

InfoExpress CyberGatekeeper: Financial Services and Investments Case Study

In the World of High-Stakes Financial Investment Services, There's No Room for Exposure

A Customer Case Study on Fortifying Network Security Using Endpoint Policy Enforcement

In the highly competitive world of financial services and investments, few companies have rivaled this North American investment powerhouse. Beginning as a mutual fund company in the early 1940's, this firm has evolved to where today it offers more than 300 mutual funds, discount brokerage services, retirement services, estate planning, wealth management, securities execution and clearance, and life insurance. Throughout its decades of dynamic growth, two business drivers have remained constant - peerless customer service and the use of advanced technologies. The company is often credited for many technological innovations that have become standards in the financial industry, including the use of stringent security practices.

Using Security to Enable Mobile Computing

Like many companies in recent years, this firm saw the many advantages with the remote computing trend. Armed with a laptop, modem or network card and VPN client software, road warrior employees could travel for extended periods of time, or work from remote locations, and still access network resources. But, like other technological advancements, mobile computing involved serious trade offs that had to be addressed. Employee machines used in a nomadic work style off the network and beyond the watchful eye of the IT department could be more vulnerable to malicious code attacks. Mis-configured, unpatched or other non-policy compliant issues could open the door for an infection that could spread rapidly to other computers on the network. Without inspection capabilities at network connection and the enforcement of security policies, an infected laptop could bring severe consequences to network operations, and to the online business itself.

Before, it could allow mobile computing, the firm needed to make sure that its strict security policies were enforced through all network access points. They wanted to make sure that key software programs such as anti-virus, VPN, and OS were properly updated and patched, and that high risk unauthorized software was not installed. Continuing to protect the confidentiality of sensitive customer and corporate information could not be imperiled by the employees working with remote and mobile access.

CyberGatekeeper - Secure Network Access Control

In their initial search, the IT staff found products that could scan or monitor systems, while others just performed asset checks. Yet others could assess vulnerabilities and patch machines. However, none of these products provided the ability to enforce the policies, until they found the CyberGatekeeper appliance from InfoExpress.

With CyberGatekeeper, they not only found a product that could scan and check for infections and required software updates, but it also offered a quarantine process, where all security policy compliant systems would be allowed network access. In addition, they learned CyberGatekeeper could also help remediate problem machines.

After installing CyberGatekeeper, more surprises were in store. During the initial roll-out and audit, it was determined that some users were using unauthorized or non-supported O/S platforms such as Windows 95/98/ME/NT. Many of the violators were traced to home machines used to access the network. The use of outdated vulnerable systems represented a real risk to the enterprise, so they quickly made changes to "enforce" a corporate standard of Windows 2000 or XP only.

After a smooth roll-out with only a handful of questions to 1st level support, the firm embraced the fact that CyberGatekeeper offered a comprehensive network access control process from assessment and auditing, to enforcement, and remediation. Purchasing point products from different vendors and then trying to integrate them seamlessly would not have been cost prohibitive, but from an administrative and management perspective, a nightmare.

Cybergatekeeper has now been deployed on a global basis to well over 10,000 employees, all VPN gateways, some WAN links, several wireless infrastructures, and LAN enforcement is under review. Risk and Security Managers can now move very rapidly to assert new audit requirements and enforce 100% compliance across all remote access workstations.

Customer Opportunity

- 1) Maintain corporate commitment to customer service and support
- 2) Maximize user productivity
- 3) Lower cost of administration
- 4) Lower overall risk to the business

Main Security Issues

- 1) Protect against exposures of mobile computing
- 2) Incorporate stronger network security via an enforcement process
- 3) Block admission of potentially harmful devices from network access

Customer Benefits

- 1) Consistent security process in place - No more grey areas
- 2) Ability to expand remote access safely - No fear in rolling out
- 3) Comprehensive, all-in-one solution - Multiple, point products not required