

WHAT IS SOFTWARE-DEFINED IT OPERATIONS? SDITO EXPLAINED



Enterprise organizations adopted virtualization, automation and orchestration to realize the promised value propositions such as ease of infrastructure provisioning, management and maintenance. Yet, enterprise IT spends most of its time in efforts to merely keep the systems alive. With the increasing dependence on manual efforts, organizations find themselves violating IT policies, governance frameworks and organizational best practices pertaining to infrastructure management operations.

When the policies are inadequate and inflexible, IT teams may struggle to enforce them. When policies are too rigid and restrictive, organizations may fail to realize true growth and transformation potential of the IT. For instance, organizations may require IT to react before a particular incident escalates and impacts the wider infrastructure performance based on changing organizational policies. Considering the growing complexity of large infrastructure deployments, the process of manually investigating and identifying the vast events metrics for potential issues may be insufficient in understanding the root cause of potential issues. And when issues are detected, Ops personnel may limit the service availability and functionality to Devs working toward Agile sprints and rapid development, delivery and release cycles.

To automate the operations processes in alignment with dynamic policies and cross-functional IT requirements, progressive enterprises embrace a holistic and scalable approach to manage infrastructure environments and IT services.

Software Defined IT Operations (SDITO) aims to meet these goals by leveraging automation and a

software-driven approach to handle the growing IT management needs of complex and dynamic infrastructure environments. The evolving concept may not have a specific definition just yet but can be referred to as the automation and abstraction between the management layer and the control plane of the infrastructure. It can be seen as a software-focused approach to realize autonomous IT operations around management of infrastructure configurations, performance, service availability, issue resolution and [security](#), among others.

The key difference from standard IT procedures that may involve some levels of automation and intelligence is that the solution focus is on the software functionality instead of the underlying hardware. SDITO is not about a collection of disconnected software technologies offering various features to automate ITOps, but the entire software system abstracts the underlying manual procedures and hardware that is otherwise involved in delivering IT Ops functions. Modular functions are further managed using software and scaled across various infrastructure management operations without disrupting the systems. At the same time, the limitations of individual functions are also removed from the systems to ensure end-to-end Software-Defined IT Operations.

SDITO strategies can encompass four key aspects of infrastructure management and IT operations:

Automation: As an integral part of SDITO, the Ops processes are automated and software-based instead of slow and error-prone manual procedures. Automated protocols designed to enforce organizational policies should encompass the dynamic and complex IT environments without compromising the infrastructure scalability and performance or limiting the intended functionality for end-users. For instance, if the policy requires encryption of a particular set of server instances and Devs request scaling of the resources to meet new workload demands that fall within the same policy framework, then the policy enforcement should scale consistently with the infrastructure expansion. This automation is facilitated by the abstraction between the infrastructure control and management planes.

Intelligence: Using advanced algorithms, the system makes intelligent decisions based on key metrics and service requirements. For instance, automated noise reduction lets IT Ops identify the most impactful events and focus only on actionable incident alerts. Some events may need prioritizing based on changing service levels and dynamic infrastructure provisioning. The mechanism of intelligent decision making allows organizations to ignore the deluge of disconnected events and trigger proactive remediation of potential issues. The intelligence can be complemented by advanced Artificial Intelligence and Machine Learning capabilities to correlate events, understand the impact of incidents and perform self-healing measures to maintain infrastructure performance and service health for end-users. Intelligence is critical to understand the context of the incidents. Instead of relying on the limited human memory and capacity, the software processes and interprets incident data to anticipate otherwise unpredictable incidents or complex relationships between the anomalies.

Self-Service Operations: Growing technical debt, islands of automation and siloed IT environments make service provisioning a bottleneck process for Devs that require production-like environments for continuous deployment and release processes. With Software-Defined IT Operations, traditional ticket-based approach to infrastructure delivery is replaced with automation in compliance with organizational policies and governance frameworks. The infrastructure service delivery itself is automated and workloads are dynamically orchestrated to maintain optimum service levels, performance and governance standards.

Centralized Management and Integration: The dynamic nature of complex, siloed and

disconnected IT infrastructure forces organizations to perform manual changes repeatedly. ITOps personnel themselves fail to effectively coordinate infrastructure management responsibilities across those siloed IT environments. The lack of standardization further prevents organizations from scaling resources in compliance with the governance policies and framework. By applying software-defined processes to integration, IT Ops can consistently and programmatically configure, manage and maintain the entire lifecycle of IT service assurance that aligns with organizational goals.

Moving Toward Software-Defined Everything

The concept of commoditizing functional components in the enterprise IT segment was first applied to networking infrastructure, which resulted in the mature technology trend of [Software-Defined Networking \(SDN\)](#). Similarly, the concept applied to the technology infrastructure in the form of [Software-Defined Data Center \(SDDC\)](#) has allowed organizations to increase business agility and infrastructure scalability at a lower cost.

Moving forward, using software-defined capabilities to perform IT Operations has emerged as the next logical step to enable true [DevOps](#), where operations must meet business demands of infrastructure management, governance, control and service assurance. As the infrastructure resources adapt and perform in response to dynamic workload changes, IT managers struggle to enforce policies, optimize systems and adjust configurations based on evolving organizational requirements. Automation is a key enabler to fill this gap and intelligence is further required for the software systems to make the right decisions at the right time. At the same time, organizations also need abstraction from the underlying functional limitations of the hardware to enable agile implementation of automated, intelligent and software-based IT operations, also known as Software-Defined ITOps.