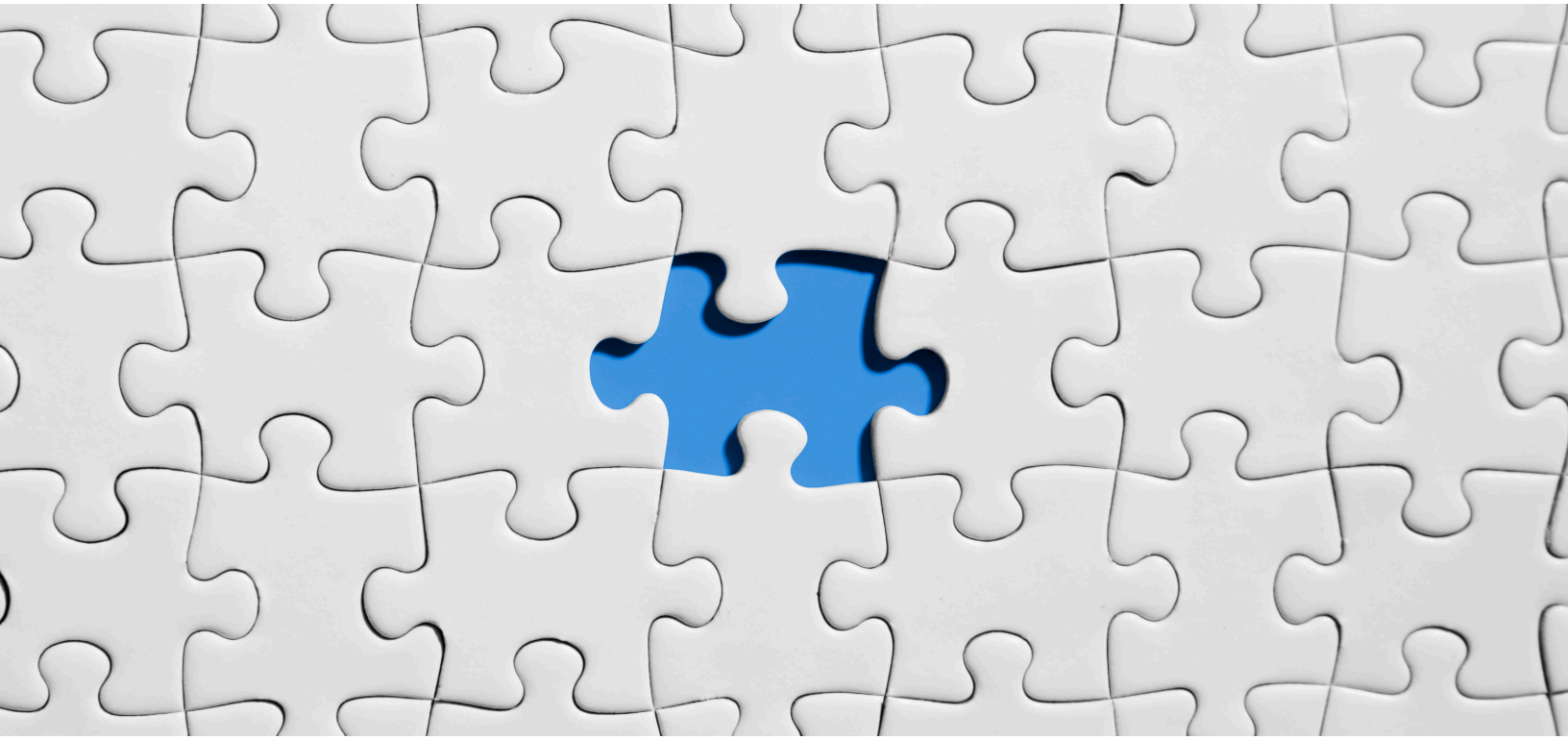
DELL Technologies

REDEFINING WORKPLACE PARADIGMS THROUGH AUTONOMOUS OPS



Mohammed Hashim

Head - Technology Innovation Council

Digital Infrastructure

Brillio

Mohammed.hashim@brillio.com

Knowledge Sharing Article

DELL Technologies Proven Professional

Table of Contents

1. Overview

A long holiday weekend of fun with friends and families was on the minds of thousands of air passengers in UK traveling with British Airways on May 2017. However, the days turned out to be one of the largest computer system outages[1] leaving about 75,000 passengers stranded, 400+ flights cancelled, the airline incurring compensations to the tune of more than USD 100 Million and losing its market value by USD 200 Million on the next trading session. Can you imagine all this just started with an IT support person unintentionally pulling a wrong plug in the datacenter of British Airways? To add to the woes, their IT Ops Command Center took more than a day to recognize the problem, act and fully restore services over three days. Apparently, no one was prepared to deal with such human error!

According to Veriflow Survey[2], 97% of datacenter outages are caused due to human errors such as support professionals inadvertently adjusting the temperature from Fahrenheit to Celsius; accidentally pulling power cords from an IT asset; or overloading a circuit by accidentally plugging in a server. These examples and more pose one of the biggest internal threats to enterprise business continuity.

So, is there a smarter way out?

Although we might never eliminate human errors completely, there are smart choices in both technology and platforms to reduce the severity and impact. As machines increasingly mimic and complement humans in the workplace, the future of work is shifting towards Autonomous Ops (AO) otherwise known as AI Ops (coined by Gartner) or Cognitive Ops (coined by Forrester).

Although Artificial Intelligence (AI) is driving the Fourth industrial revolution, CIOs are struggling to integrate AI into their regular IT operations which in turn affects overall business outcomes. In today's highly competitive digital world, business outcomes are only as good as the overall customer experience that IT Ops teams enable directly or indirectly. However, with the ever-increasing volume, velocity and variety of data, alongside the presence of multiple tools and platforms, it is becoming increasingly difficult for IT teams operating in domain silos to simultaneously ensure a reliable experience and run efficiently at scale. Although domain-centric tools can provide a deep dive into the nuances of a specific domain, they lack the ability to provide a correlated, end-to-end view across domains. This widens the gaps of accuracy and agility for critical decision making on the fly as depicted in Figure 1.

