An Introduction to AIOps

Application development has evolved over past 25 years, but **monitoring and operations management has stood still**. As cloud computing environments grow more complex, enterprise firms face new challenges that burn time and capital expense, inhibiting growth and stifling their success. In this paper, we explore a new paradigm of IT operations, **AIOps, which provides cloud-first companies a path forward** to more intelligent, efficient operations.

ENTERPRISE IT FOR A CLOUD FIRST WORLD

The prominence of cloud computing has changed the way enterprises build, manage and scale apps. Large organizations have reorganized their IT and development centers. Enterprise companies must deliver great products with the challenge of rising Operating Expenses (OpEx). Agile development practices have changed the way we architect every aspect of the application stack. These systems output tremendous amounts of data about user behaviors and application health. Companies can find insights within this data to create efficient operations, reducing OpEx. Due to environment complexity, businesses must use advanced analytics to uncover these insights.

Due to cloud environment complexity, businesses must use advanced analytics to uncover insights that lead to reduced cloud OpEx.

These analytical practices ushered in the discipline of IT operations and analytics (ITOA). In 2012, a Forrester report [1] shaped the early ITOA narrative. “IT analytics tools hold the promise of helping IT organizations better manage the technology that runs their business,” the report notes. “Think of it as turning the concept of big data inward to make better decisions about the business technology services and the underlying infrastructure and applications.” By 2020, 25% of the Global 2000 companies will deploy an ITOA platform, compared to 2% today [2]. Spend on ITOA amounted to $1.7B in 2014, and will grow by an estimated 70% in 2015 [3]. These trends show that businesses believe in ITOA as a critical discipline in the cloud computing age.

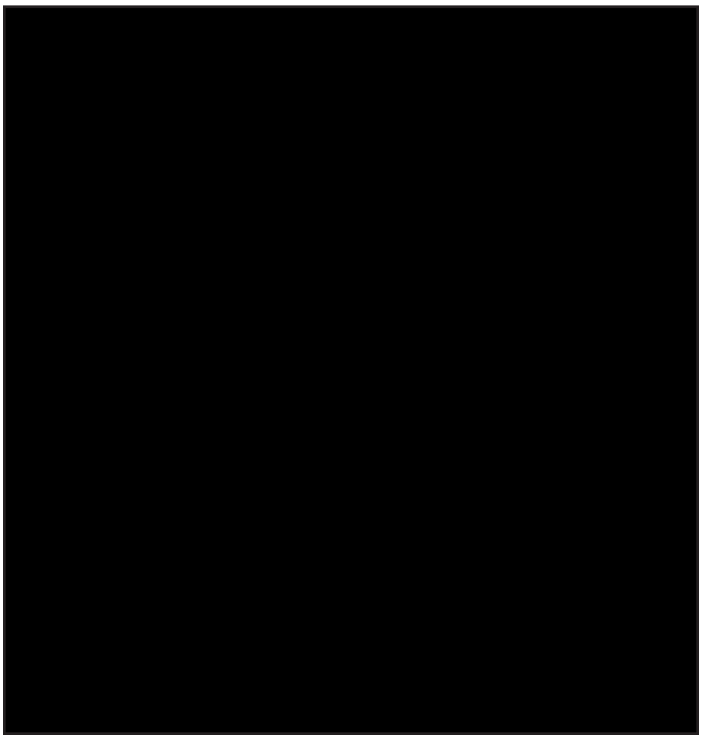
The ample amount of raw data combined with mathematical algorithms gives businesses an edge in IT management. Cloud device data (i.e. telemetry data) provides a clear depiction of environment activity. With OpEx on the rise, businesses hope insights from this data can curb cloud spend. Furthermore, this data can create other competitive advantages as well. YMor, a Netherlands based ITOA consultant, notes ITOA “[brings] together multiple sources of data to enable data-driven IT Operations, delivering consistent, high-quality results for maximum digital performance, availability, security and agility” [4]. To underscore this point, ITOA provides the most value when organizations can correlate several data streams together. A DevOps team determining the root cause of an application issue would need data available from the host as well. ITOA platforms that bring these streams together can provide a significant operational advantage.

