filtering.

Logging Services

CenturyLink logs multiple streams of activities in its cloud datacenters. Selected logs are available to customers as needed. By default, CenturyLink does not do OS level logging. However, we do have optional services available to provide a complete logging solution based on LogLogic and Tibco based solutions.

Data Encryption

With IaaS, the customer is responsible for data encryption. However, we offer guidance on best practices and enable customers to use many different encryption technologies and third party providers in their cloud instances, including Vormetric. The Vormetric Data Security Platform offers an enterprise cloud security solution that can help you address compliance concerns that delay or minimize the migration of sensitive assets into private, public and hybrid clouds with its robust, comprehensive security capabilities. For instance, we recommend encrypting data at rest and encryption at the application level, not at the OS layer. This practice helps mitigate the risk of unauthorized data access by an entity that has attained access to the OS.

Anti-Virus

Anti-Virus is a customer security responsibility, though CenturyLink is able to facilitate the use of many third party anti-virus tools. Nessus vulnerability scanning is also available.

E-mail Defense

CenturyLink's Email Defense safeguards the customer's business from unsolicited spam e-mail, viruses, worms before they can enter the network. This is a gateway-based managed security service that filters and cleans e-mail from the Internet before it reaches the customer's network. The service can also block inappropriate content coming in and going out, and prevent e-mail malware from infiltrating the network.

- E-mail Defense Features
- Spam blocking
- Gateway-based content filtering
- Virus scanning and worm detection
- Web-based interface for monitoring and administration
- No additional hardware or software required
- E-mail backup support
- Automatic user account provisioning and reporting
- Customized allow lists and deny lists
- Customized threshold levels
- Quarantine reports
- 24/7 support

Network Security Services from CenturyLink

CenturyLink's network security assessment services can help protect the customer's business against all these threats. Table 2 summarizes the Security Service offerings. Our security experts will analyze and assess data vulnerabilities and then design and implement a portfolio of solutions to help build you a better data security system.

PROFESSIONAL SECURITY SERVICES	HOW WE PROTECT CUSTOMER DATA
Penetration Testing	Identify attempts to exploit vulnerabilities to gain access to systems and information from either WAN or LAN.
Web Application Security Reviews	Assess web applications for various vulnerabilities and misconfigurations.
Information System Security (INFOSEC) Risk Assessment	Perform a 16-area network security risk assessment based on the NSA's INFOSEC Assessment Methodology (IAM) guidelines and ISO standards, creating a roadmap for how to improve your current situation.
War-Dialing / VoIP Security Testing	Discover and test analog devices and VOIP systems.
Wireless Reviews	Use various hacking techniques to discover, identify, and penetrate WEP- and WPA-protected wireless network threats.
System Interrogation / Architecture Reviews	Review system configurations, architecture, and policies for compliance with minimum security baselines.
Security Program Manager	Build, implement, and manage the enterprise security architecture as a co-sourced security offering.
Data Forensics	Develop an incident response program, and provide preservation of data services and expert testimony.
Cross Compliance Support	Develop a cross-utilized matrix for each regulation to reduce scope and increase efficiency (GLBA, HIPAA, SOX, PCI, FISMA, NERC CIP, TG-3, etc.)
Security Design & Implementation	Plan, deploy, integrate, and configure a system to support information security architecture.

Table 2 – CenturyLink Security Services

Secure IP Gateway

Secure IP Gateway, offered through CenturyLink IQ Networking Enhanced Port, diverts Internet traffic designed to meet customer-defined security policies. This is one of the most secure methods for connecting your on-premises infrastructure to our cloud, hosting and colocation services. Secure IP Gateway provides a convenient and cost-effective solution that eliminates the need to maintain separate network ports and premises-based firewall services. Features include:

- OC-192/Nx10Gig E IP backbone network
- Flexible QoS functionality (available on the Private Networking side of Enhanced Port)
- Single port combines Internet & private corporate enterprise traffic
- Any-to-any connectivity
- Optional Secure IP Gateway firewall with customer-defined NAT and firewall policies for each port
- Multiple access and port speeds ranging from DS-1 to OC48 and Ethernet access from 1 Mbps up to 10 Gbps

Web Defense

Web Defense, powered by McAfee, is an easy-to-use business Internet security solution. By routing client web traffic through CenturyLink Web proxy server, the web security solution enables the client to conduct business on the Internet more safely and cost-effectively. Web Defense effectively blocks quickly evolving Web threats, including spyware, viruses, and phishing attacks. It also helps prevent access to inappropriate sites. Web Defense adds several necessary layers of protection by enabling administrators to enforce policies that prevent users from accessing popular Web mail sites and fraudulent phishing sites.

