# See More. Stop More.

## CenturyLink® Security Log Monitoring Service

The longer it takes to detect a cyber threat, the worse the consequences will be. Collecting logs and alerts on possible security breaches is never enough. Effectively mitigating attacks requires continuous monitoring of all elements within your infrastructure to identify activity that's out of the ordinary. To stay ahead, you need near-real-time incident tracking paired with expert analysis and immediate action.

CenturyLink Security Log Monitoring collects your logging events, categorizes them by severity or alerting, and prioritizes ticketed incidents that require action. Our Security Operations Center (SOC) analysts stand ready to provide additional review if needed, enabling enterprises like yours to evolve their security posture from reactive to proactive — beyond mere compliance and into active threat management.

## Business Solutions

CenturyLink helps organizations correlate security events for meaning, adding historical context and trending information, and analyzing the outcomes to quickly spot patterns that indicate malicious activity. Security Log Monitoring can be customized to your needs with our suite of optional services and upgrades.

- **Foundational Monitoring:** The core tenant of this service offers a complimentary tier of 10GB per day of log management. CenturyLink gathers raw logs, parses metadata into normalized events and retains it remotely for viewing in our portal and mobile application. As your monitoring requirements grow, you can easily accommodate additional log ingestion at reduced volume-based rates.

- **Security Analytics:** Access advanced search capabilities and extend threat detection visibility to the last 12 months, making low and slow attacks easier to recognize. Search all metadata with enhanced reporting features and visualization tools. Have your ingested data enriched with the high fidelity threat intelligence derived from CenturyLink's threat research and operations team, Black Lotus Labs, which leverages CenturyLink's expansive visibility from our global network backbone, as well as community feeds, honeypot infection records and third-party research to provide current, company-specific insight with fewer false positives. Request the creation of up to five custom correlation rules per month.

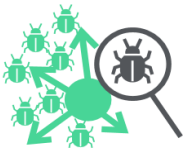
- **Cloud Security Monitoring:** Leverage threat intelligence on suspicious behavior from sanctioned applications accessed by employees in cloud service providers' environments. This gives you visibility into all your cloud environments and accounts, applying best-practice controls to cloud service configurations. Rapidly find misconfigurations and detect malicious use from inside and outside of your organization.

- **SOC Monitoring with Incident Handling:** Leverage our team of experts to reduce resource and infrastructure costs. CenturyLink SOC analysts provide 24/7 monitoring, triage and notification when an event occurs. Once incidents are detected, our Incident Handling experts will perform forensic investigation and make recommendations to restore normal operations and minimize loss or theft of information, as well as disruption of services caused by security incidents.

On average, it takes

**197 DAYS**

to detect an advanced attack.*



**How Security Log Monitoring Works**

**Collect and Forward**
CenturyLink log collection platform (Customer Premise or Data Center)

**Normalize, Correlate and Contextualize**
CenturyLink Platform (Data Center)

**Analyze and Visualize**
CenturyLink Portal and Mobile App

## Technical Features / Capabilities

CenturyLink Security Log Monitoring automates integration of the security ecosystem, simplifying setup and enabling the system to work seamlessly. Key features of the service include:

- Single sign-on service with support for multi-factor authentication
- 24/7 monitoring, proactive customer notification and escalation of items of interest
- Intuitive dashboard with customizable widgets for leads, investigations, ingestion rate and an interactive map
- Seven years of backup and storage, and visibility of up to 12 months of full-text indexed, searchable log data to investigate and provide deep context to threat trends
- Advanced asset risk profiling and unique risk-based alert process combining automation with rigorous human review to evaluate multiple transaction types: CEF, syslog, LEAF and a variety of other standard log types
- Correlation from multiple streams of data — pulling insights from both real-time events and our ATI-curated threat intelligence to detect threats with greater fidelity at the earliest stages
- Predictable, consumption-based pricing model based on volume of security-related data transmitted per day, eliminating capital expense, administration and maintenance costs
- Flexible implementation models including comanaged and maintained by CenturyLink
- No implementation costs or licensing fees for log collection appliances
- Dedicated delivery lead to oversee coordination of the onboarding process
- Incident Handling service designed to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

## Why Choose CenturyLink Security Log Monitoring Service?

**Improve Your Security Posture:** Transition from a defensive approach to an offensive strategy that addresses threats holistically.

**Gain Visibility:** See what's happening inside your infrastructure at every point — view your attack surface, monitor user activity, watch and verify SOC activity.

**Improve Operational and Cost Efficiency:** Focus your team on the events that matter and reduce the noise from false positives.

**CenturyLink combines a significant local presence with an expansive global network to keep you secure and connected — wherever business happens. We have the expertise and next-generation networking solutions to put it all to work for your organization.**

**Call** 1.877.453.8353 | **Click** centurylink.com | **Email** info@centurylink.com

CenturyLink®

* Ponemon Institute, 2018 Cost of Data Breach Study: United States, October 2018

Services not available everywhere. CenturyLink may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2018 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.