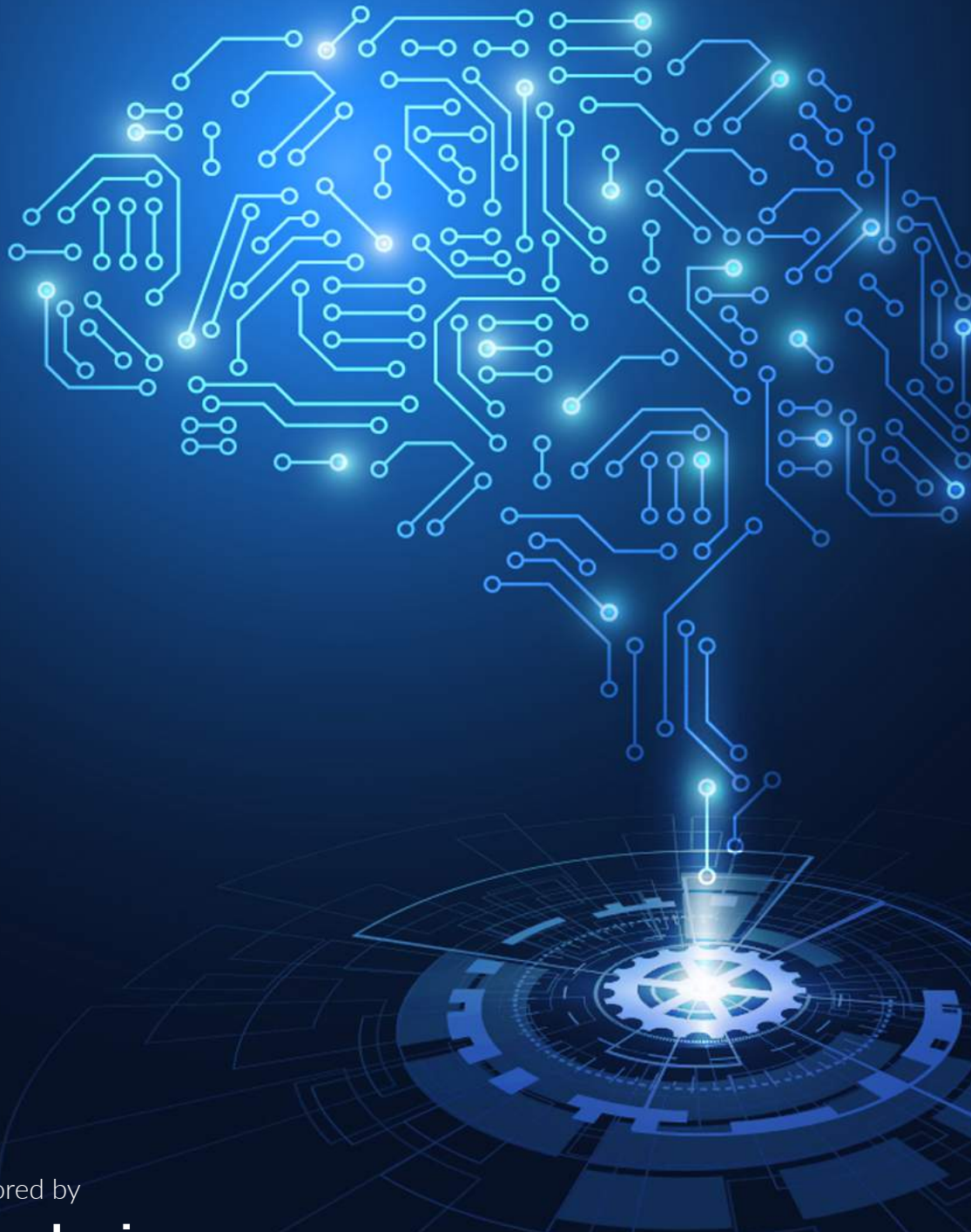
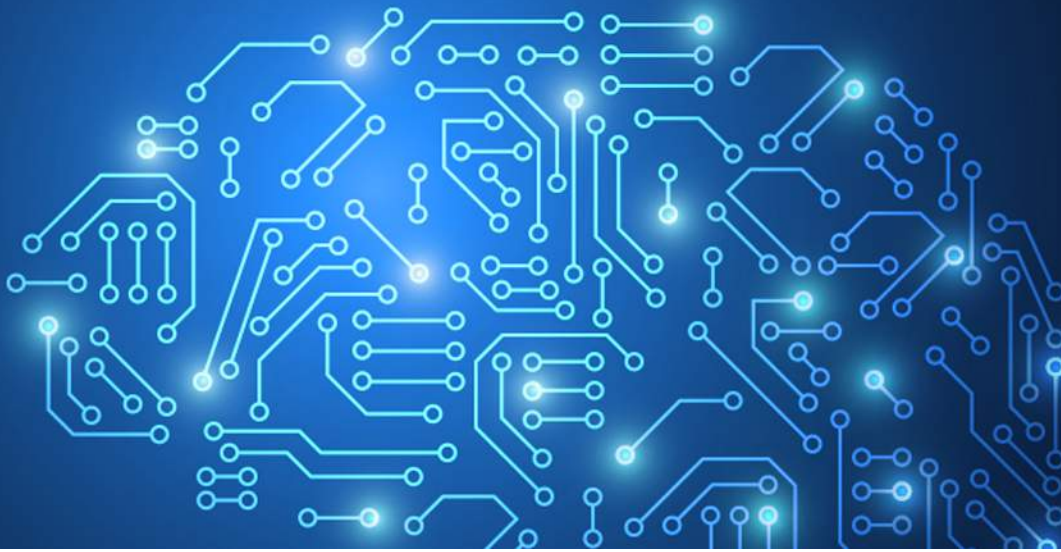