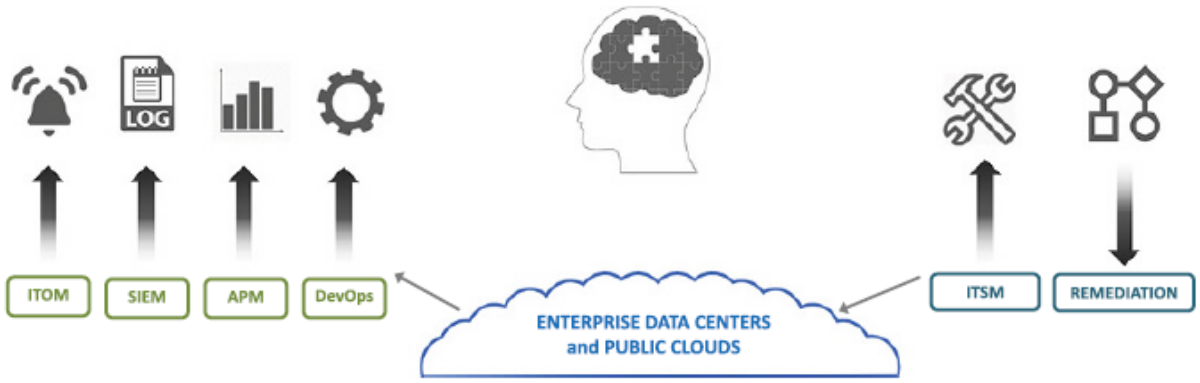


Figure 1: IT Operational silos limit Digital Business velocity (Source: FixStream)

To be future-ready and support the development and deployment of innovative models or applications, organizations need Autonomous Operations (AO) solutions. In the coming decade, AO powered by AI technologies and Intelligent Automation will transform the workplace as people increasingly interact with ever smarter systems. This would also require higher cognitive skills such as creativity, critical thinking, decision making and complex information processing across workplaces leveraging AO platforms.

This article discusses in-depth the application of AO primarily leveraging Big Data Mining, Deep Learning and Cross-platform data processing platforms to drive auto-remediation, self-optimization and self-healing. It would also guide enterprises for pragmatically adopting AO into mainstream business to usher in higher productivity and enhance business performance while changing the skills required of human personnel. Strategic and technology catalysts for tackling various hurdles during solution implementation and the workplace of the future are also examined.

The article would help organizations, CxOs, technology partners, solution architects and futurists on the tactical and operational aspects for exploring beyond conventional IT service delivery models to evolve and discover newer digital opportunities.

2. Where is the Industry Headed?

Digital transformations of Social Computing, Mobility, Analytics and Cloud (SMAC) has not only accelerated the pace of business across industries, but also led to organizations adopting hyper-connected applications, thereby increasing reliance on the underlying enterprise infrastructure running their critical business applications. Additionally, IT infrastructure is becoming more geo-distributed, heterogeneous, intelligent, open and virtualized to support the rapid growth, agility and scale of the business. Application architecture is also changing to adopt new technologies such as containers to create 'build once, run anywhere' code for portable applications, enabling faster deployment of application entities in multiple data centers and clouds.

While Infrastructure and Applications have radically transformed and advanced, IT Operations has not kept pace even with conventional scripting and basic process automation techniques where changes happen on the fly.

- Yankee Group estimates[3] the Total Annual Spend on IT Operations Center Salaries today is in the range of USD 120 Billion.
- The Average Cost per Minute for Service Outages[4] is about USD 72 Thousand, according to a Digital Enterprise study.
- According to Trace3 research[5], the Average Cost of a Data Center outage is about USD 740 Thousand.
- Gartner forecasts[6] that about 40% of CIOs will lose their jobs in the next 5 years as a result of failing to deliver business outcomes.

IT Ops has to be well ahead in this heterogeneous dynamic environment to track continuous changes and correlate system events by processing massive amounts of varying data, in order to identify patterns, detect anomalies and predict Capacity, Availability, Performance (CAP) requirements. So much system noise makes it extremely difficult to uncover the true events and resolve the priority incidents. This results in tremendous business risks and hindered business innovations. In today's digital economy, Autonomous Ops powered by AI is becoming mainstream for transforming IT Operations across industries.

3. Demystifying Autonomous Ops

Today, only a fraction of organizations has deployed and used Autonomous Ops (AO) at scale. CIOs are already being challenged to create an agile infrastructure to support their organization's AI strategy:

a. To build AI native infrastructure architectures and business applications.

b. To augment IT capabilities with contextual intelligence to help them make smarter and faster decisions.

c. To redefine End User Experience from service or product design to consumption across increasingly diverse environments.

This involves migrating from a less complex deterministic to very complex non-deterministic model requiring continuous, proactive, creative testing, AI training, monitoring and adaptive evolution in the technology world. AO platforms leverage Machine Learning (ML) and Deep Learning (DL) to augment human intelligence and pave the way for phenomenal user experiences and boost operational efficiencies. Figure 2 shows the functional building blocks of a typical AO platform.

