Protect Your Organization with Application Audit

While the mainframe is the enterprise's most intrinsically secure platform, businesses must still proactively protect mainframe systems and data against cybersecurity threats. Authorized users can access mainframe applications and data for nefarious purposes, or their credentials can be hijacked by malicious outsiders. Since standard security practices may not flag these attempts, they often go unnoticed by security personnel. Data breaches are often not discovered until days or months after the fact, if at all, resulting in massive costs to the business, forced public disclosures and irreparable brand damage. Enterprises must have the ability to capture and analyze mainframe application session user activity in real time to reduce the risk of potential breaches.

TODAY'S SECURITY LANDSCAPE

Most enterprise security teams rely on disparate logs and SMF data from security products such as IBM® RACF®, CA ACF2™ and CA Top Secret® to monitor their environments, track activities and send alerts when attacks and suspicious events take place. However, these tools typically only capture data about who is logging in and out and when, or when unauthorized attempts are made to access systems, applications and data. Security information and event management (SIEM) tools also have their limitations: The richness of the data they report is determined by how well they monitor environments. Overall, the data provides little visibility into end-user activities, including whether a user accessed sensitive data and what they did with it, leaving security teams with blind spots.

APPLICATION AUDIT

Application Audit enables security and compliance teams to easily capture start-to-finish mainframe user behavior in real time, including all successful logins, session keyboard commands and menu selections, and specific data viewed without making any changes to mainframe applications. Enterprises can use this rich, complete data about mainframe user behavior by itself or have it automatically sent to SIEM systems to easily:

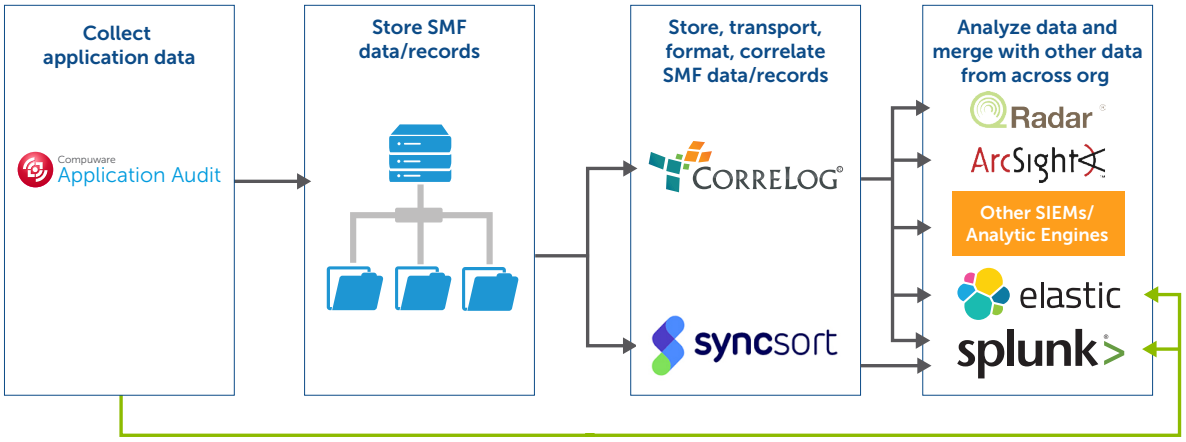
- Detect, investigate and respond to inappropriate activity by internal users with access
- Detect, investigate and respond to hacked or illegally purchased user accounts
- Support criminal/legal proceedings with complete and credible forensics
- Fulfill compliance mandates regarding protection of sensitive data for regulations such as the Health Insurance Portability Accountability Act of 1996 (HIPAA); the **General Data Protection Regulation** (GDPR); and the Australian Notifiable Data Breaches (NDB) scheme
- Take advantage of additional capabilities provided by SIEM engines

