

Customer Profile

TELUS

TELUS improves compliance and strengthens security with the RSA enVision® platform

Acceleration

“The easy to use, optimized reporting capabilities of RSA enVision have enabled us to accelerate compliance with PCI legislation whilst improving security - both internally and on behalf of our managed security services customers.”

Alan LeFort,
General Manager, TELUS Security Labs

AT A GLANCE

Business challenge

- Comply with Payment Card Industry (PCI) security standards regulation by protecting card transactions across the network
- Find and deploy an easy-to-use and maintain Security Information and Event Management (SIEM) solution to meet the PCI requirement for continuous monitoring of security logs

Solution

- RSA enVision simplifies compliance with comprehensive accounting of network activity, customized reporting and retention of and access to complete log and event records
- Security operations augmented by RSA enVision's real-time notification and reporting on high-risk events

Results

- Ensures PCI compliance, enabling security of customer card details, significantly reducing time spent satisfying auditors' requests, and negating the need for time-consuming re-audits
- Identifies the small subset of high priority security incidents automatically from millions of logs, reducing the burden on the security team

TELUS is a leading national telecommunications company in Canada, with \$9.7 billion of annual revenue and 11.6 million customer connections including 6.1 million wireless subscribers, 4.2 million wireline network access lines and 1.2 million Internet subscribers. TELUS is a recognized leader in IT Security providing managed security services, consulting services technology integration services to organizations across Canada. Additionally, through TELUS Security Labs, TELUS provides threat and vulnerability research to more than 50 security product vendors.

BUSINESS CHALLENGE

As the largest telecommunications company in Canada, TELUS handles a large volume of customer payment card information and is therefore subject to PCI Data Security Standards (DSS). These standards require the company to track and monitor networks and applications as well as to alert and report on threats to ensure compliance is achieved.

Having purchased a software-based SIEM solution in 2005, TELUS found that deployment, management and scalability was challenging with a database-centric architecture. Database-centric SIEM solutions cannot scale to meet the tens of thousands of events per second



required to monitor a carrier network, and critical compliance data was at risk of being lost.

Without a complete record of its audit and security activity, TELUS risked not being able to demonstrate its PCI compliance consistently, potentially causing a serious problem for management as well as the security team. TELUS wanted to eliminate any chance of this happening. These factors led it to seek a reliable and scalable SIEM solution.



The Security Division of EMC





SOLUTION

Following evaluation of several leading SIEM solutions and an extensive internal pilot, the TELUS team selected RSA enVision to provide automated collection, alerting, retention and analysis of log data.

The key factors in the decision-making process were the dependability and reliability of the platform, which would be essential to ensuring compliance with PCI regulation. During the pilot, enVision's reliability proved to be outstanding.

Additional elements that impressed the TELUS team included enVision's stability as a purpose-built appliance and its lack of dependence on a potentially unscalable relational database for critical log collection. The team could also reduce its manpower because enVision requires much less care and feeding.

LeFort was also impressed by the platform's scalability from small to large systems and the quality and quantity of reports and correlated alerts that RSA enVision provided.

Thanks to the ease with which TELUS was able to deploy RSA enVision, it met a very aggressive timeline. Integrating systems into the platform proved to be uncomplicated, ensuring the rollout was completed by a small team over a short period.

"We only needed two days' training to understand how to write up correlation rules and alerts compared to two weeks on the previous system. It has been really easy for the security team to pick up and monitor - a huge bonus for us when things are busy or when we're on boarding a new employee," comments LeFort.

RESULTS

Compliance with PCI regulation is now assured as the high reliability and PCI-ready reporting capabilities of RSA enVision enable payment card transactions to be recorded accurately. Whereas the previous system could not scale, RSA enVision has given TELUS the confidence that it will pass any PCI audit. Since the introduction of RSA enVision, TELUS' security staff have spent much less time managing the SIEM infrastructure and much more time responding to critical threats that are detected.

"This is time-saving for us as we don't need to worry about the SIEM going down or logs being dropped. This increases our ability to deal with the threats presented and implement protection measures before incidents become a real problem. It also saves valuable time, enabling us to do more with less," LeFort comments.

TELUS is using RSA enVision not only internally but also on behalf of its managed security services customers. This presents an additional challenge for TELUS, as it needs to balance the need to be proactive with regard to threats while avoiding unnecessary intervention that might cause the customer alarm. The company has many long term customers whom it has been supporting for at least 3 years. It chose enVision to support not only the growth in this installed base but also to position the company to support new customers' growth needs as they consume ever more log and event source data.

Using RSA enVision, TELUS is able to achieve PCI compliance and security for its managed security services customers. In fact, it has become necessary for managed security service providers (MSSPs) to offer integrated security monitoring if they are to bid for and win new business. For this reason, the SIEM platform is helping TELUS to stay competitive in a challenging market and open up new lines of revenue across its network. Because RSA enVision is a highly scalable solution, TELUS can focus on growing its MSSP business and increasing profitability.



"Organizations don't want to manage a SIEM, they want to reduce risk. Many vendors seem to miss this distinction; RSA has not. If you are looking to spend your time securing your organization and have limited resources, RSA enVision is the solution you should evaluate."

Alan LeFort,
General Manager, TELUS Security Labs



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC



RSA, the RSA logo, SecurWorld and SecurID are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2003-2007 RSA Security Inc. All rights reserved.

TELUS_CP_o809