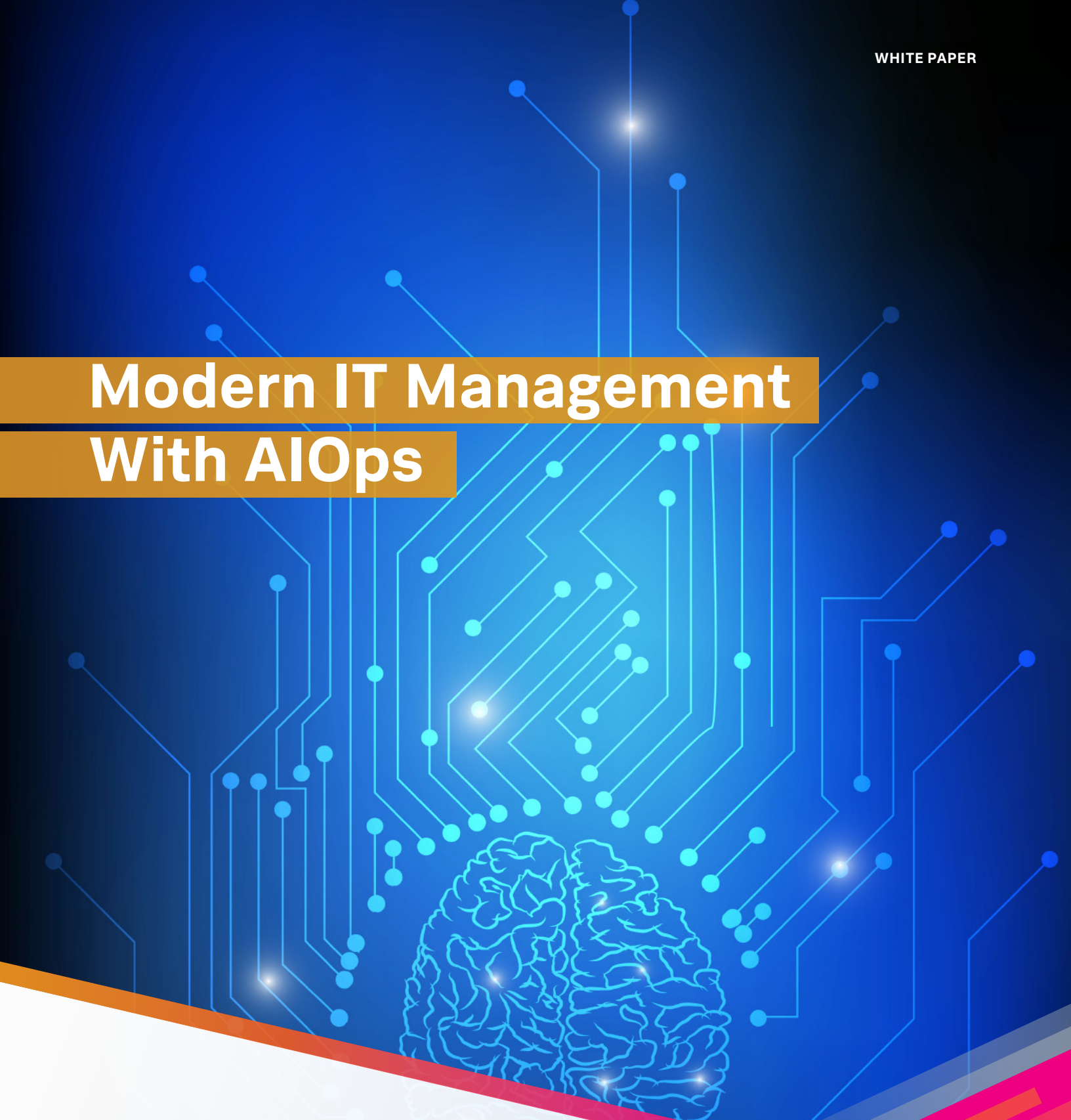
WHITE PAPER

Modern IT Management With AIOps



Embrace digital transformation with Splunk for IT Operations

splunk>
turn data into doing™

What's Your Digital Transformation Strategy?

