Software Delivery in the Age of Experience-on-Demand

A Faster Approach to Building, Running and Securing Today's Applications
The emergence of digital business is an era of unprecedented change in the way business products and services interact with customers, partners, employees and shareholders. Both new and established companies are relying on software and applications to drive differentiated customer experiences, reduce capital expenses and transform traditional businesses models. This new business approach is also changing the way companies build, run and secure today’s modern applications.

What Do You Do When Your Customers Are Accustomed to Speed?

To consumers, waiting is not an option. Getting what they want is fast and gratifying: swipe, tap, select, send—and it just happens. A spontaneous ski weekend? Airbnb gives you a choice of lodging. Just stumbled off the redeye at 2:00am in a strange city? Ask Uber for a ride. Need some Korean fusion cuisine NOW? Let Yelp sniff out the closest restaurant and reserve a table. Want to curl up with a good book? Kindle for your smartphone will drop the latest best seller in your lap. Or, if a book is not your cup of tea, binge-watch the show everyone’s talking about—an entire season instantly—on Netflix. And all of this happens in seconds or minutes, not hours, days or months.

To the businesses on the back end, maintaining this new world of “instant gratification,” is extremely demanding and complicated.

Modern applications are customer-facing, revenue-generating and absolutely critical to the business—essentially, they differentiate today’s winners. To quickly capture new market value, digital businesses are increasing the velocity of application improvements, a process known as continuous innovation, to respond with speed and agility. Traditional companies utilizing the traditional enterprise application model with its lengthy development cycles struggle to keep up.

Digital Businesses Consume IT Services

Modern applications are not built and run on traditional legacy data centers and software development environments. New technology practices are becoming standard for modern application development like “containers,” “microservices” and “public cloud.” In-house deployments are giving way to IT purchased in the form of services.
Examples are infrastructure as a service (IaaS), in which providers such as Amazon AWS, Microsoft Azure and Google Compute Engine sell compute, storage and other data center resources the same way power companies sell electricity. Companies are also leveraging platform as a service (PaaS), whereby development teams use a services-based development environment. Vendors range from public-cloud PaaS providers like Salesforce Heroku to private-cloud PaaS solutions supported by products such as CloudFoundry.

New Expectations and New Technology Demand New Processes
Because applications and IT infrastructure are evolving at light speed, time-honored processes and development models are changing dramatically. Newer agile software development models drive software quality through the velocity of iterative releases. These releases, or code pushes, occur daily, weekly or monthly depending on application needs.

Arguably the biggest change taking place—and one that enterprises mired in traditional practices can’t ignore—is the elimination of IT siloes, reinforced by the traditional “waterfall” development process. With “waterfall” development, software releases follow a distinct sequence of phases that cascade from discrete function to discrete function. Development cycles are long—measured in years—and individual teams handling each phase have their own tools, processes and information repositories. Cross-functional teams are reluctant to

And many additional IT and business needs are fulfilled through a service delivery model called software as a service (SaaS), which enables customers to reap the benefit of technology services without the cost of maintaining the application or infrastructure. SaaS vendors deliver new functionality constantly, leveraging agile development practices to push new updates weekly and monthly, so customers are always working with the latest version and avoiding the hassle of costly, time-consuming upgrade cycles.

Figure 1. Modern applications are at the heart of today’s businesses. To better support them, you will need to re-think how you build, run and secure applications.
share information, which leads to rework, conflicts and finger-pointing when something goes wrong.

For many leading companies today, this siloed process has given way to iterative agile development and cross-team collaboration. Businesses can no longer afford to architect, deploy and maintain heavy, monolithic applications with multi-year development cycles while their competitors run modern applications that are updated rapidly and deployed on whatever infrastructure is most appropriate. The new model combines development and operations teams that share tools, information and responsibilities.

All IT departments today need to re-think their approach to the tools they use to build, run and secure modern applications. For traditional applications, IT departments rely on a variety of disparate tools for development, deployment, monitoring, troubleshooting and securing their applications. These siloed, legacy tools cannot provide the breadth and depth of information needed to accelerate application delivery, troubleshoot problems across complex applications and infrastructures, and proactively identify and remediate security threats. Today's modern applications require a new approach that is more in line with modern infrastructures, modern business expectations and modern organizational responsibilities.

