



# SKANDIA: NETWORK SECURITY BUILT TO TRUST

Skandia provides financial products and services designed to meet the specific needs of each of its customers. And Skandia has built its business by concentrating on the areas the company knows best: fund selection, concept development, and market support and service. This focus serves its customers well, and Skandia's success is the proof. An international business, with core markets in Great Britain and Sweden, Skandia's reach also includes, Continental Europe, Asia Pacific, and Latin America. Skandia gives its customers the confidence, expertise, quality and the freedom of choice they need to build financial security to last a lifetime.

Another vital element of Skandia's success – really the success of any financial services provider – is trust. Customers must trust the advice they receive, the products they purchase, and the viability of the financial firms they hire. And today, more than ever, they must be able to trust the IT systems on which their financial provider runs its business. That means they must trust that the firm's network, applications, and data are secure, confidential, and available.

A crucial aspect of maintaining a trusted business-technology infrastructure is being able to detect and mitigate software vulnerabilities and system misconfigurations that place the infrastructure at risk of attacks. For some time, to help ensure that its systems remained secure, Skandia undertook manual network assessments and regular penetration tests. But as the company grew, in size as well as in its reliance on its IT infrastructure, it wanted to find a way to streamline its vulnerability management processes.

"We wanted to move away from manual assessments and automate our vulnerability assessments so that we always would know our security posture, and our systems would be updated on a regular schedule," says Alan Osborne, lead security architect at Skandia. "Essentially, the idea was to create a way to continuously monitor our systems so that we could find and remedy vulnerabilities," says Richard Taylor, service assurance specialist at Skandia.

For Skandia this was no small undertaking, with externally facing servers located around the globe, and more than 4,000

internal IP addresses to manage. Also, because much of Skandia's IT management is outsourced, it would have to be easy to remotely manage the network scans and access assessment reports. Verifiable Network Security and Compliance After evaluating a number of software-based network assessment solutions, it was QualysGuard Enterprise, from Qualys Inc., and its on-demand Software-as-a-Service (SaaS) delivery model that Skandia Group chose. "It was clear that it was extremely accurate and easy to use," says Osborne.

Today, QualysGuard Vulnerability Management (VM) automates the life cycle of network auditing and vulnerability management across much of Skandia's operations, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Driven by the most comprehensive vulnerability KnowledgeBase in the industry, QualysGuard remedies the flaws that make the latest exploits and attacks possible. As an on-demand SaaS solution, there is no additional infrastructure for Skandia to deploy or manage.

To vet Skandia's relevant global IT infrastructure for vulnerabilities, the company deployed eight QualysGuard appliances around the globe. Because QualysGuard can evaluate the security status of each IT asset automatically and on demand, every IT asset has its security assessed several times a month. Also, due to the fact that QualysGuard's software, security checks, and service all are centrally managed by Qualys, Skandia knows each scan will perform as expected. "Now all of our scans are managed centrally on a weekly or biweekly cycle," Taylor explains. "Everything gets scanned every two weeks at a minimum. And those reports are reviewed in our standard security and patch meetings," Taylor says.

The detail and insight provided by the QualysGuard reports are what the team has found so valuable. "We've gained the visibility we sought around vulnerability management," says Taylor. "We're now able to see which systems are in need of new patches as they're released, validate that the patches are in place, and provide a graphical representation of our progress," he says. QualysGuard's intuitive and easy-

to-read reports provide both executive-level summaries and detailed technical analysis. And the technical reports include a detailed description of each vulnerability, the severity of the security threat, consequences if the vulnerability were to be exploited, and the recommended solution to fix the vulnerability, including links to the appropriate patches.

QualysGuard's reporting not only helps Skandia remain secure, but keeps it compliant to the relevant financial and European data regulations. "We have to demonstrate that we have active controls in place, and be able to provide concrete information which validates that we are meeting our regulatory requirements," Osborne says. "Qualys is a tremendous help in those efforts." Skandia set out to build an automated, verifiable vulnerability management program, and with its QualysGuard deployment, that's exactly what the firm has achieved. "We've done what we expected; we've not only increased efficiencies through automation, but we now can validate our level of security," says Osborne.



Alan Osborne, lead security architect at Skandia

Skandia is currently expanding its use of QualysGuard in additional offices around the globe, and putting QualysGuard to use in new ways. One example is the way Skandia is leveraging QualysGuard as part of the process of on-boarding new systems to its network. "All new systems are subject to a QualysGuard scan to make sure their patch levels are up to date and there are no misconfigurations," says Tim Selby, service assurance manager at Skandia. "Today's IT environments are very dynamic, and vulnerabilities and patches come out nearly every day. Qualys gives us the full picture of where we stand, and the insight we need to make sure our infrastructure is solid," Selby says. ■

More at [www.skandia.com](http://www.skandia.com) and [www.qualys.com](http://www.qualys.com)