Companies are going digital, whether their IT infrastructure is ready or not. Digital transformation initiatives like migrating to cloud promise speed, adaptability and reduced costs to effectively respond to today's real-time, customer-focused world. These initiatives come with new technologies and methodologies (like microservices and CI/CD), creating increasingly hybrid, complex environments to support.

Traditional IT operating solutions weren't built to support these diverse, cloud-driven environments, and leave teams with ineffective tools to manage operations. A decade ago, IT's role was different: ensure on-prem infrastructure is up and running and support monolith applications with predictable architectures and no interaction with customers. Today, customer demands are driving faster development cycles, more ephemeral application architectures and higher visibility incidents. IT is now responsible for ensuring traditional, critical services don't suffer while supporting future innovation initiatives and technologies. Ensuring reliability for this diverse range of applications and services using traditional IT management tools poses a challenge, and prevents organizations from innovating.

Organizations recognize their current infrastructure limitations[1] and are investing in new operating models like AIOps to manage the rapid growth and diversification of system architectures[2]. AIOps is "the combination of big data and machine learning to effectively automate operations"[3]. AIOps equips IT organizations with the ability to respond to the variety, velocity and volume of data created from digital businesses.

Splunk for IT Operations enables teams to embrace AIOps at every stage of digital transformation. Recognized as a market leader in ITOM by analysts and Fortune 100 customers, Splunk delivers business value to companies, no matter where they sit in their transformation journey.

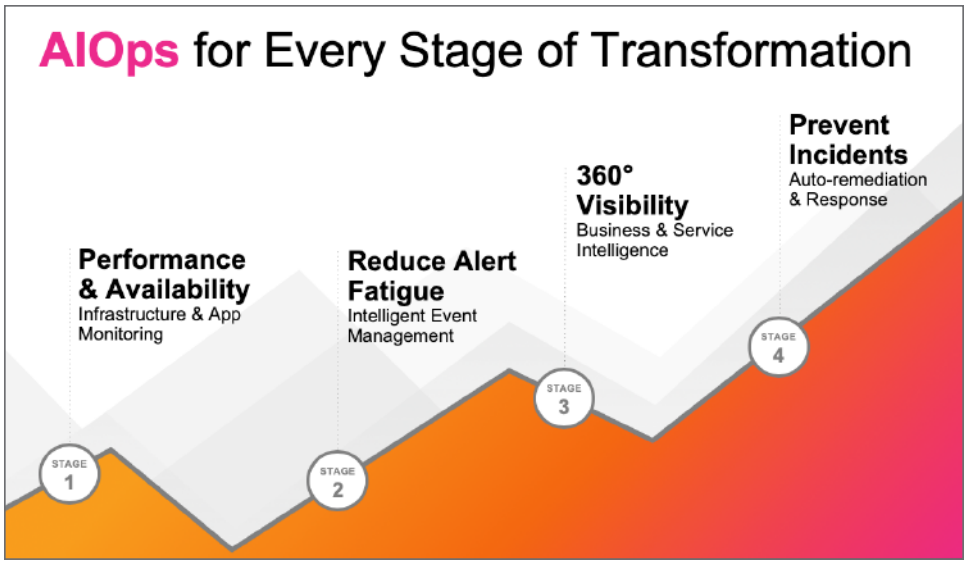
Splunk for IT Operations

With traditional IT solutions, the mere act of resolving an incident comes with inefficient, frustrating byproducts like alert storms and war rooms, thanks to siloed tooling and teams. Resolution times are delayed by different teams using different tools, and lack of visibility into other parts of the environment.

With Splunk's AIOps capabilities, inefficient processes are eliminated with machine learning and automation, reducing alert noise and investigation time up to 90 percent. Over time, with predictive analytics and automated remediation, Splunk can learn a service's behavior, detect and resolve an issue on its own, without human interference.

