How Snare Helps with ATM Data Analytics

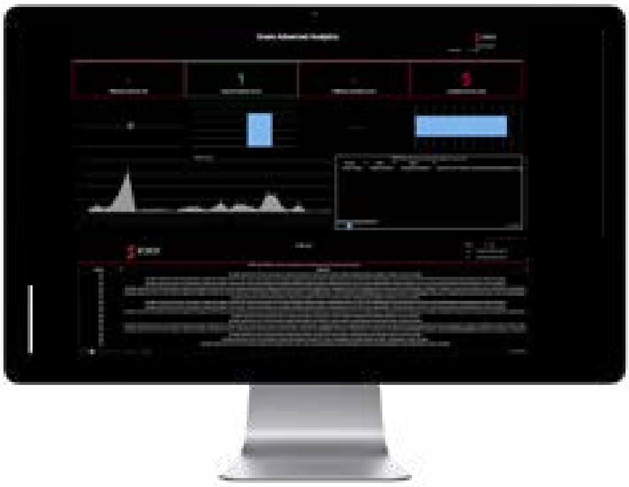
Snare works closely with a large international North American Bank and has drastically improved their forensic and investigation capabilities across their ATM systems. As with many large banks they have thousands of ATM systems deployed around the country and internationally. All of these systems generate transactions daily both small and large. The problem with performing any form of forensic investigations is having timely and accurate access to all the information as well as the manual labour cost to do the investigations with the typically limited resources. Manual investigations can require a large amount of human resources to review all that data. So a new better automated solution was needed that could allow the bank to scale out its investigation capabilities.

So how does Snare help you may ask?

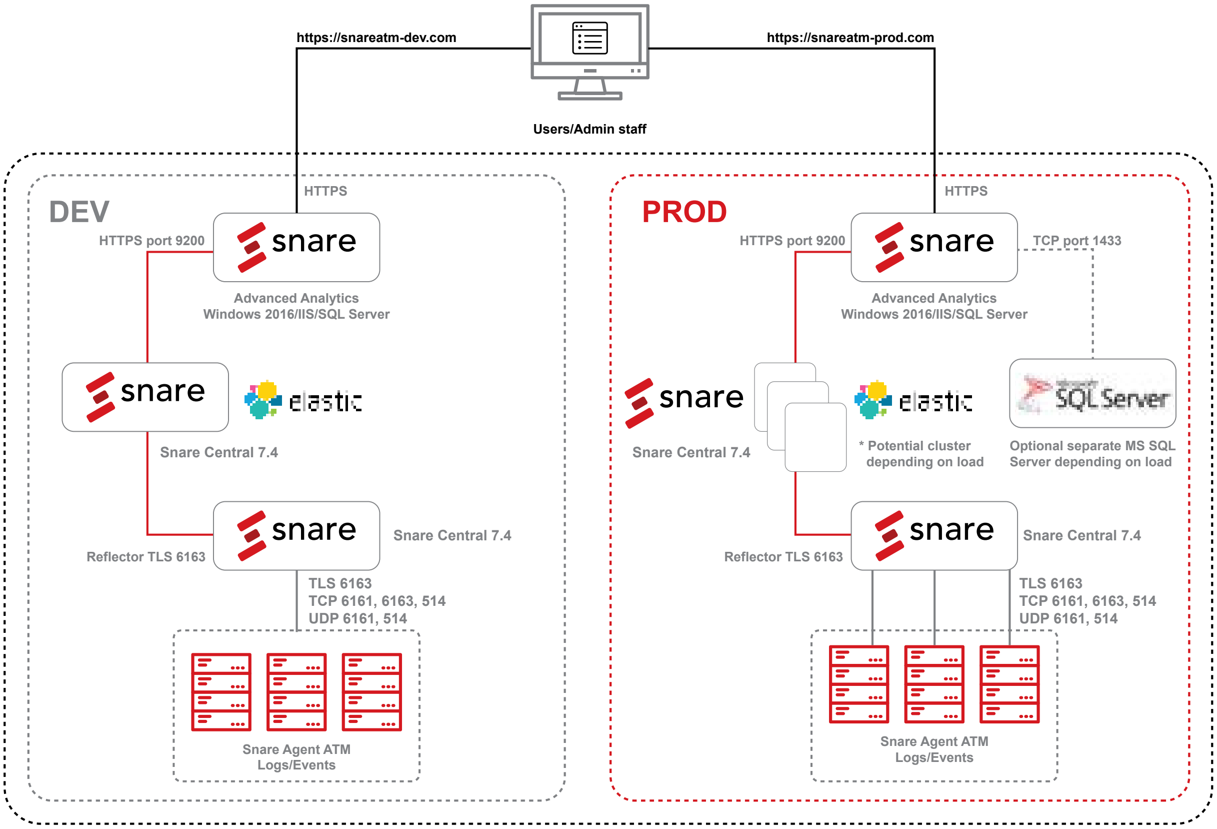
By using our Snare Agents, we fully automate the collection of the system event logs and the application logs from the systems all in near real time. This means valuable forensic data is collected and stored securely in our Snare Central log management platform, away from the systems that generated the logs. This way there is less opportunity for data loss or log tampering on the ATM systems. Even if the ATM had some form of compromise, we have all the logs off the compromised system, up to that point in time, to aid in any forensic investigation.

Now we have the logs centrally stored we can perform various forms of forensic investigations on the data. The areas that we assist in are:

- Review of system health from the operating system. As most ATM systems are Windows based there are lots of windows event logs that are important to review both from user access, admin access, privilege escalations, applications executed, policy changes, data transfers, patch levels, HIPS events etc.
- ATM application logs. The ATM systems also create their own application logs (XML and others) that contain details of all the transactions such as card inserts, cash withdraws, cheque deposits, hardware errors, card jams, retries, failed PIN logins etc.



Basic architecture of collection and processing which can vary depending on the business needs and objectives.



By using the power of our Snare Advanced Analytics, we can provide real time dashboards of all the ATM systems and allow the technical teams to investigate a particular customer issue or a broader incident investigation across their ATM fleet. When an unusual or common theme of failures occurs, this can be highlighted and raise alerts on the affected systems. Individual user investigations for complaints with the ATM can also be searched on more easily. This allows the bank to use the system to scale out and perform analysis over all of their ATM systems with less effort than could be achieved from other manual processes. Specific KPI, dashboards and reports can be created for each of the business areas looking at specific areas of interest to aid in rapid reporting and alerting of problems or incidents. In the end efficiency if the key in managing larger volumes of data and this is where Snare helps the business with doing more with the same resources.

One of the many powers that our Snare Advanced Analytics and Threat Intelligence platform has is being able to bring in disparate data source and allow review and correlation data over all these data sources. This helps to provide valuable context to the data and what it means with other activities and logs from other systems. With 70+ adapters we can access and link data from a multitude of other systems being from standard API, ODBC, CSV imports, XML, JSON. Depending in the business need we also have adapters to collect data from STIX, Active Directory GPO, O365, AWS, WSUS, Jira, TFS, ticketing and incident tracking systems and many more.

If your organisation needs help in this area and wants more information please contact our friendly sales team at snaresales@prophecyinternational.com for a chat on how we can help your business achieve more.

Steve Challans Chief Information Security Officer

snaresolutions.com

snare