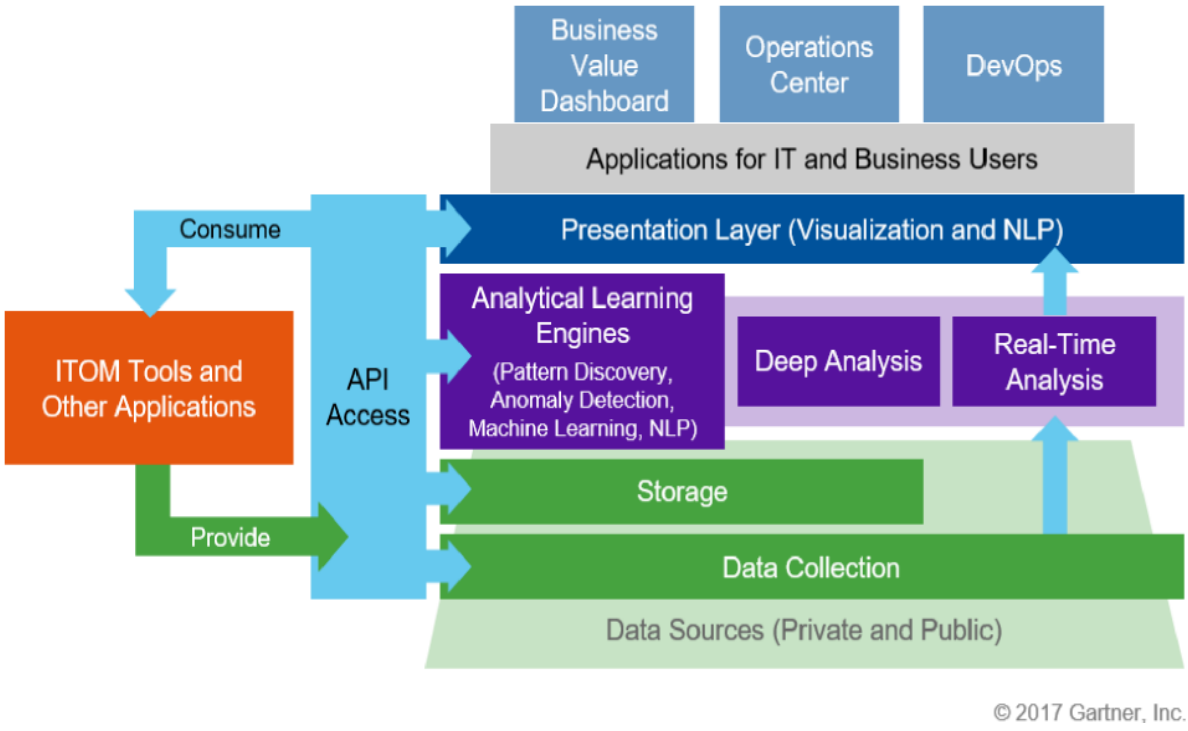


Figure 2: Functional Diagram of AO Platform (Source: Gartner7, August 2017)

As depicted in Figure 2, there are three primary components to AO:

1. **Big Data**: Multifaceted data gathered across the various data touchpoints and includes Application and Infrastructure monitoring, transaction job details, system event logs, service tickets and business metrics among many others.
2. **Machine Learning/Deep Learning**: Comprehensive analytics and ML/DL algorithms applied on the combined collated data.
3. **User Persona-based Actions & Visualizations**: Tasks and process automation based on processed data to yield continuous business insights and aid continuous service improvements.

An AO platform typically bridges three disciplines to accomplish strategic business and tactical operational goals:

1. **IT Service Management**: The entire set of activities directed by policies, organized and structured in processes and supporting procedures that are performed by an organization to plan, design, deliver, operate and control IT services offered to users.
2. **Application Performance Management**: The monitoring and control systems that ensure that the applications and underlying infrastructure that users work with meet best in class performance standards and provide a quality end user experience.
3. **Business Process Automation**: Automation of business processes for simplifying usage, achieving digital transformations, increasing service quality, improving service delivery and/ or containing costs.

So, the first thing needed is to get your enterprise data together. If you don't have sufficient data that's worthy of analysis, AO isn't going to help you much. If you have huge and varied data spread, i.e. events, tickets, metrics, logs, etc. or issues with data quality where 'structured' data is poor and critical information is in 'unstructured' data, AO solutions are pretty good at handling it. There are a wide variety of AO platforms available that bring AI and Business Intelligence to IT Operations. Prominent names in this space include Splunk IT Service Intelligence, Moogsoft AIOps, BMC TrueSight Operations Management, IBM Netcool Operations Insights, MicroFocus Ops Bridge and FixStream.

4. Changing Workplace Paradigms

First, AI adoption to realize AO does not literally replace IT personnel. Rather, it helps them execute daily operational tasks such as system troubleshooting, CAP management, transition and planning. It can also offload many mundane menial error-prone tasks from IT personnel, letting them focus on more strategic and advanced activities that can directly improve business operations.

"Most recent advances in AI have been achieved by applying ML to very large data sets," notes McKinsey. "ML algorithms detect patterns and learn how to make predictions and recommendations by processing data and experiences, rather than by receiving explicit programming instruction. The algorithms also adapt in response to new data and experiences to improve efficacy over time."

AO platforms support auto-discovery and ML to uncover, correlate and analyze all the data from multiple enterprise applications and infrastructures quickly and accurately, providing advanced visibility into their vulnerabilities by detecting patterns and predicting outages. Thus, AO can help IT personnel thwart system failures, security issues and performance bottlenecks; thereby keeping the business running and satisfying customers. Figure 3 shows a high-level view of AO platforms breaking IT operational silos and integrating the various domains.

