ScienceLogic

Seismic Shifts in NetOps: The Case for Modern Tools

Last updated: Apr 2021

Table Of Contents

Executive Summary

In recent months, a lot has changed in network operations (NetOps). Networks, architectures, and entire operational models have shifted dramatically—disrupting and destabilizing digital business services. Unfortunately, most NetOps teams are still relying on legacy tools and approaches. This white paper offers a look at how the world has changed, and the new capabilities your team needs to succeed. It also offers a close look at ScienceLogic SL1 and reveals how the platform offers you differentiated advantages.

Introduction: Shifting Business and Networks, Seismic Demands

For quite some time, your NetOps teams have been under intense pressure. They're tasked with playing a fundamental role in your organization's most strategic digital transformation initiatives. At the same time, they're responsible for ensuring optimized performance and service levels, while their environments continue to evolve rapidly.

These intense, mounting pressures were in play before the COVID-19 pandemic hit. Now, those demands have only grown more urgent. Virtually overnight, your teams had to adapt to entirely new operating models—not only for your external customers and internal workflows, but for the entire workforce. These new models present fundamentally different requirements for network resiliency, capacity, security, architectures, and more. Further, many of the digital transformation initiatives that may have been longer-term ambitions soon became need-to-have-it-yesterday mandates.

Given these changes, NetOps teams are struggling to adapt, forced to contend with unprecedented data:

Volume

Modern environments continue to grow more complex and hybrid in nature, featuring an increasingly diverse, distributed array of standards, services, technologies, platforms, and vendors—generating rapidly expanding quantities of data.

Velocity

In the wake of the increased reliance on cloud services, DevOps approaches, microservices architectures, and so on, environments—and the data used to manage them—continue to change ever more quickly.

Variety

More complex environments continue to generate a significant expansion in data sources and types.

The Challenge: Legacy Tools and Approaches Aren't Equipped to Address Modern Requirements

Within your organization, your teams are working with a set of tools and workflows that have taken shape over the course of many years. Over time, your teams have continued to add an array of point tools, focusing on a specific domain or technology. With these point tools, your teams lack a way to get a complete, end-to-end view of your modern, hybrid networks and the business services that rely on them.

Further, with increasing speed, those tools are being rendered obsolete by the volume, velocity, and variety of data that are in play today. As a result, when issues arise, unless the root cause is obvious, multiple team members are required to get involved, jump on calls or video conferences, and so on. Invariably, each team member will have their own set of tools, stifling effective collaboration. Following are just a few of the implications of these realities:

Poor User Experience

Too often, your teams are surprised by issues—and are left scrambling to address incidents after the fact.

Without a clear understanding of how the network impacts business services, your customers and end users encounter spotty service performance, which can translate to costly missed SLAs and outages, which lead to customer churn, lost revenue, and lost productivity.

Costly Inefficiencies

Lacking any unified visibility and automated triage, your teams wrestle with time-consuming, labor-intensive troubleshooting efforts. According to Gartner, root-cause identification typically accounts for 70% of the time it takes to restore a service to normal operation.[1] Because your teams lack cohesive visibility and controls, not only are operations inefficient, but environments are suboptimal. Consequently, as you strive to keep pace with growing demands, costs threaten to spiral out of control.

Stifled Agility

According to one report, 73% of teams spend more than half of their time just maintaining the status quo.[2] In recent months in particular, it has taken a concerted, bordering-on-heroic, effort merely to keep networks and the business running. However, this effort simply isn't sustainable. What's more, being all-consumed by the status quo means your teams are ill-equipped to adapt to accelerate application deployments, manage a cloud migration, boost security, and other strategic digital transformation initiatives.

[1] Will Cappelli, Vivek Bhalla, Take Six Steps to Find the Real Root Cause, Gartner, 17 May 2017.
[2] 2020 Cisco Global Networking Trends Survey,Cisco, 2020.

The Requirements: Why AIOps Is Critical

Now, successful teams are modernizing their toolsets to align with the unprecedented demands and realities they're facing. Ultimately, to establish these capabilities, top teams are investing in Artificial Intelligence for IT Operations (AIOps) platforms that deliver the following key capabilities:

Complete Service Visibility

To make sense of their complex IT environments, top teams are establishing a unified view across the entire ecosystem, compute, storage, networks, applications, and more. Further, successful teams will harness this data to establish visibility into services, not only network services but top-level business services as well. This visibility is vital in prioritizing efforts and investments based on business impact.