LEVERAGE SIEM ENGINES FOR COMPREHENSIVE INTELLIGENCE

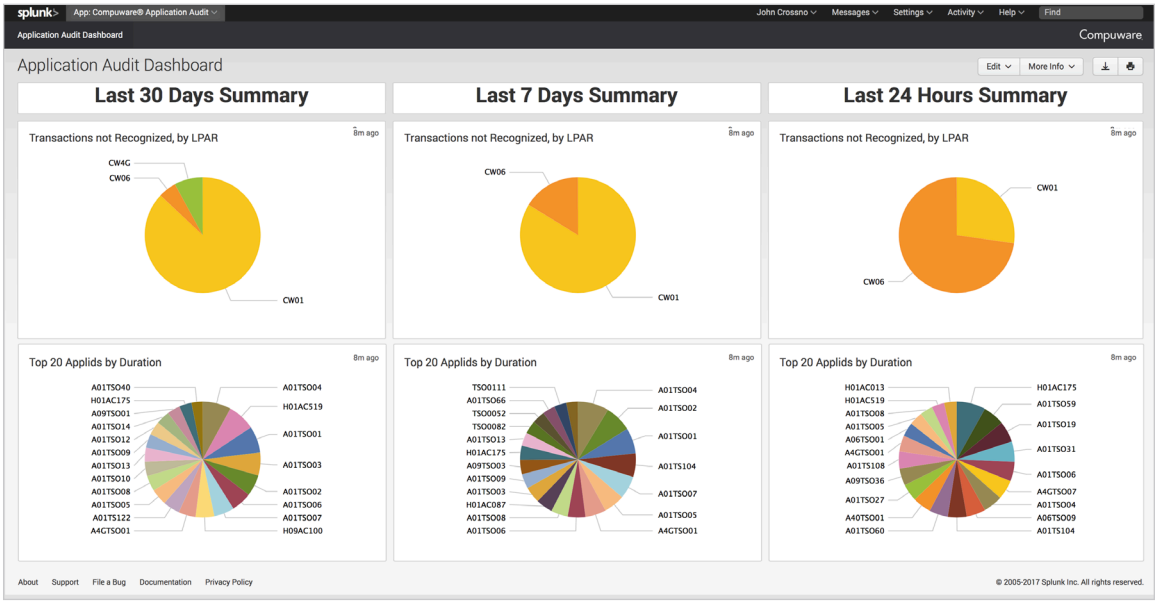
Through integrations with **CorreLog® zDefender™** and **Syncsort Ironstream®**, Compuware enables enterprise customers to integrate Application Audit's mainframe intelligence with popular SIEM solutions such as **Splunk®**, IBM QRadar®, HPE Security ArcSight™ ESM and Elasticsearch. In addition, Application Audit data can be sent directly to Splunk and Elasticsearch for analysis. Analytics-rich dashboards provide organizations with a larger picture of their overall application environment. With

this comprehensive coverage, the operational intelligence gained is more comprehensive and yields fewer false positive alerts so personnel can spend more time on scrutinizing legitimate threats. Security teams are also able to determine the true end-to-end user activity for applications, whether they are only running on the mainframe or, as is becoming more common, part of a distributed application spanning multiple environments.

Application Audit integrates with popular SIEM solutions for cross-enterprise security intelligence.



An out-of-the-box Splunk-based dashboard provides a multitude of statistics around mainframe application user behavior.



INTUITIVE WEB USER INTERFACE ENABLES SEPARATION OF DUTIES

Application Audit's intuitive web interface empowers even mainframe-inexperienced security and compliance staff to set session recording parameters, review recording activities, enable the data to be delivered to SIEM systems and perform other administrative tasks. The web UI enables separation of the auditor role, who has no mainframe expertise, from the system administrator's duties, so that no single person is in a position to engage in malicious activities without detection.

Compuware
Application Audit

FACT SHEET

THE VALUE OF APPLICATION AUDIT

- Provides granular, mainframe user behavior intelligence, including what specific data was viewed, who used it, how long it was viewed and which applications were used to access it.
- Enables the automatic delivery of data directly or in combination with CorreLog zDefender for z/OS or Syncsort Ironstream into an organization's SIEM platform for immediate analysis.
- Provides the ability to gain near real-time insights that fuel faster mitigation, strengthening security.
- Delivers granular intelligence and reporting capabilities needed to comply with privacy and other regulations as well as security policies.
- Gives organizations the information they need to show compliance with regulations such as HIPAA, GDPR and the NDB.
- Reduces dependency on specialized mainframe knowledge.

Learn more at **compuware.com/application-audit.**

The Mainframe Software Partner For The Next 50 Years

Compuware empowers the world's largest companies to excel in the digital economy by fully leveraging their high-value mainframe investments. We do this by delivering highly innovative solutions that uniquely enable IT professionals with mainstream skills to manage mainframe applications, data and platform operations.

Learn more at compuware.com.

05.18_31827_Application_Audit_fs