Web Security Service

CenturyLink Web Security service features protection of the customer network, including remote users. It provides continuous updates to protect against the latest threats and reliable, around-the-clock service and support. The service includes a wide variety of threat activity and Internet usage reports. Benefits include:

- Lower IT costs associated with removing malware from infected personal computers (PCs)
- Reduce business disruption
- Increase network capacity by limiting on-the-job surfing and blocking unauthorized bandwidth-intensive downloads
- Increase employee productivity
- Effectively enforce Internet usage policies
- Limit employee access to inappropriate content

Conclusion

CenturyLink Cloud is entrusted with hosting many sensitive, business-critical systems for clients that include some of the world's largest corporations. This guide describes how CenturyLink Cloud manages security for its clients. It starts by reviewing CenturyLink's "Shared Responsibility Model" for security. The guide outlined the CenturyLink Cloud security features, processes and best practices used to secure the cloud platform and its data and explains the role of customer and provider for managed services. It went into detail on change and incident management, data and storage segregation, cage protection, personnel policies, access controls, network security, compliance and audit frameworks, replication, and disaster recovery.

Please note that this guide did not go into specifics about CenturyLink Cloud's compliance programs. A subsequent guide will go into depth on this topic and will be available later this year (2015).

Additional Resources

Web Pages and Blog Posts

- CenturyLink Cloud Security Web Page
- Five Features to Secure Your Cloud Future
- Complete list of IDP/IDS supported "screens"
- The Six Commandments of Achieving Isolation in a Multi-Tenant Cloud Environment

Relevant Knowledge Base Articles

- Managed Services KB Articles
  - Managed Services FAQ
  - Managed OS Patching and Updates
- Ticket Prioritization Matrix
- Authentication Overview
- Creating Cross-Data Center Firewall Policies
- Connecting Data Center Through Firewall Policies Security Scanning
- Creating a Self-Service IPsec Site-to-Site VPN Tunnel
- Roles FAQ
- Practical Guide for Using Roles
- Using SAML for Multi-Factor Authentication to CenturyLink Control Portal
- Add CenturyLink Personnel to a Role in Control

Appendices

Role Permissions Matrix

(Excerpt of full matrix. To see the entire matrix, visit http://www.ctl.io/knowledge-base/

Capability	Account Administrator	Account Viewer	Billing Manager	DNS Manager	Network Manager	Security Manager	Server Administrator	Server Operator
Account Billing								
Change account company info	x					x		
Change payment method details	x		x					
View account company info	x	x	x	x	x	x	x	x
View billing details	x	x	x					
View billing overview	x	x	x					
View billing usage history	x	x	x					
View payment method details	x		x					
Account Branding								
Change customer support settings for an account	x					x		
Change site branding title, logos, and color scheme	x					x		
Edit email templates and email signature	x					x		
View customer support settings for an account	x	x	x	x	x	x	x	x
View email templates and email signature	x	x	x	x	x	x	x	x
View site branding title, logos, and color scheme	x	x	x	x	x	x	x	x
Account Management								
Change sub account settings	x					x		
Create a new sub account	x					x		
Re-enable a sub account	x					x		
Suspend a sub account	x					x		
View list of sub accounts	x	x	x	x	x	x	x	x
View sub account settings	x	x	x	x	x	x	x	x
Account Notification								
Change notification contacts	x					x		
View notification contacts	x	x	x	x	x	x	x	x
Account Settings								
Add custom field associated with account	x					x		
Change account settings for site footers, default DNS	x					x		
Change custom field associated with account	x					x		
Delete custom field associated with account	x					x		
Disable a data center for an account	x					x		
Enable a data center for an account	x					x		
View account settings for site footers, default DNS	x	x	x	x	x	x	x	x
View custom fields associated with account	x	x	x	x	x	x	x	x
View list of preferred data centers	x	x	x	x	x	x	x	x

About CenturyLink Cloud

CenturyLink Cloud is the complete platform to easily manage your entire business application portfolio, from application development to business-critical workloads across public and private cloud infrastructure. CenturyLink Cloud offers high-performance, scalable, self-service virtual machines across our global network of data centers. Built-in automation, orchestration, and management tools provide a flexible, scalable, cost effective IT-ready and developer-friendly platform.

For more information, visit www.ctl.io.

About CenturyLink Business

CenturyLink Business delivers innovative managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in cloud infrastructure and hosted IT solutions for enterprise customers. Parent company CenturyLink, Inc. is the third largest telecommunications company in the United States, and empowers CenturyLink Business with its high-quality advanced fiber optic network. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations.

For more information visit www.centurylink.com/technology.

Global Headquarters
Monroe, LA
(800) 728-8471

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6591 8824

CenturyLink® Business