AI/ML-Driven Insights

To keep pace with the volume, velocity, and variety of their environments, effective teams harness the power of AI/ML to deliver actionable insights. As mentioned earlier, analysis is the most time-consuming aspect of incident management. Through AI/ML, teams can automate root cause and impact analysis of network operations, which can yield dramatic improvements in mean time to resolution (MTTR) and service levels.

IT Workflow Automation

Successful teams are maximizing the use of AIOps to automate routine operational tasks based on AI/ML-driven insights.

This includes automating the collection of diagnostic data, the exchange of real-time operational data between systems/platforms, the management of configuration items, ticketing and remediation workflows, and more.

By delivering the capabilities above, AIOps solutions offer the intelligence and automation that your teams need to manage dynamic, complex IT, and enable adaptable, shock-resilient operations and services.

The Solution: ScienceLogic SL1

The ScienceLogic SL1 platform delivers the advanced AIOps capabilities your IT and NetOps teams require. The platform monitors every layer in your complex ecosystems, making it a solution that one team can start with and the entire business can build upon. SL1 enables a shift from manual, device-centric efforts to automated, service-centric operations through three core capabilities: see, contextualize, and act.

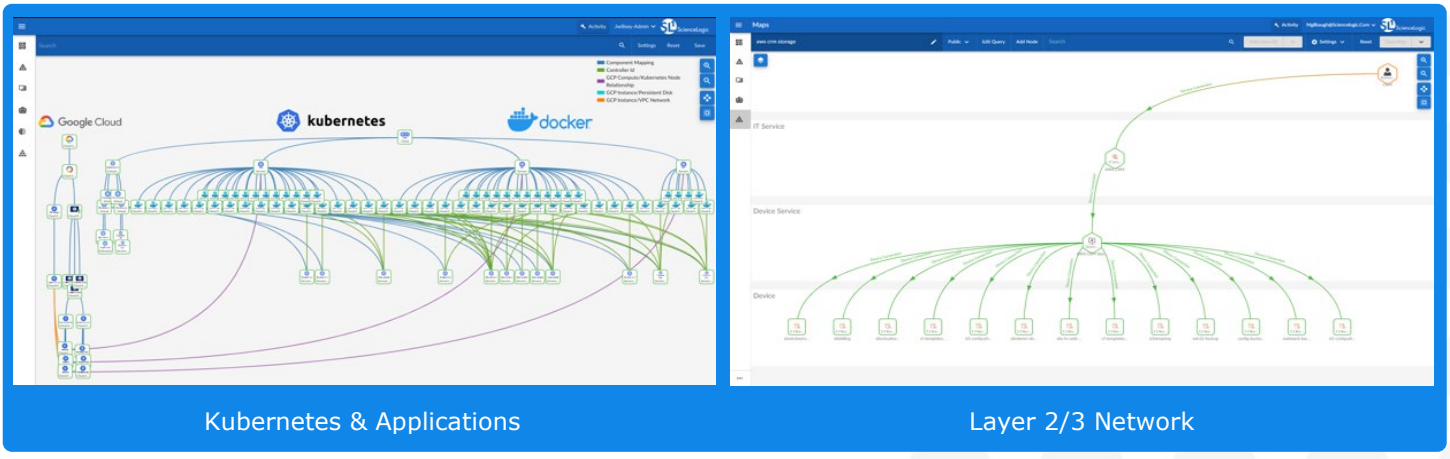
See

With SL1, you can automatically establish a comprehensive, real-time operational data lake that offers a standardized view and central location for all network and IT data. SL1 can ingest structured, unstructured, and topological data. The solution aligns, merges, aggregates, dedupes, and normalizes the data captured, helping to ensure the data collected is clean. According to Gartner, data scientists spend 79% of their time collecting, cleaning, and organizing data[3]. With SL1, you can minimize the time and cost to leverage your operational data.

SL1 discovers, maps, and monitors all network components across physical, virtual, software-defined, microservices-based, and cloud environments; including contextual insights into layer 2 and layer 3 connectivity, topological relationships and dependencies between applications, devices, and more.

