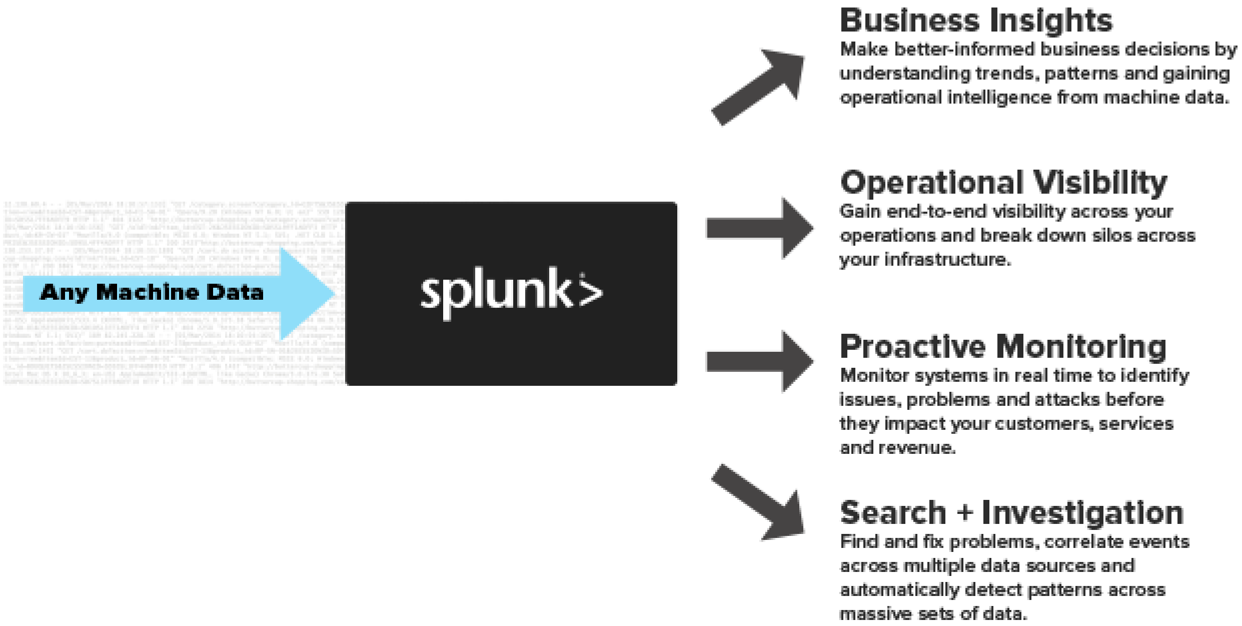
Operational Intelligence

Operational intelligence (OI) is a category of real-time dynamic, business analytics that delivers visibility and insight into data, streaming events and business operations. Operational Intelligence solutions run queries against streaming data feeds and event data to deliver real-time analytic results as operational instructions. Operational Intelligence provides organizations the ability to make decisions and immediately act on these analytic insights, through manual or automated actions

Turn Machine Data Into Insights

Machine-generated data is one of the fastest growing and complex areas of big data. It's also one of the most valuable, containing a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Splunk turns machine data into valuable insights no matter what business you're in. It's what we call operational intelligence.

Operational intelligence gives you a real-time understanding of what’s happening across your IT systems and technology infrastructure so you can make informed decisions.



Business Insights
Make better-informed business decisions by understanding trends, patterns and gaining operational intelligence from machine data.

Operational Visibility
Gain end-to-end visibility across your operations and break down silos across your infrastructure.

Proactive Monitoring
Monitor systems in real time to identify issues, problems and attacks before they impact your customers, services and revenue.

Search + Investigation
Find and fix problems, correlate events across multiple data sources and automatically detect patterns across massive sets of data.

What Is Machine Data?

Machine data contains a definitive record of all the activity and behavior of your customers, users, transactions, applications, servers, networks and mobile devices. And it's more than just logs. It includes configurations, data from APIs, message queues, change events, the output of diagnostic commands, call detail records and sensor data from industrial systems and more.

Machine data comes in an array of unpredictable formats and the traditional set of monitoring and analysis tools were not designed for the variety, velocity, volume or variability of this data. A new approach, one specifically architected for this unique class of data, is required to quickly diagnose service problems, detect sophisticated security threats, understand the health and performance of remote equipment and demonstrate compliance.

Machine Data Sources

Every environment has its own unique footprint of machine data. Here are a few examples with what the data can provide insight for.

Data Type	Where to Find It	What It Can Tell You
Application Logs	Local log files, log4j, log4net, Weblogic, WebSphere, JBoss, .NET, PHP	User activity, fraud detection, application performance
Business Process Logs	Business process management logs	Customer activity across channels, purchases, account changes, trouble reports
Call Detail Records	Call detail records (CDRs), charging data records, event data records logged by telecoms and network switches	Billing, revenue assurance, customer assurance, partner settlements, marketing intelligence
Clickstream Data	Web server, routers, proxy servers, ad servers	Usability analysis, digital marketing and general research
Configuration Files	System configuration files	How an infrastructure has been set up, debugging failures, backdoor attacks, time bombs
Database Audit Logs	Database log files, audit tables	How database data was modified over time and who made the changes
Filesystem Audit Logs	Sensitive data stored in shared filesystems	Monitoring and auditing read access to sensitive data
Management and Logging APIs	Checkpoint firewalls log via the OPSEC Log Export API (OPSEC LEA) and other vendor specific APIs from VMware and Citrix	Management data and log events
Message Queues	JMS, RabbitMQ, and AquaLogic	Debug problems in complex applications and as the backbone of logging architectures for applications
Operating System Metrics, Status and Diagnostic Commands	CPU and memory utilization and status information using command-line utilities like ps and iostat on Unix and Linux and performance monitor on Windows	Troubleshooting, analyzing trends to discover latent issues and investigating security incidents
Packet/Flow Data	tcpdump and tcpflow, which generate pcap or flow data and other useful packet-level and session-level information	Performance degradation, timeouts, bottlenecks or suspicious activity that indicates that the network may be compromised or the object of a remote attack
SCADA Data	Supervisory Control and Data Acquisition (SCADA)	Identify trends, patterns, anomalies in the SCADA infrastructure and used to drive customer value
Sensor Data	Sensor devices generating data based on monitoring environmental conditions, such as temperature, sound, pressure, power, water levels	Water level monitoring, machine health monitoring and smart home monitoring
Syslog	Syslogs from your routers, switches and network devices	Troubleshooting, analysis, security auditing
Web Access Logs	Web access logs report every request processed by a web server	Web analytics reports for marketing
Web Proxy Logs	Web proxies log every web request made by users through the proxy	Monitor and investigate terms of service and the data leakage incidents
Windows Events	Windows application, security and system event logs	Detect problems with business critical applications, security information and usage patterns.
Wire Data	DNS lookups and records, protocol level information including headers, content and flow records	Proactively monitor the performance and availability of applications, end-user experiences, incident investigations, networks, threat detection, monitoring and compliance