Operational Intelligence: What It Is and Why You Need It Now

April 2013

Sponsored by Splunk
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>What Is Operational Intelligence?</td>
<td>1</td>
</tr>
<tr>
<td>Trends Driving the Need for Operational Intelligence</td>
<td>2</td>
</tr>
<tr>
<td>The Road to Operational Intelligence</td>
<td>5</td>
</tr>
<tr>
<td>What Is Splunk?</td>
<td>8</td>
</tr>
<tr>
<td>Operational Intelligence in Action: Using Machine Data to Instrument the Enterprise</td>
<td>10</td>
</tr>
<tr>
<td>Conclusion</td>
<td>12</td>
</tr>
</tbody>
</table>
Introduction

Few need convincing that the pace of change in modern business is skyrocketing and that the complexity of operations is increasing just as quickly. Less clear is the path to better methods of managing that change and conquering complexity. This paper introduces the concept of operational intelligence, a way of gathering information and creating a real-time foundation for better business performance.

This white paper also explains trends driving the need for operational intelligence, examines the benefits from implementing systems to support operational intelligence practices, explores some use cases, and reviews some of the applicable technology.

What Is Operational Intelligence?

Operational intelligence refers to a category of methods and technologies for gaining visibility into the business and discovering insights for IT and throughout the enterprise. Operational intelligence is not an outgrowth of business intelligence (BI) but a new approach based on sources of information not typically in the purview of BI solutions. Behind every IT infrastructure, behind the systems that run your business, are massively growing streams of machine-generated data. Leading organizations realize that this data can be incredibly valuable for improving the overall efficiency of not only IT, but also other parts of the business. Operational intelligence is designed to specifically address this opportunity.

Operational intelligence enables organizations to:

- Gain a deeper understanding using all relevant information, especially from machine data
- Reveal important patterns and analytics by correlating events from many sources
- Reduce the time to detect important events
- Leverage live feeds and historical data to understand what is happening, identify anomalies, and make effective decisions
- Quickly deploy a solution and deliver the flexibility needed now and in the future
Trends Driving the Need for Operational Intelligence

Operational intelligence emerged in response to the rising value—and amount—of machine-generated data. This value can be seen in a variety of arenas. Here are a few examples:

- Transaction monitoring for online businesses providing 24x7 operations
- Security monitoring to map and visualize modern threat patterns and strengthen security posture
- Web activity data to improve understanding of customers, capacity, and digital asset usage
- Service level monitoring information from managed service providers to fulfill agreements with the business
- Call and event detail records to uncover more profitable services for communications
- GPS and other data to enrich customer behavior information with location data

With the proper approach, companies can derive value from all this data—not just let it fly by untapped and unanalyzed.

Winning the Race Against Time

Most companies use a complex, layered mix of business applications, reporting and analysis tools, and methods of collaboration. But even after years of experience and refinement, most of us have unanswered questions:

- Why can’t I see what is actually going on in our business right now?
- Why does it take so long to answer questions about key business metrics?
- Why is it so hard to handle exceptions when things go wrong?
- Why can’t we capture and preserve knowledge about how to be more effective?

Our frustration stems from a disconnect between the applications and systems used to run our businesses and the immediacy of modern markets. The speed of business has increased beyond the capacity of the previous generation of IT, which focused on tracking and automation of transactional activity. It told us what happened. The new generation of IT must not only capture what has happened—it must tell us what is happening now and facilitate timely action.
This new generation of IT will take shape in many ways, but CITO Research believes that operational intelligence is an important organizing principle for systems and methods to run businesses in real time and to meet the demand for speed and agility.

The Information Explosion

Available information today is exploding, a trend called “big data.” Information generated inside every company is increasing due to automated data collection, technologies such as RFID and GPS, web clickstreams, email, and the logs and machine data created by technologies inside and outside of the enterprise. For the most part, this is “data exhaust”—if captured at all, it is usually filtered and either partially or never used. Organizations typically look to the traditional systems of record and BI technologies to enable decision-making. Yet within this data lies a vast amount of untapped insights that could be leveraged within IT and elsewhere in the business. The challenge has been how to effectively capture, store, correlate, and analyze this data.

Adding to this data are other sources of information, like watch lists, asset directories, customer data, shipping and logistics data, and web-based feeds—like real-time stock feeds, travel reservations data, popular searches, and more. These internal and external sources can provide added context to what’s happening in the business.