The platform offers pre-packaged support for a broad range of systems and technologies, and it provides the extensibility required to incorporate data from specialized or new systems. SL1 offers extensive coverage of network environments (see figure 1), including:

- Utilization metrics, including uplinks, ISP connections, and P2P circuits
- VPN services, including concentrators, firewalls, and equipment
- Control plane and gateway protocols, including OSPF, EIGRP, BGP, and MPLS/LDP
- SD-WAN infrastructures, including those running on Aruba, Meraki, Silver Peak, and Viptela
- SDN environments, including those running Cisco ACI and VMware NSX
- Voice and video traffic, tracking IPSLA, jitter, packet loss, latency, and more
- Hardware, including Cisco IOS, Junos, and NX-OS



[3] Gartner, Deliver Cross-Domain Analysis and Visibility with AIOPs and Digital Experience Monitoring, 5 July 2018, ID G00352799, Charley Rich, Padraig Byrne

Figure 1: SL1 consolidates your toolsets into a single operational foundation for your entire IT landscape.

Contextualize

Once data is captured and prepared, teams can model and view their entire IT environment from a service context. This can include network services, for example, a virtual private network service delivered to employees, or full-stack business services engaged by consumers, such as finance, retail, and healthcare (see figure 2).

SL1 then applies a rich set of analytical techniques to effectively gauge the health, availability, and risk of business services. The solution's behavioral correlation employs ML to correlate not just events but also anomalies within a service context. With these capabilities, the solution cuts through the noise to quickly establish the impact and root cause of an issue. Because the solution can sift through massive volumes of data, it enables your team to keep in front of constantly changing environments. With the solution, you can:

- Rapidly identify service-impacting issues when they occur
- Uncover likely root causes in a few mouse clicks
- Detect anomalies that your team might never think to look for, and alert operators that a service-degrading event is likely to occur
- Recommend best practice triage and remediation actions

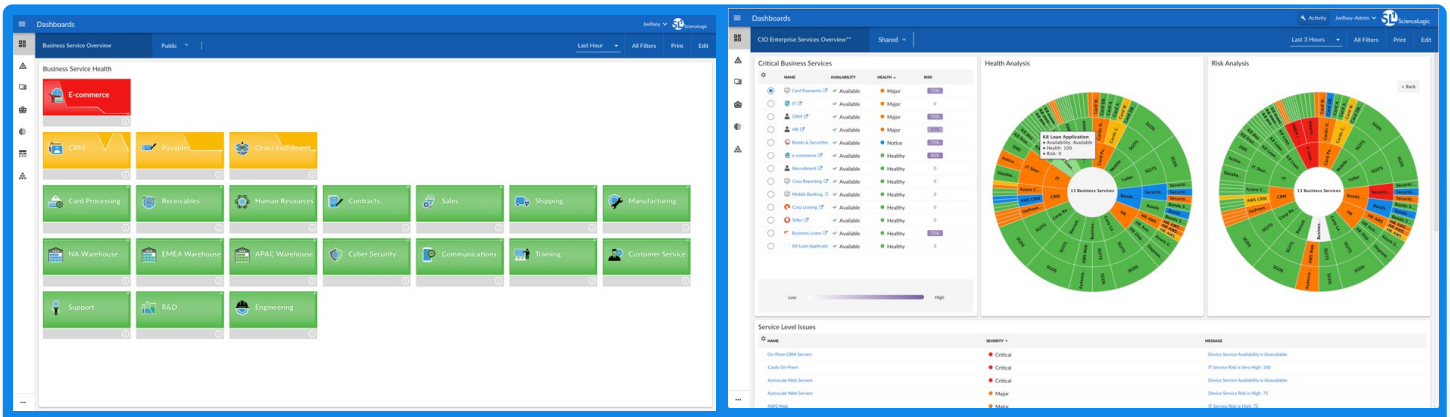


Figure 2: Shift from device to service-centric monitoring to prioritize work based on business impact

Act

SL1 enables you to gain a clear understanding of what's happening in your environments, and then take automated, fast action in response. With the solution, your teams can integrate and share data across technologies and your IT management ecosystem in real-time. Also, you can apply multi-directional workflow integrations to provide scalable automation for both responsive and proactive actions.

SL1 offers an extensive library of pre-built automations, featuring more than 350 triage best practices and 185 remediation actions. The solution also provides pre-built activities and low-code approaches that you can use to easily automate complex operational workflows.

The solution can automate incident management, including automatic enrichment of incidents with diagnostic data collection at the time that a problem occurs (see figure 3). In addition, it can synchronize all monitored configuration items, along with their relationships and dependencies, with CMDB platforms. For some service desks, SL1 can also pull scheduled maintenance windows to reduce event noise during scheduled downtime. The solution can also integrate with case management to support your use of incidents or cases in communicating with end clients.

