



Bremer Bank

Bremer Bank Selects ForeScout CounterACT™ for Real-time Visibility, Guest Access and Automated Controls

INDUSTRY

Financial

ENVIRONMENT

Approximately 1,900 employees throughout its 87 branches and corporate locations and 4,200 endpoints

CHALLENGE

- Ensure a reliable method is in place to classify and monitor the devices connecting to the corporate network from its headquarters, or from one of the Bank's 80 plus branches.
- Increase its defenses against the ever-increasing landscape of advanced persistent threats (APT) through continuous monitoring and mitigation.

SOLUTION

- Agentless solution, allowing them to migrate off of their existing complicated 802.1X infrastructure.
- Non-intrusive installation and operation easily integrating with Bremer's existing Cisco network.
- Out-of-Box functionality for automatic identification of devices, users and software, flexible policy actions, and alerting and reporting.

RESULTS

- Comprehensive, real-time network visibility across endpoints.
- Extremely fast and easy deployment with rapid time-to-value.
- Automated guest management and registration, thereby segmenting guest traffic from the company's internal network.
- Improved compliance to security policies without negatively impacting end-user experience and productivity.
- Automated isolation of devices and alerts sent when malware and malicious activity are detected.

Overview

Bremer Financial Corporation is a privately held, \$8.7 billion regional financial services company jointly owned by the Otto Bremer Foundation and Bremer employees. Founded in 1943 by Otto Bremer, the company provides a diverse portfolio of banking, investment, trust and insurance products and services throughout Minnesota, North Dakota and Wisconsin. Clients include individuals and families, mid-sized corporations, small businesses, agribusinesses, nonprofits and public and government entities.

The Bank has approximately 1,900 employees throughout its 87 branches and corporate locations and 4,200 endpoints, excluding servers. The IT team is responsible for the company's security infrastructure, as well as the design, implementation and management of related components and processes. The team works closely with all business areas, especially information security, enterprise architecture and senior management to align with corporate strategy while maintaining a high-level of security to protect the sensitive assets of the Bank and its customers.

Business Challenge

Bremer had an existing 802.1X network access control (NAC) implementation to assist with the influx of diverse corporate and user-owned devices, but it required heavy support, and was prone to false positives and disruption. Bremer's IT team had significant challenges deploying and maintaining the system, which required setting up numerous exceptions, particularly at remote sites. The implementation required agents and created 802.1X supplicant management overhead, as well as unplanned outages, which negatively affected the user experience and Bremer's customers.

To rectify the situation, the Bremer team began a search for a new NAC solution to boost network security and access control. The Bank preferred an agentless approach, to reduce management overhead, improve system resiliency and enhance user experience, thereby delivering significant time and cost savings for IT.

Why ForeScout?

After an exhaustive evaluation process, working in conjunction with his infrastructure security engineers, network engineers, enterprise architecture department, and information security team, Joseph Thornell, network architect and vice president of Engineering at Bremer, ultimately chose ForeScout CounterACT™ as Bremer's NAC for its ease of installation, management capabilities and robust feature set.

"We required a fluid, secure method to identify corporate assets, and secure access for personal and guest devices at the same time," said Thornell. "In addition, it was very important that we offer and maintain a good user experience, especially because our previous solution caused a lot of frustration in the user community. We needed the new solution to help fix the negative perception the original one had created. ForeScout fit the bill, and we chose it almost immediately."



ForeScout CounterACT delivered value the minute we plugged it in. By giving us the ability to see and gain intelligence on more than 4,000 endpoints, we now have a better way to manage and control our network security. Since the initial deployment, the solution has grown with us, and we've realized added value as we incorporate more functions into our security policies. — I'm excited to see where we will go with it in the future.