The good news is that there are now ways to aggregate and understand the vast streams of machine data with methods that scale as quickly as data is increasing. It’s practical now to use this real-time and historical data across a broad set of venues and applications. This is the basis of operational intelligence.

Adding Operational Intelligence to Business Intelligence

BI draws on data sources that are historical, batch-loaded, and structured. This structure is added through normalization and data processing for loading into relational databases, a process commonly referred to as extract, transform, and load (ETL). The difficulty of adding new data sources, or asking new questions of the data, is well documented, as is the time to design, deploy, and evolve these decision-support infrastructures.

Operational intelligence is typically used with time-series unstructured or semi-structured data (for example, specific machine events or transactions that have a timestamp associated with them). The data in operational intelligence systems enables
you to see what is happening now and compare it to what has happened in the past. Operational intelligence answers questions that traditional BI systems are not designed to answer.

Nonetheless, rather than thinking of operational intelligence as an alternative to BI, it is helpful to see BI and operational intelligence as complementary. With the right tools, you can exploit the wealth of data offered by the data explosion and gain new insights for running your business while supplementing it with the best analytics you have about your customers and what has succeeded in the past. You can synthesize and correlate data from external sources and use this data along with traditional BI tools to provide more visibility into your business.

Common Scenarios

Companies that have implemented operational intelligence reap many of the benefits described in the following scenarios:

- Security-related data sources across all business units can be correlated to help identify anomalies and incidents in real time
- New feeds of real-time data representing consumer behavior and operational activity can be analyzed to detect problems and opportunities
- Processes that cross applications can be tracked so that problems and exceptions can be handled automatically
- Events from a myriad of data sources can be connected to provide a deeper understanding of business activity in time to take effective action

Data doesn’t have to be real-time to offer business insight. Months or years of historical logs can be mined quickly, revealing trends.

There are countless ways that operational intelligence can make a company more effective, productive, secure, and agile. Operational intelligence helps you take advantage of new categories of rich real-time data whose business utility you have probably not begun to exploit.
What Is Machine Data?

An emerging class of data is being generated by web servers, applications, machines, on-premises applications, and SaaS systems of all types. It includes clickstreams, GPS readings, call logs, RSS feeds, social media comments, weather data, fleet locators, and more. This data is one of the fastest growing categories of big data.

Until now, analysis of this data focused on finding out about machines and their operations, not on what it could tell us about business. Today’s systems generate massive amounts of information that can be ignored, used for finding and fixing problems, or leveraged for strategic business advantage. The machine data explosion requires a new way of analysis that sits alongside established practices.

How can you observe machine data? The semantics of machine data are complex and that is why it is up to CIOs to enlighten the business about the value of this data. Without a deeper look, machine data is only cryptic numbers, encoded cookies, unrecognizable fields, and references to data that must be looked up elsewhere. Little good comes from handing such data to business staff in raw form. IT must make the data usable so that business staff can analyze operational data and gain valuable insights.

The Road to Operational Intelligence

The fastest road to operational intelligence comes through creating business value from the explosion of machine data. CEOs, CFOs, and senior managers are accustomed to seeing data from a historical perspective. They analyze past performance and predict future results based on historical data points such as sales figures, buying trends, and raw material price fluctuations. It requires experience and intuition to drive a business this way, but it’s like celestial navigation, which tells you where you were and directs you toward where you are going, but doesn’t reliably tell you where you are. Operational intelligence is more like a GPS. Managers who use data in motion can make real-time course corrections or quickly chart new directions.
Bringing operational intelligence practices to a company is a gradual process. Figure 1 shows a typical roadmap.

**The Roadmap to Operational Intelligence**

- **Proactive**
  - **Real-Time Business Insights**: Dashboards, events, and predictive models are used by the business to prevent problems and seize opportunities.
  - **Operational Visibility**: The business becomes engaged with machine data analysis. Advanced models of behavior are created.
  - **Proactive Monitoring**: IT finds problems in advance and learns how to present machine data to the business.
  - **Search + Investigation**: Machine data begins to be understood as a business asset.

- **Reactive**

*Figure 1. The Roadmap to Operational Intelligence*

Now let’s look at each of the steps along this roadmap in more detail.

