

# Predictive IT

How leading organizations use AI to deliver exceptional customer experiences



**splunk>**  
turn data into doing™

# Reactive IT Is So Yesterday

**Across industries and geographies, IT operations teams face complex issues**

Floods of events, complicated, connected services, organizational silos and demanding SLAs are just a few of the things that make managing IT operations more than a little stormy. At the same time, entire organizations depend on IT teams to prevent outages, especially those that might negatively affect the customer experience.

The most forward-thinking IT organizations steer through all of the chaos and pinpoint the source of the problem to fix it—fast.

But that's just the first step. These teams are also using machine learning to predict anomalous behavior and stop an outage before it even happens—with Splunk IT Service Intelligence (ITSI).

See how organizations use Splunk ITSI to predict, prevent and troubleshoot the most difficult IT challenges. Read their stories:

**Leidos**

**ENGIE Global Markets**

**Micron Technology**

**Econocom**

**CenturyLink**

**TransUnion**

Leidos is a Fortune 500 science and technology solutions leader working to solve global challenges in defense, intelligence, health and other markets — and facing its own challenges to ensure its services are always available to customers.



## Better Event Management: Splunk ITSI at Leidos

# 97% Reduction In Event Noise

### THE CHALLENGES

Leidos' Don Mahler, Director of Performance Management, needed a solution that could bring together sub-departments, IT and functional silos and triage a flood of events — spanning more than 120 IT services due to the following challenges:

- Monitoring and response required for 24/7 customer access
- Separate silos created a Balkanized IT department
- Needed to pare down thousands of alerts and events

### BUSINESS IMPACT

In addition to basic requirements such as consolidating events from its heterogeneous IT environment, detecting and suppressing duplicate alerts, clearing solved alerts and distilling them down to actionable events, the company needed extra functionality such as automatically escalating an alert after a period of time

or suppressing one when a device was taken offline on purpose. Leidos achieved all of this with Splunk ITSI. "There are days when you get a flood of events; Splunk ITSI prioritizes the events, gives you insight into not only that this is broken but what's been affected right as you look at the alert screen," Mahler says.

Another big benefit, Mahler says, is that the Splunk platform breaks silos by enabling teams to see data across the service stack. Today, approximately 20 management systems, from Microsoft System Center Configuration Manager (SCCM) to SolarWinds network management tools, more than 4,500 configuration items (CIs) across 120 IT services and 240 locations worldwide, feed into Splunk ITSI at Leidos, helping the company boil 3,500 to 5,000 daily alerts down to roughly 50 tickets for network and datacenter operations to act on. Passing CMDB information into Splunk ITSI allows different alert displays for different staff. The bottom line: easier access to more relevant data, with staff time devoted to the issues that matter most.

**I've been in IT management for over 20 years and I've never seen a product that does this. This is the first time I've been truly able to do heterogeneous, up-and-down-the-stack monitoring of my IT environment because Splunk has all the data and allows me to search it all in the same way."**

— **Don Mahler**, Director of Performance Management, Leidos



ENGIE Global Markets (EGM) is the energy trading platform at the heart of ENGIE, a global energy player in gas, power and energy services. ENGIE Global Markets needed a centralized, real-time view of the health of its critical trading application to speed troubleshooting and ensure performance.



## Splunk Ensures

# Performance of Key Trading Application

## at Engie Global Markets

### THE CHALLENGES

The health of the application is critical and the EGM team needed a centralized, real-time view of that health, as well as the ability to deliver information about system performance quickly and simply to business stakeholders. This was challenging due to the distributed nature of the grid system the application is built on. EGM also faced additional challenges:

- Need to ensure performance and availability of the core trading application
- Requirement for a centralized, real-time view of system health
- Distributed grid system meant homegrown solution was complex and impacted performance

### BUSINESS IMPACT

Before deploying the Splunk platform, the development

and infrastructure teams used their own siloed monitoring tools, which required a lot of back and forth to resolve issues. Using Splunk software has improved collaboration between the teams and reduced incident resolution time.

