sumo logic

WHITE PAPER

Improving federal IT modernization outcomes with data analytics

Federal agencies are increasingly adopting cloud technologies and services as part of their digital transformation strategies and initiatives.

Market analysts point to significant increases in federal cloud spending from year to year, and many expect this trend to accelerate as cloud adoption reforms outlined in the government's Cloud Smart initiative take hold.

However, as agencies move more applications and workloads to the cloud, their applications, security, and DevOps teams are experiencing new security, performance, and compliance challenges. They are finding that their traditional IT security and operations tools, skill sets, and approaches are not designed to meet the unique needs of cloud environments.

This should come as no surprise since cloud environments differ significantly from the on-premises IT environments that are common across government.

For example:

- Cloud environments are highly virtualized and dynamic. As a result, applications also must be built and deployed in ways that take advantage of cloud computing as a delivery model.
- Cloud-based applications are typically separated into containers and oriented around microservices to provide greater efficiencies in both software development and deployment into multiple production environments. This focus on applications from the perspective of containers and microservices is at the center of modern software development, operations, test, and security approaches, such as DevOps, DevSecOps, and Agile.
- Cloud-native environments rely heavily on automation, so tasks occur more rapidly and at greater frequencies.
- Cloud environments are extremely dynamic because the applications operating in them are extremely dynamic. Applications are programmed to use only the resources they need at a given moment, so they allocate and de-allocate resources on the fly.

For IT organizations used to managing single-tenant, on-premises infrastructure environments, these features can be disorienting. In addition, the state of commercial information technology has changed considerably in recent years and federal agencies are trying to keep pace. For example:

- IT teams today work far more collaboratively than they used to. IT operations, DevOps, and security teams at many enterprises are organized today in ways that promote greater communication, shared effort, and integration.
- Acquiring modern IT capabilities no longer consists of a rigid process, outlining the requirements upfront. Instead, IT capabilities are developed iteratively, using agile approaches, and undergo constant evolution to respond to dynamic needs.
- Tools used to monitor applications — which, until recently, were highly fragmented and disparate — today must deliver more holistic and integrated views of what is happening across distributed, cloud-based environments.

Different Tools, Approaches Are Needed for Today's IT Environments

Federal agencies that have made the strategic decision to integrate data and IT as central pillars of their operations have embraced these and other shifts occurring across the IT landscape. But to adjust to this shifting IT landscape, agencies needs tools and approaches that are optimized for cloud-native environments.

A key aspect of this shift is a recognition that IT infrastructure, applications, and digital services must be viewed and monitored in terms of security, availability, and performance in a holistic, data-driven way. Traditional approaches to IT monitoring, which tend to be slow and fragmented, cannot effectively mitigate against security, operational, and cost risk. Specific dimensions of this problem include:

- Slow and costly mean times to identify (MTTI) and mean times to repair (MTTR) problems. As DevOps teams release products with greater frequency and employ automation more, performance and availability problems have increased. The result is that ops teams spend more time troubleshooting, while development teams are drawn into production troubleshooting. Consequently, reducing MTTR and MTTI is more important than ever.
- Delays in discerning between performance problems and security problems. Traditional IT monitoring tools focus on one segment or dimension of the infrastructure, so they lack the ability to "connect the dots" from multiple data sources to truly understand what is happening. This leads to delays that can lead to a worsening of the problem.
- Obstacles to collaboration between IT operations, development, security teams. DevSecOps merges two seemingly opposing goals — "speed of delivery" and "secure code"— into a single streamlined process that incorporates security into the code level. Security testing is done in iterations without slowing down delivery cycles, and critical security issues are dealt with as they become apparent, not after a threat or compromise has occurred. Siloed thinking is replaced by increased communication and collaboration, and responsibility for security tasks is shared during all phases of the delivery process. There are too many interactions taking places in a DevSecOps environment to decipher without a unified approach for monitoring. Monitoring tools must be capable of developing desired baseline and alert levels, so that IT teams can interact in real-time and automate common responses to conditions or threats.

Modern IT Monitoring Requires a New Data Analytics Approach

STo effectively address these risks and challenges, federal agencies today require cloud-native, machine-learning, data analytics capabilities to manage the operation and security of mission-critical modern applications and infrastructure.
Only by collecting and analyzing machine data of all types — logs, metrics, events — in real time can a federal enterprise effectively identify, troubleshoot, investigate, and resolve performance, security, and compliance issues. Many of today's monitoring solutions collect only one or two varieties of data, making it challenging to pinpoint the root cause of a problem, especially if the cause is complex.

Today's modern DevSecOps platforms empower teams to quickly identify, triage, and investigate issues that span diverse operating environments much faster than traditional tools. Unified log analytics platforms give cross-functional teams an easy way to collect, analyze, and develop insights from largely fragmented systems because of the ability to bring together highly disparate data from multiple sources. Once data is inside the platform, on-demand resources are provisioned to index and search workflows that make metric extraction simple for graphing trends in dashboards, generating alerts for complex behaviors, and resolving incidents by understanding root causes.