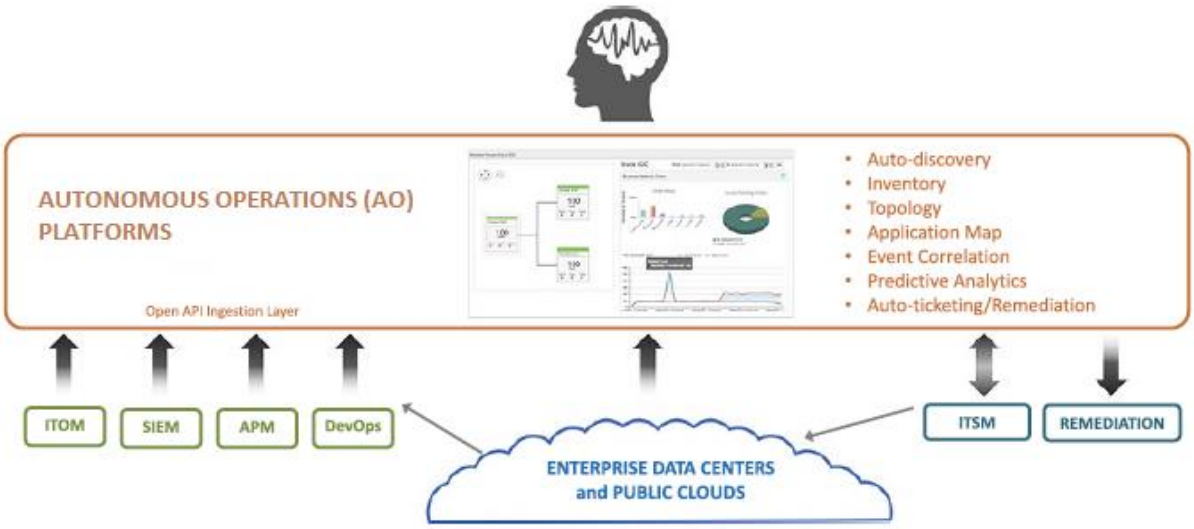


Figure 3: AO Platforms breaking IT Operational silos (Source: FixStream)

Here, ML and DL can correlate and analyze data from multiple enterprise applications and infrastructures, dealing with the volume, velocity and varieties of data generated. It can uncover patterns to show what has occurred; use current conditions and past learning to spot exceptions and make predictions and even recommendations based on various scenarios.

Common use cases where AO platforms enable IT Operations with AI capabilities include:

- Multivariate anomaly detection across various dependent entities. Such anomalies may signal that a planned or unplanned event has occurred. For example, a multivariate anomaly group may represent an unplanned event such as a Distributed Denial of Service (DDoS) cyberattack or a planned business event such as Black Friday.
- A time-series sequential-pattern-detection algorithm can predict business outages triggered by events anywhere business functions are deployed in the stack.
- Applying AO to automatically recognize common infrastructure performance issues and then help recommend fixes or just automate common steps in remediation such as cycling power on hosts, logging information to databases, entering trouble tickets or restarting a failed service.
- AO can also interactively predict CAP requirements based on different capacity/demand scenarios and help in proactive demand management. For example, it could simulate and assess a potential deficiency of storage-disk volume capacity and probable excessive network-bandwidth utilization which in turn can affect business performance and service availability.
- AO can continually and completely look for traffic exceptions. As a result, they can be far more effective in preventing and quickly responding to cyberattacks to keep businesses up and running round the clock.
- Site Reliability Engineering (SRE) incorporates aspects of software engineering and applies that to IT operational challenges of running production systems at scale by focusing on reliability as a primary goal. SRE involves extremely complex systems that enable the business to navigate the tricky path between feature velocity and operational stability. AO can help automate critical incident response to improve user experience and business service levels.
- Microservice architectures, containers and cloud help simplify the application development process, providing environmental consistency and speeding updates. However, there are operational trade-offs due to the transient states combined with API-centric communications resulting in a data deluge of objects, dependencies and metrics. AO can help DevSecOps teams with advanced analytics and valuable insights for efficiently and securely managing these modern application environments of cloud and containers that eventually affects the end user experience.

AO platforms are disrupting traditional IT Operations management using AI-driven analytics, correlation and dynamic visualizations to provide real-time actionable insights that help radically reduce MTTD/MTTR, optimize resources, predict outages, avert disruptions and automate corrective decisions, de-risk migrations, improve compliance and enhance business outcomes. As AI becomes more embedded onto devices, applications and infrastructure, users may not even be able to differentiate between the native and applied innovations that help solve the many problems facing enterprises in this age of digital transformations, where IT becomes more virtual, dynamic and distributed over time. Here, the technological nuances of collating data across various entities (e.g. users, business, marketing, IT, facilities, etc.), interpreting the data, finding anomalies and patterns, performing data correlations and presenting it back to an integrated command center may seem oversimplified.

AO helps with simplification, automation and costs optimization. It also enables moving away from siloed operations management and provides intelligent insights that drive automation and collaboration for continuous improvement and faster IT Operations. Gartner defines AI Ops platforms as software systems that "combine big data and AI or machine learning functionality to enhance and partially replace a broad range of IT operations process and tasks." These platforms ingest data from a variety of sources, store the data, provide access to the data, and enable data analytics at the point of ingestion and storage. They do so in a timely and cost-effective manner to predict potential issues, detect security vulnerabilities and remediate incidents in real time. The ultimate goal is to predict a problem and act before the problem actually occurs.

5. AO Adoption Approach

Today data is flowing across the digital ecosystem at the speed of light. Sensors, mobiles, smart gadgets, intelligent appliances, supercomputers, cybernetic applications and smart buildings; all are sending user data, systems data and business data. Gathering this vast amount of data from multiple sources at one place, analyzing it, and processing it to generate meaningful insights for the business is an epic challenge for the digital enterprises of the future.

While technologies become complex, IT becomes bimodal and user behavior drives IT consumption. Enterprise Operations Support will need to drive IT as proactive IT operations analytics rather than a reactive task force. Compounding the data volume, variety, velocity and value challenges is the ever-growing variety of specialized monitoring tools for network, logs, applications, storage, databases, cloud, web and system resources.

Although, many next-gen monitoring solutions have attempted to collapse the growing variety of siloed solutions through "Single Pane of Glass" initiatives, usually the only lasting result is the implementation of an overarching event aggregator layer to consolidate events from the various silos with limited correlations; meanwhile, the variety of dozens of underlying specialized monitors remain. This complex and dynamic operational haze just increases troubleshooting time, complicates decision making and slows service restoration. Actually, support teams alone can't keep up with the volume, value, variety and velocity demands of today's IT Ops environment. Apparently, we are becoming the problem and not the solution.

