CenturyLink Anti-virus Management Services
Networx Service Overview

Get the Security of Comprehensive Protection

CenturyLink's Antivirus Management Services (AVMS) safeguard Agencies' public and private networks and application servers from malicious content. CenturyLink leverages industry-leading AVMS software and hardware components, so your Agency can enjoy robust antivirus safeguards, all as part of CenturyLink's comprehensive data protection service. CenturyLink's AVMS is expertly designed and engineered by our staff of certified security professionals. CenturyLink's AVMS is one of the many solutions we offer within CenturyLink's Security Services suite.

Features

CenturyLink's AVMS provides the following features:

- Perimeter protection, through the gateway antivirus appliance, by scanning all traffic entering/leaving your Agency's intranet.
- Protects your Agency's application servers from viruses that could originate within your Agency's intranet.
- Isolates suspicious files for off-line analysis, disinfection, or deletion.
- Automatic reporting of virus disinfection or quarantine activity by the gateway or server to appropriate central management consoles; and in the case of e-mail, to the sender and recipients.
- Automatic updating of virus definitions from a centrally controlled resource.
- 24x7 monitoring of events (and the ability to intercede as requested by your Agency) by the CenturyLink Managed Security Services (MSS) Team's Security Operations Center (SOC).

Benefits

- Compliance with the Federal Information Security Management Act (FISMA)
- Customized development and deployment of appropriate policies and infrastructure to protect your Agency's information assets
- Centralized monitoring and control of perimeter and critical Agency server antivirus efforts, 24x7 from CenturyLink's SOC
- Automatic maintenance of current virus definitions
- Ability to rapidly respond and centrally manage a virus incident requiring application of specialized virus definition/remediation patches
- Access to the expertise of security professionals from our Managed Security Services Team

Geographic Availability: Available world-wide

How it Works

Gateway-Based AVMS

Perimeter gateway appliances are installed at appropriate points of interface between your Agency, other Agencies and/or the Internet. These appliances scan all inbound and outbound traffic for:

- Known viruses (from the virus definition database)
- Behaviors and patterns that may indicate the presence of viruses
- Malicious mobile code
- Different strains of polymorphic viruses
- Viruses residing in encrypted messages and compressed files
- Viruses in different languages (e.g., JAVA, ActiveX, Visual Basic)

Contact your CenturyLink Representative today!
Visit GSANetworx.com and click on "Locate your Account Manager".
Or contact the CenturyLink Customer Support Office: 866-GSA-NETWorx
(866-472-6389) Email: federal@CenturyLink.com

CenturyLink™ Government

- Trojan horses and worms
- Macro viruses

In the event of an identified threat, the item is quarantined and a report is sent to CenturyLink's SOC for investigation. Trained security professionals take immediate action, including notifying your Agency to take preventive measures to thwart the attack.

Server-Based AVMS

Server-based AVMS are provided using host-based client applications loaded on each application server to be protected. Each application server on which an AVMS client has been loaded will be associated with an AV Library Server provided by your Agency. CenturyLink's MSS Team will load the Virus Definitions and the Quarantine Repository software on the AV Library Server. CenturyLink's MSS Team will update the AV Library Server with periodic updates of software and virus definitions from the AV product vendor.

The host-based agent provides real time scanning of all inbound and outbound traffic to the protected server. Additionally, this agent can respond to a scheduled full scan (of all memory and disk drives) command or a one-time SOC-originated command to perform a full scan. The agent also produces activity reports and alerts that are routed to the CenturyLink MSS Team for review.

When any scan by the host-based agent identifies a suspect file, the agent takes action according to your Agency's defined rules. Options include:

- Disinfecting the file, with deletion or quarantine as alternate actions if disinfection fails
- Sending the file to the designated quarantine location (typically the AV Library server)
- Deleting the file

Why Buy from CenturyLink?

- CenturyLink provides a comprehensive service that is vendor and device independent. This allows your Agency to retain its current infrastructure and simplifies future technology refresh decisions.
- CenturyLink's AVMS provides a flexible solution to protect public and private networks.
- CenturyLink's AVMS provides specific application servers which frees resources to pursue Agency missions.
- CenturyLink offers a broad range of expertise in defense modernization efforts, intelligence and homeland security.

Other Security Services Available from CenturyLink

CenturyLink provides a comprehensive data protection services portfolio. When combined in a managed service, your Agency will benefit with extensive threat mitigation and protection capabilities across your Agency's private and public networks. Other CenturyLink security services include:

- Managed Firewall Service
- Intrusion Detection and Prevention Services
- Incident Response Service
- Managed E-Authentication Service
- Secure Managed E-mail Service
- Vulnerability Scanning Service
- Managed Tiered Security Service

Contract Vehicle

Networx Universal & Enterprise

- An overview of CenturyLink's contract is available on the CenturyLink Networx Website at http://www.gsanetworx.com

Contact your CenturyLink Representative today!
Visit GSANetworx.com and click on "Locate your Account Manager".
Or contact the CenturyLink Customer Support Office: 866-GSA-NETWorx
(866-472-6389) Email: federal@CenturyLink.com

CenturyLink™ Government