# Continuous Intelligence and the era of real-time, data-driven business



Sponsored by

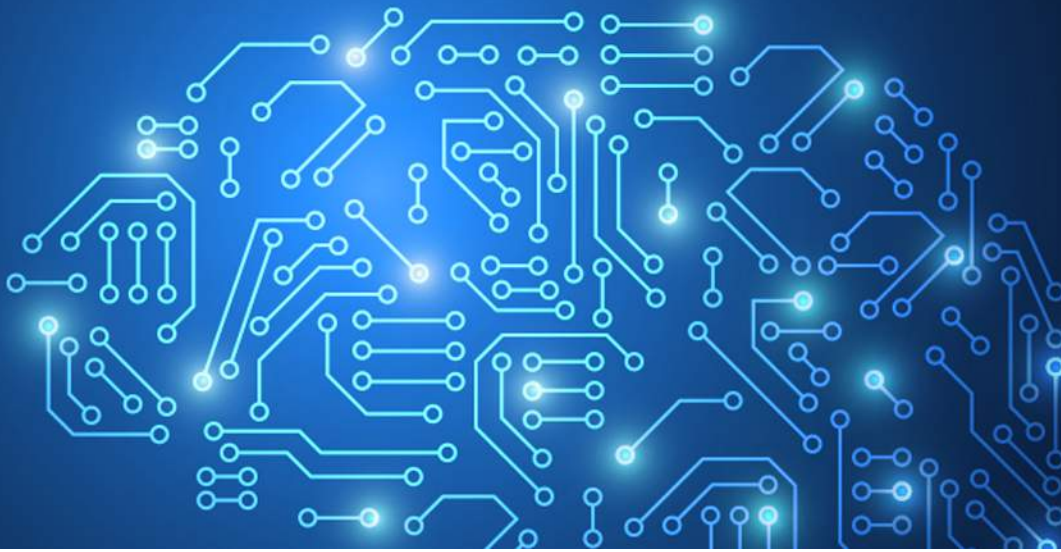
**sumo logic**



## Introduction

As a CTO, CIO, CSO, or high-level engineering manager, you're tasked with a few essential tasks: Keep the applications running. Stay on top of security threats. Deploy new code faster. Innovate faster than all the disruptive thinkers employed by the competition. But most important of all is consistently giving your expert employees all the tools, resources, and information they need to excel at their jobs.

