# SERVICE SCHEDULE FOR THREAT MONITORING AND DEFENSE

**SERVICE DESCRIPTION:**

This Service Schedule describes and contains additional terms that apply to EarthLink's Threat Monitoring and Defense (the "Service"). This Service Schedule supplements, or amends and restates, each Agreement for Service, the Network Service Agreement or any other applicable agreement for the provision of services entered into by Customer with the applicable EarthLink entity and any applicable tariffs, which are specifically incorporated into this Agreement by this reference. ("Agreement") used to order the Services by the Customer identified in the Agreement ("Customer") and the other documents comprising the Agreement between the Customer and EarthLink with respect to providing, accessing and using the Service (collectively, the "Agreement") as follows:

Service Overview. EarthLink's Threat Monitoring and Defense offers monitoring of your Point of Sale (POS), endpoints, laptops, workstations, routers, servers, and network equipment to alert you of suspicious security events according to your service selection tier.

Detailed description of various service components associated with Threat Monitoring and Defense service are included below:

Threat Manager:

Threat Manager is a managed intrusion detection solution with built-in vulnerability assessment scanning including PCI scans. Unlike other intrusion prevention systems, host vulnerability assessment information gathered by Threat Manager is automatically correlated by an expert system with deep packet traffic analysis to suppress false attacks and provide the customer with detailed insight into the nature of the attack and its risk to the environment. This allows the system to identify threats as they evolve or unfold over minutes, hours or days. All updates, upgrades, and infrastructure required to deliver the service are included as a part of service. The client can configure scans, dashboards, and reports according to their internal requirements.

Key Benefits

- Patented 7-Factor Threat Scenario Modeling - purpose-built grid computing infrastructure, with the ability to automatically aggregate and correlate anomalous behavior patterns to quickly identify threats and attacks to your network - reduces false positives and improves threat detection.
- Optional SSL Decryption module that actively decrypts SSL traffic and enables customers to detect attacks that may be injected over encrypted SSL channels.
- Regularly scan internal and external networks—whenever and as often as you choose
- Global threat visibility incorporates thousands of sensors into the expert system's decision process
- Comply with a wide range of regulatory mandates (PCI DSS, SOX, HIPAA, GLBA, etc.) with audit-ready reports
- 24x7 Security Operations Center (SOC) provide around-the-clock monitoring services
- Use custom reports or leverage the dozens of out-of-the-box dashboards and reports to effectively track and manage security incident activity
- Easy-to-use web console to view reports, run queries and perform drilldown analysis from any browser
- SaaS delivery model means quick deployment with minimal capital investment
- Integrated ActiveWatch services provide shared SOC monitoring services at a fraction of the cost

ActiveWatch for Threat Manager:

ActiveWatch builds upon the Threat Manager foundation to provide 24x7 monitoring and expert guidance services from state-of-the-art Security Operations Center (SOC). The ActiveWatch team augments your existing IT team to ensure rapid detection and response to network incidents, around the clock. It delivers customized tuning and customization of the Threat Manager IDS to fit the unique needs of customers.

Key Benefits -

- Telephone notification of incident from security professionals working in the Security Operations Center (vs. e-mail notification for Threat Manager-Only service)
- 60 minute response upon discovery of incident
- Human expert analysis of all incidents
- Incident and remediation response advice
- Cost-effective, turnkey security at a fraction of the cost of an in-house dedicated, Security Operations Center.

- Improve the breadth of coverage for network security monitoring to include off-hours time windows when attacks are more likely to happen.
- Ensure end-to-end coverage for PCI-DSS requirement 11.4.
- Enables staff to focus on business-critical initiatives without the capital expenditures, deployment headaches, training and other commitments required for self-managed solutions.

Log Manager:

Log Manager offers log collection, archival, search, customizable reporting. The customer must configure sources to be collected, set up alerting rules, and build reports to satisfy internal needs. Support is available to assist with rule or report creation.

Key Benefits -

- Meet compliance requirements for log management, such as PCI, HIPAA, and others
- Increase IT security posture with greater visibility into asset activity via log message data
- Collect logs from virtually any environment (public, private, hybrid clouds, on-premise)
- Store log data safely in our SSAE 16 Type 2 verified, redundant data centers
- Access dozens of out-of-the-box reports and dashboards
- Utilize cloud-powered infrastructure that provides powerful search, analysis, and forensic capabilities
- Correlate events, set automatic alerts, and schedule reoccurring reports
- Prepare for compliance audits and security events

ActiveWatch for Log Manager:

ActiveWatch for Log Manager enables you to turn data from your daily logs into security intelligence that helps to protect your IT infrastructure. ActiveWatch for Log Manager is a managed service that delivers 24×7 analytics and continuous security monitoring of your log data, identifying potential security and compliance issues that could be impacting your organization. ActiveWatch for Log Manager not only identifies security issues, but also provides you with the recommended steps you need to resolve the issues.  SLA is 60 minutes.