Digital Enterprises should consider AO as a tactic because AO is not a strategy or goal in itself. The biggest mistake would be when large enterprises initially discount the importance of AO and wait until most of the early AO limitations are addressed before trying to catch-up at great costs. Figure 4 shows the keys to a successful AO adoption, based on the Gartner research[8].

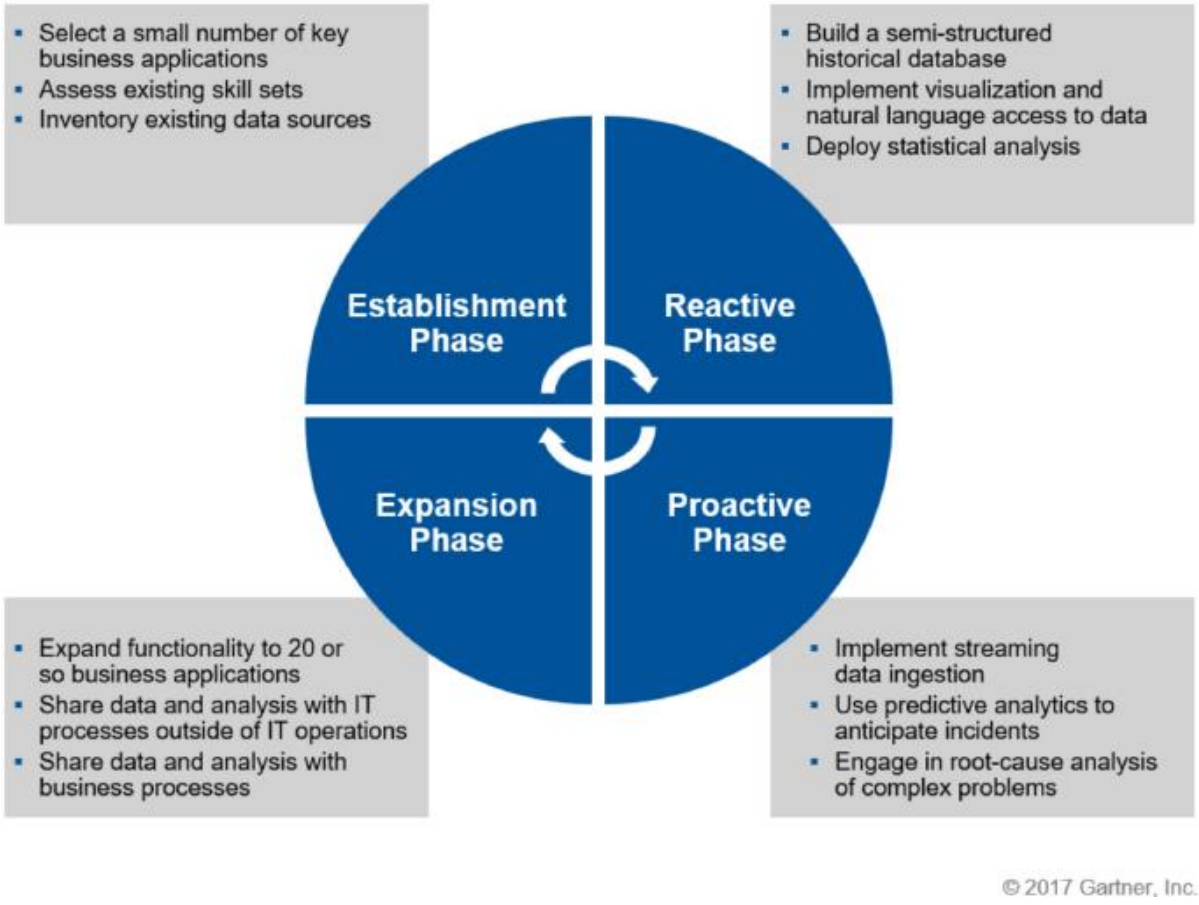


Figure 4: AO Adoption Approach (Source: Gartner[8], 2017)

The four-phased AO adoption approach are:

1. **Establishment Phase**: Setting up the starting point for deploying AO by piloting a small set of Test Cases and determining Existing Resources.
2. **Reactive Phase**: Deploying AO technologies and processes for Reactive Use Cases by applying Visualization and Statistical Analysis to a Historical Semi-structured Database of IT Operations Data.
3. **Proactive Phase**: Deploying AO technologies and processes for Proactive Use Cases by applying Machine Learning and Causal Analytics to both Streaming and Historical IT Operations Data.
4. **Expansion Phase**: Extending AO capabilities across the Enterprise by applying proven AI processes and technologies to a broad range of Business, Application and Infrastructure Issues.

Figure 4 lists the 12 steps across above 4 phases for adopting AO into mainstream IT. An enterprise scale AO platform reference architecture is covered in Appendix-B.

6. Market Drivers and Restraints

According to Gartner research[9], "by 2022, 40% of all large enterprises will combine big data and machine learning functionality to support and partially replace monitoring, service desk and automation processes and tasks, up from 5% today."

AO basically involves applying AI for enhancing IT Operations by using ML/DL to analyze the data that's collected from various sources and help spot and react to issues in real time. AO platforms also can consume (ingest, monitor and analyze) vast amounts of machine data generated by Business applications and IT infrastructure to predict issues before they occur. An overreliance on AI could result in people missing out on what's right in front of them. With the massive and rapid shift towards cloud adoption, intelligent automation and continuous improvement, AO is here to take care of the new entrants into the digital ecosystem – Virtual BOTs, Machine agents, Artificial Intelligence, IoT/IIoT devices etc. These new entrants are impossible to service and maintain by humans alone and with billions of connected devices, the ideal way forward is to adopt AI algorithms that can tackle known problems.

