CLABBY ANALYTICS

Research Report

Compuware: Real-time Capture of Mainframe User Behavior for Cybersecurity and Compliance

Executive Summary

In early April 2017, Compuware introduced yet another new product – this time enabling enterprises to capture and analyze start-to-finish mainframe user session activity data to provide security teams with deep visibility into user behavior in mainframe environments. This is Compuware's tenth consecutive quarter of new products/product extensions since November 2014.

What is going on at Compuware is a textbook lesson in how to reinvigorate a company and greatly improve profitability. Over the past three years Compuware has clarified its strategy; rationalized its product offerings; rejuvenated its development organization; expanded its portfolio; structured new relationships with former competitors; formed strategic relationships with third-party software suppliers that align with its strategic directions; opened new and different market opportunities; and has made itself again relevant to its customer base.

Compuware's newest offering is "*Application Audit*"– an application investigation tool that provides real-time capture of user behavior. It focuses specifically on insider application usage, seeking to identify unusual or suspicious activities. It is also useful for proving compliance to meet regulatory requirements.

What is particularly interesting about Compuware's new offering is the way that it has been "assembled." Application Audit examines and captures customer defined application user activities. The data collected can be sent directly to Splunk for analysis or written out as IBM System Management Facility (SMF) data for CorreLog and Syncsort Ironstream to store, format and transport. Once the SMF information has been properly structured it can be passed to Splunk, other popular SIEM tools, or analytics engines like Hadoop, where it can be merged with data from across the organization, analyzed and presented to security administrators looking for suspicious behavior. The captured user behavior data can also be made available in report form for compliance purposes.

In this *Research Report, Clabby Analytics* takes a closer look at Compuware Application Audit. We like the way that Compuware is providing full visibility into mainframe session behavior and integrating that intelligence with popular SIEM engines for analysis – in essence, using systems to do a lot of the work that security administrators have had to do manually over the years to find security breaches. We also like the company's new approach to building software solutions: the company listens closely to its customers, finds creative ways to address real world operational problems – and uses the offerings of business partners as well as its own internal development resources to create unique product offerings that address mainframe market needs. And with the company's plans to continue to introduce new capabilities, enhancements to classic offerings and integrations with preferred DevOps tools every quarter – we can't wait to see what blended solutions the company will come up with next.

Solving the Data Volume Analysis and Time-to-Breach Issues

The main idea behind Compuware's Application Audit offering is to detect breaches that occur when unauthorized users access sensitive data. Application Audit collects information on who is accessing which applications and databases. It organizes that information and presents it to an analytics program that can quickly evaluate vast amounts of data, looking for suspicious behavior.

To date, enterprise security administrators have manually sifted through SMF data, scanned through mountains of disparate log data, and used security integration and event management tools to examine user behavior by tracking application usage and data access. However, these approaches and tools put far too much pressure on security administrators to locate needle-in-a-haystack breach behavior. Now enriched mainframe user behavior intelligence coupled with SIEM tools can streamline user behavior analysis – helping enterprises protect data more efficiently.

> ***Among the problems that Application Audit solves is data volume overload and the time it takes to identify malicious behavior. Security administrators are being bombarded with massive amounts of monitoring data – far too much for the human mind to analyze in the short timeframes required to deal with incursions. And because these data stores are so vast, it takes too much time for humans to analyze data, find patterns and identify threats to data security. Application Audit fixes these problems by providing application user-specific behavior data thereby reducing the volume of data to be analyzed to detect insider threats.***

According to IBM's X-Force Research: 2016 Cyber Security Intelligence Index report, breach attempts are on the rise, increasing 5% last year. Further research shows that it is taking administrators too long to find breaches – with the global average time to detection taking 146 days. To address the volume sifting and time-to-identify-breaches problem, security software providers are increasingly integrating analytics software with their respective security management products. Analytics software can read massive amounts of data quickly, searching for patterns, identifying policy violations and tracking user behavior.

