CENTURYLINK® SECURITY LOG MONITORING

TRANSFORM RAW DATA INTO ACTIONABLE INSIGHT

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. Efficiently mitigating attacks requires continuously monitoring all elements of your infrastructure to identify activity that's out of the ordinary. You need near-real-time incident tracking paired with expert analysis and immediate action.

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

Business Solutions

CenturyLink helps correlate security events for meaning, add historical context and trending information, and analyze the outcomes to quickly spot patterns that indicate malicious activity. The solution 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 threat monitoring. CenturyLink gathers raw logs, parses meta data 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.
- **Trending and Analytics:** Access advanced search capabilities and extend threat detection visibility to the last 12 months, making low and slow attacks easier to recognize. Trending and Analytics delivers the ability to search all meta data with enhanced reporting features and visualization tools.
- **Threat Intelligence:** Dig deeper into log data with intelligence from community feeds, social media searches, dark web searches, honey pot infection records and third-party research. We provide current, company-specific insight by integrating data from our extensive visibility across our global network backbone with third-party threat intelligence
- **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 of 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:** Leverage our team of experts to reduce resource and infrastructure costs. As incidents are detected, our analysts will escalate them and provide transparent access to the same event console. Stay on top of events as they arise without requiring an in-house team.

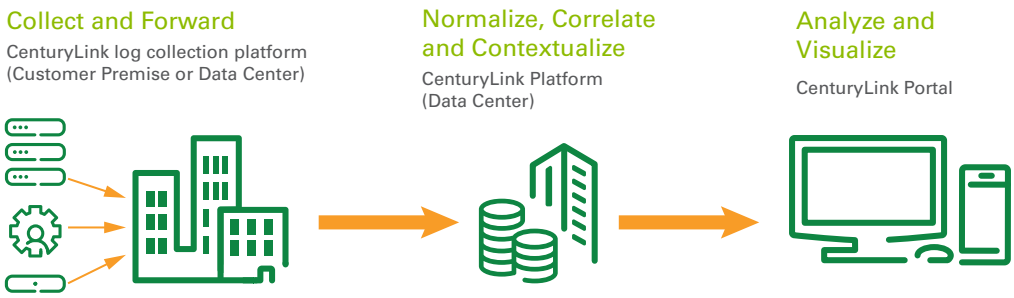
CenturyLink®

Advanced Monitoring Algorithms:

This upgrade helps identify additional items of interest and threats to your business. Advanced Monitoring Algorithms is compliance-focused for PCI, HIPPA, etc. — with more sophisticated alerting. Benefit from full library access to CenturyLink's proprietary use-cases and build and maintain your own use case libraries. This upgrade also allows you to define ten additional advanced rules each month, customized for your environment.

On average, it takes
191 DAYS
to detect an advanced attack.*

How it Works



Technical Features / Capabilities

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

- 24/7 monitoring, proactive customer notification and escalation of items of interest
- Ongoing configuration of the monitoring technology
- 7 years of backup and storage, and visibility 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 customer asset risk profiles to detect threats at the earliest stages and reduce false positives
- 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 ranging from co-managed to fully managed and maintained by CenturyLink
- No implementation costs and dedicated project manager to oversee coordination of the onboarding process
- Integrates with Incident Management and Response Service for full-service approach
- No licensing fees for log collection appliances

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

* Ponemon Institute, *2017 Cost of Data Breach Study:* United States, June 2017

CenturyLink®