This telemetry data and information from systems of record need further human expertise and interpretation, making it a challenge for businesses to adopt an ITOA practice. Cloud

computing has contributed to explosion of available data, which can be cumbersome for IT to manage. According to Big Panda, “IT is struggling to keep up with the pace of change, and the rush to modernize is leaving DevOps leaders looking for a better solution” [5]. Many companies rely on several tools to monitor and analyze telemetry data. Most of these companies dislike their ITOA and monitoring strategy. One major pain point stems from human operators to using intuition to create arbitrary, threshold based alerts to stay on top of IT data. Many monitoring platforms lack the flexibility and ease of use to help operators pick the right thresholds for alerting. Big Panda notes, “Of those who receive 100+ alerts per day, only 17% are able to investigate and remediate the majority within 24 hours.” As a result, one can trace most OpEx spend back to the need for talent to close the monitoring gap and make ITOA practices succeed. Unfortunately, firms are struggling to find and keep experienced IT operators. In one study by McKinsey&Company, 35% of executives surveyed believed improving IT talent and capabilities would lead to better IT performance. The study notes that “two-thirds [of executives] agree that it’s a significant challenge for their organizations to find, develop, and retain talent, with IT executives even more concerned about this than their business peers” [6]. While ITOA can provide promising insights, tools within this space today are still unable to address these concerns.

IT Operational Analytics platforms can reduce some cloud monitoring complexity, but it does not tie into the rest of the DevOps ecosystem to provide significant value alone.

Even with ITOA platforms, enterprise organizations have trouble bridging the gap from insight to action. The most advanced ITOA platforms often serve up information with little additional value. During a major incident event, ITOA tools provide tertiary information that provides the most help in hindsight. Companies spend between 3 to 6 hours repairing an app related problem [7]. Almost 15% of the time, more than 10 people are necessary to resolve such problems. According to the EMA, “[a] majority of companies are still trying to manage complex applications with a combination of “all hands on deck” interactive marathons and tribal knowledge” [7]. While ITOA can reduce some monitoring complexity, it does not tie into the rest of the DevOps ecosystem to provide significant value. In the end, enterprises need a comprehensive solution to reduce the IT burden ushered in by cloud computing.



THE PROMISE OF AIOPS, BROUGHT TO YOU BY GROK

Grok (online: grokstream.com) provides an answer to ITOA's shortcomings by combining machine learning and automation, dubbed AIOps. "In ITOA, network managers were getting analytics about the network after the fact; it was all observational data," Colin Fletcher, Gartner, explains. "Now, we can look at what's going on in the network in real time, diagnose the issue and then automate a fix" [8]. By combining machine learning analysis with IT automation, businesses can create systems that proactively respond to cloud events based on advanced insights from telemetry data. Rather than putting the explanatory burden on human IT operators, the system can take steps to go the last mile during critical incidents. Instead of having several people in a situation room, machines can do the heavy labor and let humans conduct further analysis to prevent further issues. Grok and AIOps stands to change the face of enterprise cloud management forever.