SL1 features data and workflow integrations with a variety of third-party solutions and platforms, such as:

- Service desks/CMDBs (Cherwell, ConnectWise, Remedy, ServiceNow)
- NetFlow analytics solutions (LayerX)
- Network change and configuration management tools (RestorePoint)
- CI/CD tools (Puppet, Chef, Ansible)
- Notification tools (PagerDuty)

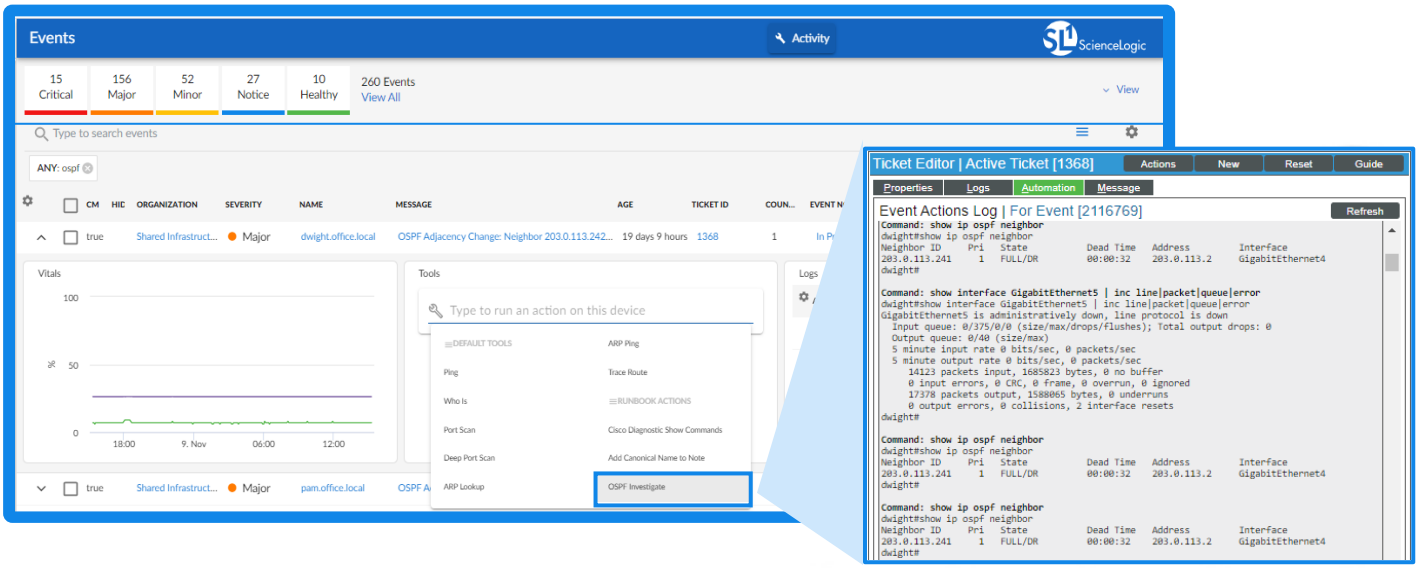


Figure 3: Drive NetOps efficiency and agility with automated ticketing, triage, and remediation workflows powered off the SL1 operational data lake.

Advantages

SL1 offers a number of distinctive advantages:

Near- and long-term value. The SL1 platform provides a single foundation that can easily support your immediate needs and accommodate more environments, teams, and use cases over the long term.

Breadth and depth of monitoring. SL1 helps you establish complete visibility of even the most distributed and complex environments. The solution collects events, performance, fault, configuration, and log data for a wide range of technologies, including network, storage, cloud, applications, and services.

Cloud-scale. SL1 offers a modern, scalable microservices-based architecture to support the high-volume, transaction-intensive environments of the most demanding enterprises and service providers. SL1 monitors over 500,000 devices; ingests more than 50 million metrics in under five minutes; for one client.

Advanced analytics and automation. SL1 makes it easy to apply advanced analytics and automation across all your monitored data, from within one platform, and completely at your own pace.

Full-stack business services. The platform rapidly discovers and maps topological relationships within and across vendors and technologies, aligning networks to business services. Easily extend your network monitoring to full-stack service monitoring across systems, storage, clouds, containers, and more.

