CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Managed NIDS Care Services

This Service Guide ("SG") sets forth a description of CenturyLink Managed NIDS Care Service ("Service") offerings including technical details and additional requirements or terms, if any. This SG is subject to and incorporated into the Master Service Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order.

Products Included

Managed NIDS Care in the IDC, Managed NIDS at Customer Premises

Version	Previous	Section Modified	Date
SEC-20140430-SG-ManagedNIDSCareServices	SEC-20091208-External-SSG-GL-Managed_NIDS_Care_Services	Rebrand	April 30, 2014

Table of Contents

Managed NIDS Care in the IDC

Service Description

The Service provides managed intrusion detection with 24/7 monitoring and response to computer security incidents. The Service includes installation, 24/7 monitoring and support of Customer-owned Cisco NIDS devices.

The Managed Network Intrusion Detection System (NIDS) Care Service is a dedicated Network IDS residing in the CenturyLink managed security facility or Customer's server-hosting facilities at CenturyLink. The NIDS is capable of monitoring one point on the network. The service includes customized on-site NIDS monitoring and a separate management console device.

Common Service Description

Common service elements including the description of installation, configuration, Service inclusions and exclusions, monitoring, and other service details common across Managed Security Services are defined here. These service elements are in addition to specific Service details provided within the body of each SG offering.

For a full description of common SG Managed Security Service elements, please reference the ***Common Service Description*** section.

Included in Service

The following Service elements are included in this Service,

- A dedicated Network IDS residing in the CenturyLink managed security facility. The Network IDS is capable of monitoring one point on the network.
- Access to CenturyLink managed security web portal where IDS alerts are available for customer review.

Installation

CenturyLink will provide customized on-site NIDS management and monitoring.

Customer Installation Requirements

The following Customer Installation Requirements apply to this Service,

- Customer must maintain a supported platform and associated support contracts
- Customer must provide IP addresses for all network connections to the NIDS device and the secure management device, the number of which will be determined by CenturyLink.
- Give CenturyLink and others working for CenturyLink access to equipment as follows:
    - Immediately if there is a service outage
    - At reasonable times in all other situations.
- If the Customer has an ACL that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.
- Customer must allow CenturyLink personnel to access the NIDS device, where CenturyLink determines such access is necessary to deliver the service or respond to a security incident.

Maintenance and Support

The following Maintenance and Support element applies to this Service,

- CenturyLink will work with the NIDS hardware or software manufacturer to facilitate repair of hardware. CenturyLink will assist in the reinstallation of the required equipment, but any other repairs or parts costs are the Customer's responsibility.

Managed NIDS Care Service at Customer Premises

Service Description

The Service provides managed intrusion detection with 24/7 monitoring and response to computer security incidents. The Service includes installation, 24/7 monitoring and support of Customer-owned Cisco Network IDS devices. The Service provides management and monitoring services for a dedicated Network IDS residing at the customer premise. The Network IDS is capable of monitoring one point on the network. The service includes a separate management console device.

Common Service Description

Common service elements including the description of installation, configuration, Service inclusions and exclusions, monitoring, and other service details common across Managed Security Services are defined here. These service elements are in addition to specific Service details provided within the body of each SG offering.

For a full description of common SG Managed Security Service elements, please reference the Common Service Description section.

Included in Service

The following Service elements are included in this Service,

- A dedicated Network IDS. The Network IDS is capable of monitoring one point on the network.
- Access to CenturyLink's managed security web portal where IDS alerts are available for customer review.
- Remote managed services via an on-site secure modem, which gives CenturyLink access to the NIDS device over a dial-up connection.

Not Included in Service

The following Service elements are excluded from this Service,

- Management network connection, which must be purchased separately.
- NIDS hardware and/or software.
- On-site spares.

Customer Requirements

The following Customer Installation Requirements apply to this Service,

- Customer must maintain a supported platform and associated support contracts

- Customer must provide CenturyLink with a topology of their existing network prior to security review and installation of the equipment.
- Customer must provide IP addresses for all network connections to the NIDS device and the secure management device, the number of which will be determined by CenturyLink.
- Ensure that all permissions of any kind needed for the installation and operation of CenturyLink-owned equipment are in place at all times.
- Give CenturyLink and others working for CenturyLink access to equipment as follows:
    - Immediately if there is a service outage
    - At reasonable times in all other situations.
- If it is not already available the Customer must purchase an always-on connection to the public Internet (DSL, T1, cable modem etc.) Dial-up connection is not sufficient.
- If the Customer has an ACL that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.
- Customer must allow CenturyLink personnel to access the NIDS device, where CenturyLink determines such access is necessary to deliver the service or respond to a security incident.

Maintenance and Support

The following Maintenance and Support element applies to this Service,

- CenturyLink will work with the NIDS hardware or software manufacturer to facilitate repair of hardware. CenturyLink will assist in the reinstallation of the required equipment, but any other repairs or parts costs are the Customer's responsibility.

Incident Response ("IR")

Incident Response ("IR") is initiated by or with the consent of the Customer upon the occurrence of a suspicious event or condition indicating a possible compromise of the Customer's digital security. An IDS or IMS alert, the Customer, or other indicators may signal this event or condition.

For a full description of the included Incident Response ("IR") service elements, please reference the ***Incident Response ("IR")*** documentation.

Common Service Description

The following service definitions apply to all CenturyLink service offerings describe in this SG. Any Service definition specific to individual Service offerings will be defined within the body of the Service offering.

Not Included in Service

The following are not included in the Service offering,

- Management of the Customer's internal network.
- Support over any protocol other than TCP/IP.
- Permanent archival storage of log files.
- Internet Access.
- Incident Response, which must be purchased separately.

