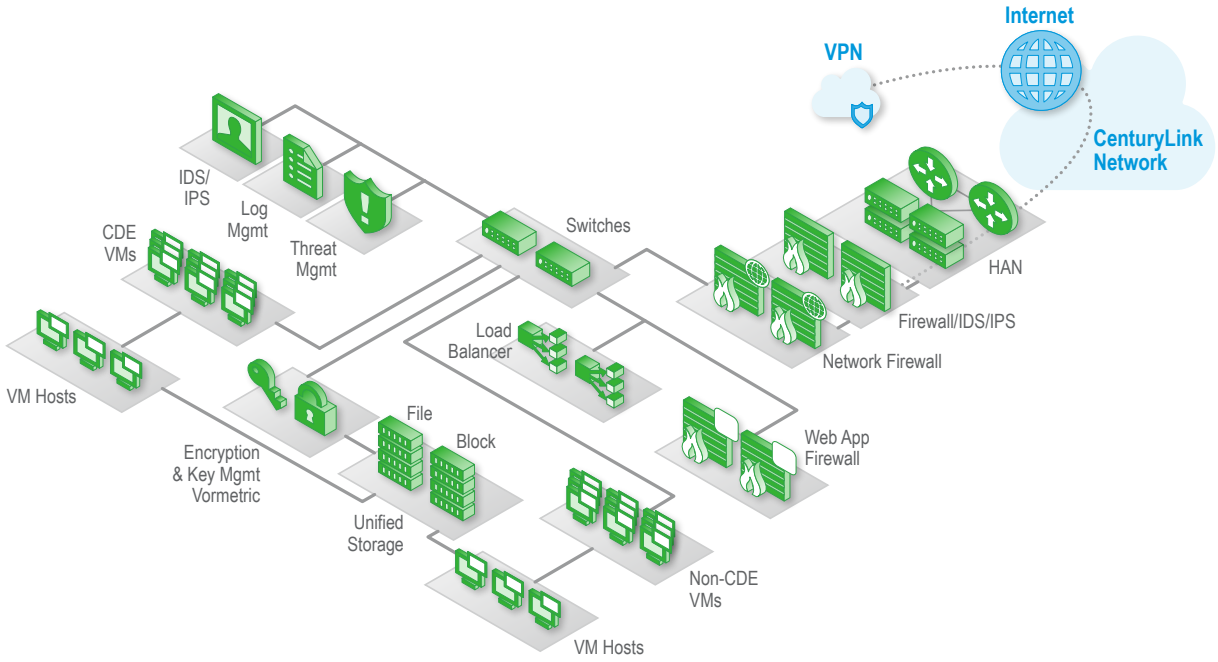
REFERENCE ARCHITECTURE

CenturyLink® Security: PCI DSS Compliance

CenturyLink achieves PCI compliance for your data through strict adherence to required guidelines, policies and procedures, including multiple firewalls as well as encryption and key management.



PCI is the security certification that applies to any organizations & merchants that accepts, transmits or stores any credit cardholder data. If any customer of an organization ever pays the merchant directly using a credit or debit card, then the PCI DSS requirements apply.

CenturyLink has PCI DSS compliant solutions and is a listed service provider on the VISA PCI Compliance Directory. We've obtained the following passing Reports On Compliance (ROC):

Data Center Services
Physical and administrative security controls in the majority of CenturyLink branded data centers

Managed Firewalls and NIDS Services
Cisco ASA and Check Point firewalls, and Network Intrusion Detection Systems (NIDS)

In addition to delivering PCI compliant solutions, CenturyLink developed a detailed matrix of PCI controls for organizations with broader PCI requirements, customizable for each solution specifying the responsible party for each PCI control. In addition, it is appended to a PCI Addendum which defines CenturyLink's commitment with respect to the matrix.

Technical Specifications

Dedicated managed firewall service with intrusion detection & prevention
- Install and maintain a firewall configuration to protect cardholder data. PCI REQ. 1.1 – 1.5

Dedicated managed web application firewall
- Install and maintain a firewall configuration to protect cardholder data. PCI REQ. 1.1 – 1.5
- Develop and maintain secure systems and applications. PCI REQ. 6.1 – 6.7
- Regularly test security systems and processes. PCI REQ. 11.1 – 11.6

CenturyLink® Security: PCI DSS Compliance

Vormetric encryption and key management

- Cardholder protection methods such as encryption, truncation, masking and hashing. PCI REQ. 3.1 – 3.7

Managed VPN with two-factor authentication

- Encrypt transmission of cardholder data across open, public networks. PCI REQ. 4.1 – 4.3

Managed threat management security scanning and penetration testing

- Develop and maintain secure systems and applications. PCI REQ. 6.1 – 6.7
- Regularly test security systems and processes. PCI REQ. 11.1 – 11.7

Managed intrusion detection & prevention (IDS/IPS)

- Develop and maintain secure systems and applications. PCI REQ. 6.1 – 6.7
- Regularly test security systems and processes. PCI REQ. 11.1 – 11.7

Log management

- Restrict access to cardholder data by business need to know. PCI REQ. 7.1 – 7.3
- Identify and authenticate access to system components. PCI REQ. 8.1 – 8.8
- Track and monitor all access to network resources and cardholder data. PCI REQ. 10.1 – 10.8

The CenturyLink Products and Services illustrated in this document are guidelines for implementing a PCI compliant solution using Dedicated Cloud. Attaining overall PCI compliance remains the responsibility of the Customer.

CenturyLink® Business