Sumo Logic is that new approach. Sumo Logic is a cloud-native, machine data analytics service that unifies logs and time-series metrics to provide full-stack and lifecycle visibility into modern applications—from code to end-user behaviors. Powered by machine-learning algorithms and graphical, visual dashboards, Sumo Logic turns unstructured, semi-structured and structured data (logs and time-series metrics) into continuous intelligence that enables organizations to move more quickly and adopt new technologies that support disruptive business models. With Sumo Logic, IT has the power to transform from business enabler to business partner.

This paper will outline Sumo Logic’s unique value proposition for building, running and securing the modern application.

---

To understand and manage modern applications, IT departments need access to the real-time intelligence that is buried in machine data to guide them forward.

**Build**

For the digital enterprise, applications are not just task enablers or productivity enhancers: they are the business—that is, they are the direct conduit between the business and its customers for service delivery and revenue generation. Airbnb is a good example—
an enterprise with no inventory, just intellectual property encapsulated in software to provide travel and accommodation services to its global customer base in exchange for fees. In such an enterprise, the lines between traditional IT functions—development, operations and security—blur because everyone who plays a role in supporting the application shares in the responsibility of the application’s performance and viability. Team collaboration is essential to application optimization in the midst of constant code updates. Sumo Logic understands this and provides a platform in which build, run and secure teams can share real-time data from multiple data sources to monitor and troubleshoot issues that threaten application performance or security.

DevOps makes team collaboration a business imperative to unite application lifecycle teams towards a common purpose—the health and viability of application itself. But DevOps is not without its challenges: accelerated release cycles lead to new deployment complexity, increased performance and availability issues and difficulty syncing multiple development work streams.

Modern applications, with their architectural complexity and high volume of change, make monitoring, tracking and troubleshooting particularly difficult. Logs, which capture each and every event and activity of the application and underlying infrastructure can be combined with time-stamped metrics to provide a single source of the truth. However, in modern applications, logs are distributed across locations in the cloud or across servers, or occupy many locations on each server, and traditional tools may not capture custom metrics common in modern applications. SSH + GREP doesn’t scale, and log size can be immense. With no real-time visibility and no way to easily assemble meaningful views, data mining requires a high degree of expertise. And even if companies have this expertise, the myriad of disparate tools make the process painstaking, incomplete and lengthy because the tools are not integrated across a universal platform.

In addition, as companies migrate to public cloud, end-to-end visibility and real-time access to metrics and log data are critical so that IT has a full view from development to testing to production—enabling a more predictable and faster deployment of applications. But within an environment of disparate tooling and data siloed by functions or teams, operations teams are forced to spend more time troubleshooting, often pulling in development teams into the troubleshooting processes. Companies may create investigative "war
room” scenarios, where valuable time is wasted on finger-pointing and countless searches for identifying the problem. As the clock ticks to a resolution, customer service levels degrade and application performance and availability suffer.

**Modern Application Development Leads to IT Complexity**

Modern applications use modular pieces of code that developers iterate on that are packaged into “containers” to automate deployment. This practice is known as “microservices.” The result is an application-building process that is faster, predictable and repeatable. Teams also are adopting agile development and increasing release velocity—not only for building applications, but for maintaining them so they operate consistently at peak performance.

First, the shadow side of containerization and increased release velocity is the growing complexity and risk it creates for overall environment stability. In this scenario, incompatible code pushes can not only impact one microservice but can even bring other services down. Therefore, in this accelerated build process, real-time access to metrics and log data becomes imperative to delivering quality code. However, the challenge is getting access to logs and metrics data quickly because the growing environment complexity is also generating an unprecedented volume of data and that data is changing constantly.

In addition to delivering higher quality software, machine data also provides insights into which features customers are using and how they are adopting applications, so business managers and developers understand their customers better and can push new features and tweak customer experiences to continuously improve satisfaction.

**Sumo Benefits**

Sumo Logic helps you accelerate the development and deployment of applications in a modern software environment.

