



## JOURNAL COMMUNICATIONS GETS THE SCOOP ON RISK MANAGEMENT

*This company transformed its disparate security efforts to archive a company-wide, standardized view of risk and regulatory compliance remediation efforts.*

*“It used to take us a month, or more, from the time a vulnerability was announced to when we knew it was resolved on our systems. Now, thanks to QualysGuard, it’s down to hours.”*



James Herzfeld, Vice President of Information Technologies, **Journal Communications**, CIO **Journal Sentinel**

If you want to know what’s happening in Milwaukee, chances are you’ll get the news from one of Journal Communications’ media and information outlets. This diversified media company operates 49 community newspapers and shoppers, 35 radio stations, and 12 TV stations in twelve states, plus 96 individual web sites. With a circulation of 390,840, the Milwaukee Journal Sentinel is the company’s flagship newspaper.

Such a vast and varied assortment of properties requires a dynamic IT architecture. “Each media division essentially manages its own IT. While we share many core applications, the underlying infrastructure is separate,” says James Herzfeld, vice president of information technologies and CIO, for Journal Sentinel (one of the 5 companies owned by Journal Communications).

While providing each business unit this level of autonomy certainly helps the company remain nimble, it also makes it more challenging for the company to measure risk across the entire enterprise. “During these past few years, the number of exploits has been growing exponentially. We started asking how we could be more efficient at keeping up with these IT risks,” says Herzfeld. That was a savvy move: according to the federally-funded Internet security watch group the CERT Coordination Center, the number of vulnerabilities reported more than doubled in three years, from 3,784 in 2003 to 8,064 last year.

With each business unit’s own IT team researching its own software vulnerabilities and potential threats independently, redundancies in vulnerability management throughout the company surfaced. “Each group had its own level of security; yet we didn’t have a baseline of our security posture across the entire company,” he says. “We needed to find a way to streamline the network assessment and patching process — and get an accurate baseline for each unit.”

That company-wide, standardized view of risk would enable management to know how well the entire company’s IT security efforts were faring, better prepare IT teams for regulatory compliance, and make sure that at-risk systems were patched. “Not only would we cut redundant efforts, but we’d have better peace of mind knowing that our systems were configured properly and up to date,” says Herzfeld.

### **Software-as-a-Service proves to be the most effective way to maintain security and regulatory compliance**

To get there, Journal Communications needed to find an automated, repeatable, and verifiable way to conduct vulnerability management across each business unit. To that end, Herzfeld and his team evaluated a significant number of vulnerability scanners and assessment tools available, but none seemed to provide the accuracy, ease, and thoroughness they sought. “We looked at quite a few different products, and most fell well short of our expectations,” he says.

But one solution exceeded Herzfeld’s expectations — that was QualysGuard, from Qualys, Inc. “We immediately identified a clear differentiation in how QualysGuard is delivered as a Web-based service. It placed how we would conduct vulnerability assessments in an entirely new light,” he says.

QualysGuard enables organizations to reduce risk and manage their regulatory compliance efforts by automating the processes associated with vulnerability management and regulatory compliance into a single solution. In fact, QualysGuard automates the processes of network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking, according to business risk. Policy compliance features allow security managers to audit, enforce, and document compliance with internal security policies and external regulations.

Because QualysGuard is delivered as an on-demand software-as-a-service (SaaS) solution, QualysGuard doesn’t require costly and time-consuming software installations or ongoing upgrades. Its SaaS delivery method provides predictable and low total cost of ownership, is scalable, easily deployed, and distributed, and can be used anytime, anywhere from any Web browser.

### **The shift from manual to automated security management**

“QualysGuard clearly was easier to deploy than a traditional scanner or appliance, and it proved itself more accurate,” says Herzfeld. Journal Communications deployed five QualysGuard appliances, one for each business unit. Now, vulnerability assessments are conducted on internal systems each week, while Internet-facing systems are evaluated every day. “This makes it possible for us to stay on top of the growing number of software vulnerabilities, and make sure we’re patched against fast moving threats and attack tools,” he says.