Deploying Splunk ITSI has made it even easier for EGM to correlate data across the IT stack to improve incident management and resolution. "When there's an issue, Splunk ITSI shows us where to look so we can solve the issue," says the Head of Infrastructure at ENGIE Global Markets. "With machine learning in Splunk ITSI, we don't have to create thresholds manually to measure performance of each server. We can adapt them dynamically to account for expected performance variances. This eliminates the cost of frequent configuration and tuning and frees our team to focus on triage on actual incidents before they impact end user experience."

**“With machine learning in Splunk ITSI, we don't have to create thresholds manually to measure performance of each server. We can adapt them dynamically to account for expected performance variances. This eliminates the cost of frequent configuration and tuning and frees our team to focus on triage on actual incidents before they impact end user experience.”**

— Head of Infrastructure  
ENGIE Global Markets



As a global leader in advanced semiconductor systems and with a broad memory solutions portfolio, Micron Technology, Inc. strives for high service quality that is critical to ensuring a great customer experience and keeping the competition at bay.

# Analytics Driven Approach Transforms IT Operations

## At Micron Technologies

### THE CHALLENGES

According to Brian Best, Micron's IT director, the Manufacturing IT department previously lacked enterprise-wide visibility into its IT operations. To maintain its competitive position in the industry, Micron needed to maintain service quality and to innovate its IT operations strategy to address the following challenges:

- Data silos limited teams' abilities to identify, resolve and prevent IT issues
- This reactive approach to IT monitoring hindered the company's primary mission — to ensure that its manufacturing facilities produce and ship wafers without any system interruptions or unexpected system impacts

### BUSINESS IMPACT

Today, Micron Technology relies on Splunk ITSI for everything from event management, alerting and incident management to problem and change management. The solution is helping Micron not only gain much needed

real-time visibility but also save time and reduce the impact of IT incidents on its business. Overall, Best notes that **Splunk ITSI has helped Micron reduce business-impacting IT incidents by more than 50 percent, mean-time-to-resolve IT incidents by 32 percent, and the number of major IT incidents by 23 percent.** "We don't have to wait for a network engineer to get on the phone and tell us that the network is healthy. Everyone is able to see that for themselves," Best says.

Every morning, based on custom reporting provided by Splunk ITSI data, Best and his team receive a report of KPIs, typically the top 10, that have been alerting over the previous 24-hour period. If a certain amount of alerting has occurred, there is a requirement to address that KPI. According to Best, in the event that an issue does occur, all the teams can be involved to ensure that something critical isn't missed. In addition, Splunk ITSI has expedited the Manufacturing IT team's ability to build dashboards that provide a macro view of the environment.

**+50%**  
**Reduction**  
in business impacting  
IT incidents

**If we do happen to wind up in a major incident, Splunk ITSI is the first place we go. We always ask ourselves the question, 'Did ITSI help us figure out where the problem was?' Every time the answer has been, 'Yes.' That tells us that we have the right KPIs in place and the right services and dependencies defined."**

— Brian Best, IT Director, Micron Technology

With 10,000 employees in 19 countries and revenue of 2.5 billion euros, Econocom designs, finances and oversees digital transformation solutions for companies. Meeting the strict SLAs associated with those services is critical to Econocom's business.

**10X**  
**Reduction**

in number of events generated  
by system performance issues

## Event Analytics Helps Econocom

# Deliver Better Services to Customers

### THE CHALLENGES

Prior to Splunk, the Econocom operations teams had almost a dozen different monitoring and event consoles. Econocom operators also lacked the ability to:

- Apply analytics across multiple data sources to accelerate incident investigation
- Visualize data with business-service context and apply capacity planning
- Unable to measure SLAs effectively with events in multiple silos

### BUSINESS IMPACT

Splunk ITSI was implemented at Econocom in full production in just weeks, and is now used by a number of different teams within the IT organization. Econocom has been able to centralize events from all its different siloed solutions into a single solution with Splunk ITSI. Event analytics in Splunk ITSI helps Econocom to better

prioritize and react more quickly to customers' infrastructure events, ultimately providing a better service. Splunk ITSI also allows Econocom to exclude events considered false positives from the event management process, **reducing total event volume by 60 percent** and helping operators focus on the events that really matter.

This has led to a **10x reduction in the number of events generated by system performance issues**. Econocom's approach includes using the adaptive thresholds in Splunk ITSI, which leverage integrated machine learning to learn normal behavior. Spikes in CPU would traditionally trigger threshold breaches, whether or not this really indicated a problem. Now, the machine learning in Splunk ITSI can understand which spikes may be normal in certain circumstances, preventing thresholds being breached and reducing the number of events being created.