Major Market Drivers

1. Increasing demand for Predictive analytics solutions
2. Need for accelerated time-to-value in the Digital economy
3. Growing demand for Business Intelligent IT Operations/systems
4. Increasing hyper-connectivity across Applications and Infrastructure
5. Government/Geographical requirements for cybersecurity-compliant IT solutions
6. DevSecOps requirements to come up with agile value propositions at speed and scale
7. Enterprises pursuing rapid digitalization for adapting continuously to changing markets, customer needs/behavior and advanced technologies such as AI

Major Market Restraints

1. Technology hype and earlier AI tools and platforms failing at cost and business value realization
2. Cultural inertia against adopting newer technology for unsupervised analysis of massive digital data sprawl
3. Nascence of Industry vertical knowledge in AI platforms to generate meaningful outcomes specific to the core domains
4. Fragmented AI Market flooded with many variations lacking uniform standards in data processing, management, security and system integrations

The market drivers would shift the balance and offset the restraints in due course with rapid advancements in AI and as most digital-savvy enterprises begin embracing AO on a larger scale.

7. Study of AO in Hybrid Data Center & Multi-Cloud Management

The promise of AO lies in bridging the gaps between predictable operations and dynamic business demands of the digital era. In Hybrid Data Centers and Multi-Cloud environments, AO platforms should primarily address the below functions:

1. Unified monitoring and management of Applications and Infrastructure
2. IT process automation for incident remediation and service restoration
3. Real-time analytics and business service management

AO platforms adopted here should have the capability to:

1. Detect operational anomalies and determine root cause
2. Provide noise reduction and intelligent event correlation
3. Ingest and aggregate event data from various monitoring silos
4. Provide decision support mechanisms for IT personnel during troubleshooting
5. Integrate with the IT process workflows for ticketing, notification, event and incident management

In the digital age of connected systems, networks and ecosystems, enterprises run business 24x7 irrespective of physical location or time zones. Organizations expect their systems to be "always on" and their users expect data to be immediately accessible. Hence, even minute unplanned service downtime is risky, expensive and unacceptable. This in turn ceases productivity resulting at times in lost, damaged or destroyed data. Consequently, as systems become inaccessible for longer durations, a domino effect unfolds with the organization's customers, business partners and/or suppliers unable to access data to conduct business and process transactions.

How costly are unplanned DC outages? Businesses stand to lose thousands to even millions of dollars per minute. A 2016 report[10] from the Ponemon Institute found that the average total cost of a data center outage is USD 740,357.

What are the top causes of unplanned downtime? The major causes in descending order of incidents are: Human errors, Security flaws/breaches, Hardware/Software related problems, Systems interoperability and Migration issues and Natural disasters.

The Information Technology Intelligence Corp.'s (ITIC) 2018 Global Server Hardware, Server OS Reliability Survey[11] cited Human error as the No. 1 cause of unplanned downtime, Security ranked a

close second as a cause of outages. Other causes of downtime included software bugs and flaws, inadequate server hardware and complexity in configuring and provisioning new applications.

What are the common Human errors resulting in downtime? Common errors are misconfiguration of server hardware, OSes, applications and devices; failure to upgrade or right-size servers to accommodate more data and compute-intensive workloads like virtualization, data analytics, AI and storage; failure to upgrade outmoded applications that are no longer supported by the vendor; failure to keep up to date on patches and security.

Adding to the list are classic oversights such as unplugging power cords, leaving a crucial port open, failing to disable a guest account, not adjusting the temperature in the data center or, forgetting to monitor server or disk capacity until it fails, or the machine's performance slows drastically.

What are the common Security aspects? Security[12] is part and parcel when it comes to downtime. The proliferation of mobile devices, endpoints and IoT deployments means that the attack surface has grown commensurately. This results in more potential vulnerabilities and entry points into systems, servers, applications and devices that must be monitored and managed. Additionally, an assortment of ever-more pernicious and pervasive security threats including viruses, ransomware, malware, phishing scams, BOTs, trojans, brute force attacks, Denial of Service, attacks on firewalls, switches and unified communication systems needs to be chased and deterred in real time.

Others include failure to implement upgrade policies and procedures to address issues surrounding cloud computing, mobility, remote access and bring your own device; failure to construct and enforce strong computer and network security policies.

Also, niche OEM/ISV vendors sometimes take weeks or even months to acknowledge and respond to security flaws in devices and applications. The longer the lag time before the vendor releases a patch, the higher the risk that organizations may experience a detrimental attack.

Do Business decisions also play a role? Yes indeed. This includes failure to allocate the necessary funds to upgrade systems and applications; failure to provide crucial training and certification for IT and security administrators; and failure to implement computing policies and procedures such as performing regular backups and having a comprehensive disaster recovery (DR) plan in place. External business factors such as regulatory compliance can result in on-site inspections and litigation, forcing organizations to shutter operations for days or weeks before the situation is resolved. Examples of short-sighted decision making include: failure to calculate total cost of ownership (TCO) and ROI,

failure to track hourly downtime costs, failure to track and assess the impact of service level agreements (SLAs) and regulatory compliance issues (e.g. Sarbanes-Oxley or HIPAA).

What are the key takeaways from the root causes? Although, the root causes of most downtime are the same as they were two or three decades ago, the frequency has increased. The prevalence of technologies like virtualization, cloud computing, mobility and Internet of Things (IoT), which link servers, applications, devices and people potentially heighten the risk and severity of downtime occurrences. So many systems are now interconnected, there's a much higher risk of collateral damage, i.e. more servers and devices can get taken out at once, even if they're isolated in containers.

Post-outage remediation is always time-consuming and costly. Further, unplanned outages are a risky business and they increase the risk of litigation and damage to the company's overall reputation too.