While Journal Communications certainly benefits from that ease of use and management, without requiring much training, it found the high level of trust it can place in the scan results to be vital. “It’s extremely advantageous knowing that QualysGuard is so accurate. If QualysGuard spots a vulnerability, you know with high certainty that it’s real,” he says. That’s much different than many other solutions on the market that force security managers to sift through pages of false-positives to find the true security flaws on their systems.

**“It’s helped us to stay secure through its automation, accuracy, and ability to make sure our risk management and vulnerability management processes are in place.”**

James Herzfeld, Vice President of Information Technologies, **Journal Communications**, CIO **Journal Sentinel**

## Journal Communications Gets the Scoop on Risk Management

QualysGuard also has helped Journal Communications to streamline its vulnerability risk management efforts through automation. Not only does the company leverage QualysGuard to conduct daily and weekly scans of specific systems, but its continuous vulnerability reporting alerts security administrators to the current remediation level of each work ticket they're assigned, and what actions are still pending. Each report provides tickets modified in the past 24 hours, and whether the ticket is still open or resolved. "Everyone knows what they need to be working on," he says.

"It used to take us a month, or more, from the time a vulnerability was announced to when we knew it was resolved on our systems. Now, thanks to QualysGuard, that window has been reduced to hours," he says. "It's helped us to stay secure through its automation, accuracy, and ability to make sure our risk management and vulnerability management processes are in place."

### Regulatory compliance efforts eased through verifiable processes

As a public company, Journal Communications must comply with the Sarbanes-Oxley Act of 2002. Section 404 of Sarbanes requires business managers to demonstrate that they've established appropriate organizational and technical controls to safeguard their financial processes. In essence, Sarbanes requires that the systems that manage financial data not only be kept secure, but that the efforts used to attain security must be provable.

For those efforts, QualysGuard makes it possible for Journal Communications to cost-effectively generate SOX-specific reports that measure, help to align, and document ongoing efforts to safeguard financial systems and data. "We use QualysGuard quite a bit for Sarbanes. The reports serve as proof that we've patched on a timely basis. The reports and historical data demonstrate to the auditors our processes and how well we are doing," he says.

Journal Communications set out to improve its vulnerability and risk management processes, cut redundant efforts, and establish the health of its overall IT security posture. And that's what they've been able to achieve: accurate, insightful, and automated vulnerability assessments, and repeatable processes throughout their enterprise.

"QualysGuard has become very important to our organization. Think about all that we used to have to do manually — research and scan for vulnerabilities, investigate fixes, patch, and remedy, and then scan again. Qualys automates most all of that for us," says Herzfeld. "And we now have the piece of mind that vulnerability management is being done."

### JOURNAL COMMUNICATIONS, INC SCOPE & SIZE

Regional  
3,500+ employees  
\$672+ million annual revenue

### BUSINESS

Multi-state diversified media company providing news and entertainment through operation of newspapers, 96 Web sites, 35 radio stations, and 12 television stations.

### BUSINESS PROBLEM

Journal Communications needed to streamline how it manages software vulnerabilities and demonstrates regulatory compliance throughout its five business units.

### SOLUTION

QualysGuard

### WHY JOURNAL COMMUNICATIONS CHOSE QUALYS

- Ability to discover and prioritize all network assets
- Rapidly identify, visualize, and organize network assets (including all network devices and applications) into Business Units and Asset Groups
- Accurately detect and eliminate the vulnerabilities that make network attacks possible
- Proactively identify and fix security vulnerabilities
- Manage and reduce business risk
- Document regulatory compliance

### WEBSITE

[www.journalcommunications.com](http://www.journalcommunications.com)



**USA – Qualys, Inc.** • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • [sales@qualys.com](mailto:sales@qualys.com)  
**UK – Qualys, Ltd.** • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101  
**Germany – Qualys GmbH** • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146  
**France – Qualys Technologies** • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70  
**Japan – Qualys Japan K.K.** • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296  
**Hong Kong – Qualys** • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 3163 2888