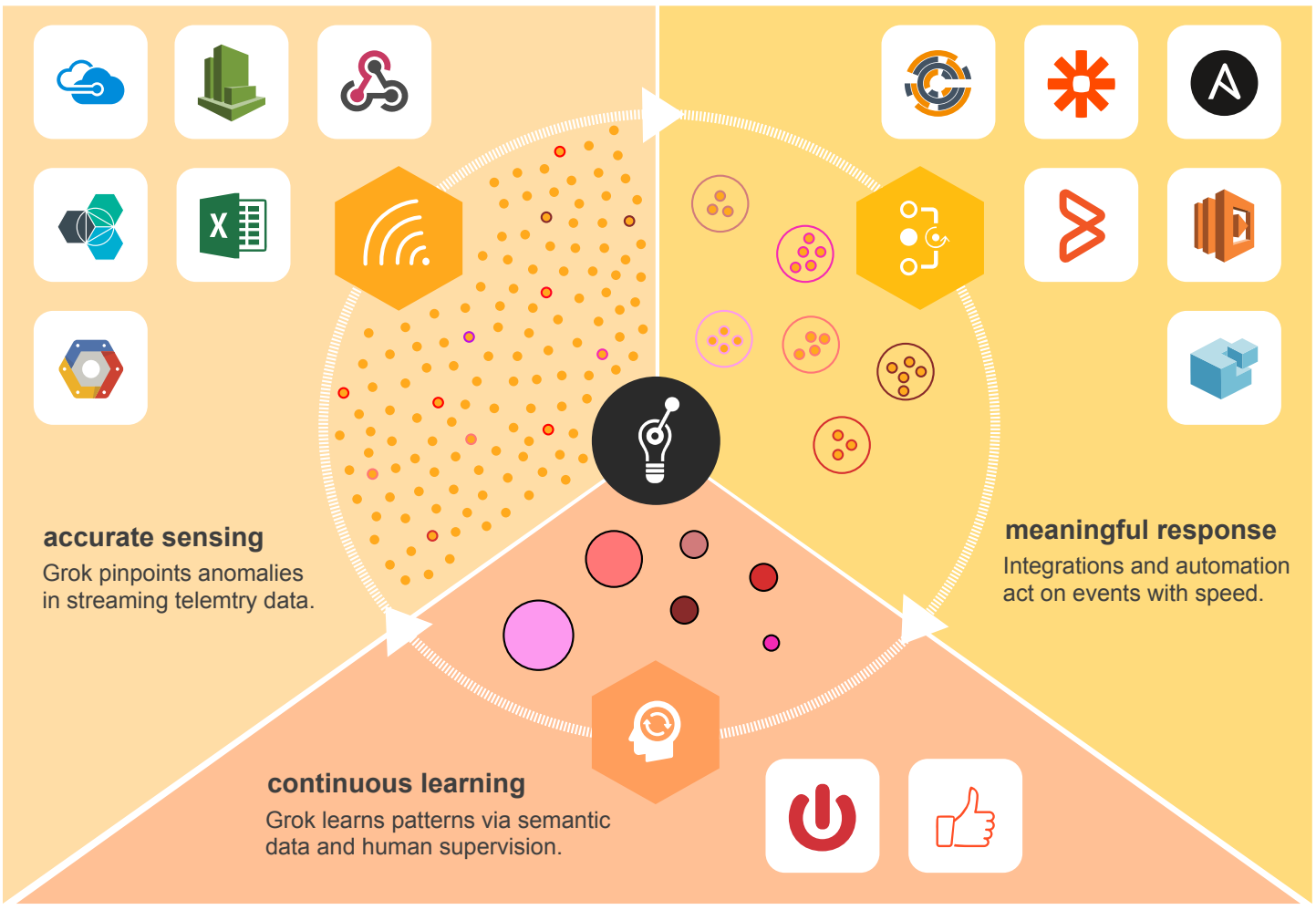
By combining machine learning with IT automation, businesses can create systems that proactively respond to cloud events based on advanced insights from monitoring data.

IT telemetry data can be an ideal dataset Grok's advanced machine intelligence capabilities. Enterprises that wish to move to an AIOps based practice must reconsider the storage, management and retrieval of telemetry data. The benefit of this analysis are immense. According to one survey of enterprise companies, most IT organizations believe ML will increase IT staff productivity; improve performance; heighten security; extract business insights; and reduce IT costs (OpEx) [9]. Since cloud computing can lead to device proliferation, IT may need to spend some effort building a foundation for AIOps by breaking data silos across cloud environments and customer experience data. Grok provides adapters and expertise to bring enterprise companies along this journey, making it easy for IT to get started with AIOps in minutes.

Grok's AIOps platform for the most common, challenging events that IT operations face today:

- Grok can detect DDOS attack at network level, shutting off ports to prevent further intrusion and issuing a security alert.
- Grok can detect a bad code push via a sudden activity on CPU utilization and a memory leak, which leads to rolling back a change and using failover to ensure users are not disrupted by code.
- Grok can even track spend on cloud servers and can produce reports on nefarious resources which lead to high costs.

Grok's unique, biologically inspired, approach provides a competitive edge for enterprises moving at the speed of cloud computing.

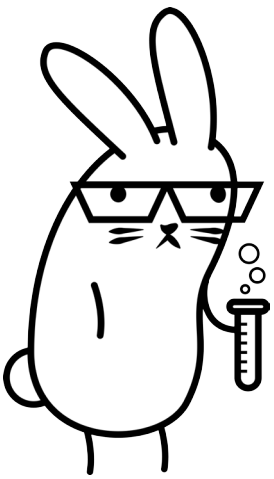

accurate sensing
Grok pinpoints anomalies in streaming telemtry data.
meaningful response
Integrations and automation act on events with speed.
continuous learning
Grok learns patterns via semantic data and human supervision.

