Case Study: Large International Bank

Background

A large, international bank must secure its headquarters on each continent, along with a large number of branches and representative offices around the world. The bank is subject to very strict security regulations in some countries to ensure that the bank's internal network is completely separate from the outside. As a matter of best practice, the bank aims to implement those same stringent standards at all locations. At headquarters, this involves a complex and costly security operation. The difficulty is even more acute at the remote offices, some of which do not have on-site IT, and at Disaster Recovery sites.

The Challenge

A key element of the bank's security policy is to maintain a complete separation between the bank's internal network and the internet. At main facilities, two completely separate networks are maintained. This is a very effective security practice as there is no communication permitted from the internal network to the outside, and any deviation would be immediately noticeable. However, there is a price to be paid in terms of both IT support and user training. Employees need to learn how to access the internet using special tools and procedures which enable them to view information from outside the bank, but not to interact with it.

Implementing, maintaining and servicing this two-network paradigm is feasible at headquarters, but it is difficult to accomplish at the bank's remote branches and representative offices. Yet these offices are connected to the bank's critical systems. The same problem exists at the disaster recovery sites, where the cost of a two-network infrastructure was prohibitively expensive, but left the site exposed to risk should it be called into service.

The Chief Information Security Officer of the bank looked for an alternative solution to two networks, that would enable the bank to maintain a barrier between the bank's systems and the internet, but would be simple and cost-effective to implement, manage and use.

The Solution

The bank's CISO heard about BUFFERZONE's virtual container solution for endpoints, which was being used at other large financial institutions to protect the bank's network from exposure to the internet, while enabling employees to use their web browsers and email freely.

BUFFERZONE isolates web browsers, email attachments and downloaded documents in a virtual container that keeps the application separate from the real memory, registry, files and network resources of the computer. If an employee is tricked into downloading malware, it is stuck inside the container, where it can simply be erased. The CISO was particularly interested in BUFFERZONE's network separation capabilities, which effectively divide the computer into two zones – one can only access the internal network, and one can only access the internet.

Americas: +1 646 432 6848 | EMEA: +972 3 6444012

> “BUFFERZONE is easy to deploy, manage and use, making it a perfect fit for our remote locations that do not have full-time IT support.
>
> The bank’s CISO

The CISO decided to deploy BUFFERZONE at the bank’s main disaster recovery site and found BUFFERZONE easy to deploy and manage. The bank uses McAfee’s ePolicy Orchestrator, which he used to distribute BUFFERZONE and update the policy. Users on site found BUFFERZONE virtually transparent and did not have to change the way they worked. That meant that the bank did not need to invest in training and support and could go ahead and roll out BUFFERZONE to the remote branches and representative offices that were currently unprotected. Employees now use BUFFERZONE to protect their web browsers, email and removable media including mobile phones and thumb drives.

“BUFFERZONE is easy to deploy, manage and use, making it a perfect fit for our remote locations that do not have full-time IT support. Now, we can maintain the same high standards of network separation and endpoint security at our remote sites using logical rather than physical network separation. And our employees are happy, because they can continue to access the internet to do their jobs,” said the CISO.

The bank has completed implementation at their disaster recovery facilities and branches, and continues to roll out BUFFERZONE over dozens of representative offices on two continents. As a next step, the bank will be deploying the BUFFERZONE Secure Bridge to enable employees to safely transfer files downloaded from email or the internet from the BUFFERZONE virtual container to the bank’s internal network.

Benefits for the Bank

- Safe browsing and email attachments at dozens of sites
- Compliance with security standards, including network separation
- Protection from targeted attacks, ransomware, zero-day exploits and other advanced threats
- Transparent user experience and fast performance increased productivity
- Simple and cost-effective to deploy and manage with McAfee ePO

Americas: +1 646 432 6848 | EMEA: +972 3 6444012