CenturyLink® Business

DATA SHEET

Security Log Monitoring with Trending and Threat Analysis

Transforms Piles of Unorganized Data Into Actionable Information

When it comes to cyberattacks, the longer it takes you to detect them, the more time threat actors have to conduct surveillance, steal data and spy upon your organization -- pushing up the cost, and the consequences, of an attack.

It's never enough to simply collect logs and alerts on possible security breaches against your IT infrastructure. To find and mitigate malicious attacks quickly, you need to continuously monitor all the elements of your infrastructure, correlate the security events for meaning, add historical context and trending information, and analyze the outcomes to smartly and quickly spot trends and see patterns that are out of the ordinary. This is the job of Security Log Monitoring with Trending and Threat Analysis.

Security Log Monitoring with Trending and Threat Analysis collects and tracks incidents in near real-time, categorizing them by severity and sending them to an expert team of CenturyLink SOC analysts for review. Our security experts then cull the data and prioritize events into the top incidents that require greater analysis or immediate action.

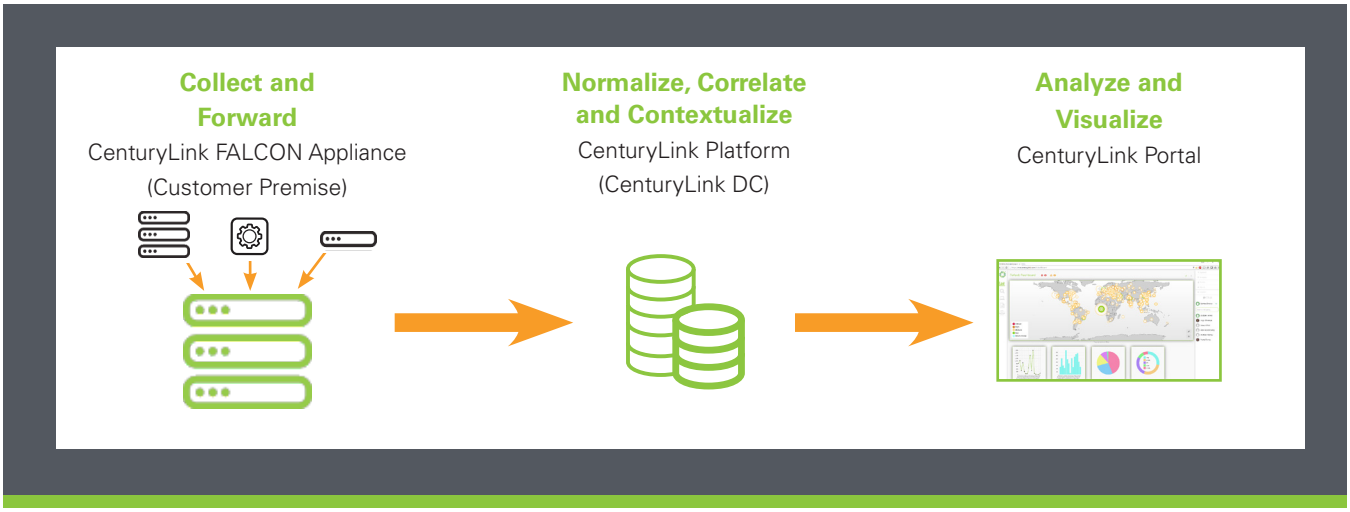
CenturyLink's advanced platform takes an industry best-practice approach to automation that weeds out a greater number of false positives than standard systems by combining log data from the risk profiles of each customer asset with near real-time threat intelligence data from CenturyLink's global corporate network and partner threat intelligence feeds.

On average, it takes

170

days to detect an advanced attack*

How It Works



1. CenturyLink-built FALCON log collection and forwarding appliance is installed in your environment and receives logs from your devices and applications including existing log management systems, SIEMs, and on-premise, hosted and/or cloud devices. Supports all syslog standards.
2. A secure connection from the FALCON appliance terminates into CenturyLink's platform where your data is normalized, correlated and enriched with threat intelligence, risk profiles and trending information, and indexed for accessing, viewing, manipulating, searching and reporting.
3. The CenturyLink® Managed Security Service Portal is the single pane of glass that allows you to visualize correlated events and the severity and priority of incidents in near real-time, leveraging role-based access to give analysts, executives, incident responders, admins and auditors the right level of access, information and tools needed to do their jobs. CenturyLink SOC analysts use the portal to continuously monitor your environment and notify you of alerts requiring attention.

CenturyLink® Security Log Monitoring with Trending and Threat Analysis allows you to:

Improve Your Security Posture

- Evolve your security posture beyond compliance into true threat management, from reactive to proactive, from defensive to offensive

Get Visibility

- See in near-real-time what is happening inside your infrastructure at every point — view your attack surface, monitor user activity, watch and verify SOC activity performed by your own staff and even CenturyLink SOC staff
- Provide leadership with updates, customized reports and visual outputs showing true insights about activities inside your network

Improve Operational and Cost Efficiency

- Focus your team on the events that matter and reduce the noise from false positives
- CenturyLink leverages your existing investment in log collection assets, SIEM solutions and other security hardware and tools by integrating them into the CenturyLink solution
- Control costs by selecting what logs to send and in what volume

CenturyLink Security Log Monitoring with Trending and Threat Analysis 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
- 90 days 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, LEEF 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
- Available as stand-alone or to augment multiple alternative assessment tools
- Integrates with Incident Management and Response Service for full service approach

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure, security solutions and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

Don't wait 170 days to detect an attack. Become more proactive today!

Take us for a test drive; see what CenturyLink can do for your business before making a commitment. Contact your CenturyLink Sales Professional.

* http://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released

Global Headquarters
Monroe, LA
(800) 784-2105

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6768 8098

Canada Headquarters
Toronto, ON
1-877-387-3764

838072116 - security-log-monitoring-trending-and-threat-analysis-datasheet-SS160408

CenturyLink® Business