RTInsights.com

Continuous Intelligence in the Real World

Sponsored by

sumo logic

Introduction

Nearly every company in every industry has unique challenges and drivers around how to use data effectively to drive their business. The daunting task of dealing with the vast volumes of data that are used to spot problems in the making, optimize operations, and safeguard the business, has given way to a new era of digital transformation. Leveraging real-time insights and cloud-native applications to deliver secure and reliable digital experiences are the new requirements to become a modern business.

According to IDC, 70 percent of all organizations will have accelerated the use of digital technologies, transforming existing business processes to drive customer engagement, employee productivity, and business resiliency by the end of 2022. As more businesses rely on software to drive revenue, they're becoming more reliant on real-time insights to drive reliable and secure digital experiences delivered through cloud-native applications.

Continuous Intelligence (CI) provides the insights that help companies rapidly deliver reliable applications and digital services, protect against modern security threats, and optimize their business processes in real time. Businesses implementing CI can look not just to peers in their industry but to any business using CI for guidance, best practices, and more. This eBook showcases examples from across a variety of industries to help business leaders see what is possible with CI.

Chapter 1
CI in Fintech and Banking

Fintech and banking operations face extraordinary headwinds of competition and risk. They're dealing with massive flows of sensitive customer data. In addition, they are under pressure to offer more products and services digitally, develop innovative offerings by partnering with other entities, and provide customers with easier access to their accounts. Those changes make companies increasingly more vulnerable to cybersecurity attacks on their infrastructure, systems, and people. Any breach can incur immediate financial consequences, loss of customer confidence, and regulatory penalties.

Understanding the exact state of business in real time and taking action based on that heartbeat is a critical differentiator for companies looking to scale and meet demand while keeping customer satisfaction high. That's why many of them are turning to continuous intelligence. Consider these examples:

Improve time-to-market: A fast-growing fintech startup leverages banking transaction data via Open Banking, which is a set of APIs for third-party access to financial data, to create personalized money-saving recommendations for their customers. Because they're dealing with banking data, both individual transactions and the aggregate recommendation logic must be impeccably secure.

Once they were ingesting security, developer, and operations data from across their infrastructure into a single CI platform, their DevOps team found enormous efficiency in identifying and resolving potential incidents that required input from both security and observability professionals. That occurred without DevOps and security as a bottleneck in their operations. The company is now deploying new applications faster, and horizontally scaling its infrastructure, with the confidence that all its machine data is going into a single source of real-time truth.

Detect early warning signs of cybersecurity attacks: After suffering a devastating cybersecurity attack, a cryptocurrency exchange revamped its entire suite of applications and underlying infrastructure. It needed more mature security processes built on more meaningful log data.

They ingest all the raw data and deliver a single place to build new queries, enabling their security team to identify anomalies that signal potential attacks in a fraction of the time. These queries help the team identify unauthorized SSH connections, detect malicious messages, and match network logs. With the platform providing such insights, the security team saves time and can work more efficiently compared to searching through data manually. Additionally, the CI platform helps prioritize problems and automatically routes high-priority bulletins to on-call staff.

Modernize security operations: A leading payments technology provider that helps its customers process billions in transactions annually needed to upgrade its security operations center (SOC) team with a new security information and event management (SIEM) platform that could reliably ingest log data, provide prioritized threat alerts, and allow for customized processes.

Because CI platforms unify all machine data—including logs, events, and performance metrics—across all the environments, the SOC team is confident that they will see the complete picture. Their platform takes that capability one step further by assigning alerts with a Global Confidence Score which helps the company prioritize their reactions based on aggregate information they would never have access to otherwise.

Chapter 2
CI in Tech

Technology-centric companies face massive challenges in how they grow profitable lines of business and meet customer demands. They need to deploy faster and ensure higher levels of quality, from infrastructure to the end-user experience, to compete and keep customers happy.

At the same time, tech companies want to implement the latest in DevOps methodology and cloud-native architectures to deliver reliable and secure digital experiences. They want to migrate from on-premises data centers into multi-cloud environments and deploy hyperscalers to ensure they can handle rapid changes in data volume. They want to modernize their applications by transitioning from VMs to microservices and Kubernetes. Mixing those improvements with a deployment velocity is an inherently risky process that is prone to bugs and incidents that go unnoticed until they affect the end-user experience or bring an entire service offline.

Compounding matters is the fact that modern applications based on microservices and containers produce many logs, traces, and alerts. The volume of such data makes it harder to assimilate information, draw insights, or take action. CI can help improve the software development lifecycle with better observability and faster speed to market. Such improvements are critical in any technology-centric company, which in today’s digital world is just about every company.

