



“Catbird’s state-of-the-art automated protection and compliance monitoring of both virtualized and physical servers, managed from a single portal, is the ideal solution for vigilant bank IT managers looking to sleep well at night.”

Stephen Lewis, Thomaston Savings Bank SVP/CFO

Bank Background:

Established in 1874, Thomaston Savings Bank is a community bank with a large presence in northwest Connecticut and New Haven County. Through its 9 branches, it provides a range of high-quality financial services to customers in the communities in which it does business.

Like many banks, Thomaston’s IT department is small but tasked with a big mission: protecting the over half a billion dollars in assets under management. These assets include bank documents with sensitive information such as account numbers, commercial and consumer loan files and email. While some of Thomaston’s core processing is outsourced, other IT responsibilities, including systems and network administration, and help-desking, is done on site and needs to be continuously monitored for internal and external threats. Supporting customer conveniences such as online banking and ATM use also opens up further security risks.

Threat Landscape

The increasing number of news reports about malicious hacks on banks, particularly card processors, had caught the attention of Thomaston. While there had been no successful Thomaston Bank hacks yet, they had seen attempts. The liability and risk associated with such intrusions was not something Thomaston could afford to ignore. Industry figures put a typical audit cost at a minimum \$10,000, but an audit after a breach starts at ten times that. A bank’s reputation could also be incalculably damaged.

They decided to investigate stronger security protection for their assets, with a particular emphasis on network security. Given that outside hacks invariably have to come from the network, they knew they had to make sure theirs was bullet-proof. But they also knew that whatever solution they deployed had to be architected for virtualization as well.

Going Virtual

In 2008, the bank confronted the issue of consuming too much power for its servers, blowing circuits and facing trouble cooling the machines in the data center. To remedy this, IT decided to virtualize many of Thomaston’s servers. Virtualization, and the introduction of a SAN, enabled consolidation and a dramatic reduction in the amount of electricity needed to run the data center.

Over the ensuing months, the bank upgraded the majority of its servers to VMware®, including the servers under the management of its outsourced core processing host. Virtualization was a huge cost and energy saver, while improving reliability as well, as the cluster of virtualized machines coordinated for failover.

But, in moving to virtual infrastructure, Thomaston also knew it had introduced significant potential security issues.

Virtualization Security Problem

Traditional security appliances and approaches are inadequate for virtualized infrastructure. Standard devices which sit on the physical wire and monitor



network traffic cannot see inside the virtual host —resulting in a potentially catastrophic blindspot as malicious traffic between virtual machines will not be detected. Moreover, virtual machines are characterized by mobility, with virtualized servers routinely, and automatically, migrated from one host to another, independent of physical location. This constant movement cannot be tracked by stateful traditional security appliances which will soon lose sight of where a machine has gone and what it is doing. Compliance and policy further challenge classic security strategies, as guidelines are difficult to monitor and enforce from within a virtual host and existing policies may not even be adequate for the new architecture.

Catbird vSecurity

Thomaston was already using Catbird to protect its physical networks from attack, including as a network monitor to block rogue PCs from joining the bank's network. Catbird was also deployed to prevent tech-savvy staffers from installing unauthorized rogue access points and unwittingly exposing the whole network to hackers.

When IT managers learned that Catbird was the industry leader in virtual security and compliance, they were thrilled. “We still have physical servers, working alongside our virtualized ones,” noted Patrick Quinn, Network Administrator at Thomaston. “It’s really nice to have one product protecting both our physical and virtual infrastructure. Having two separate security solutions would be extremely confusing.”

Catbird vSecurity is now deployed throughout Thomaston’s virtualized data center. vSecurity’s comprehensive set of features including vulnerability monitoring; IPS/IDS; network access control and network segmentation; and firewalling via Catbird TrustZones, automatically monitor and enforce

security 24x7 in the mission-critical environment of the bank.

Quinn particularly appreciates Catbird TrustZones™ to firewall and prevent unauthorized communication between virtualized servers, irrespective of physical location. TrustZones groups virtual machines according to a set of policies, then tracks the machines through mobility events while continuing to enforce the established policy. If a bank standard, for example, states that HR servers may not communicate with Accounting servers, TrustZones will enforce that policy, even if the machines share a virtual network. TrustZones will also quarantine unauthorized machines which try to join the network, or authorized machines which have violated policy.

Quinn is also a fan of Catbird’s vulnerability monitoring. “It is a really phenomenal benefit. We need to stop or slow the spread of viruses on our virtual network, as these machines now co-reside with each other on the same physical host. An infection in one machine could easily infect all other machines instantly. Catbird instantly detects and prevents such a problem.” Catbird vSecurity vulnerability monitoring is updated automatically with all of the current industry-standard threats, and provides 24x7 monitoring for any change in the posture of the virtual machines it is protecting.

As an added benefit, Catbird vSecurity provides 3rd party standards-based compliance, including GLBA and SOX monitoring. This ensures that banks can maintain regulatory compliance and pass their audits as they transition to virtual infrastructure.

Quips Quinn, “We have so much confidence in Catbird that we do all data transfer over the network, even where we used to use sneaker net. The risk of a courier losing a tape is higher than the risk of a successful attack on a virtual or physical network protected by Catbird.”