Splunk acts as a strategic partner to customers and provides AIOps capabilities at every phase of digital transformation. Whether it's just getting visibility across services, reducing alert noise or complete AI-powered automated remediation, Splunk provides value at every step, helping customers grow beyond where they are today.

1. Reinventing tech finance: The evolution from IT budgets to technology investments: January 7, 2020
2. CIO Tech Poll: Tech Priorities 2020: February 20, 2020
3. AIOps (Artificial Intelligence for IT Operations): Gartner Glossary



Splunk's IT Ops Suite supports these use cases with solutions powered by machine learning and big data.

Performance Availability

Infrastructure and Application Monitoring

Reduce mean-time-to-resolution (MTTR) and improve IT availability with one unified view for monitoring and troubleshooting, across infrastructure and applications. Combine metrics and logs to monitor cloud, server and application data and investigate incidents at full-fidelity from the same place.

Reduce Alert Fatigue

Intelligent Event Management

Say goodbye to alert storms with intelligent event management for real-time clustering and automated incident prioritization to reduce alert noise by up to 95 percent.

360° Visibility

Business and Service Intelligence

Position IT as a strategic business partner with dashboards that map underlying systems to business-critical services and their KPIs. Use predictive analytics and alert teams on future service issues 30 minutes in advance. Apply adaptive thresholding and anomaly detection to create alert rules and ensure they are consistently updated, never stale.

Prevent Incidents

Auto-remediation and Response

Combine predictive alerting with integrated on-call, bi-directional ticketing and automation to resolve incidents based on historical behavior. Use smart routing and suggested responders to deliver alerts to the right people, and execute playbooks for closed-loop, automated remediation.

Splunk's Approach

Splunk's unique approach to IT Operations comprises three core pillars:

- Expansive Data Access
- Machine Learning and Predictive Analytics
- Closed-Loop Incident Management

Expansive Data Access With Splunk

Today's environments produce data from increasingly diverse sources — including containerized workloads, microservices and unique SaaS provider APIs. Applications themselves are now highly distributed, making it even more difficult to collect and use incoming data to gain actionable insights in the environment. Modern IT tools must be agile and flexible to support any demand from the business, and that starts with its data story.

Splunk's Data-to-Everything Platform is unmatched. Splunk can capture large data sets — of any type — for comprehensive analysis and a fully observable environment.

Data Collection

With more than 2000 integrations — including out-of-the-box and custom solutions — Splunk can ingest all of your data and correlate it, whether it's in the cloud, on-premises, within the infrastructure or generated by apps.

Full-Fidelity Data

Many solutions can't handle data at scale, using aggregate sums to power their algorithms and outlier alerts. Splunk correlates all data at full-fidelity instead of a sampled subset — so no anomaly goes undetected.

Observability

Observability equips teams to respond to "unknown unknowns." By correlating metric, log and trace data in one system, Splunk provides full-stack visibility, giving teams the context and detail needed to fully understand the behavior of complex environments and their unknown failure conditions.

Metrics Do I have a problem?	Metrics are regular, numerical snapshots of how a system is performing. Metrics are useful for real-time detection and alerting, particularly in large-scale environments. They serve as the foundation for predictive analytics.
Traces Where is the problem?	Traces show where an issue arises. They provide critical context around the error, down to the line of code where the failure takes place. Tracing supports troubleshooting service dependencies, to faster pinpoint where something went wrong.
Logs Why is the problem happening?	Logs provide the detail teams need to understand why a problem is happening. This context accelerates root cause analysis, so teams can set in motion steps to prevent similar problems from happening again.