In the following paper, we're focusing on Continuous Intelligence, a growing practice of providing a single cloud-native platform for real-time analytics and insights. Faster decision-making drives improvements to application deployment, security, and ultimately customer experience by empowering the individual experts who make tech-savvy businesses run. The era of real-time, data-driven businesses has arrived—do you have all the information you need to react and respond?



## **Chapter 1**

Continuous intelligence for the modern,  
secure business and its applications

PAGE 4

## **Chapter 2**

CI brings full observability at exabyte scale

PAGE 6

## **Chapter 3**

CI's role in the single pane of security glass

PAGE 8



## Chapter 1

# Continuous intelligence for the modern, secure business and its applications

The transition to digital business has been decades in the making, largely driven by two key factors: **1)** the pursuit of new markets to drive new sources of wealth creation and growth; and **2)** the ongoing pursuit of new ways to serve and delight customers. Today, through digital transformation, we've reached an era of immediacy, in which products, services, and experiences are consumed in real-time, all the time.

Real-time experiences create an entirely new playing field for companies, which demands not only the creation of these new services, but also a new digital business model to run, manage, monitor, and secure them continuously. This new digital business model is a reality thanks to new modern applications consisting of hundreds or thousands of microservices (also code) that interact and communicate with each other automatically to enable the service.

For example, think of all the new ways we shop, share information, or engage with entertainment, travel, and hospitality—things we were doing before the Covid-19 pandemic. Our digital life and work styles were well underway. Even during the pandemic, our collective digital “world” accelerated. We saw remote workstyles incorporating video conferencing and chat communications, telehealth, distance learning, grocery and food home delivery, plus the emergence of advanced new technologies like 5G communications and devices, robotics, drones, and more.

These new technologies and services are leveraging modern applications to enable the way we live, work, learn, and enjoy our lives.

As microservices drive modern applications, they generate data—specifically machine data—at a rate and volume that is now measured in terabytes and exabytes, and in the near future, yottabytes. When captured, stored, secured, and analyzed, this data is a rich source of information and insights to improve service availability, health, and engagement.

Analytics tools from the days when businesses built their own physical data centers to deliver products or services through physical locations aren't adaptable to this new digital world. Services are largely consumed through digital interfaces, driven by applications running in cloud-based environments. Analytics also provides the most value when a business can capture, store, secure, and turn it into business decisions in real-time.

A new analytics approach is required—one that mirrors the operational and economic model of cloud computing. This approach needs to serve domain practitioners with contextual insights across the software development lifecycle, including quality code development and delivery, application deployment and management, troubleshooting, feature improvement—all with security embedded at each stage of the lifecycle process.

To enable this new approach, many digital businesses adopt a new category of software called continuous Intelligence (CI). CI provides real-time analytics and insights from a single, cloud-native platform across multiple use cases to ultimately speed decision-making and drive better customer experiences.





Delivered as a real-time, platform service, continuous intelligence brings together real-time data generated from the modern application's underlying microservices. With a continuous intelligence platform, domain-based practitioners—developers, operators, security analysts, product managers, sales/marketing professionals, and customer success operators—can leverage a single “pane-of-glass” to monitor, troubleshoot, and secure the application service. They also can cross-correlate information for faster remediation and deeper customer engagement insights to continuously improve the service.

Continuous intelligence platforms also leverage machine learning and AI technologies to automate many of the lower-level processes of data collection, detection, analysis, and remediation. Expert practitioners are freed up to work on high-level work tasks, such as insight-driven decision-making for greater service reliability, security, and customer engagement.

By enabling a way for all functions to have access to real-time insights in context from a single, continuous intelligence platform—regardless of the disparate technologies powering the application service—continuous intelligence is opening up the era of real-time, data-driven businesses.

In the next two chapters, we'll dig deeper into how CI enables key components of digital transformation, including cloud migration, modern application reliability, and security modernization.

