Group Case Study

Capital City Bank

Capital City Bank Group deploys NETSHIELD's Network Access Control

Capital City Bank

Website: www.ccbg.com
Number of sites: 70
Location: Tallahassee, Florida
Solution: Network Access Control

NETSHIELD Benefits:
• Rapid and simple deployment of over 70 remote sites; all centrally managed by the Command Center
• Prevents breaches and hardens the internal network to keep customer's sensitive financial information safe and secure
• No need for forklift changes or upgrades to infrastructure means a big cost savings and stress-free integration
• Strong compliance reporting for the FDIC's IT audit requirements under the GLBA leads to less headaches for the IT staff

"It was so easy to deploy NETSHIELD. We were up and running in a matter of days, which would have not been possible with other, more complex NACs."

Lynne Jensen, Vice President / IT Network Manager of Capital City Bank Group

To quickly gain control of 70 remote sites for simpler management of all trusted network devices

Capital City Bank Group, Inc. provides a full range of financial services at 70 banking offices, one mortgage lending office, and 79 ATMs throughout Florida, Georgia, and Alabama. None of this would be possible without the vision and dedication of George W. Saxon, the dry goods store owner who founded Capital City Bank more than a century ago.

Capital City Bank Group's goal was to bring additional network security to its headquarters and all branch locations in order to gain visibility and control over the thousands of endpoints attached to the network. With each branch office presenting risk of rogue or mobile device access, Lynne Jensen, Capital City Bank Group's VP / IT Network Manager wanted to block the Bring Your Own Device (BYOD) syndrome plaguing so many financial institutions across the globe. They wanted network security endpoint granularity along with stronger compliance reporting for the FDIC's IT audit requirements under the GLBA.

Because of their limited IT staff and budget, Capital City Bank Group did not want to deploy 'forklift' switching upgrades or make any additional changes to their existing infrastructure. They wanted a solution that would provide insight into the daily activities of network access at every branch office location. After reviewing several other big-name Network Access Control providers, they ultimately chose NETSHIELD due to their ability to cost effectively and simply manage access control for thousands of devices within their 70 locations.

Capital City Bank Group rapidly deployed NETSHIELD's Network Access Control across their headquarters and remote locations and used the built-in Command Center functionality to manage all of the locations with ease. Because of the ease-of-use of NETSHIELD's Network Access Control solution, Lynne Jensen and her team were able to fully configure all of the remote site appliances from the headquarters before sending them out to each remote site. From there, an employee from each remote site simply plugged the appliance into the network and it functioned correctly: "It truly is a plug-'n-play solution," said Jensen.

Capital City Bank Group deploys NETSHIELD's Network Access Control

Once the solution was deployed, Capital City Bank Group ran a scan of all of the endpoint devices connected to the network to build a trust list for their organization. Then to ensure that the BYOD policies they put in place were enforced by employees, Lynne Jensen and her team enabled NETSHIELD's blocking technology across all sites to ensure devices that weren't supposed to access the network were automatically blocked. This gave Capital City Bank Group an advantage since they were protecting their customer's sensitive information while at the same time, making sure that BYOD was no longer a burden for their organization. According to Lynne Jensen, "BYOD is a huge problem facing all financial organizations today, but NETSHIELD's blocking technology lets us have ultimate control over who and what is accessing our network, so we always have peace-of-mind."

Also, since Capital City Bank group is under strict FDIC mandates under the Gramm-Leach-Bliley-Act (GLBA) for their information security, the Network Access Control solution they chose had to enforce their business security needs while providing the reporting that is necessary for audit and compliance purposes mandates that financial institutions implement "administrative, technical, and physical safeguards" for customer records and information, which is why having NETSHIELD's Network Access Control solution in place to block the untrusted or malicious devices from accessing their network was a critical need for Cap tal City Bank Group.

NETSHIELD began delivering measurable value from the minute Capital City Bank Group chose them for their network security needs. NETSHIELD's Network Access Control solution provided them with rapid deployment and ease-of-management across their 70 locations. In addition to core access control, Capital City Bank leverages the NETSHIELD appliance to deliver vulnerability assessments, compliance reporting, zero day malware and phishing attack quarantining. Lynne Jensen says in closing: "Now, we have complete control of our IT network security and FDIC compliance posture across 70 locations, from the inside-out, thanks to NETSHIELD."

> "Now, we have complete control of our IT network security and FDIC compliance posture across 70 locations."
>
> Lynne Jensen, Vice President / IT Network Manager of Capital City Bank Group

About NETSHIELD Corporation

NETSHIELD's Mission is to be a trusted provider of cost effective, proactive security solutions to enhance organizations cyber-risk mitigation strategies.

NETSHIELD delivers critical network access control to ensure only trusted assets access corporate networks. Additionally, zero-day malware and phishing attack real-time quarantine, mac-spoof detection, TLD blocking, comprehensive auditing, vulnerability assessments, and compliance reporting & enforcement make this a comprehensive and compelling offering. NetSHIELD is available as a hardware appliance that scale from 25 to 10,000 protected assets per appliance. In addition, an embedded command center allows administrators to manage up to 1000 remote sites.