**Search and investigation.** The journey begins as IT departments explore machine data as a means to figure out what is going on during an incident happening in a datacenter. The IT staff uses the data to find a root cause. Each data set should be examined not just for what it can say about the system that produced it but also for what information it offers about customers, key events, or performance of business processes.
Proactive monitoring. IT proactively monitors data for clues to help avoid risks they’ve identified. Simplified forms of predictive models can be created at this stage. Events and trends that may lead to trouble are identified so that failures can be avoided. At this point, IT usually understands machine data well enough to start proposing ways of helping the business.

Operational visibility. IT starts measuring its SLAs and KPIs across the organization as a way to engage the business. Once the business becomes interested, users are able to answer questions and track consumer behavior in ways not possible without machine data. Then the conversation begins in earnest. IT begins to understand what the business needs. Business staff starts to understand the value of machine data. A more sophisticated model of customer behavior and important business processes start to emerge. At this point, business staff presents IT with additional questions and IT responds with a quick custom dashboard instead of a pointer to unintelligible raw machine data or a three-month wait for a new report.

Real-time business insights. The pinnacle of operational intelligence comes when machine data is used to track and correlate activity in real time and to predict behavior. Dashboards are put in place, events are recognized that spur other activity, and predictive models help forestall problems or identify opportunities. At this stage, use can be broad across an organization—often with more business users than IT users. This level of operational intelligence provides the largest payoff.
What Is Splunk?

To achieve operational intelligence, the first thing CIOs and CTOs must do is find technologies to help them. Splunk is a platform for machine data. It collects, indexes, and harnesses machine data generated by any IT system and infrastructure—whether it’s physical, virtual, or in the cloud. Splunk laid its foundation helping IT find and fix problems faster, but its applications are far broader, as we will see.

Splunk makes sense of machine data to support business goals. It handles both the form and the semantics of machine data. It accomplishes this through a unique approach of universally indexing any machine data across the infrastructure. It consumes network traffic and app server logs and tracks hypervisors and GPS, as well as social media activity. It even absorbs PBX and IP telephony data.

Splunk does this without requiring costly connectors or agents. It does not need to filter or parse the data to load it into a database. By providing users an index of all the machine data generated by all systems and infrastructure, Splunk enables users to ask any question and find answers quickly to the most simple or strategic propositions.

Splunk was born to help IT manage and monitor the datacenter. System administrators were sniffing out security threats, server inefficiencies, network outages, and bandwidth bottlenecks, not looking for business insights. But along the way, that’s exactly what they discovered in the wealth of machine-generated data that is driving operational intelligence.

Analysts can have a conversation with the data and gradually uncover the structure and relationships between elements. They can create custom applications, dashboards, and reports that don’t just present information, but allow for deep drill-downs into the data to answer questions. Splunk also offers prebuilt integrations to common data stores, such as Hadoop and traditional relational databases.
Step 1: IT uses Splunk

IT uses Splunk to monitor systems. A spike in failed credit transactions signals trouble.

Once machine data is understood, IT sees new possibilities for Splunk.

Step 2: IT creates dashboards for business users

With an understanding of machine data, IT creates dashboards for business users to gauge response to promotions.

Step 3: Business people use Splunk

Business people ask for more data sources as they use Splunk to analyze business problems.

As the use of Splunk expands, the number of business users is often double or triple the number of IT users.

Figure 2. Finding Business Insights in Machine Data
Operational Intelligence in Action: Using Machine Data to Instrument the Enterprise

After understanding the breadth and scope of operational intelligence, many people are daunted. With the wealth of opportunity, where do you start? While the first generation of operational intelligence systems showed up in industries with large R&D budgets (such as military research, financial services, and telecommunications), new technologies have lowered the barriers to entry and made it easy to start somewhere and begin to gain unprecedented levels of visibility, insight, and intelligence. Literally any company that has a website or a stream of transactional data can quickly get started with operational intelligence. The rest of the paper explains how organizations can get started by focusing on the value of machine data and the power of technologies like Splunk to analyze it.

Case Study: Cars.com

Cars.com is designed to inform consumers who are interested in buying cars. Partners include some 17,000 local dealerships, which receive referrals from some of the 12 million people who visit the site each month to search for information about buying their next car. The site garners advertising revenue from auto manufacturers and others.

To improve the site, analyze usage, and optimize performance, developers needed timely access to data. The Application Management Team could not permit developers access to the production environment: it was too risky. Nonetheless, developers and business analysts needed access to performance data to ensure a quality user experience, as well as to get data about ad performance to fulfill stakeholders’ needs for metrics. With the challenges of keeping the popular site up and running, the Applications Management Team was frustrated by numerous ad hoc requests for log files and other data.
The team deployed Splunk Enterprise to enable developers and analysts to search through real-time data feeds, providing them with all the data that they needed without putting production systems at risk.1 In addition to providing this type of operational visibility, through analyzing the log files, the Cars.com team was able to identify and decommission underused hardware, saving the company money while increasing performance.