"We originally invested in ScienceLogic to modernize our monitoring toolset, replacing multiple legacy monitoring tools, and allowing us to fuse data from across a wide range of network and infrastructure (including Aruba, Cisco, Palo Alto, Google cloud, VMware, and more) that support multiple branches and ATMs into a data lake that allows us to apply analytics consistently and drive automated workflows for notifications, ticketing, troubleshooting, and remediation.

Our primary business objective is to deliver secure online banking, anytime, wherever you are. ScienceLogic is providing the core foundation for infrastructure management which now allows us to introduce AIOps across our entire IT environment - from our data center to the cloud to end user edge devices."

— IT Network Edge manager, Financial Institution.

AIOps Use Cases Supported

With SL1, your NetOps teams can address the following core use cases:

Onboard new technologies and customers with speed and agility. Manual, multi-tool processes for provisioning new technologies and services lead to lengthy onboarding. By integrating with your Service Desk and provisioning tools, SL1 can automatically discover and populate new resources and relationships in your CMDB, and immediately start monitoring newly provisioned resources. By chaining tools together, SL1 increases IT agility while speeding onboarding and quote to cash processes.

Eliminate visibility gaps while consolidating tools. Organizations have major gaps in visibility across networks and business services resulting in high costs and poor user experience. SL1 helps consolidate and minimize your toolset, filling in monitoring gaps while reducing tool integrations and management costs required for full-service visibility. Thus, NetOps can more effectively focus on achieving business objectives.

Diagnose root cause faster to lower MTTR. Multiple legacy monitoring tools colliding with modern IT environments create the perfect event storm that overwhelms NetOps and extends the time to pinpoint root cause. SL1 ML-based behavioral correlation analyzes events and anomalies within a service context to quickly identify service impact, isolate root cause, and recommend triage and remediation actions.

Achieve CMDB accuracy with real-time sync of monitored environment. Many organizations struggle to keep track of their rapidly changing networks. Gartner states 75% of CMDB deployments fail because they are not built to handle today's huge volumes of frequently changing data. SL1 synchronizes your monitored network environment with your CMDB, which enables you to automate more IT processes.

Resolve incidents faster with automated ticketing and troubleshooting. NetOps teams often waste time manually gathering diagnostic data from a variety of methods, often well after network issues occur. SL1 provides a real-time operational data lake that enables automated ticketing and troubleshooting.

Automate operational data exchange for performance insights. SL1 can help you integrate and orchestrate people, systems, and processes across teams through data federation. Examples: service desk/CMDB, orchestration, financial management, business intelligence/analytics tools.

Benefits

When you employ SL1, good things happen. By leveraging the platform, your organization can:

Enhance network performance and user experience. Gain the intelligence and automation that can help your teams preempt outages and reduce the duration of those that occur. Customers have achieved a 98% reduction in downtime and cut SLA breaches by 60%.

Improve business outcomes. Deliver workflow automations that fuel agility and free staff up to focus on the most strategic transformation initiatives. One logistics customer digitally transformed its terminal operations to move 10 million containers a year by reducing their gate system checkpoint processes by 20X, from 10 minutes to 30 seconds per truck.

Boost operational efficiency. Realize significant reductions in operational costs by better understanding the impact of network changes on the health of business services. Establish effective NetDevOps competencies and better prioritize remediation efforts, investments, and plans. One customer reduced operational costs by more than $1 million dollars per year.

Navigate the AIOps journey successfully. The path to AIOps is an ongoing journey. SL1 is uniquely equipped to help your teams navigate this journey by building a foundational real-time data lake that powers AI/ML and automation. As such, you can advance your maturity in how you manage data, analytics, and automation, as you shift from human- to machine-driven operations (see figure 4).