HOW GROK ENABLES SELF-HEALING SYSTEMS

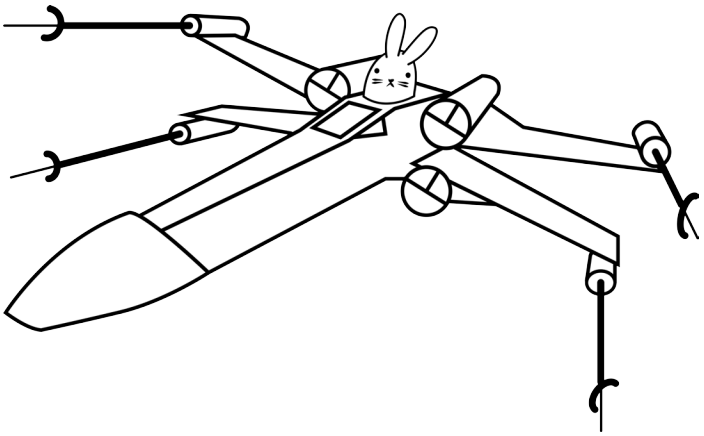
Grok combines industry leading machine intelligence and automation to create self-healing cloud operations. The future of cloud operations will behave much like human biology. Humans have a high resilience to change and can adapt to their environments in a moments notice. Responses to sudden shifts come from constant monitoring and the use of heuristics

Grok combines industry leading machine intelligence and automation to create self-healing cloud operations.

developed after years of observation and evolution. Analogously, enterprise applications will respond to problems first sensed within signals available in telemetry data. Grok finds anomalies within this data, correlating them with findings from other streams to trigger cloud operations events. These triggers can kick off automations to a wide variety of DevOps tools companies trust today, such as Ansible or SaltStack. Grok's sense engine leverages 10+ years of R&D in the ML space, providing the most accurate anomaly detection available today



[10]. The platform's REST API provides an intuitive interface to the entire platform, creating an open layer of intelligence for the entire business.



Grok provides a developer friendly user experience and turnkey integrations to tools IT operators trust. Within minutes, developers can stream any data to Grok to begin analysis, with the first insights coming in just a few hours. Grok alerts operators based on patterns found within the data, rather than arbitrarily assigned thresholds. These patterns update with each additional datapoint, providing the real-time analysis companies need to move with speed during an IT incident. Grok will integrate with systems of record to provide semantic understanding to the insights it generates, providing a critical vector to resolving an incident and reducing MTTR. These insights can also provide another layer of intelligence on customer experience metrics, received by Grok via Webhook or a .csv file. With a small amount of effort, businesses can see measurable improvement with Grok's AIOps platform.

Grok leverages readily available cloud data, IT systems of record and automation capabilities to provide a powerful application of an AIOps strategy. Within minutes, IT organizations can harness the power of machine learning and automation to detect issues before they occur and act with speed.

Enterprise, cloud-first companies across the world need AIOps more than ever so they can stop on fighting fires and focus on innovation. It only takes a few minutes to begin the AIOps journey with Grok, and our combined 30+ years of enterprise expertise can help guide you on the journey to smarter, more efficient operations.

We look forward to helping businesses on their AIOps journey. Visit our website at grokstream.com for more information. If you'd like to request a demo or learn more about our AIOps vision, please email us at:

contact@grokstream.com

[1] O'Donnell et. al. (2012). "Turn Big Data Inward With IT Analytics." Forrester. Available Online.

[2] Cappelli (2013). "IT Operations Analytics: Big Data for the Data Center." Gartner IT Infrastructure & Operations Management Summit: Orlando.

[3] Cappelli (2015). "Organizations Must Sequentially Implement the Four Phases of ITOA to Maximize Investment." Gartner. Available Online.

[4] YMor. "IT operations Analytics, from rear iew mirror to glass globe." Available Online.

[5] Big Panda (2016). "State of Monitoring 2016 - Full Report." Available Online.

[6] Khan and Sikes (2014). "IT under pressure: McKinsey Global Survey results." McKinsey&Company. Available Online.

[7] Enterprise Management Associates (2015). "Application Performance Monitoring (APM), 2015 -- Industry Challenges, State of the Art, and the Case for Unified Monitoring." EMA Whitepaper. Available Online.

[8] Zurier, Steve (2016). "ITOA to AIOps: The next generation of network analytics." SearchNetworking by TechTarget. Available Online.

[9] Extrahop (2017). "Machine Learning Survey -- Hope or Hype for IT?" Extrahop. Available Online.

[10] Numenta (2017). "NAB -- The Numenta Anomaly Detection Benchmark." Numenta. Available Online.