**Operational Intelligence Benefit:** Some 750 million queries per month are now available to 100 developers in real time, enabling them to gain visibility into traffic and usage patterns, identify ways to improve performance and improve efficiency of operations.

**Case Study: Message Bus**

Message Bus was founded in 2010 as a cost-effective, outsourced alternative for business-class email. The firm furnishes email and mobile messaging services that are scalable, secure, and provide delivery verification. The company’s IT and service delivery infrastructure is entirely cloud-based.

Message Bus needed visibility across its cloud-based business. Ensuring availability and performance demanded continuous monitoring of applications across multiple clouds. Message Bus also needed analytics to audit customer usage for billing and to track email delivery status. To protect its customers from fraud and attacks, Message Bus needed to monitor message traffic for anomalous behavior.

Developers use Splunk to gain visibility across the Message Bus infrastructure, enabling them to troubleshoot applications and rapidly deploy solid code.2 Operations uses Splunk to monitor performance and gather metrics, viewing performance in real time and receiving alerts if a system is about to be overutilized so they can avert any problems before service delivery is impacted. Using natural language queries, account managers can support their customers’ needs using Splunk.

**Operational Intelligence Benefit:** Across departments, Splunk infuses Message Bus with operational intelligence and visibility across its infrastructure to help drive the company’s success.

---

1 Enterprise Management Associates authored a detailed case study on the use of Splunk at Cars.com; see http://www.splunk.com/view/splunk-roi/SP-CAAAFVN for details.

2 A detailed case study on Message Bus’s use of Splunk can be found at http://www.splunk.com/view/splunk-at-message-bus/SP-CAAAHPA.
Case Study: Otto Group

The Otto Group is the world’s biggest online retailer for fashion and lifestyle products, and the world’s second-largest web retailer overall. Online stores, warehouse management systems, CRM call centers, and the central processing system must run 24/7/365. The central processing system processes all customer, product, and order information. All 20 Otto Group call centers in Germany, as well as the largest Otto Group web store, use this system. Otto Group needed real-time monitoring that could provide operational and web intelligence across its critical infrastructure.

GTP, the IT service provider of the Otto Group, deployed Splunk as part of a production monitoring system. GTP now uses Splunk in a DevOps capacity to optimize code, configurations, and setups before entering production. The operations team uses Splunk for reporting and analytics.

Before Splunk, GTP could only monitor exceptions in single call centers. Using Splunk, all 20 call centers are monitored in real time. GTP can recognize and resolve system errors, often before they impact users. The average time to act on an issue is just five minutes.

Operational Intelligence Benefit: Otto Group’s infrastructure is complex and distributed. Splunk has helped GTP innovate new ideas that give Otto Group visibility across its infrastructure and spur its continued leadership position in online retail in the face of dire competition.

Conclusion

“Einstein’s memorable quote could easily apply to business. Companies often rely on today’s leading analytic applications to answer questions using static, historical data. In the past, if new questions arose, new applications had to be designed to answer them. However, a new class of data has emerged—machine data.

Organizations must learn to ask questions about this new class of data because now they have the tools to examine and understand it in its raw form. With the advent of operational intelligence, there is an opportunity to gain insight from all of the data that machines are creating.

1 For more information about Otto Group’s use of Splunk, please see http://www.splunk.com/view/splunk-at-otto-group/SP-CAAAHGW.
The ability to benefit from operational intelligence crosses all lines within an organization. Splunk provides visibility across the infrastructure, across departments, and up and down the technology stack. A common pattern for deployments is to bring Splunk in for one or two use cases, experience a dramatic ROI, and then think of many other applications and groups that can benefit. Splunk can help you leverage machine data in new ways to instrument the enterprise.

CITO Research recommends Splunk on three fronts:

- **As a technology for exploring and understanding the potential of machine data**
- **For its incremental approach to operational intelligence.** Companies can download Splunk for free, start experimenting, and see results immediately
- **For its breadth.** Though Splunk has made a name for itself in the IT space, at most large deployments there are a handful of core users and dozens of other users ranging from developers, to product managers, business managers, and C-level executives, all of whom gain new visibility and insights from their data.