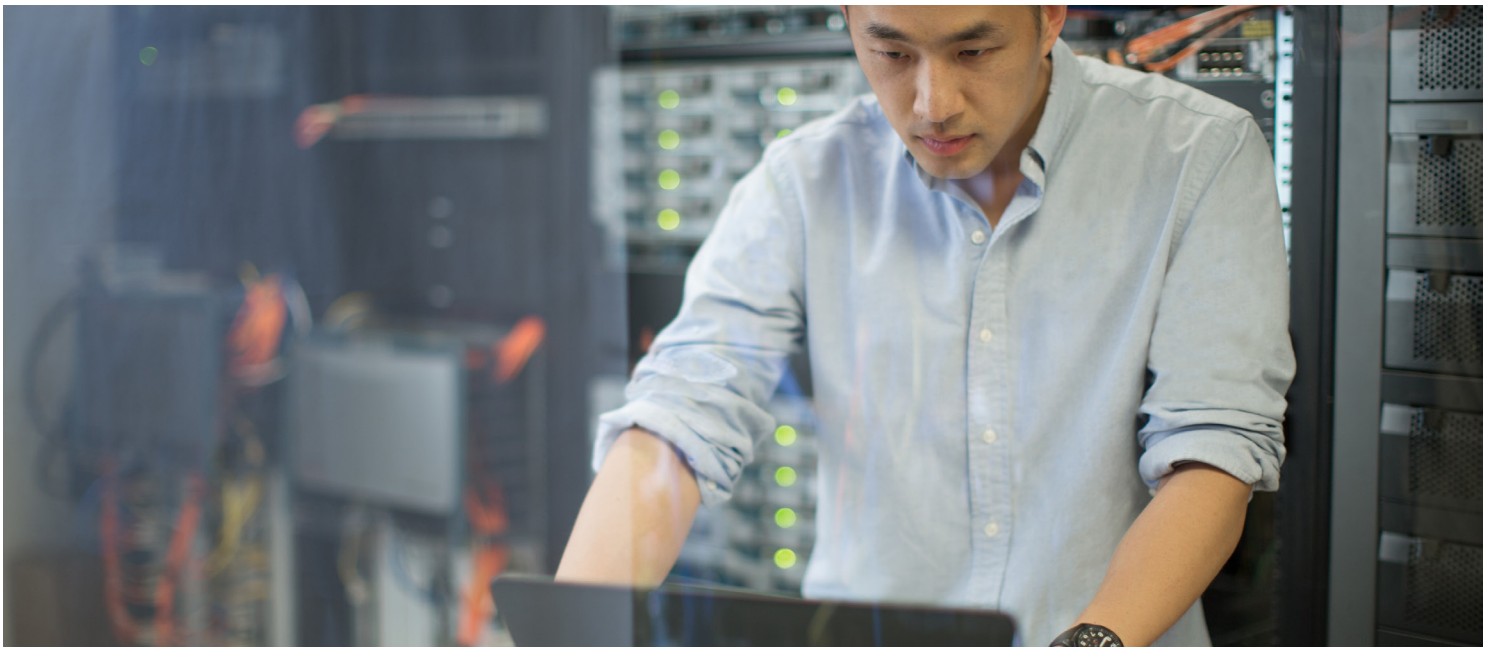
USING MACHINE DATA TO IMPROVE IT TROUBLESHOOTING

Cisco and Intel® partnering in innovation



How log files and other machine data can help boost the health and performance of an application environment.

Application monitoring and troubleshooting used to be far easier. If something went wrong, there were only so many places where the error could have occurred. Only a few potential culprits.

- In today's world of hybrid IT, where systems and applications are spread among physical, virtual, and cloud environments, finding the root cause of a problem can be daunting.
- What used to be a defined trail of breadcrumbs has been scattered across the floor, in a variety of rooms.

"Modern application environments are so distributed and complex," says Jon Rooney, senior director of solutions marketing for Splunk, a leading provider of operational intelligence and data analytics solutions. "If a problem occurs, was it the application server, the web server, the database tier, the API gateway, something else? Without full visibility across all of them, you just don't know."

- Application Performance Management (APM) tools can help, but they are inherently limited. While they can detect hiccups with availability and performance, they can't show where or why the problem is happening unless it is related to the application code itself.
- That's why companies are beginning to combine APM information with other kinds of data—like machine data.
- Created by every application, operating system, network device, and IT service, machine data comes in a variety of formats, from logs and wire data to mobile application and API endpoint data.

"Log data is becoming increasingly valuable," says Tim Grieser, program vice president for enterprise system management software at IDC. "But you need to combine and correlate the logs from multiple systems to effectively triage, troubleshoot, and remediate problems."

REAL-TIME MONITORING AND PATTERN DETECTION

Many companies disregard their machine data entirely. Some have developed what Rooney calls "duct tape and super glue solutions" for monitoring and managing machine data formats like log files. Others have attempted conventional methods to process these unconventional files.

"You can't monitor and analyze log files with a relational database. That's like placing a fire hose in a Dixie Cup," Rooney quips. "Batch processing isn't viable either, because you need to analyze log files in real time and respond immediately to anomalies or performance dips."

- Splunk provides industry-leading software to aggregate, integrate, and analyze every type of machine-generated data—including logs—in both structured and unstructured formats.

- Pretested and prevalidated on the Intel® Xeon® processor-based Cisco Unified Computing System™, the software helps identify, resolve, and prevent operational, security, and business issues through real-time monitoring and pattern detection.

"Companies have been doing this in bits and pieces, but they have an opportunity to go deeper," says Grieser. "They can correlate logs from many systems to see across the layers of an environment, from the server and virtualization layers to the network and web layers to mobile and device layers."

AN ADDED DIMENSION

With a depth and breadth of visibility, organizations don't just improve their ability to troubleshoot problems. They also increase their understanding of the systems and circumstances that affect application behavior. And they can work to proactively prevent problems altogether.

"Troubleshooting is a big part of the equation, but effective log monitoring can lead to predictive and preventive IT maintenance," says Grieser. "Organizations can apply machine learning to better understand application usage patterns and contingencies. And they can set dynamic, automated thresholds and alerts that help circumvent potential problems before they occur."

In doing so, they can better manage the health and performance of their application environment, which is vital for the health and performance of the business.

"Log management helps blur the lines between IT and business performance, and can provide visibility on both sides," says Grieser. "It's an added dimension that is well worth exploring."

This article first appeared in *Unleashing IT* Volume 5, Issue 3, and online at www.unleashingit.com. available after subscribing at www.unleashingit.com/LogIn.aspx.