Modern software development lifecycles: One technology company has operated for decades as a traditional business in the physical mailing solutions space. To remain competitive and meet changing customer preferences, the company made a concerted transition toward creating software products for global eCommerce and shipping logistics. That change required an entirely new software development lifecycle, beginning with migrating all customer-facing applications from traditional on-premises infrastructure to the cloud.

The company invested in a CI platform that could modernize how their developer teams understand the health and performance of their applications with deep, real-time visibility. With new infrastructure and CI to help resolve issues, the company is deploying new code at speeds any company—much less one that’s more than a century old—would be proud of.

mov eax,4
; The system call for write (sys_write)
mov ebx,1
; File descriptor 1 - standard output
mov ecx,hello
; Put the offset of hello in ecx
mov edx,helloLen
; helloLen is a constant, so we don't need to say
int 80h
; Call the kernel
mov eax,1
; The system call for exit (sys_exit)
mov ebx,0
; Exit with return code of 0 (n
#include <stdio.h>
int main(void)
printf("Hello, world!\n");
return 0;
import <Foundation/Foundation.h>
main (int argc, const char * argv[])
NSAutoreleasePool *pool = [[NSAutoreleasePool alloc] init];
NSLog (@"Hello, World!");

Observability: One multinational enterprise software development company recently saw enormous growth in new regions they had not serviced before, which created snowballing demand for expanded data residency requirements, not to mention more volume and velocity. Their legacy observability strategy and tooling simply couldn’t cope.

The company skipped over traditional open-source observability platforms and opted instead for a CI platform that could provide high-quality dashboards and machine learning-based models out of the box. Without having to waste time on ramping up, the company's development teams could focus on surpassing ambitions availability and page load speed targets on a brand-new Kubernetes infrastructure.

Speed to market: With millions of daily active users, an AI-powered SaaS company needed to move quickly while keeping its customer base of individuals, businesses, and enterprises happy. Good customer experience, however, starts with exceptional engineering experience, and that led the company toward a single observability tool for both customer-facing and internal support applications.

The company used CI to ingest and analyze massive amounts of daily data from logs and event streams from hundreds of microservices. Using that data, developers can see both real-time and historical data to spot issues quickly, and they can uncover long-running trends and focus on shipping features knowing they’ll be well-monitored. Such capabilities and insights are essential in today’s business environments that are increasingly customer- and user-centric. Software users expect rapid fixes to problems, fast responses to new feature demands, and a constant stream of innovation. The insights delivered by a CI platform provide the needed feedback loop between developers and users.

Chapter 3

CI in Retail and Manufacturing

Retail and manufacturing businesses contend with complexity on both digital and physical fronts. Unlike a company that primarily employs developers and those required to support software development, these companies have production facilities, retail stores, and global footprints that often add up to tens of thousands of pieces of hardware. They need to observe and improve operations at unprecedented scale and complexity. DIY platforms might be capable of ingesting data but not helping their users understand what to do with it.

For these companies, CI is proving to be a panacea that delivers robust security and user experience insights through a single common "language" for data. It's more than dashboards, sophisticated queries, or real-time analysis. The value of CI is being able to bring together people from disparate teams to collaborate on business problems that can't be tackled with a narrow-minded band-aid or bugfix.

SecOps and threat hunting: A global consumer packaged goods (CPG) company operates in countries around the world, and that equates to an enormously complex security posture. A few years ago, they wanted to move away from their existing managed security service provider (MSSP) with SIEM into a new integrated platform that had the capacity to handle collected log and event data.

Once that company's CI platform was online, they immediately noticed a reduction in alert noise thanks to event correlation. Their previous MSSP implementation, which was limited to single-event alerting rules, once created 2,500 alerts in a single hour. They also leveraged anomaly detection to receive alerts for behavior they would never think to account for, like PowerShell calling a command prompt to run a script that's using Base64 encoding to hide itself.

Improved user experience: An online travel booking company hinges its brand on a differentiated user experience—faster search, faster payments, and unmatched fairness in settlements and refunds. That's how they've grown to more than billions of searches a day, a number that was both a signal of success and a warning sign for their data infrastructure. Despite producing a massive number of logs every day, the company had no centralized monitoring or alerting capabilities on that data. Each microservice had its own logging function, and the team responsible for it had custom tools and commands for analyzing it.

Once they moved to a CI platform with standardized data, monitoring, and alerting, the company's teams could identify and troubleshoot incidents cross-functionally. The turnaround time for resolving production issues—those directly affecting those billions of daily searches—was reduced from its original time of 60 to 40 minutes.