Key Benefits -

- Dedicated 24×7 security monitoring by certified experts
- Incident identification from a variety of sources, such as network devices, operating systems, and other security products
- Automated log review that meets the requirements of PCI DSS 3.0
- Correlation rules library designed to identify the most common threat vectors and security issues
- Up-to-date threat intelligence and security content
- Detailed information regarding incident origins, as well as issue resolution recommendations

Log Review (for Log Manager):

Log Manager with Log Review solution brings together the technology and human expertise required to meet PCI compliance within your environment. Each day, a team of security and compliance experts from the Security Operations Center (SOC) will review your data against 21 reports designed specifically for PCI-DSS 3.0. Our team will provide you with insights into any security or compliance issues discovered and maintain an auditable case history of each daily review.

Key Benefits -

- Eliminate need for dedicated IT resources to collect, archive, and review logs on a daily basis
- Optimize time by only getting involved when action is needed
- View event log analysis reports and daily activity from our web portal
- Monitor and archive all event logs without having to worry about storage, backups, or access
- Demonstrate daily log review compliance to PCI DSS 3.0
- Cover any environment from corporate, co-lo, private cloud, public cloud, and AWS

1. **Term**: The Service can be ordered for a term of 2 or 3 years (“Term”) as set forth on the Agreement. Each Term commences at the earliest date between when the Service is available for use or sixty (60) days after the Service Agreement has been signed. (“Service Commencement Date”). The Service will continue, subject to the terms and conditions of the Agreement, as defined in EarthLink’s Terms and Conditions. Upon expiration of each Term, the Service will continue on a month-to-month basis pursuant to the terms of the Agreement, unless Customer has given EarthLink written notice of termination at least 30 days before the end of the Term. Thereafter, Customer or EarthLink may terminate the Service with 30 days advance written notice to the other Party. Any Service terminated before the end of its then-current Term is subject to the early termination fee (“ETF”) and any other charges set forth in the Agreement or that may apply through a promotional offer or otherwise.

2. **Billing and Payment:** Billing will commence on the Service Commencement Date. The first invoice will include the initial set-up fee, any installation with a pro-rated monthly recurring charge (“MRC”) for the Service from the Service Commencement Date through the date for which the invoice is issued. It will also include, the MRC invoiced monthly in advance. Thereafter, the invoice will include the MRC invoiced monthly in advance and any applicable non-recurring charges, which will be billed monthly in arrears. If arrangements for payments by credit card have been made, EarthLink may charge the Customer’s account on or after the invoice date. Unless otherwise described in this Service Schedule, all invoiced amounts are due and payable within thirty (30) days of the invoice date in accordance with the terms of the Agreement.

3. **Threat Monitoring and Defense Components Breakout:**

Using EarthLink’s advanced Threat Monitoring and Defense tools, our security engineers can remotely perform Security Monitoring functions and alert the Customer to vulnerabilities. The MyLink portal will be leveraged as the Customer interface to generate reports and to initiate moves, adds and changes, (MACD).

- As part of the threat manager service, the Security Operations team will also support a vulnerability management service that will scan Customer network and individual devices for security vulnerabilities.
- A Log Manager, installed as a virtual or physical appliance, will be provisioned to collect log information from the assigned devices to be analyzed by the EarthLink SOC.

**EarthLink Responsibilities:**

- Providing the Log Manager and the Threat Manager, (if applicable) for event log monitoring.
- Alerting Customer of security events
- Provide periodic vulnerability scanning

**Customer Responsibilities:**

Deploying the devices at each specified location.
Identifying technical points of contact and availability for escalations.
Completion of the Service Commencement Worksheet (SCW)
Corrective action based on incident response.

4. **Definitions:**

**Change Management.** Applies only to EarthLink’s change management process not a specific Customer change management. If the Customer has a specific internal change management process it will be the responsibility of the Customers Technical Contacts, to make sure that any changes to devices that fall within their scope of management go through the Customer internal change control process. Once through the Customers internal change control process EarthLink representatives can be notified with consent to perform maintenance. If the Technical Contact needs a representative from EarthLink to explain the scope and impact of the changes to their internal change management team, as far in advance as possible to allow for the proper scheduling of resources.

**Planned or Unplanned Maintenance and Remediation**. EarthLink will send notification 48 hours in advance of any planned maintenance occurring outside of the Scheduled Maintenance window and make efforts to accommodate the needs of the Customer regarding the additional maintenance requirement. EarthLink will notify Customer as soon as possible if an unplanned maintenance needs to be implemented.

**Proactive Hardware Monitoring and Management –** If hardware was provided by EarthLink and/or its partner, it is the responsibility of the provider to maintain and service the specified device.