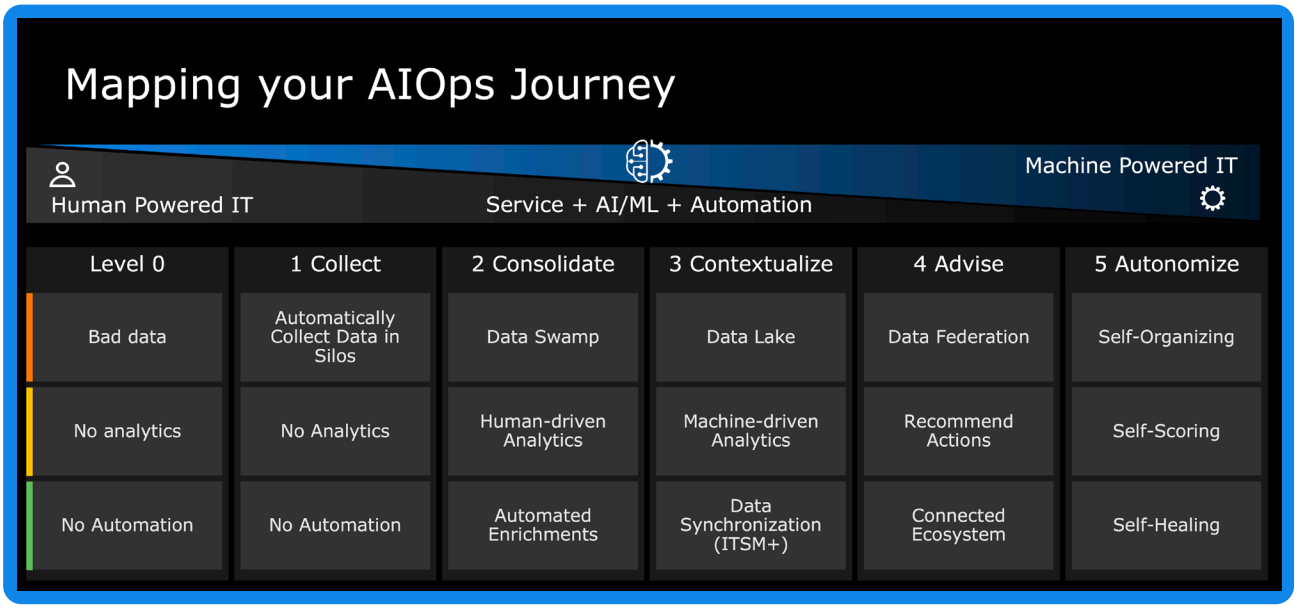


Figure 4: SL1 helps you advance your journey to AIOps at your own pace.

How MSPs Can Help

SL1 offers all the capabilities you require to move to advanced AIOps. However, your teams may lack the bandwidth and expertise to make this shift quickly and smoothly. In these cases, managed service providers (MSPs) can offer invaluable assistance. MSPs can provide the expertise and services that help your teams streamline the journey to AIOps and maximize the results you receive from your AIOps investments.

You can choose from range of MSPs, services, and tiers. Expert MSP teams can help with a range of efforts:

- Devising strategies and approaches
- Establishing optimal solution architectures
- Adapting to hybrid environments

In addition, you can work with MSPs that offer tiered network monitoring as a service that aligns to the ScienceLogic SL1 Solutions, enabling your teams to partly or fully offload ongoing monitoring and management efforts.

To learn more, be sure to visit ScienceLogic MSP.

"ScienceLogic leads at scale and automated RCA. SL1 applies an algorithmic approach to contextualize and search a real-time data lake that can speed an operations team's identification of root cause and remediation of incidents. … [Customers say] that the solution has allowed them to grow their businesses without adding staff due to its advanced automation capabilities, including run-book automation, predictive capacity management, automate incident management and CMDB accuracy."

—The Forrester Wave™: Artificial Intelligence For IT Operations, Q4 2020

Conclusion

To keep pace with intensifying, evolving network demands, your NetOps teams require advanced AIOps solutions. The ScienceLogic SL1 platform delivers the advanced monitoring, ML-driven analytics, and automation to see, contextualize, and act with ultimate speed and efficiency. Stay in front of the unprecedented volume, velocity, and variety of data you're contending with today—and nimbly contend with the seismic demands you'll be facing in the future so you can enhance your service levels, operational efficiency, and business results.

About ScienceLogic

ScienceLogic enables companies to digitally transform themselves by removing the difficulty of managing complex, distributed IT services. Our IT infrastructure monitoring and AIOps platform (SL1) provides modern IT operations with actionable insights to predict and resolve problems faster in a digital, ephemeral world. The SL1 platform sees everything across cloud and distributed architectures, contextualizes data through relationship mapping, and acts on this insight through integration and automation. SL1 solves the challenges and complexities of today and provides the flexibility to face the IT monitoring and management needs of tomorrow. Trusted by thousands of organizations, ScienceLogic's technology was designed for the rigorous security requirements of United States Department of Defense, proven for scale by the world's largest service providers, and optimized for the needs of large enterprises.