



Case Study: Financial Ombudsman

Financial Ombudsman Service Remains

No Compromise on Data Protection

Negotiation is an important part of daily business dialog, however, when data security is the topic on the table, there is little room for compromise. Business travelers have come to expect that their data be as mobile as they are. Balancing the security and integrity of corporate data with the need to efficiently transport information has become downright crucial.

A myriad of devices are available to keep our information mobile; the question of how to keep it secure both inside and outside the office, is one that sparks debate among IT professionals the world over.

The Organization

Financial Ombudsman Service (www.financial-ombudsman.org.uk) was established in 2001 by the British Parliament to help settle disputes between businesses that provide financial services and their customers. Located near Canary Wharf in London's docklands, the organization employs about 1,000 people at one location.

The Conflict

Financial Ombudsman Service mediates complaints between consumers and their banks, mortgage providers, insurance agencies, and other financial institutions.

The information the organization gathers for mediations is highly sensitive, including personal consumer data such as bank account and insurance policy numbers, physical addresses, and details of complaints that often involve health information. Frequently, the company's representatives are required to travel, utilizing removable storage devices in order to keep data readily accessible.

The Financial Ombudsman Service has fortunately not suffered a security breach; no laptops have been stolen or USB drives lost. Yet, as stories of data theft and tampering have made media headlines, they are regularly reminded of the need for a secure way to utilize transportable communications devices. According to William Knock, Infrastructure Developer for the organization, "More than a year ago we began looking for a security solution that would help us to maintain our current secure and stable environment without impacting the use of portable storage devices for business purposes."

Weighing the Options

Knock and three other colleagues began researching available solutions both on the Internet and through local specialist distribution company, Vigil Software (www.vigilsoftware.co.uk).

"We needed a product that would manage access to USB storage devices along four primary lines," he said. "We wanted to implement a solution that blocks input/output devices as a security defense against system outages; we needed to appropriately allow the safe use of USB memory sticks but we wanted to block dangerous file types from entering FOS from allowed memory sticks. We also needed the ability to audit USB usage and content as well as monitor unauthorized attempts to connect USB devices."

Vigil Software suggested products from endpoint security firm, Safend, to accommodate the organization's need for ironclad data security with flexible and granular policy definition capabilities.

Safend Protector offers reliable, easy-to-use, tamper-proof endpoint monitoring as well as device identification and blocking based on administrator-defined policies. It secures all local, physical communications ports including USB, Firewire, PCMCIA; wireless endpoints including WiFi, Bluetooth and IrDA, and removable storage devices such CD/DVD-RWs, iPods, and flash drives. Additionally, Safend Protector transparently encrypts data copied to removable media devices and protects data from the threat of hardware keylogger devices. The accompanying product, Safend Auditor, transparently and rapidly queries all organizational network endpoints, locating and documenting all devices that are or have been locally connected.

"We tested Safend Protector, along with a few other competitors, in a development environment to see if they met the criteria we had before any decision was made," said Knock. "After comparing product features and cost, along with the company roadmaps for future product development, Safend emerged as the most appropriate solution for us."

The Solution

After extensive testing of Safend's products, Knock and his team began deploying Safend Protector and Safend Auditor on nearly 1,000 desktop PCs in February, 2006. The rollout progressed smoothly with no major issues or negative business impact. According to Knock, "Safend Protector's interface is straight-forward and well presented and the deployment caused no disruption in the day to day business operations of the company. Those benefits combined with the fact that we have not experienced any security breaches since the deployment means the project can be considered a complete success."

Final Ruling

Knock and his colleagues at Financial Ombudsman Service have been pleased with the outcome of the decision to implement Safend Auditor and Safend Protector to monitor and secure their corporate data assets and the use of USB devices and prevent any potential security breaches. While the deployment's monetary benefits are still being assessed, Knock has found that the customized, highly-granular security policies of Safend Protector have been a time-saver for his department, "They have allowed us to enable access to certain USB devices for certain business users, which negates them having to contact the helpdesk every time they need access."

Safend's solutions have been in use at Financial Ombudsman Service for more than a year and Knock asserts that Safend's products continue to be the right solutions for their current and evolving endpoint security needs, "Considering the quality, reliability and success of the Safend's solutions we've implemented, I would have no hesitation in looking at future solutions offered by Safend or in recommending their products to other organizations."