**“Thanks to the integrated machine learning in Splunk ITSI, we now have a reduced number of events to process and the streamlined event analytics framework allows us to process events eight minutes more quickly, on average. This has led to a 15 percent improvement in SLA performance.”**

— Laurent Amouroux, Technical Director, Infrastructure Management Services, Econocom



Since 1930, CenturyLink has grown from a rural telephone carrier to a consumer, business and enterprise broadband, security, IT services and cloud provider across the U.S. and around the world.

## Steep decreases

in mean-time-to-identify (MTTI) and mean-time-to-resolution (MTTR)

From Switchboards To Dashboards:

# Communications Leader Finds New Solutions

## THE CHALLENGES

Due to acquisitions, CenturyLink had a need for quick insight into in-house and third-party applications. CenturyLink's call centers were challenged after the acquisitions, not because its systems weren't up to speed but because its call mix and the time to complete or modify an order had changed. CenturyLink faced challenges such as:

- Assembling information from a variety of silos and legacy apps
- The need for executive-level visibility into IT and business operations
- Call centers and other divisions turning to IT for help instead of assessing their own problems independently

## BUSINESS IMPACT

With Splunk Enterprise in place, instead of calling IT, the

centers can use real-time dashboards to see how they are performing compared to other centers. According to Tim Kerrigan, a manager in the Systems Engineering Group, "They can ask themselves whether anything has changed procedurally before we get 30 to 50 people on a triage call." With Splunk Enterprise deployed across a booming population of users in almost every CenturyLink department, the company recently added Splunk ITSI to its arsenal to aggregate an array of key performance indicators and granular-level detail for executive review.

Apps to receive the Splunk ITSI treatment so far include XenApp and a suite of other Citrix desktop and server products, as well as a critical API that allows multiple external applications to interface with the billing system. Comparing one month in 2017 to the same month a year earlier, the improved monitoring has yielded a decrease in IT outages, MTTI and MTTR.

“CenturyLink puts a heavy focus on customer experience, and Splunk helps ensure our end users are always satisfied with their service team interactions. Splunk Enterprise and Splunk IT Service Intelligence give us real-time, executive-level visibility into the health of our IT applications. This ensures that our representatives can get the information that matters most to each customer at all times.”

— Tim Kerrigan, Manager, Systems Engineering Group, CenturyLink

With a global presence in more than 30 countries and territories, TransUnion helps businesses manage risk while also helping consumers manage their credit, personal information and identity

## Transunion Invests In Splunk Solutions for **Enterprise Monitoring, Machine Learning**

### THE CHALLENGES

TransUnion provides consumer reports, risk scores, analytical services and more for over one billion consumers and business customers, including Tier-One financial institutions. Edward Bailey, senior monitoring and operations architect at TransUnion, was looking for ways to improve:

- Performance monitoring for external customer traffic
- Customer volume transactions

### BUSINESS IMPACT

TransUnion experiences variable traffic cycles on its website, with higher transaction volumes at certain times of the day and week. With automation and machine learning algorithms in place, the company has a new way to monitor these traffic cycles and

transactions. TransUnion is using Splunk ITSI to visualize and combine machine data from multiple applications to create an end-to-end transaction flow. “With Splunk ITSI we have a new way to visualize the health of each app,” Bailey says. “It helps us speed up root cause determination to achieve faster resolution.”

TransUnion analysts recently looked to Splunk dashboards when troubleshooting traffic for a large banking customer. With accrued knowledge of expected traffic at specific times of day, traffic that fell outside that data was considered an anomaly and generated an alert. “Understanding customer volume patterns is important for the business. If traffic falls outside of a certain range, an alert is created,” Koelpin says, adding, “Splunk machine learning allows us to investigate early to ensure a seamless customer experience.”

Discovered incident root causes **in minutes instead of hours** and reduced the number of false alerts

**“Understanding customer volume patterns is important for the business. If traffic falls outside of a certain range, an alert is created. Splunk machine learning allows us to investigate early to ensure a seamless customer experience.”**

— Steve Koelpin, Lead Splunk Developer, TransUnion

