



CASE STUDY: Standard Chartered Bank

Standard Chartered Bank

Standard Chartered is the world's leading emerging markets bank headquartered in London. It offers both consumer and wholesale banking services.

The bank employs 30,000 people in over 500 locations in more than 50 countries including the Asia Pacific Region, South Asia, the Middle East, Africa, the United Kingdom and the Americas.

The world-wide IT infrastructure features 5,000 servers and 35,000 desktops. IT supports 600 different applications.

Business Problem

Needed an effective method for tackling critical security problems quickly and efficiently in a high risk high profile environment.

Developing an effective, global, risk-driven approach to security in a highly distributed enterprise.

Standard Chartered's Requirements

- Prioritise patching effectively
- Detect vulnerabilities quickly
- Integrate easily with existing proprietary security approach

Solution

QualysGuard Enterprise to

Underpinning a Risk-Driven Strategy

"The stakes are very high indeed. With our many large and complex interconnections to the outside world, it's vital to carry out effective patch management. Our aim is to achieve the right level of security through implementing an appropriate risk-based strategy. This cannot be achieved without a clear and accurate understanding of what needs patching and ensuring that it remains reliably patched. We use QualysGuard as a dynamic tool to underpin this process." says John Meakin, Group Head of Information Security, Standard Chartered Bank.

"Our aim is to achieve the right level of security on our global networks. This means a clear and accurate understanding of what needs patching and ensuring that it remains reliably patched. We rely upon QualysGuard to underpin this process."

"Being able to report on remediation and response plans has also helped us meet strict financial compliance requirements. QualysGuard reports give me and my security team an instant overview of the overall level of health of security in my organisation."

John Meakin

Standard Chartered's Need for Vulnerability Management

Security monitoring in an environment like Standard Chartered's requires the capability to cover diverse IT platforms - including both

automate the network discovery, scanning, patching and verification process

Why Qualys?

- Accuracy
- Ease of global deployment
- Scalability
- Value for money
- Integration with established security operations

Windows and Linux - and many applications and services. Its goal was to consolidate these ad-hoc efforts into one cohesive, global process with clear visibility, follow through and accountability.

Before the introduction of enterprise vulnerability management, Standard Chartered's network topology and system configurations were unknown. Local operating teams performed only occasional scanning with various tools. Spot audits were made through penetration- testing and there was no rigorous methodology to assess exposure and take corrective action.

The bank evaluated four alternatives including tools from Foundscan, ISS, Vigilante and X-Force but eventually, it selected QualysGuard on six clear criteria: scanning accuracy, deployability, scalability, ease-of-use, integration capabilities and overall cost effectiveness.

"It was the only solution which met our demands without compromise, giving us a reliable, centralised method for protecting our critical assets worldwide," says Meakin. "Our experience of rolling out QualysGuard has been remarkably painless. Working with our integration team in both London and Singapore, the service has been consistently high."

The role of Vulnerability Management at Standard Chartered

By introducing vulnerability management, Standard Chartered gained a clear picture of the exposure with common standards worldwide. The company has been able to quickly prioritise remediation; get security and operating teams to work together smoothly and effectively and empowered outsourcing vendors to meet specific security service level agreements.

Many major viruses have the ability to recur and creep insidiously back into the network causing considerable problems; another reason why on-going scanning is important.

"Although Standard Chartered Bank was not hit the first time round by SQL Slammer, it did manage to infect our network a number of months later due to difficulties in restoring patched server builds after operational problems. Our IDS engines and QualysGuard enabled the Bank to pinpoint rapidly the source of the problem and close it down, avoiding major infection." said Meakin.

Standard Chartered, like many other global organisations, has had to grapple with the challenge of integrating disparate elements. Qualys's partnership with NetSec, SCB's chosen Managed Service Provider, has integrated vulnerability and asset data into the Finium V event management platform, minimising the integration effort required by Standard Chartered itself.

"Regulatory pressures and increased exposure are driving more complex requirements for managing security risks. With this integration we gain the ability to view and act upon security risk as it pertains to our organisation's assets," said John Meakin. «In addition, being able to report on remediation and response plans has helped us meet strict financial compliance requirements."

Reports Help to Improve Risk Management and to Address Regulatory Requirements

QualysGuard's easily accessible reports provide a clear audit trail

for fixing vulnerabilities. Delivered on a monthly basis to the bank's operational risk committee, they have enabled Standard Chartered to improve its risk management methodology and address regulatory requirements that impact financial institutions.

These reports help the security group support the front-line production operations team more effectively to patch and maintain the security of the whole network. They allow centralised management by checking the patch management performance, tracking patching actions to completion and distributing tasks to the relevant geographic support group. They also give John Meakin a real-time snapshot of the bank's security levels.

"Regulatory pressures and increased exposure are driving more complex requirements for managing security risk. Our vulnerability management strategy gains us the ability to view and act upon security risk as it pertains to our organisation's assets" said John Meakin.

"The reports also enable me to justify the investments we need and further define our security strategy. Today, we really can deploy our security manpower much more effectively in both preparing and responding to security incidents." concludes Meakin.