Customer Installation Requirements

- The Customer should consider this service as just one tool to be used as part of an overall security strategy, and not as a total solution. If the Customer wants to expand their overall security strategy, they should contact their designated CenturyLink Account Executive for further information on additional CenturyLink security services and offerings.
- CenturyLink will manage all system administration and NIDS passwords. Customer will not have access to NIDS passwords or be able to make direct changes to the NIDS configurations. Instead, Customer must request changes by contacting the CenturyLink Response Center. Customer must provide complete authentication credentials to the CenturyLink Response Center when requesting changes. (Changes and updates to this process are available at http://CenturyLink.net/customer/techsuppt.html).
- Customer must not have sustained bandwidth exceeding rated capacity of the device, without resulting degradation in service.
- The Customer will, using CenturyLink's standard procedures, notify CenturyLink of the initial and later changes to the NIDS information to be configured by CenturyLink with the NIDS device.
- Customer must purchase Installation and a minimum of 40 hours of Incident Response with any NIDS service listed on this CenturyLink Service Guide.
- Customer shall not, and shall not permit or instruct any other party to, take any action that would reduce the effectiveness of the Network IDS Service or any device used to deliver the service. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled penetration testing or external network scans.
- The Customer must notify CenturyLink in advance of any network topology or system changes that may affect the IDS or the effectiveness of the IDS policy. Failure to notify CenturyLink of system changes may result in the inability to monitor traffic or the generation of false alerts. CenturyLink will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, CenturyLink may modify the IDS configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents.
- For NIDS devices that are not installed within a CenturyLink Utility Hosting Environment, the Customer must provide the necessary space, power, environmental conditions and security precautions at each Customer site, and otherwise prepare the site for IDC hardware as follows:

Item	Requirement
Physical Environment	Predefined and adequate rack shelf or tabletop space for installation, with unobstructed entry for CenturyLink and others working for CenturyLink.
Electrical Power	Electrical outlets for both the NIDS devices and the secure management console
	Extension wiring available if distance to electrical outlets is greater than 6 feet.
	Power supply ready at installation location

Item	Requirement
LAN Connectivity	Ethernet LAN topology (for NIDS device)
	Extension wiring if the distance to the NIDS connection is greater than 6 feet.

Response Times

CenturyLink's response notification for this Service is defined as follows,

Event	Response Time
IDS Critical Alerts	CenturyLink personnel will review critical alerts within 15 minutes and notify Customer within 60 minutes, by telephone, pager or electronic mail, as required by Customer, upon receiving a HIDS alert deemed critical by CenturyLink.
IDS Configuration and Policy Change	CenturyLink will respond to configuration and policy change requests within 12 business hours.
IR Consulting	CenturyLink will respond to Incident Response request within the timeframes designated by the IR CenturyLink Service Guide (provided separately).

Upgrades

CenturyLink may periodically upgrade the firewall software to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the normally scheduled Internet Data Center (IDC) maintenance window. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer

Additional Charges

The Customer will incur additional charges if CenturyLink dispatches a technician to a Customer site to install a device on a date agreed with the Customer, and the technician must return to the Customer site to complete the installation because the Customer was not ready when the technician first arrived at the Customer site.

Optional Security Services

The following Security-related services are available through CenturyLink's Professional Services organization, and are not included with the Service:

- Application Security Review

- Network Penetration Testing
- Risk Assessment Services
- Security Architecture & Design
- Security Account Manager (SAM) Service
- Security Policy Creation & Documentation

For more details regarding the services outlined above, please contact your CenturyLink Account Executive.

Monitoring

- CenturyLink incident response personnel receive and review alerts issued by the NIDS sensor(s) according to the response time chart provided below. Sensors generate alerts upon encountering network traffic patterns that may indicate suspicious activity.
- CenturyLink will, upon Customer's request, provide a bi-annual review of the Customer's NIDS policy and log summary. Each review (up to 8 hours per review) may be conducted telephonically. To initiate a bi-annual review, the Customer should contact the response center to open a ticket.
- CenturyLink will provide the Customer with access to NIDS alert reports for the previous 90 days via a secure Web-based interface.
- Where practicable, CenturyLink may implement various health checks such as ICMP (e.g., ping) monitoring and pre-set test event triggering of the NIDS sensor to determine system availability (24/7). Due to network design issues, these health checks may not be available for all monitored devices.
- In the event that the NIDS fails to respond, CenturyLink will notify Customer via phone and/or email and initiate corrective action.

Maintenance and Support

- 24/7 support for NIDS problem resolution and Customer inquiries are included.
- Secure and encrypted management connections are included.

Additional Service Requirements

Response Times SLA

In the event that CenturyLink is unable to provide service within the “Response Time” windows outlined above, the Customer’s sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure. In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer’s credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. “Excluded Event” means any event that adversely impacts the Service that is caused by,

- the acts or omissions of Customer, its employees, customers, contractors or agents
- the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink
- Force Majeure events
- scheduled maintenance
- any suspension of Service pursuant to the Agreement
- the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer shall,

- provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
- not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.
- Notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
- purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialing) for each Customer Site to enable CenturyLink to perform remote network management functions.
- designate and maintain a Customer Contact during the Service Term (including current contact information). “Customer Contact” means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and
- access to address configuration issues, event notifications, system or infrastructure
- modifications and authentication of applicable CenturyLink systems. f) For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those
- included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer’s compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:

- Customer impairs the Service;
- CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived; or
- Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.