**Key Capabilities**

- **Full-stack visibility** for gathering event streams from modern applications at every stage and combining them with time-stamped metrics for comprehensive visibility in real time
- **Secure, real-time access** to production logs for full-stack visibility and live tailing
- **Machine learning** using pattern recognition and outlier detection to correlate logs and metrics across multiple data sources by reducing hundreds of thousands of results into a handful of meaningful patterns—for identifying errors before and after releases, lowering false positives and comparing behavior across clusters
- **Integrations across the development and operations tool chain** for out-of-the-box monitoring and troubleshooting of Github, Dockery, Artifactory, Chef and other tools

**Value Delivered**

- **Improved visibility** across development and production environments for a full view of everything for more predictable releases and fewer problems in production
- **Continuous development, testing and delivery** with deep visibility into the DevOps toolchain and processes for quality code and rapid releases
- **Monitoring of how users are interacting** with applications to drive the design of better software

**Run**

In the run phase of continuous innovation, continuous intelligence delivers visibility across modern applications and underlying infrastructure, including deep integration with AWS or other public-cloud platforms and integration across existing toolsets and the helpdesk.

While **build** is about accelerating development and deployment of applications in a modern software delivery lifecycle, **run** is about ensuring performance and availability through full-stack visibility of the modern applications and the underlying infrastructure. Applications are not an island separate from the infrastructure anymore—managing an application is essentially managing the entire IT stack that the application depends on.

In this environment where applications are running on complex, abstracted architectures such as IaaS, PaaS, containers and microservices, many of them outsourced from third parties, full application stack visibility becomes the key to success. By correlating real-time metrics of key indicators such as CPU utilization, number of sessions, errors and so forth with event streams from log data, operations teams can better track the performance of applications and perform troubleshooting, root-cause analysis and advanced
analytics. This visibility has to go beyond the application and extend all the way through the containers, the infrastructure layers and into the database.

Advanced analytics and machine learning are critical to transforming raw machine data intelligence into business, operations and customer intelligence. Machine learning can alert IT to problems they haven’t detected, suggest questions they haven’t asked and give advanced notice that enables them to take action before problems affect customers ensuring that modern applications deliver the highest levels of performance and availability. Issue identification and problem resolution times need not be negatively impacted when using modern application architectures and processes.

**Sumo Benefits**

Sumo Logic delivers full-stack visibility, real-time monitoring and advanced analytics for troubleshooting to help you ensure the performance of your applications and infrastructure—moving from incidents to insights.

**Key Capabilities**

- **Real-time monitoring** with a unified view of logs and metrics that enables you to surface streamed data on customizable dashboards, dynamically alert on key metrics and KPIs immediately, identify problems and detect outliers and abnormal behavior

- **Visualizations of key metrics and KPIs**, including image usage, container actions and faults, and CPU, memory and network statistics

- **Troubleshooting and root-cause analysis** for quickly getting to the source of problems across applications and infrastructure to improve IT operations

- **A powerful query language** for creating custom and aggregate KPIs and metrics

- **Advanced analytics based on machine learning**—with powerful features such as LogReduce, LogCompare and Outlier Detection—to identify patterns and anomalies, detect problems and predict issues before they impact your customers

**Value Delivered**

- **Move from reactive to proactive problem solving** by troubleshooting problems quickly and using machine learning to surface potential issues before they impact your customers

- **Frictionless cloud migration** with better visibility into cloud applications and underlying infrastructure, including pre-built dashboards and collectors for AWS and other common technologies

- **Insights into customer behavior** to make data-driven decisions (based on your log and metrics data) by understanding critical usage, customer and system trends to influence business, technology and investment decisions
Secure
As application teams work to secure their custom applications and the infrastructure stack those applications run on, as well as SaaS-based productivity solutions such as Office 365 and Salesforce.com, the next phase of collaboration—DevSecOps—needs the visibility into those workloads to address security monitoring, forensic investigations and regulatory compliance mandates such as PCI DSS and HIPAA.

What is DevSecOps?
DevSecOps is a new way for security practitioners to operate and contribute value with less friction. DevSecOps embraces the agile principle of rapid iteration and strives to develop security as code versus a bolt on approach.

A major shift is underway in the way that IT approaches application security. In traditional data centers, security was an afterthought, bolted on, with chokepoints and limited visibility. And for the last 10 to 15 years, security information and event management (SIEM) systems have been the primary tool of choice for IT Security teams.