To understand why incidents occur, teams need to reconstruct timelines of events leading up to an incident. Corrective action only begins when teams can build deep insights from large swaths of unique data types such as OS logs, host metrics, and access logs at endpoints in addition to environmental information in network components such as firewalls, load balancers, and threat detection systems. Unified log analytics platforms make this type of data easily accessible in a secure way. With a fully managed analytics solution, teams never have to worry about deploying servers, installing software, or scaling their monitoring system when they need it the most.

This is the approach used by many top commercial enterprises, including AirBnB, Ameriprise, Anheuser Busch, Twitter, JetBlue, Salesforce, Caesars, MLB.com, Fidelity Investments, Marriott, Toyota, and others, to improve security, IT performance, and customer experience.

The Value of Modern, Unified Monitoring Solutions

Cloud-native monitoring platforms and tools enable agencies to reduce the complexity of administering, managing, and securing modern applications and infrastructures in the cloud. They automate delivery of visibility, intelligence, and insights that can be leveraged across the enterprise for use in the rapid detection, isolation, investigation and response to security, performance, and compliance threats.

Modern monitoring platforms also facilitate the integration of DevSecOps workflows, enabling agencies to have a shared source of visibility, truth, and analytics in the cloud, fostering greater collaboration, security, and efficiency in their application development lifecycles.

It is also important that monitoring solutions adapt natively to modern architectures to meet stringent demands for performance and scalability. Organizations today are increasingly employing technologies such as containers, microservices, and Kubernetes on cloud platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Traditional on-premises tools are not relevant for these new architectures because they just don't integrate or scale with the changing demands of cloud-native applications. Digital application workloads typically have highly variable loads that generate a tremendous amount of machine data.

Modern monitoring platforms enable agencies to straddle both modern and legacy architectures by providing a cloud native platform for any type of data to be brought in and quickly analyzed. Teams can correlate data cross the complete lifecycle of applications and hybrid infrastructure during projects.

These capabilities assist agencies across multiple use cases:

- **Migrating to the cloud**. Most agencies today appreciate the high value that machine data analytics brings to the task of managing application performance, security, and compliance. But as they head to the cloud, they will need a service optimally designed for the unique rigors and scalable, elastic architectures of cloud environments. To proactively monitor and troubleshoot application issues in real time, agencies need a cloud-native, multi-tenant solution that can transcend organizational silos to provide end-to-end, full-stack visibility into their applications to quickly understand and resolve operational, security, performance, availability, and compliance problems. With this level of visibility, agencies can accelerate time-to-market for cloud-destined applications.

- **Improved security posture.** As infrastructure defenses solidify for cloud environments, cyber attackers are finding targets of opportunities moving up the IT stack to exploit vulnerabilities in applications and digital services. Consequently, there is a greater need today to investigate threats at both the application and infrastructure layers and for security and IT operations to work together during threat detection and investigation. With cloud-native monitoring platforms and tools, agencies can effectively monitor and analyze the security posture of their applications and infrastructure, whether on premises or in the cloud, in real time and proactively alert security teams to suspicious anomalies or potential unauthorized access. Monitoring capabilities not only span activity occurring at the network's perimeter but throughout the infrastructure, including internally, to address insider threat activity and compliance enforcement (e.g. DISA STIG, DoD RMF, FISMA, NIST, etc.).

- **Improved customer experience.** Cloud-native machine data analytics also can assist agencies with monitoring and enforcing performance SLAs; improving end-user experience; minimizing downtime and reduce MTTI/MTTR; reducing IT operations cost and TCO; improving DevOps collaboration; and centralizing machine data management. Maecenas rhoncus nisi sit amet vehicula tincidunt. In id libero ac ipsum tincidunt congue. Sed bibendum ullamcorper laoreet. In id libero ac ipsum tincidunt congue. Sed bibendum ullamcorper.

Conclusion

Federal agencies today are encountering a fast-shifting IT landscape that presents new challenges and requires new rules of engagement. Traditional monitoring tools designed for on-premises IT environments cannot keep pace with the needs of dynamic cloud environments, DevSecOps practices and approaches, and modern IT diagnostics. Agencies require cloud-native monitoring platforms and tools that will deliver holistic visibility, intelligence, and insights and reduce the complexity of administering, managing, and securing modern applications and infrastructures in the cloud.

About Sumo Logic

Sumo Logic's secure, cloud-native, data analytics platform, turns machine data into real-time continuous intelligence, providing customers with full-stack visibility, analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers leverage a service model advantage to accelerate their shift to continuous innovation, thereby increasing competitive advantage, business value and growth.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Accel Partners, DFJ, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital and Sutter Hill Ventures.

s u

See business differently

m o

sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com