Machine Learning and Predictive Analytics

Machine learning is the application of mathematical algorithms on data to automate repetitive tasks and predict future incidents. Splunk applies machine learning to identify problems in complex environments through these features:

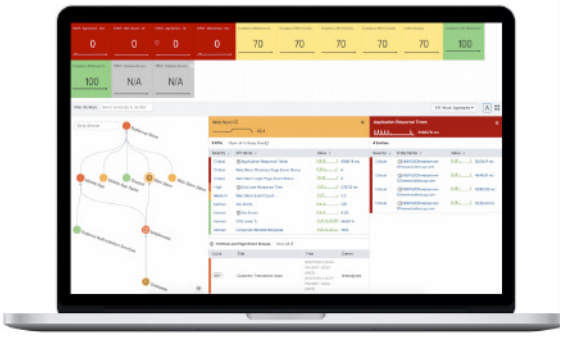
- **Adaptive thresholding** continuously defines and updates normal service thresholds with observed behavior to reduce alert noise and prevent analysis from going stale.
- **Anomaly detection** tracks behavior on a single key performance indicator (KPI) or across multiple services simultaneously to spot trending early indicators and minimize impact on performance.
- **Intelligent event correlation** to automatically group events and prioritize incidents that are impacting KPIs. Default aggregation policies or custom rules are available.
- **Automated escalation policies** and suggested routing gets the right teams and people involved.
- **Predictive health scores** create a historical service health score and correlate it to KPI data to predict a service's health 30 minutes in advance.

Closed-Loop Incident Management

Splunk provides IT teams an end-to-end, closed-loop solution for incident management, to streamline response and reduce friction across teams.

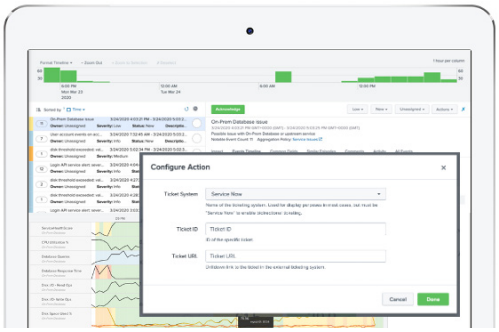
Real-time service monitoring and directed troubleshooting

Monitor critical services and drill down to investigate underlying infrastructure, all from one dashboard.



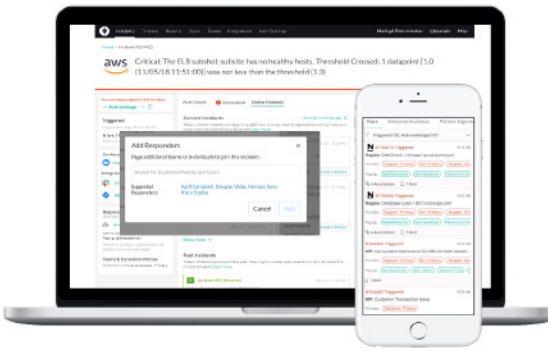
Integrated event and incident management

Prioritize and triage incidents by severity of impact to services. Create a ticket, run a script or alert a team from the same view.



Intelligent on-call and automated remediation

Notify response teams with smart routing and suggested responders. Unlock orchestration and self-remediation with 70+ playbooks and apps for IT operations.



Leader in IT Operations and AIOps

Splunk empowers teams to respond to digital transformation and modernize their IT management tools with confidence and agility. With Splunk's continued innovation and growth in IT Operations, analysts recognize Splunk as a market leader year over year. Splunk is the trusted platform of 92 of the Fortune 100, and customers see quantified, measurable ROI by implementing a modern approach to IT. With improved cost savings, operational efficiency and positive business impact tied to revenue, customers can position IT as a strategic business partner and retire the identity of a "cost center."

Customer Benchmarks

- **Infrastructure costs savings.** Up to nine hundred thousand dollars per year on average, as a result of improved capacity optimization.
- **Operational efficiency.** 65-90% faster incident response time and 15-45% fewer incidents.
- **Revenue acceleration.** Millions of dollars a year on average, with improved availability of critical business services, and replacing legacy ITOM licensing costs with Splunk.