Single data "language:" An integrated communications company for supply chain data has a strong vision for helping suppliers, retailers, and logistics firms make sense of complex problems. They had a two-pronged approach to modernization, migrating to the cloud from legacy infrastructure while adopting containers to simplify deployments. That degree of change stretched their existing stack of open-source products—Elasticsearch, Logstash, and Kibana (also known as the ELK stack)—to its limits. They could extract some meaningful insights, but not without enormous investment in managing the deployment.

CI gave the company a single tool, usable by multiple teams, that allowed them to collaborate in ways the previous ELK stack didn't. Development teams understood how to interact with operations data, and security teams could ask questions about developer data. That led to improved collaboration across the board. In the face of an ongoing incident in their environment, security and operations teams could sit down in the same room together, look at the same dashboard or console, and immediately be on the same page. There were no more data mistranslations or wasting of time trying to find a middle ground.

Chapter 4

CI in Gaming and Media

As media and gaming platforms become more complex and drive more revenue, companies are under increasing pressure to deliver seamless yet secure customer experiences. Many are looking to continuous intelligence to help navigate matters and improve operations. Comparable issues are present in media organizations as they cater to ever-more demanding customers and the need for highly personalized experiences.

Companies are dealing with customer databases, reaching into hundreds of millions of records, with data that is regulated by the Children's Online Privacy Protection Act (COPPA) or the European Union’s General Data Protection Regulation (GDPR). They face a battering of cybersecurity attacks, and there is enormous pressure on engineering and DevOps teams to deliver internal tools as quickly as possible so they can get back to developing competitive content in a fast-moving industry.

CI helps those companies focus on aggregating and standardizing data from many disparate sources, a common need as they acquire new media studios/sources. With one source of data truth, they’re able to improve their processes and reduce time to market, even as they undertake complex migrations to or between cloud providers.

Data standardization: A European gaming company needed to build repeatable processes for onboarding new game studios they were acquiring, all of which came with different infrastructure. They could concentrate log files from both AWS and Azure into a single CI platform, which minimized the need to train their SOC on each environment. Instead, they focused on aggregated information in their CI platform, helping them cut the time to investigate and resolve problems by 20 percent.

InfoSec, SecOps, and SOC improvements: One gaming company had traditionally focused on game consoles, but they saw unprecedented success with a new mobile game that reached more than a billion downloads. With such a huge increase in new users, there was simply no way the company could hire enough analysts to manually carry out the work of protecting sensitive user information.

The company’s security leadership quickly pushed for a state-of-the-art security operations center (SOC). After they centralized their machine data into their CI platform, they could apply automatic logic to most potential security incidents, and that freed their SecOps professionals to focus their talents on reacting to the most threatening incidents.

Process improvement: The same gaming company also achieved enormous benefits in how they scope and deliver on internal tooling to help other business functions move faster. Because they were ingesting all their machine data into their CI platform, they could streamline processes that required buy-in from multiple departments and integration between disparate data. In one case, a business process that required eleven touchpoints, and typically took five to seven business days, was reduced to two touchpoints and five minutes.

Enabling migration and application modernization: A popular newspaper and media company needed to discover and implement new ways to improve their speed to market and to better serve internal customers. To build a stronger foundation for application delivery, the company’s platform engineering team undertook three simultaneous migrations: 1) from AWS to Google; 2) from monolithic applications to containers and Kubernetes; and 3) from one CI platform to another.

With this new infrastructure, the DevOps team was confident that each internal application would create logs for its containerized workflows, which would get picked up by CI for discoverability. When a DDoS attack struck one of their properties, they could rapidly discover the source and work to mitigate it with their CDN partner, Fastly.

Conclusion

Today, our daily lives are filled with the use of digital experiences that are powered by digital services. We eat, shop, bank, travel, socialize, and are entertained with a variety of streaming digital services that are often available with apps on our cell phones.

CI provides the needed insights to help companies rapidly deliver reliable applications and digital services, protect them against modern security threats, and optimize their business processes in real time.

RTInsights.com
Accelerate Your Business with Real-Time Insights

About RTInsights

RTInsights is an independent, expert-driven web resource for senior business and IT enterprise professionals in vertical industries. We help our readers understand how they can transform their businesses to higher-value outcomes and new business models with AI, real-time analytics, and IoT. We provide clarity and direction amid the often-confusing array of approaches and vendor solutions. We provide our partners with a unique combination of services and deep domain expertise to improve their product marketing, lead generation, and thought leadership activity.

sumo logic

About Sumo Logic

Sumo Logic, Inc. (NASDAQ: SUMO) empowers the people who power modern, digital business. Through its SaaS analytics platform, Sumo Logic enables customers to deliver reliable and secure cloud-native applications. The Sumo Logic Continuous Intelligence Platform™ helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers around the world rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications.