Solution: StillSecure Safe Access
Client: Intercontinental Bank

It is no secret that five of the top seven networks switch vendors partner with StillSecure for the Safe Access NAC technology. Also three branches of the U.S. military rolled out massive Safe Access implementations. Safe Access has also won so many of the top IT industry awards. This is because; Safe Access is the world's best secure network access control (NAC) product.

Safe Access:

- Prohibits guests from bringing down the network Ensures devices have the latest patches and have not been compromised
- Is future-ready, supporting both DHCP to 802.1x network configurations
- Stops the insider threat to the network
- Gives network admins real-time status of the endpoint environment, letting them take immediate deny/allow action on individual devices
- Tests endpoints quickly without inhibiting the end user
- Rolls out in controlled, graduated phases
- Provides help-desk users with a graphical heads-up display of quarantined devices and the actions required to remediate them
- Protects against spyware and malware.

StillSecure Safe Access Delivers It All

Safe Access is a complete NAC solution that stops unauthorized access, prevents malicious endpoint activity, and enforces your organization's security policies.

When we say it's a "complete" solution, we mean that Safe Access delivers the full range of NAC functionality: pre- connect testing, post-connect monitoring, enforcement and quarantining, identity-based management, and remediation.

With Safe Access, you control how security policies are defined and enforced across your network. You establish and enforce the rules/criteria that devices must adhere to gain access. When devices don't meet your criteria, you have enforcement options that can be applied globally or on a group-by-group or case-by-case basis. For example, when a machine fails policy testing, you can:

- Quarantine it to a segment of the network where it can't cause harm
- Deny access entirely
- Allow access for a specified 'grace period' during which the device will be remediated
- Grant it access (say in the case of your senior execs). Best part? It's all automated.