Vulnerability Management Begins at the Endpoint

Wolfgang Kandek
CTO, QUALYS

Wolfgang Kandek is responsible for all innovation aspects of Qualys Cloud Platform. He has more than 20 years of experience developing and managing information systems. He is the main contributor to the Laws of Vulnerabilities blog. www.qualys.com/research/vulnlaws.

FOR A FREE TRIAL OF QUALYS CLOUD AGENT PLATFORM VISIT
www.qualys.com/forms/cloud-agent-platform

As mobility and the global network infrastructure expands, the need for security assessment and policy compliance is essential. Qualys offers some insight on how CIOs, CSOs and CTOs can stay ahead of evolving global network security and the next phase of innovation in security assessment.

What are the top challenges for IT decision makers with current vulnerability management and compliance?

The current IT environment is dealing with extreme quick changes due to cloud computing. Suddenly business units can get their own access to computing resources and don't need to talk to the IT dept. Security is getting more difficult to manage. Now there is more mobility, which means vulnerabilities such as network attacks and malware are not just coming from the outside anymore.

What is missing with traditional vulnerability management?

Traditional vulnerability management helps you identify what types of machines, operating systems, and weak spots are at risk on your internal network. When resources migrate outside of that network, it's harder to control. Desktop users work on laptops at home or on the road. Traditional vulnerability management tools won't see home-based or cloud computing and servers. Where you could once install patches at your discretion, now servers outside the environment make it harder to control the situation. We lose visibility and security if users are not on the network.

How does Cloud Agent address these challenges?

Cloud Agent gives you an X-ray of the infrastructure of machines you have. Traditionally we could only do this on the enterprise network. Machines from outside escaped us. Now we can install lightweight agents on each machine before it is distributed, or in the case of servers, spun up. The agent constantly communicates with us so that we can know of any changes on the machine or if more servers have been added.

Why should companies move toward endpoint security and cloud agent?

It's the architecture of the future. In the future, everyone will have a laptop or mobile device and work from anywhere. You won't have control over their network access. The average company will be very mobile and have servers virtualized in an environment that they don't control. We need to protect the endpoint so that it's not at risk.

What are the deployment benefits of Qualys Cloud Agent?

You gain complete visibility into the infrastructure, and you see the configuration of all the machines. To get that visibility, you need to embed the agent and install it before you distribute the machines. This includes BYOD and virtualized servers. Traditional vulnerability management has time windows that you must maintain so that you don't impact network traffic. With cloud agent, you are time-window free, because it runs constantly. It doesn't require password credentials to perform. Setup is simplified, and tool management is automatic and less costly.

What are the core values Qualys brings to IT and businesses?

You can't secure what you don't know. Today, data breaches are detected and customer data and intellectual property are stolen. The reality is that we're not managing vulnerabilities. You have to be aware that you might fall victim to attacks, and you still have to do business.

What future developments can we expect with Qualys Cloud Agent?

The next version of Qualys Cloud Agent will be Mac OS X and Linux. The Cloud Agent can also perform file integrity monitoring, looking at how a file changes, why it changes, and who did it. We're also looking at improving logging, enforcement, and fixing for efficiencies in future network security issues. ■

QUALYS® CONTINUOUS SECURITY

IDG INTERNATIONAL DATA GROUP