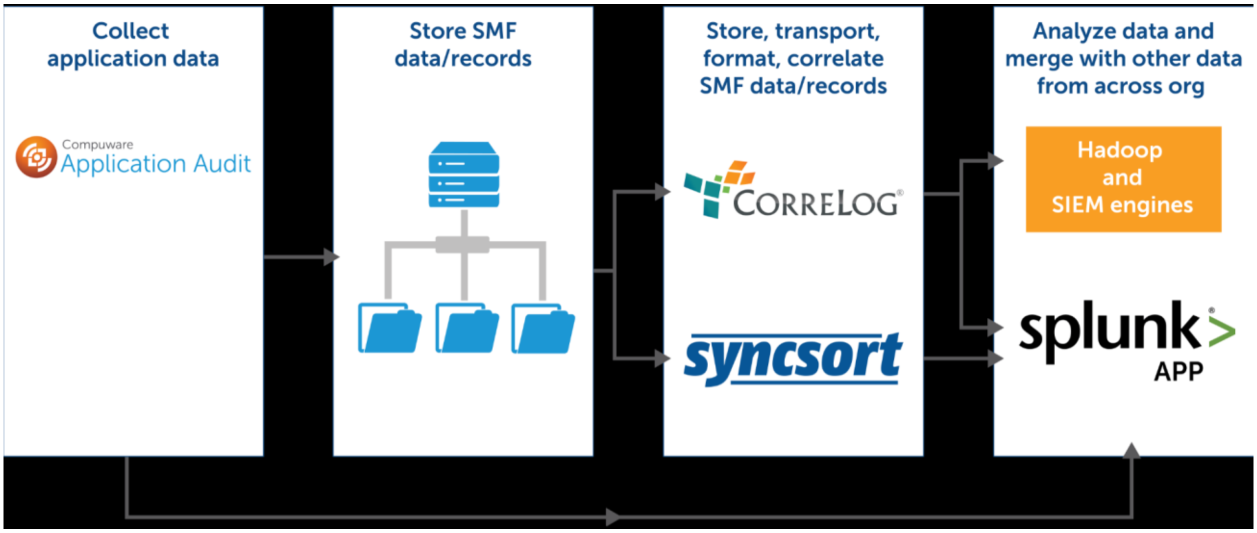
How It Works

Application Audit has been designed to provide application usage data to detect and investigate inappropriate data access activity, primarily by internal users. Illegal access activity can come from hacked user accounts, illegally purchased account information, or even from malcontent users looking to sell enterprise data to parties of a nefarious nature.

Application Audit's recording process does not require any modifications to the applications being monitored. It also provides a Web interface enabling an auditor with no mainframe experience to easily set session recording parameters, review audit data, configure feeds and perform other administrative tasks. This is significant because it means that an organization can separate the auditor's role from a mainframe user's role, so that no single person is in a position to engage in malicious activities without detection.

As Figure 1 illustrates, the data gathered by Application Audit is written to SMF and may be read by Syncsort Ironstream, which formats the data for secure delivery into Splunk, adding additional z/OS mainframe log data. Alternatively, the same SMF data can be read by CorreLog zDefender for z/OS, which in addition to using its own alerting and dashboard capabilities, can deliver the data into SIEM systems such as HPE ArcSight ESM, IBM QRadar, Splunk as well as other analytics engines, such as Hadoop. Additionally, Application Audit provides an out-of-the-box Splunk-based dashboard that delivers value on Day One.

Figure 1 – Compuware's Integrated Application Audit Workflow


Collect application data
Compuware Application Audit
Store SMF data/records
Store, transport, format, correlate SMF data/records
CorreLog
syncsort
Analyze data and merge with other data from across org
Hadoop and SIEM engines
splunk> APP

Source: Compuware, April, 2017

How Customers Are Using Application Audit

Compuware's customers are primarily using Application Audit in two ways: 1) to gain insight into the activities of privileged users; and 2) to ensure and prove compliance with regulatory requirements.

One European bank was faced with a security breach during which a celebrity's credit card information was stolen. The bank needed insight into why the breach had occurred – which meant that it needed to examine mainframe application usage. Further, the bank needed to show auditors proof that their practices met regulatory compliance requirements for sensitive data. With Application Audit, the bank was able to monitor applications that are used to access sensitive data – and send that monitoring data to Splunk for behavior analytics. The audit revealed that an outsourced contractor was abusing privileges – and the bank now meets European Union General Data Protection Regulation (GDPR) requirements through ongoing monitoring using Application Audit.

As is the case with numerous enterprises, another European bank had no insight into privileged user activities. Executive management, to meet regulatory requirements, required auditable evidence of users' activities. This bank choose to use Application Audit to define monitoring criteria; to then monitor privileged user activities – and then send that data to the Splunk analyzing environment. As a result of using Application Audit, this bank now can spot abuse and inappropriate access, and take steps to ensure that insider access does not result in a breach.

A healthcare insurance company decided to use Application Audit to help ensure compliance with HIPAA (Health Insurance Portability and Accountability Act) requirements. The company chose to log internal users' viewings of personal and sensitive information – and then send that information along with other relevant parameters to Splunk for analysis. This company can now prove HIPPA compliance – and has mitigated exposure by being able to identify breaches as they occur.

Summary Observations

In short, systems can read through vast amounts of data far more quickly than humans. Log files, monitoring data, authorization conflicts and other policy violations can be identified in real-time instead of hours or days. Capturing user behavior data and using SIEM engine analytics to do the work of humans results in breaches being identified more quickly – and opens the door for analytics discoveries that may have eluded human observation.

A side benefit of integrating user behavior intelligence software with SIEM engines is lower security management costs. With systems identifying illicit behaviors, lesser skilled individuals are needed to do deep log and monitoring analysis. Lesser skilled individuals cost enterprises less in terms of salary, while also making it possible to more easily fill positions where skills are in short supply. It should also be noted that using a tool like Application Audit makes security administrators more efficient and effective – and their skills and knowledge grows when using such a tool. So Application Audit can also be used as an effective training tool.

Application Audit is a huge step in the right direction for Compuware. The company has clearly recognized the value of adding best-of-breed software mixes to its portfolio and Application Audit is the latest example.

We're expecting several more "analytics enabled" software products to be made available by Compuware in the near future. On its current tangent, the company should continue to see solid growth as it finds new and creative ways to address challenges in mainframe management and administration.

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 239-1211

April, 2017

Clabby Analytics is an independent technology research and analysis organization. Unlike many other research firms, we advocate certain positions — and encourage our readers to find counter opinions —then balance both points-of-view in order to decide on a course of action. Other research and analysis conducted by Clabby Analytics can be found at: www.ClabbyAnalytics.com.