Analyst Recognition

- IDC ranks Splunk #1 market leader in ITOM
- Gartner ranks Splunk #1 market leader in Performance Analysis
- Splunk debuts as visionary in Gartner MQ for APM

Customer Successes

Allied Irish Banks (AIB): Payments Platform Transformed with Predictive Analytics

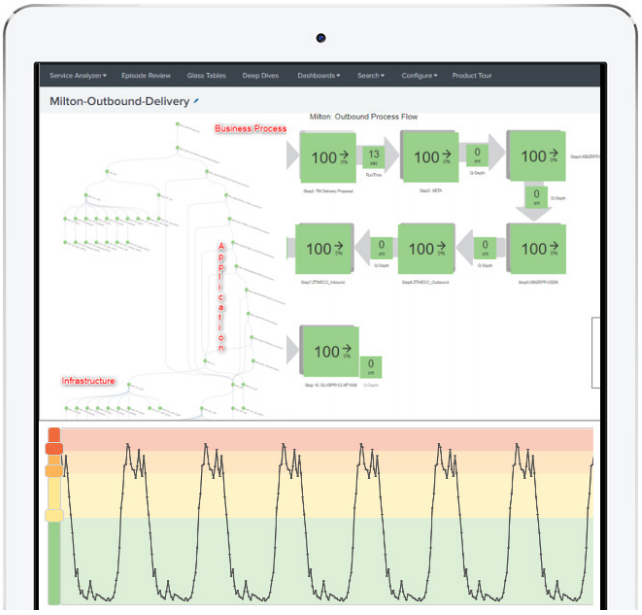
AIB (Allied Irish Banks), one of Ireland's major retail banks, required robust monitoring for 600 critical payment services. AIB turned to Splunk to maintain 100% service availability and implement predictive analytics to prevent customer-facing outages. As a result, AIB dramatically increased customer satisfaction and retention, and their Service Insights platform was shortlisted for a "Best Application of AI in Large Enterprise" award.

"It has allowed us to go from real-time reactive to proactive and predictive."

— Services Engineer, Allied Irish Banks (AIB)

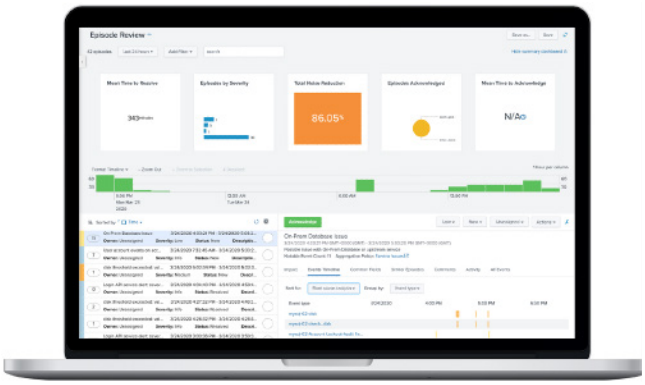
3M: MTTR Reduced by 70% with AIOps

With $32.8B in annual sales, 3M is one of 30 companies on the Dow Jones Industrial Index. 3M needed an integrated incident management solution to reduce costly outages. They replaced their outdated IT management solution with Splunk for its integrated monitoring, service management, and orchestration/automation. 3M reduced unplanned downtime and war room activity by 64%, saving $100k+/hour in expensive outages.



Leidos: 98% Reduction in Event Noise

Fortune 500 company Leidos needed to replace its traditional event management solution for more than 120 IT services. They implemented Splunk for its performance, capacity planning and end-to-end service visibility. Leidos reduced its 5000 daily alerts to 50 tickets and successfully aligned multiple teams with one unified service dashboard.



"I've been in IT management for over 20 years and I've not seen a product that does this. This is the first time I've been able to do heterogeneous, up-and-down-the-stack monitoring of my IT environment because Splunk has all the data."

— Director of Performance Management, Leidos

For more information on Splunk for IT Operations, visit our website at https://splunk.com/

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com