



SAS: MITIGATING IT VULNERABILITY RISKS THROUGH RAPID INSIGHT

When the world's largest privately held software company sought a way to transform its manual, time-consuming vulnerability management program, the company turned to QualysGuard for the accurate, automated insight it needs to keep its global Internet infrastructure secure in the most effective way possible

“The automated scans provide much more efficiency than the manual scans we conducted in the past. And our weekly QualysGuard reports provide us the insight into risk that we need to know.”



Brian Wilson, Network Security Engineer, Systems and Information Security
SAS Institute

With software in use at 43,000 locations in 112 countries, SAS is one of the largest software companies in the world. And of the top 100 firms on the Fortune Global 500 list, 96 rely on SAS' business intelligence (BI) and analytical software and services to improve their organizations' performance by culling greater insight from their data. In this way, SAS helps organizations make faster, more accurate business decisions, cultivate more profitable relationships with customers and suppliers, more effectively maintain regulatory compliance, obtain more rapid breakthroughs from R&D efforts, and improve their products and organizational processes.

While SAS' BI and analytical technology helps businesses and government agencies move forward with greater confidence and increased clarity, the company sought increased information about the system vulnerabilities that could place its global, Web-facing IT infrastructure at risk. Today, an effective vulnerability management program is more vital to network health than ever before. In fact, the number of software vulnerabilities discovered each year has been growing not only in their volume, but in their severity: In the year 2000, only 44 percent of vulnerabilities could be exploited remotely over the Internet; that number now nears 90 percent. And yet, the astonishing reality is that many organizations have failed to put into place the technology and internal processes required to keep their systems secure from these threats. According to the Deloitte 2006 Global Security Survey, only a surprising 49 percent of organizations currently have deployed a system for vulnerability management.

Manual Vulnerability Management proved time-consuming, costly, and lacked the ability to provide correlated risk levels against business asset values.

Don't count Brian Wilson, network security engineer, systems and information security at SAS, among those who are unprepared. For years, SAS has assessed its network and Internet infrastructure for systems that had fallen out of compliance to its internal security policies, and for those in need of configuration changes and security patch updates critical to keeping them secure. But for a time, SAS had relied on a manual vulnerability assessment solution that failed to gather enough granular information or provide the accuracy that the company demanded to find and fix any at-risk systems. "The quality of the reporting just wasn't up to our standards," says Wilson. "The reports couldn't correlate business units or specific systems to the vulnerabilities," he adds. The system also provided incomplete information that had to be fleshed out by hand. For instance, Wilson explains, if a system was running a certain version of an operating system, the scanner couldn't tell whether that version was actually open to a newfound vulnerability or not. "The scanner would just report that system as potentially vulnerable, whether it was vulnerable or not," he says. "We had to spend additional time figuring it out."

This simply wasn't meeting SAS' needs, especially considering the company's vast Internet-facing infrastructure, which includes several Class B networks and more than 500 active hosts.

SAS: Mitigating IT Vulnerability Risks through Rapid Insight

The result was that security managers had to invest too much time verifying the reports to eliminate all of the false positives, and few IT managers within the organization completely trusted the accuracy of the results. “We were reliant on third-party pen tests to get the results we needed to verify whether systems were at risk, or properly remedied,” he says.

QualysGuard: Deep vulnerability insight through full network, insightful, and highly-customizable reports

Last year, SAS started evaluating the security market for a better solution to help it streamline the way it manages the vulnerabilities associated with its external network. Then the company decided on a two-week trial of QualysGuard, from Qualys Inc. “I noticed the increase in quality immediately,” says Wilson.

Only QualysGuard provides organizations the most effective, automated way to simplify their control over the entire vulnerability management life cycle—asset discovery, vulnerability auditing, and security fix tracking. The on-demand solution, entirely managed by Qualys, is delivered as a Web service and requires no software or costly infrastructure to deploy. And QualysGuard’s Six Sigma accuracy and comprehensive Knowledge base of security checks is unmatched. In fact, QualysGuard identifies all networked assets and examines 65,536 system ports for vulnerabilities. The result is a powerful and highly accurate baseline of the network. Unlike SAS’ previous scanner, QualysGuard makes it possible for Wilson and his team to centrally manage the risks associated with all of their network assets, and quickly identify those that are out of policy, misconfigured, or otherwise vulnerable. QualysGuard enables assets to be custom tagged for enhanced classification levels. QualysGuard’s customized asset tags provide SAS a powerful way to track and manage networked devices, grouping them by specific business units so actionable reports can be sent when needed or requested.

For these reasons, among many others, QualysGuard proved itself to be the best vulnerability management solution to fit SAS’ pressing needs. Regular automated scans now have been put into place. In addition, QualysGuard’s ability to thoroughly discover all networked assets means that nothing goes unchecked throughout SAS’ global network. “I can tell what assets have changed. I can see if any network assets have been added, or removed, from the network,” Wilson says. This highly-automated approach to vulnerability management not only has increased the security team’s ability to see everything that occurs on the network, but it also has reduced significantly the need for expensive third-party audits and security consultants.

“The quality of our vulnerability reports is just phenomenal now. QualysGuard, through its well documented API, gives us the ability to include anything we need in our reports. There hasn’t been a report that we wanted to build that we couldn’t easily create,” he says. Qualys’ standard security reports, in addition to this highly-customizable reporting capability, can demonstrate compliance to internal IT security policies and government and industry regulations. And these reports can be generated in HTML, MHT, PDF, CSV, and XML formats to show high levels of security posture to business and IT managers, partners, and even customers. And while SAS has just started using it, QualysGuard already has established its value to SAS’ security team. “The automated scans provide much more efficiency than the manual scans we conducted in the past. And our weekly QualysGuard reports provide us the insight into risk that we need to know,” he adds. “Other than that, QualysGuard runs itself.”

SAS SCOPE & SIZE

International; World’s largest privately held software company
10,000 employees
\$1.9 billion (annual sales, 2006)

BUSINESS

Leader in business intelligence and analytics software that helps companies in every industry transform their data into predictive insights about company performance, customers, markets, risks and more.

BUSINESS PROBLEM

SAS needed an automated and fully streamlined and accurate way to keep its global Internet-facing operations secure.

OPERATIONAL CHALLENGE

Previous vulnerability scanner failed to provide the accuracy and reporting capabilities SAS sought to rapidly remedy vulnerabilities in its hosting sites. The scanner was time-consuming, with security managers having to manually vet out the false positives and correlate vulnerabilities to the business value of the at-risk systems for remediation planning.

SOLUTION

QualysGuard Enterprise

WEBSITE

www.sas.com



USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
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

