

Automating Fraud Detection with Application Workflow Orchestration



Introduction

Anomaly detection is at the heart of many IT processes. Identifying and preventing anomalies and fraud involves monitoring massive data sets and transactions for abnormal behaviors or patterns. Distilling all that data from multiple sources can make it difficult to identify outliers. In the financial space, that can include physical banks, ATMs, mobile devices, online transactions, and more, each with its own highly complex methodology. Finding those anomalies as quickly as possible is important because if they continue unchecked, they can create significant consequences for businesses and their customers.

One of the biggest challenges companies face when implementing anomaly or fraud detection programs is dealing with the complexity of all the disparate technologies and data sources required. Many applications have their own scheduling functionality, but do not provide a single point of control. That makes it hard to visualize processes end to end, which ultimately leads to scalability and service level issues

Enter application workflow orchestration.
Automating and orchestrating the process

of analyzing data and returning insights is no longer a nice-to-have; it's a necessity to yield real-time results. Application workflow orchestration can help IT teams:

- + Identify anomalies faster
- + Shorten the time to detection, prevention, and response
- + Save the costs of fraud and the ensuing fallout



Getting ahead

Putting orchestration and automation to use for anomaly detection is an idea that's gaining ground from big business. Walmart recently discussed¹ its use of deep learning anomaly detection solutions to help combat fraudulent activities, and PwC included it in its recent *Global Economic Crime and Fraud Survey 2020*². In the survey, PwC discovered that companies with a dedicated fraud program later spent 42 percent less on responding to fraud, and 17 percent less on remediation versus organizations that didn't have a program.



¹ Ahmad K hodayari, "Deep learning for fraud detection in retail transactions," Medium, November 2020.

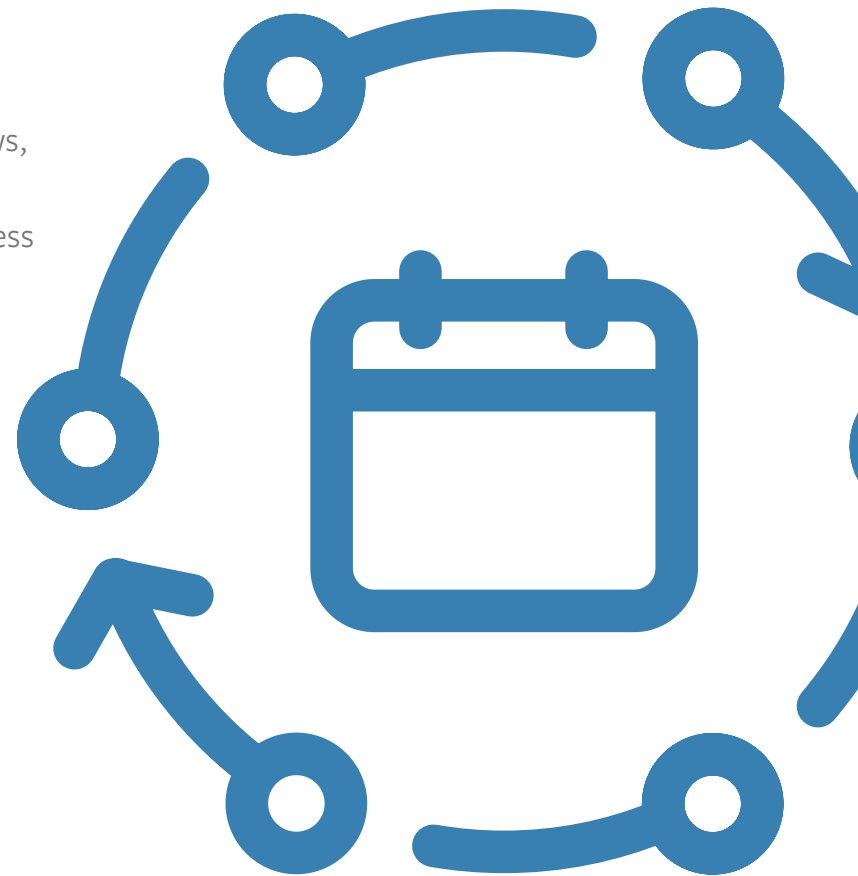
² PwC's Global Economic Crime and Fraud Survey 2020, PwC, 2020.