## How are businesses using CI?

Here are the ways in digital businesses are benefiting from continuous intelligence strategies and/or a continuous intelligence platform service:

- ✓ **Application observability:** See real-time performance metrics, logs, and traces on a single platform, even with complex microservices or Kubernetes-based deployments.
- ✓ **Anomaly detection on infrastructure:** Leverage machine learning to get notified every time an application, deployment, or asset experiences an issue to find root causes faster.
- ✓ **Compliance visibility:** Exhibit continuous compliance for regulations such as PCI, HIPAA, FedRAMP, FISMA, SOx, ISO, GDPR, and COBIT, even with complex cloud-native deployments.
- ✓ **Automated security detection:** Empower the security operations center (SOC) with response workflows based on real-time threat analysis from all available sources, not templates based on past or known attacks.
- ✓ **Decision support:** Build data- and knowledge-driven support systems that can sort through the most critical infrastructure alarms, automatically scale during performance degradation, or make inventory decisions based on last week's sales volume.
- ✓ **Data security:** Analyze, sort, and trust data wherever it happens to reside, whether that's in a multi-cloud environment, a third-party app, or an executive's bring-your-own-device setup for working from home.
- ✓ **Cross-functional collaboration:** Give business leaders a single pane of glass for operations, security, customer success, product management, finance, sales, and more to prevent blame and align teams on common goals.

## Chapter 2

### CI brings full observability at exabyte scale

A significant component of digital transformation is modernizing the way businesses develop and deploy their applications. Some are still migrating their applications away from on-prem hardware to the cloud, while others are investigating environments that allow them to deploy new code continuously. But no matter where they are in their digital transformation journey, they continue to face growing pressure to continuously innovate by developing and deploying new improvements, fixes, or features faster than ever.

Of course, these businesses can hire more developers

or IT/DevOps people to move faster or invest in new software development/deployment paradigms to rebuild their offerings from the ground up to improve agility. They can scale horizontally with their cloud provider of choice until they're comfortable there are no bottlenecks in their systems.

But throwing money or people at application modernization doesn't reveal another critical issue that contributes greatly to slowing down the speed of continuous innovation: *the lack of visibility into the performance and reliability of the system they built.*

## The benefits of application modernization



**Scalability:** Cloud-native applications automatically handle horizontal scaling and load balancing, and infrastructure providers allow for vertical scaling based on real-time analysis of logs, metrics, or traces.



**Location-agnostic:** Cloud-native applications can be deployed in a single location or many, or even proxied through a global CDN for the fastest response times regardless of where your customer lives.



**Containerized:** Developers can build new features independently of other intricate systems, and DevOps/SRE teams can build CI processes with testing suites, canary deployments, and blue-green deployments to safely deploy code multiple times every day.



**Better resource allocation:** Because businesses don't need to constantly monitor, maintain, and upgrade expensive hardware and networking equipment by passing that responsibility to a cloud provider, they can focus on the performance, reliability, and security of what drives business differentiation—the application itself.

What underpins modern application visibility challenges is their inherent complexity. These businesses are well past running monolithic binaries on a single server in the closet that only IT had the keys to. Whether it's Kubernetes, microservices, serverless, or deep ties with

a particular cloud provider's machine learning platform, these applications emit data at an unprecedented volume and velocity that is largely indecipherable. They need a way to translate the syntax of logs, metrics, or traces into meaningful analytics that humans can interact with.



Given the application is essentially a set of hundreds or thousands of microservices constantly communicating and changing their states, the ability to know a given “state” is extremely difficult without the help of real-time analytics. This idea of state is made even more complex by the reality that modern applications are heavily dependent on other platforms, APIs, and third-party data sources, many of which developers have no control over. Developers and IT/DevOps teams alike might not be aware of the complete dependency “map,” much less how each node affects others.