What is the smart way-out leveraging AO? The AO in Data Center and Cloud space fall into two broad solution categories[13]:

1. **AI-workload-optimized computing platforms**: Here, IT platforms accelerate and automate AI workloads through pre-built combinations of storage, compute, and interconnect resources. The prominent hyperconverged infrastructure appliances include:
    a. Dell EMC VxRail with AI-optimized hardware that manages complex workloads in hyperconverged infrastructure
    b. Dell EMC VxRack SDDC with AI-optimized chipsets in hyperconverged server platforms

2. **AI-augmented infrastructure optimization tools**: Here, AI is becoming an essential tool for accelerating, scaling, automating and otherwise optimizing infrastructures at every level. AO solutions enable these benefits by driving real-time monitoring, predictive analysis, root cause diagnostics and anomaly detection on system- and application-level events in IT infrastructure, and also in data, application and services at higher layers in the cloud computing stack.
    a. At the software level: There are diverse range of AO vendors such as Moogsoft, BMC, Extrahop Networks, Big Panda, and AppNomic Systems Inc.
    b. At the hardware level: Dell EMC PowerMax storage array-AI as an IT infrastructure management accelerator; Dell Precision Optimizer 5.0 - AI that configures hyperconverged hardware for application acceleration for on-the-fly system configuration to boost the application performance.

8. Future of Autonomous Ops

According to Data Bridge Market Research[14], the Global AI Ops Platform Market is expected to reach USD 18.51 billion by 2025 from USD 1.76 billion in 2017 and is projected to grow at a CAGR of 34.2% in the forecast period of 2018 to 2025.

The digital world is slowly moving towards AI systems that can make important decisions or perform vital actions on behalf of humans. AO will gradually phase out the way businesses develop and deploy next generation of enterprise applications with built-in intelligence involving multi-level structured/unstructured data integrations and running across multiple cloud platforms.

Further, the increasing scope of AO applications becoming verticalized across industries like retail, manufacturing, banking, healthcare, logistics, hospitality, gaming and others will drive demand in coming years, contributing to overall AI industry growth.

The prospects of AO are limitless as it keeps unraveling greater opportunities for transforming IT. It is also being positioned as the next generation of DevOps leading to Self-Healing applications. AO platforms reduce dependencies on specific tools and data changes, algorithms can help in bug-tracking and issue tracking services coupled with business process integrations for assessing the behavior of infrastructure, monitoring real-time application performance, evaluating end user experience and optimizing costs by dynamically managing cloud and/or platform utilization.

AO platforms would also unify user inputs across Virtual Personal Assistants such as Voice BOTs and Chat BOTs to optimize work processes and revamp end user experience. As AI algorithms evolve to combine Big Data and ML functionalities, it would lead to digitization of workforce to support and partially substitute conventional monitoring, service desk and automation processes at the workplace. A dynamic digital workplace paradigm for organizations of the future is discussed in Appendix-C.

9. Conclusion

As digital transformation's importance has continued to grow, CIOs are asked to focus on one goal: Delivering exceptional digital experiences to customers. It's a top CIO priority in 2019 and ahead.

According to Mckinsey[15], 20-30 Million new jobs (for humans) will develop to accommodate AI automation by 2030.

According to a PwC study[16], economic gains due to AI adoption in the US and China alone will reach USD 10.7 Trillion by 2030.

Many businesses are already on board with AI, and others are planning to implement it. Forrester Research[17] says more than half of organizations already have some form of AI project, and it says another 20 percent are planning AI projects soon.

With the pace of technological and global change accelerating, seismic shifts seem to happen regularly with established institutions disappearing almost overnight and disrupters themselves disrupted in ever shortening cycles. The thing that doesn't change is people and finally everything is measured against the human yardstick. Human factors continue to be the defining criteria for technology solutions designed to solve real-world business problems, even where the solutions are meant to let machines automate human tasks.

AO solution providers need to acknowledge the very real challenges customers face with tools, knowledge and culture, map that against maturity and expectations and build solutions that engage with customers in the right way for where they are while providing a path to their desired end state.

AO is poised to become the next big thing in IT management and AI-led correlation can also execute a series of changes in IT operations and overall business performance. AO platforms will also play a pivotal role in overcoming the complexities of the current enterprise IT operations model and also pave the way for digital transformations of the Fourth Industrial revolution.

Appendix A: Research References

Footnotes

[1] https://www.networkworld.com/article/3200105/data-center/british-airways-outage-like-most-data-center-outages-was-caused-by-humans.html

[2] https://www.veriflow.net/press/veriflow-global-survey/

[3] http://start.bigpanda.io/rs/778-UNI-965/images/Autonomous_Digital_Operations-BigPanda_eBook.pdf

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] https://www.gartner.com/smarterwithgartner/12-steps-to-excellence-in-artificial-intelligence-for-it-operations-infographic/

[8] https://www.gartner.com/doc/3787367/-steps-artificial-intelligence-it

[9] https://www.forbes.com/sites/forbestechcouncil/2019/01/09/the-big-problem-with-big-data/#2d02ee0523b1

[10] https://www.vertivco.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

[11] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=23015323USEN

[12] https://www.networkworld.com/article/3142838/infrastructure/top-reasons-for-network-downtime.html

[13] https://siliconangle.com/2018/07/27/aiops-optimizing-cloud-computing-stack/

[14] https://databridgemarketresearch.com/product-tag/global-ai-ops-platform-research-report/

[15] https://www.mckinsey.com/featured-insights/future-of-work/ai-automation-and-the-future-of-work-ten-things-to-solve-for

[16] https://press.pwc.com/News-releases/ai-to-drive-gdp-gains-of--15.7-trillion-with-productivity--personalisation-improvements/s/3cc702e4-9cac-4a17-85b9-71769fba82a6

[17] https://www.forrester.com/report/Predictions+2019+Artificial+Intelligence/-/E-RES144617

[18] https://www.slideshare.net/IPEXPOEventSeries/splunk-for-aiops-reduce-it-outages-through-prediction-with-machine-learning-95666040

[19] https://dellemcstudy.blogspot.com/2017/11/customizing-it-user-experience-to.html

