

CyberGatekeeper

A Case Study on Network Policy Enforcement Safeco Insurance's Innovative Spirit Extends to Building a Secure Computer Network

Securing the Network Edge

From its inception in 1923, Safeco Insurance has defied industry trends and conventions. The company was founded in Seattle, Washington far from the recognized insurance centers in the metropolitan Northeast United States. But, even as far back as 1953, the company's innovative spirit sent it in pursuit of a then-emerging computer automation technology that would give its independent agents the tools to compete with direct insurance writers.

Today, Safeco is a Fortune 500 company and still uses technological innovation as a competitive edge. To better service customers and partners, Safeco began to transfer business processes to an Internet infrastructure. However, in order to give users quick, simple and safe Web access, the IT team realized that the ease of use requirement must be carefully balanced with strong network security. Being able to thwart the growing number of malicious external code attacks was also a high priority. But similar to the innovations a half-century ago, Safeco had a strong tradition of using technology to solve business problems. Network security implemented the right way could effectively enable Safeco's Web-based business.

Safeco decided it needed a comprehensive and proactive security approach that would enforce its client and network configurations. Existing perimeter security such as firewalls and anti-virus programs did not go far enough to stop recent Web-based hacks, and those products required constant administrative or user intervention to meet compliancy requirements. Following were some of Safeco's requirements for its next generation of security:

- 1) Compatibility with existing client and network infrastructure
- 2) Automatic and persistent network-wide configuration enforcement
- 3) Intelligent scanning or monitoring of all machines to spot vulnerabilities
- 4) Quarantine of infected or non-compliant machines from network access
- 5) Options to remediate machine problems
- 6) Centralized policy management for easy updates

A brief search told the project team that there was only one vendor that could meet the company's requirements - InfoExpress, already the supplier of Safeco's CyberArmor Personal

Firewall solution. The IT team was pleased to find out that InfoExpress had just released new technology, CyberGatekeeper, an enterprise network-based security enforcement solution. Safeco elected to deploy CyberGatekeeper to secure all remote access as it offered effective protection against viruses, Trojans and worms. The CyberGatekeeper Assess-Quarantine-Remediate process fit Safeco's stringent requirement to incorporate a solution that would enforce security on all devices attempting to access their network. For employees with remote-access privileges, CyberGatekeeper was transparent and did not interfere with their activities. CyberGatekeeper, and its ability to enforce Safeco's security policies, has helped employees to think proactively about keeping their individual machines updated.

Customer Opportunity

- 1) Improved service for customers and partners
- 2) Improved employee productivity
- 3) Lower-cost technology infrastructure
- 4) Lower overall risk to the business

Main Security Issues

- 1) Thwart malicious external code attacks
- 2) Monitor and detect vulnerable, non-compliant systems
- 3) Block admission of potentially harmful devices from network access

Customer Benefits

- 1) Consistent security process
- 2) Ability to expand remote access safely
- 3) Improved Web access infrastructure