Even if each technology on this complex map comes “batteries included” with a means of reviewing analytics, that data doesn’t inherently correlate with across services. ITops, DevOps, and SRE teams are left viewing only small slices of the application, which means they have to spend more time piecing together their understanding of a situation rather than solving it. Even worse, there’s no pre-configured way to view the application holistically to learn baseline patterns—an invaluable understanding that unlocks these experts’ ability to identify unknown unknowns as they happen.

For these reasons, among others, simply observing a modern application is difficult enough, much less finding the root cause of performance or reliability issues.

Continuous intelligence is an increasingly popular analytics approach for observing complex full-stack applications. Real-time CI platforms ingest multiple machine data types—logs, metrics, events, traces,

metadata, and telemetry—from every container, microservice, cloud infrastructure, Kubernetes cluster, API, and integrated third-party technology.

A powerful capability of a CI platform is an advanced analytics feature like autodiscovery. The platform automatically detects new services, containers, and infrastructure as they are deployed. Without any development work or input from an IT or DevOps team, this component’s data is ingested and stored for analysis, even if it’s not designed to run ephemeral during periods of high load. The autodiscovery features in CI platforms monitor web servers, databases, message queues, and more, putting key metrics on pre-configured dashboards and building alerts based on industry-standard practices.

CI platforms also clarify the connections between known and unknown dependencies via service maps, providing a single pane of glass for viewing each service, its load, and how it interacts with other services. Service map views help teams understand the implications of known failure chains and illuminate the unknown dependencies, particularly during abnormal load or downtime with a third-party service.

CI helps teams quickly diagnose specific incidents with complete observability, then proactively improve performance and reliability across the infrastructure. Businesses can gain from all the benefits of application modernization while accelerating innovation, improving business intelligence, and putting actual numbers on their impact.



## Chapter 3

### CI's role in the single pane of security glass

Businesses of all sizes, whether or not they're big enough or their infrastructure is complex enough to warrant a security operations center (SOC), need to take the emerging and changing threat landscape seriously. They need to start investing in real-time security threat evaluation.

There are new, unexpected attack surfaces, particularly as organizations progress through their digital transformation and application modernization. Instead of a single on-prem installation, a business might have multiple cloud environments, some on-prem hardware, and many employees bringing their own devices to the enterprise VPN due to the ongoing Covid-19 pandemic and the trend of working from home. And while cloud-native applications might be easier to develop and deploy, they have a much wider surface area of attack, including dependencies and common services with known vulnerabilities.

With all these new variables, it's increasingly difficult to ensure that a company's digital footprint is secure when you consider these environments are dynamic, ephemeral, and borderless, especially due to the growing use of mobile applications and devices. One route is to investigate the plethora of existing security operations tools, pick out a few, and cobble them together.

Unfortunately, these businesses find that security tools most often aren't meant to work in parallel with others. They don't adequately share information, which leads to complex security environments that require an inordinate amount of maintenance and management time. Even worse, they don't provide intelligence fast enough to help security professionals stop threats before they've already affected services or the end-user experience.

For digital businesses, security as a model and strategy needs a new approach. It requires a way to identify threats in real time, respond to security incidents quickly, enforce security configurations and monitor for cloud/infrastructure drift, and the ability to analyze risk through identity and context awareness.

Achieving this approach requires a continuous intelligence platform that can collect and analyze all data from all underlying system sources, automatically trigger alerts when unusual activities or patterns arise, and enable security analysts with the contextual insights needed to quickly assess and analyze the information for faster remediation.

#### The benefits of security modernization



**Automatic detection:** CI platforms track unwarranted activity across the infrastructure, freeing the expert resource to focus on proactive, preventative improvements to rules, governance, and reporting rather than chasing every possible lead.



**Reduced alert fatigue:** ML/AI tools sort true security situations from the enormous volume of potential security alerts created by the sheer quantity of emitted data, which would otherwise overload even a well-staffed SOC. Analysts utilize their expertise on truly concerning work.



**Full dependency visibility:** When paired with a modern application, CI platforms give the SOC service maps to trace the relationship between loosely-coupled or previously-unknown dependencies across cloud, hybrid, and on-premises infrastructure.