Bibliography

[20] The Industries of the Future by Alec Ross

[21] Gartner's 2018 Market Guide for AIOps Platforms

[22] AIOps for Dummies by Bishnu Nayak and Enzo Signore

[23] Forrester 2017 Vendor Landscape: Cognitive Operations

[24] AI and Analytics, Accelerating Business Decisions by Sameer Dhanrajani

[25] Life 3.0: Being Human in the Age of Artificial Intelligence by Max Tegmark

[26] The Sentient Machine: The Coming Age of Artificial Intelligence by Amir Husain

[27] Frontiers of Intelligent Autonomous Systems by Sukhan Lee, Kwang-Joon Yoon, Jangmyung Lee

[28] Top 10 Mistakes in Data Center Operations: Operating Efficient and Effective Data Centers by Bob Woolley

[29] Decrypting Practical AI-Empowering or Enslaving Humans by Mohammed Hashim from EMC Knowledge Sharing 2018

Web links

[30] www.bmc.com/blogs/what-is-aiops/

[31] www.nexthink.com/blog/the-best-aiops-tools/

[32] jaxenter.com/ai-as-a-smart-services-151863.html

[33] https://www.loomsystems.com/whitepaper-aiops-definition

[34] www.moogsoft.com/resources/aiops/guide/everything-aiops/

[35] www.splunk.com/blog/2018/07/10/the-future-of-it-operations-aiops.html

[36] www.analyticsindiamag.com/what-is-aiops-why-it-is-the-future-of-it-operations/

[37] http://ibmsystemsmag.com/power/systems-management/high-availability/human-error-is-top-cause-of-downtime/

Appendix B: Autonomous Ops Solution Architecture

An AO computing platform is key to realizing AI Ops or Cognitive Ops. Figure 5 depicts a reference Solution Architecture based on Splunk IT Service Intelligence (ITSI) that utilizes AI powered by ML to deliver predictive IT services and ensure optimal application performance and quality. Here, ML is made mainstream with Adaptive Thresholds, Anomaly Detection and Intelligent Event Correlations. Further the solution also provides Unified insights for Data-driven actions.

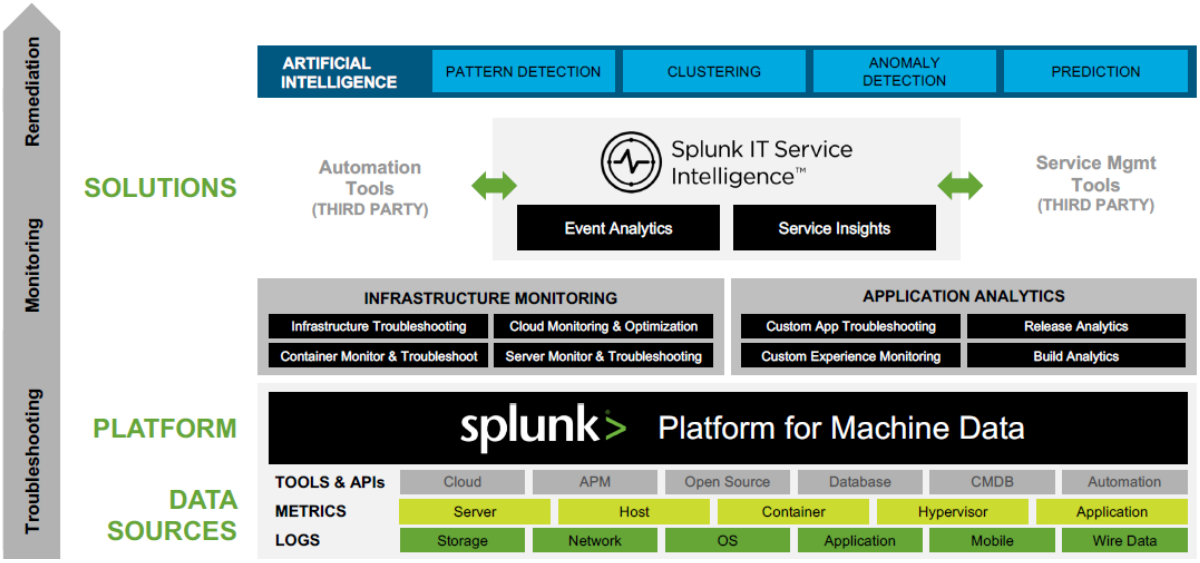


Figure 5: Autonomous Ops Solution Architecture (Source: Splunk for AI Ops[18])

The key platform components are:

1. **Machine Data Platform**: Ingests, stores and provides access to data from a variety of sources. It also enables data analytics at the point of ingestion and access.
2. **Service Intelligence Hub**: Data-defined Event analytics and data-driven service insights with integrations to third party service management and automation tools.
3. **Integrated Visualization Console**: Provides end to end visibility with real-time actionable insights across IT and Business; derived by applying AI analytics with interactive visualizations and business intelligence capabilities.

Appendix C: Digital Workplace Paradigms

Digital Organizations consist of different people with varying workstyles that today's IT workplaces need to accommodate as they strive to address the dramatic shift in what users want to be productive both inside and outside of the office. The major drivers of newly defined digital workplace experience are Flexibility, Collaboration and Mobility based on where, when and how they work.

The Digital Workplace Continuum shown in Figure 6 is based on the Dell EMC initiative to create a digital workplace that will meet the expectations of a workforce that expects technology to keep pace with what they use in their daily lives outside of work.

Figure 6: Digital Workplace Continuum (Source: Dell EMC Study[19])

It is predominantly defined around three prominent workstyles:

@home: For those who work from home via remote capabilities

@work: For those who work in the office in the more traditional workplace mode

@mobile: For those who work on the road using mobile technology

As AO platforms evolve, it should also address this by dynamically adapting to customized user experiences across the workplace to stay ahead of fast-changing working patterns, technology and shifting expectations of the Digital workforce.