Log-monitoring service meets huge management challenge

TechMatrix achieves comprehensive threat detection and optimizes application security with One Identity SSB

Customer:

TechMatrix

Industry:

IT services

Country:

Japan

Employees:

1,086

Website:

www.techmatrix.co.jp

Challenge

To protect against evolving cyberattacks, TechMatrix needed to update its existing security monitoring service and establish an improved managed security support.

Solution

The company extended its TechMatrix Premium Support powered by TRINITY (TPS) with One Identity syslog-ng Store Box (SSB), a high-performance log-management appliance, for comprehensive threat detection and security.

Benefits

- Ensures high-speed indexing of 20,000 syslog events per second
- Delivers customized reports that go straight to the business need
- Provides enhanced syslog security services to businesses
- Helps lower the cost burden of syslog management

"EDR [endpoint detection and response] optimization requires quick responses, and we believe this can be delivered with One Identity SSB."

Takashi Sayama,
Chief of Security Labs, TechMatrix

TechMatrix provides a range of managed security services (MSS) to help companies protect their networks against cyberattacks and related security threats. Among its services is TechMatrix Premium Support powered by TRINITY (TPS), a support solution that includes deploying and maintaining security products.

The Internet of Things (IoT) is causing a large increase in networked devices, and the number of TechMatrix Premium Support powered by TRINITY (TPS) syslogs, which record software events, is multiplying. As a result, the demand for security monitoring services is increasing, and customers are seeking more comprehensive solutions. Takashi Sayama, chief of security labs at TechMatrix says, "TPS meets this need, provisioning optimized functionality and integrated monitoring of multiple security products at low cost."

TechMatrix needed to make certain that TPS could process syslog data regardless of size at high speed and transfer the processed data to a security information and event management (SIEM) system for analysis without failures. Working with Jupiter Technologies, TechMatrix chose One Identity syslog-ng Store Box (SSB), a high-performance log management appliance.

Collects and transfers syslogs at high speed with no failures

TechMatrix customers with TPS can now collect and index syslogs at high speed without interruptions thanks to One Identity SSB. Notes Sayama: "We are delighted by the stability of this appliance. Even the most robust appliance will fail from time to time; however, One Identity SSB creates hardware clusters, reducing the risk and burden on the system if and when a problem arises." The big data ingestion capabilities of One Identity SSB means it can collect and index up to 100,000 syslog messages per second. "We have a maximum traffic of about 20,000 events per second, so there is headroom at the current usage levels," says Sayama.

Gains customized reports for the business need

Customers have the freedom to tailor syslog analysis to cover the areas that most concern them thanks to the customized reports available in One Identity SSB. "When we are collecting and transferring syslogs, various filters can be applied according to customer requirements, enabling detailed event log analysis that is tailored to the client's requirements as part of our managed security functionality," says Sayama.

Lowers the admin burden and enhances security

TechMatrix can easily scale the syslogs service to meet the needs of a growing customer base by adding One Identity SSB appliances to the existing cluster. Furthermore, TechMatrix is looking at ways to extend the value of the One Identity solution. Sayama says, "Another idea is automating EDR [endpoint detection and response] operations, surveys and incident reports. Because EDR optimization requires quick responses, we believe One Identity SSB is right for the job."

He adds, "We believe One Identity SSB will contribute to enhancing the information security of small and medium enterprises, and thereby reduce the management load."

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.