**Simplified remediation:** Because the CI platform collects data from every microservice behind the modernized application, it can provide all the context, including relationships between discrete services and high-granularity metrics of affected systems, to help security analysts focus not on gathering information but discovering solutions.



## Continuous Intelligence Platform: The Modern Business Intelligence Layer

Continuous intelligence offers a promising new approach for real-time data analytics to help digital businesses build, monitor, manage, and secure their modern applications and cloud/hybrid-cloud infrastructures.

### Observability

CI platforms provide visibility across all parts of the digital business footprint, transforming multiple data types—logs, events, metrics, traces, and metadata—into real-time analytics and insights. In addition, CI provides powerful ML/AI capabilities to automate many lower-level tasks required to run modern applications.

Teams can automate the discovery of new digital services and building of pre-configured dashboards and alerts for each, or diagnose application issues faster by visualizing service dependencies. CI gives them automated approaches to discover the root cause of an issue faster to speed up remediation and prevent any undermining of the customer experience.

### Security

In a sprawling digital environment, threats can come from anywhere and at any time. Alone, people can't track and remediate these threats fast enough. Real-time CI platforms operate as a partner to security analysts, automatically detecting unwarranted activity across a complex, diverse set of applications, infrastructure, devices, and services.

Analysts can automate the monitoring of their environments based on their own rules and governance and, with the aid of advanced, ML/AI-based technologies, instantly understand the context of their alerts to separate the serious threats from alert "noise." With qualified security analysts always in short supply, leveraging continuous intelligence helps companies maximize the value and productivity of their human expert resources.

### Customer experience

Digital businesses are disrupting traditional business models, providing engaging, compelling new services for people to take advantage of through digital interfaces.

As the global community continues to adapt and evolve to a "new normal," the popularity and reliance on digital services show no signs of abating—it's the new social and economic frontier. Businesses now face a customer experience paradigm in which people are won and lost in seconds and view innovation as a continuous strategy, model, and lifecycle process.

To pull this off, they need continuous intelligence—data transforming into real-time analytics and insights to better understand customer behaviors, patterns, and opportunities to achieve higher levels of customer delight. How well companies consume and act upon real-time intelligence and analytics will separate industry winners from losers.

### Bring it together: The power of real-time, cross-functional collaboration

CI brings undisputed value to each of these use cases independently, but thinking in silos masks the true value in operating a real-time, data-driven business. When a business adopts both a platform and strategy that un-silos key business functions and converges them onto a single seamless experience, they start operating in exceptionally agile, perceptive, and collaborative ways.

DevSecOps tiger teams become the default during incidents to converge on real-time data, more educated troubleshooting, and accelerated remediation.

Developers and customer success teams replace pointing fingers over customer-facing issues with deploying solutions from a data-driven playbook.

Accelerating time-to-market becomes a constant handshake between management and marketing based on real-world and real-time customer usage.

A value-chain impacting issue becomes a company-wide concern, with each expert working un-siloed on the same comprehensive layer of business intelligence.

## Conclusion

Continuous intelligence is unleashing the era of real-time, data-driven business. As companies rely more on software—in the form of cloud-based, modern applications—to drive their business models, they're tapping into a new “secret sauce” of digital business success by transforming data “exhaust” into real-time, continuous intelligence.

As CI platform models incorporate more ML/AI-based, advanced capabilities, analytics, and automation, the ability for digital businesses to focus their precious human expert resources on building, managing, and securing new sources of customer delight means we're only at the beginning of what's possible for the digital services frontier.

To learn more about the many uses of continuous intelligence from Sumo Logic, visit

<https://www.sumologic.com>



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

Sumo Logic Inc. is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic [Continuous Intelligence Platform™](#) automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. For more information, visit [www.sumologic.com](http://www.sumologic.com).

Copyright © 2021 RTInsights. All rights reserved. All other trademarks are the property of their respective companies. The information contained in this publication has been obtained from sources believed to be reliable. NACG LLC and RTInsights disclaim all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. The information expressed herein is subject to change without notice.