Lumension SECURITY™

Barclays Bank

Barclays Bank deploys Lumension Security's Sanctuary Device Control to remove USB security risk

Background

Barclays is a UK-based financial services group and an international banking organization, with branches throughout Asia-Pacific, Europe and South America, engaged primarily in banking, investment banking and investment management. In terms of market capitalization, Barclays is one of the top ten banks in the world. A leading UK retail and business bank, it also provides coordinated global services to multinational corporations and financial institutions worldwide employing over 76,200 employees and operating in over 60 countries.

The bank has recently undertaken an overhaul of the hardware in its high street banks, as part of its drive to deploy systems that further enhance the range and quality of services that Barclays delivers to its customers. The Application Development Infrastructure Renewal (ADIR) program includes transferring the old branch terminals onto a PC platform to make them easy for Barclays' staff to use, whilst ensuring that these platforms are secure. One of the main drivers for making these changes was the prohibitive cost of maintaining the old Infrastructure, the other being to improve the usability and flexibility of the core applications.

The Challenge

Barclays uses a mixture of Windows XP, Windows 2000 and Windows 2003 across it's entire PC estate. As part of Barclays' security audit and risk assessment, the bank needed to ensure that certain devices such as USB drives were not freely accessible, therefore removing the risk from intruders tampering with PC's via the USB ports.

The main aim of the implementation was to create a secure environment within the branch network and to secure against the unauthorized use of USB devices, which a purely Active Directory based solution would have struggled to do in a cost effective and flexible way. Barclays needed to guarantee that potential security breaches, through devices such as floppy drive access, USBs and serial ports, were completely eliminated. Basically, all unauthorized methods of infiltrating the network had to be locked down.

The Solution

After reviewing a number of solutions Barclays chose Lumension Security's Sanctuary Device Control which enabled complete lock down of USB ports and prevented all unauthorized connection of USB devices to the network, with the added flexibility of allowing individual permissions where appropriate – enabling IT managers to lock and unlock particular USB drives as necessary as priorities and privileges of certain staff changed. Therefore, the solution provided secure management of company wide USB device usage, while also offering more granular resource management where necessary.

Barclays appointed QinetiQ, an independent security company to carry out extensive testing of the Lumension solution before deploying the solution. Once testing was completed and they were satisfied that Lumension Security's Sanctuary Device Control had passed their rigorous criteria, QinetiQ advised that Device Control was the most fitting solution to fulfill Barclays USB security requirements. Barclays risk team agreed and the solution became the standard security solution for the ADIR implementation. Prior to roll out to the branch network Device Control was

put through an extensive independent test and pilot cycle, undertaken in a 'branch replication' environment, which mirrored the infrastructure to which it would connect.

The initial two-week pilot was carried out in three branches that varied in size from smaller branches with fewer than ten terminals through to the largest branches. Thereafter, the solution was rolled out to all 1,600 branches, equating to approximately 16,000 workstations protected with Sanctuary Device Control.

The Benefits

"One of the main benefits in deploying Sanctuary Device Control is its 'whitelist' feature, which ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in", said Paul Douglas ADIR Desktop Build Team Manager at Barclays.

"Flash memory USB devices represent a significant risk with the potential to steal company data or introduce 'malware', which could render the computer unusable and quickly infect other PCs on the same network. Device Control is a really strong, easy to use product which is why Barclays chose this solution".

The introduction of Sanctuary Device Control to the network has significantly increased the security and reliability of Barclays network infrastructure, whilst meeting Barclay's internal operational risk criteria. "In the security field we can't really talk in terms of ROI but suffice to say, you cannot put a price on the credibility of the bank and so we have to ensure that none of the branch PCs can be penetrated", said Douglas.

About Lumension Security™, Inc.

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.

Lumension SECURITY™

Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com