But in the age of modern applications that are running on cloud-based architectures such as AWS and Azure, these on-premises, high-cost solutions are ineffective.

The legacy SIEM solutions, with lengthy deployment and protracted time-to-value hinder the agility required for modern applications. According to a Ponemon study, the average time to deploy a SIEM solution is 15 months and costs over $1.3M.¹ So in cloud deployments, security needs to be built in from the outset and enabled as instances are spun up, automatically.

Security professionals need something that will help them look for the needle in the haystack where the needle is the security event and haystack is a mountain of machine data. They’re no longer looking for a specific known event, which SIEMs do well. They’re looking for the unknowns, and they don’t even know the questions to ask. So SIEMs are giving way to the new category of security analytics leveraging the latest science in machine learning.

In addition, the need to comply with internal policies and external compliance mandates such as PCI, HIPAA/HITECH, FISM, GLBA and COBIT is increasing every day, and the penalty for noncompliance can be loss of customers, additional audit cycles, fines and even lawsuits.
Sumo Benefits
Sumo Logic simplifies and automates compliance and security monitoring for a safer, more compliant cloud.

Key Capabilities
• Audit-ready compliance reports, pre-built searches and dashboards from your event logs and time-series metrics to simplify audit reporting and accelerate audit cycles
• Composite view across your network, server and application stack to strengthen your security posture
• Machine-learning algorithms to surface suspicious activity and ward off known and unknown threats rather than relying on pre-built rules and alerts
• Cloud application monitoring to audit who is logging into SaaS applications, from where and who has viewed/exported data

Value Delivered
• Continuously demonstrate compliance and shorten audit cycles with centralized logging and search capabilities to meet compliance mandates such as PCI, HIPAA/HITECH, FISM, GLBA and COBIT
• Gain visibility across your cloud and hybrid cloud workloads to correlate security data generated by networks and servers for comprehensive insights and fewer false positives
• Uncover security events without relying on rules or pre-defined schemas by applying machine learning
• Improve the security of your cloud application data such as Office 365, Google Apps and Box by identifying user and administrative actions and any unusual behaviors that may compromise security across your cloud applications

Why Choose Sumo Logic?
Sumo Logic is the market’s only cloud-native, machine data analytics platform, powered by advanced machine learning and delivered as a service. By turning machine data into continuous intelligence, the Sumo Logic platform aids application developers, operators and security professionals in their build, run and secure processes. In addition, the unifying of logs and metrics in a single platform environment increases cross-functional collaboration—from IT to Lines of Business—to enable digital businesses to execute differentiated offers and services with speed and agility.

Machine data, in the form of logs and time-series metrics, is the output of the most powerful trend in technology today—the digital transformation of the business. And as businesses embrace digital transformation, innovation and disruptive customer experiences become increasingly dependent on modern applications. Software no longer drives business processes; it drives business models.

Sumo Logic offers five value propositions that are essential to the development of modern applications.

1. Instant value. Our pure SaaS offering gets you started in minutes and gives you instant access to the latest capabilities. You can start small and expand as your business grows.

2. Elastic scalability. Our multi-tenant architecture scales on demand to support rapid application growth and cloud migration. You can burst as needed without manual intervention.

3. Proven proactive analytics. Our powerful machine learning and analytics—with pattern, and outlier detection—help you make sense of expected and unexpected behavior to shift you from reactive to proactive mode. With Sumo Logic, log and metrics are viewable in real-time, side-by-side and overlaid, for deeper, contextual insights into application needs and new customer opportunities.

4. Security by design. We are the industry benchmark in delivering secure SaaS. The highest level of security certification protects your applications—including CSA STAR, PCI DSS 3.1 Service Provider Level 1, ISO 27001, SOC 2 Type II Attestation, FIPS 140 Level 2 and HIPAA.

5. Reliability. SLAs ensure that services are always on and performing at peak efficiency and we publish live performance status.

More than 1,000 customers trust Sumo Logic to build, run and secure their modern applications. You can get started now with Sumo Logic Free: www.sumologic.com/signup-free/.

Sources:
1 IBM QRadar Security Intelligence; Independently conducted by Ponemon Institute LLC, February 2014.