BMC Helix Control-M

Rooting out and resolving variants is integral to everything from financial fraud detection to antivirus protection. In this eBook, we'll look at how two companies in different industries are using Application Workflow Orchestration as the foundation of their successful anomaly detection programs.

BMC Helix Control-M is an adaptable, easy-to-use SaaS platform that automates anomaly and fraud detection processes by ingesting, storing, processing, and analyzing data at scale, from on-premises to the cloud. By developing, scheduling,

managing, and monitoring workflows, organizations can detect anomalies and fraud faster, make sound business decisions, and maintain overall regulatory compliance.



Customer Success



When you think of fraud detection, malware prevention probably doesn't immediately come to mind. But when you look below the surface, there are many similarities, and the methods for finding and preventing fraud and malware are virtually the same—as is the financial impetus. According to the *IBM Cost of a Data Breach Report 2020*³, the average cost of a data breach is \$3.86 million and it takes 280 days to identify and contain one.

A leading anti-malware software company helps customers keep their information safe from hackers and scammers by using artificial intelligence (AI)-powered technology to proactively identify and eliminate malware, ransomware, and exploits. Its platforms run on big data—anonymous telemetry streams, Internet of Things (IoT) data, and behavioral and usage scenarios. As a major player in the constantly evolving world of cybersecurity, the company is tasked with collecting, harvesting, and mining data as efficiently as possible.

They use application workflow orchestration to coordinate all of their ETL processing, batch processing, and ingestion, which they call the “pre-feature builds,” and to orchestrate and schedule the long-running and repetitive processes of modeling, testing, and moving products to production. This also ensures the company meets its service level agreements (SLAs) by monitoring any failures and delays in the data pipeline and providing business context on their potential SLA impact.

³ *IBM Cost of a Data Breach Report 2020*, IBM, 2020.

Customer Success

In the financial world, manual processes are still widespread. In fact, *McKinsey & Company*⁴ found that of the banks it surveyed, up to 85 percent admitted their financial crime compliance and anti-money laundering activities were still done through spreadsheets and traditional methods.

This was an issue for a leading financial services provider based in Mexico with 185,000 customers. The company issues pre-paid payment cards and electronic wallets to help customers manage and distribute benefits like pantry vouchers and gasoline and restaurant credits to their employees.

Prior to leveraging application workflow orchestration, the company had teams working around the clock to manually execute numerous critical processes, which was time consuming,

error prone, unpredictable, and unmanageable, leading to significant downtime and negative customer experiences.

With application workflow orchestration, the company eliminated inefficiencies while improving processes and increasing visibility, predictability, reliability, and security. Scripted, fixed-time processing also allows the company to plan more effectively; reduce downtime, fraud, errors, and data loss; and deliver better customer experiences.



⁴ Adrian Murphy, et al, "The investigator-centered approach to financial crime: Doing what matters," McKinsey & Co, June 2020.

Conclusion

To keep pace with and get ahead of fraudulent criminal activities, companies must evolve traditional, manual processes and embrace the right automation technologies. Whether you're a bank, a software company, or retailer, there's never been a better time to automate your anomaly and fraud detection practices and streamline your data with application workflow orchestration tools. Ready to see what BMC Helix Control-M can do for you?

For more information, visit: bmc.com/helixcontrol-m





About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

www.bmc.com



BMC, the BMC logo, and BMC's other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners.
© Copyright 2021 BMC Software, Inc.



Partner Logo

 | Registered Partner

EBOOK

Automating Fraud Detection with Application Workflow Orchestration

ABOUT [PARTNER]

Ut optatius et elit faccus molori veris dioris volore preriasim et es et labores expellupta cus et ut aut voluta temque poribus alit, quidel il iderrum rescipsus rende evendametur minciet hita et aut dolorit, simin perovitat rest dolorro rersperspe min cuptate ditate serae odi debis mollaccus enestrum latinve lignates est, cor suntor Ut optatius et elit faccus molori veris dioris volore preriasim et es et labores expellupta cus et ut aut voluta temque poribus alit, quidel il iderrum rescipsus rende evendametur minciet hita et aut dolorit, simin perovitat rest dolorro rersperspe min cuptate ditate serae odi debis mollaccus enestrum latinve lignates est, cor suntor

PARTNERWEBSITE.COM | XXX-XXX-XXXX