MARKET NOTE

CenturyLink Enhances Security Log Monitoring for Hybrid IT Environments

Christina Richmond Martha Vazquez

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: CenturyLink Enhances Security Log Monitoring for Hybrid IT Environments

This IDC Market Note presents details of CenturyLink's (CTL) enhancement to its Security Log Monitoring (SLM) service. On June 28, 2018, CenturyLink announced an enhancement to its Security Log Monitoring solution, which includes threat intelligence, new cloud security monitoring features, and a real-time mobile application for rapid threat detection and real-time response. The SLM service is poised to assist in providing visibility across hybrid IT environments, no matter whether the customer is utilizing on-premises applications or managing them in multiple cloud environments.

Key Takeaways

- Reducing complexity of multiple IT on-premises and cloud environments continues to be a challenge for any managed security service provider (SP) customers. CenturyLink enhanced its security platform so that customers will have the flexibility and not have to endure any extra infrastructure costs when adding security services.
- Included in the SLM enhancement is complimentary log ingestion of up to 10GB per day, with ability to upgrade for more capacity.
- Improved machine learning capabilities are included in the enhancement to provide more valuable content and improve the user experience.
- IDC believes that this is one of the many enhancements and new services that CenturyLink will introduce as a result of its acquisition of Level 3. IDC believes the company is positioning itself as a very good option for SMBs and midsize organizations.

Source: IDC, 2018

August 2018, IDC #US44178818

IN THIS MARKET NOTE

On June 28, 2018, CenturyLink announced an enhancement and new disruptive pricing to its Security Log Monitoring solution, which includes threat intelligence, new cloud security monitoring features, and a real-time mobile application for real-time threats and rapid response. This is a new enhancement that has been added since the acquisition of Level 3. The SLM service is poised to assist in providing visibility across hybrid IT environments, no matter whether the customer is utilizing on-premises applications or managing them in multiple cloud environments.

CTL has been in the security market for quite some time, offering its Security Log Monitoring, which is a cloud-based log collection and security information and event management (SIEM) platform. The platform was launched in 2016 with the acquisition with netAura. The company has continued to transform its business by acquiring many strategic companies, including the last acquisition of Level 3.

Reducing complexity of multiple IT on-premises and cloud environments continues to be a challenge for any managed security SP customers. In addition, customers using cloud environments such as AWS were lacking visibility and were not able to send logs over to CTL. As a result of these ongoing challenges, CTL enhanced its security platform so that customers will have the flexibility and not have to endure any extra infrastructure costs when adding security services. The platform was enhanced with the goal in mind to make it more adaptable and flexible for customers. The platform can ingest multiple log sources coming in from VPNSs, firewalls, databases, cloud infrastructure, and servers.

CTL can also now integrate threat feeds it acquired from Level 3 into the Security Log Monitoring. The Adaptive Threat Intelligence service acquired through the Level 3 acquisition ingests about 120 billion NetFlow sessions every day from activity occurring in the network. With that visibility, the company can see bad traffic on the internet and have a view of real-time threats. The company plans to add the view of live threats into the SLM platform in the future.

The new enhancement can now provide customers a global view, so no matter where the instance is coming from (e.g., Singapore or the United States), any changes or reporting are visible across the board, therefore making it easier for customers to deploy, manage, and maintain their security solutions.

Along with the enhancement of ingesting logs from multiple IT environments, CTL will disrupt the market with its new offering of providing a complimentary or free tier analytics model, a service that is typically not offered by most managed security SPs. For existing customers, they can use its free monitoring service for up to 10GB per day, which will store logs for 90 days and give the ability for customers have visibility for up to 12 months. The key uniqueness of this service is that it allows for customers to build on from the free 10GB foundational monitoring log retention. Customers can add features as they go, including other services such as cloud security monitoring, threat intelligence, advanced monitoring algorithms, trending and analytics, SOC monitoring, and incident response.

CTL has been quiet in the past about its machine learning analytics, but with its new enhancement, machine learning analytics will be more valuable because it helps customers become more productive by sending them alerts that have already been detected as something serious and not just a bunch of noise. The machine learning-based analytics will not only improve the quality of experience but will also improve CTL's content and be able to show customers some real serious security issues. The technology uses a clustering method, and instead of using deviations, it is profiling attacks and then taking a known set of attack criteria. CTL will use the analytics to validate attacks that are successful and look for the same ones through a clustering method, which will assist in finding attacks with similar techniques. By providing this new technique, CTL will be able to reduce the amount of noise coming in and provide valuable alerts to customers.

Last, customers will find the improved user interface and mobile application easy to use. Customers will be able to use intuitive search capabilities and enhanced visualization tools including a new interactive threat map. In addition, security measures were strengthened with a single sign-on and support for multifactor authentication.

IDC'S POINT OF VIEW

CTL is a large U.S. telecom company that expanded its footprint by acquiring Level 3 in 2017. Today, the company provides a multilayered approach through its network-based security solutions that consist of advanced capabilities; services such as DDoS mitigation, adaptive network security, and threat intelligence; and complementary services such as incident management and response and security log monitoring. CenturyLink operates a global network that allows extensive visibility into security threats to better predict problems and quickly mitigate attacks.

CTL has acquired many companies to help strengthen its competitive position in the marketplace. It seems that the benefits are now starting to show as CTL addresses the organization's needs of today. Many organizations are needing to have visibility that goes beyond the network perimeter and extends across hybrid network environments. This trend will continue to occur as the mobile workforce continues to grow; therefore, the need to detect and mitigate threats is crucially important.

CTL's newest enhancement to its Security Log Monitoring is good timing for many organizations that are undergoing digital transformation changes. In addition, the ability to offer a free monitoring service is also a huge benefit and game changer for the market. The offering will be a great lead-in for many SMBs and midsize organizations that need the help but may not have the budget to invest in their own infrastructure.

LEARN MORE

Related Research

- *Worldwide DDoS Prevention Products and Services Forecast, 2018-2022* (IDC #US43994318, July 2018)
- *DDoS Protection Is now a Necessity and Still Growing: U.S. DDoS Prevention Survey, 2018* (IDC #US43904418, June 2018)
- *Worldwide and U.S. Comprehensive Security Services Forecast, 2018-2022* (IDC #US43622818, March 2018)

Synopsis

This IDC Market Note presents details of CenturyLink's (CTL) enhancement to its Security Log Monitoring (SLM) service. On June 28, 2018, CenturyLink announced the enhancement to its Security Log Monitoring solution, which includes threat intelligence, new cloud security monitoring features, and a real-time mobile application for rapid threat detection and real-time response. This is a new enhancement that has been added since the acquisition of Level 3. The SLM service is poised to assist in providing visibility across hybrid IT environments, no matter whether the customer is utilizing on-premises applications or managing them in multiple cloud environments.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com