— Joseph Thornell, Security Technical Architect, Bremer Bank

The ForeScout Difference

Key differentiators that contributed to Bremer's overall success:

- Ease of deployment and management of the solution
- Real time visibility across the network
- Security product integration

ForeScout's ability to provide IT departments with comprehensive visibility over devices accessing the network was crucial in Bremer's decision to deploy CounterACT. Its agentless approach, flexible guest management capabilities and segmentation options were also strong benefits for the Bank. In addition, ForeScout's ControlFabric™ technology, which enables seamless integrations with other security solutions, was a unique selling point that became a significant factor in Bremer's ultimate decision to buy.

Business Impact

Bremer deployed CounterACT to replace its existing 802.1X solution, and experienced a quick and smooth transition to the new system. With CounterACT, the Bank's network currently supports all regional branch clusters, and is centrally managed from corporate headquarters. Bremer is currently operating a CounterACT 4000, and is in the process of adding a CounterACT 10000, which is expected to come online in the near future.

"The new, bigger model will support 10,000 devices concurrently, and we will use the old hardware to ensure business continuity process," said Thornell. "In addition, we plan to add upward of 1,000 additional endpoints to our existing 4,200."

Benefits realized by Bremer Bank after deploying CounterACT include:

Real-time Visibility

For Bremer, multiple business units throughout the organization utilize CounterACT's endpoint visibility feature. The Bank uses its newfound network visibility for real-time inventory intelligence, and according to Thornell,

ForeScout's tracking is highly accurate, freeing up IT to focus on other tasks. In addition, Bremer was able to leverage this feature to view legacy software on systems, which was particularly helpful during the recent Windows XP migration.

"Real-Time network visibility is extremely useful for understanding what resides on our network," said Thornell. "It's especially efficient for all branch offices, and gives us the ability to determine what to isolate, and how to migrate — we can use the insights we gain from CounterACT to justify and validate system upgrades."

Guest Management

CounterACT is used within the four main branches of Bremer to provide wireless access to employees and guests, and while the Bank's other branches support kiosks through a different wireless provider, each endpoint is still routed through CounterACT's defenses to segment those systems on their own network, to set site access permission, and apply other controls as needed.

"The ability to manage our devices while providing additional access options for guests and employee mobile devices is key," said Thornell.

Policy Creation and Enforcement

Bremer has not only been able to create custom security policies across its organization using CounterACT, but has also been able to enforce its BYOD and mobile security policies by identifying, limiting or blocking unauthorized applications.

Another custom policy used by Bremer is the ability to classify operating systems, as well as personal and mobile devices.

Malware/Malicious Activity Identification and Isolation

Bremer leverages ForeScout CounterACT to block non-corporate and threatening devices from gaining network access to its sensitive IT resources. The Bank uses ForeScout's threat prevention, similar to an IPS, to block malware attacks on the network as well. CounterACT can also be used to audit hardware and software versions such as Adobe Flash, to prevent outdated and at-risk endpoints from connecting to the network.

Security Product Integration

ForeScout's ControlFabric technology enables CounterACT and other IT systems to exchange information and mitigate a wide variety of issues, and Bremer is capitalizing on these opportunities by integrating CounterACT with their QRadar system information and event management (SIEM) and anti-virus solutions.

Automation, Time and Cost Savings

For Bremer, the ease of management and extensive support ForeScout affords compared with its previous NAC solution cut down on calls, and saved the IT team and help desk significant man-hours.

"Asset classification processes are now much faster," said Thornell "Support staff can immediately identify corporate and non-corporate assets, and re-classify a system." "Time, energy and effort were saved compared to our old infrastructure 802.1X approach."

CounterACT's automation has helped improve security with its ability to find the user and switch port. Prior to the ForeScout implementation, in most cases, network engineering would have to make a switch exception for that user and device. As such, that device would no longer be under NAC control until the system remediated both the agent and supplicant.

Because Bremer's help desk has access to CounterACT's visibility into users and endpoints, they save considerable

time and effort in diagnosing problems. Overall, the bank has realized time savings thanks to ease of management, support cases and having access to all functionality in one place, where previously it would have required multiple people and systems to gather this data.

"To achieve the level of security and visibility that ForeScout provides, we would need multiple systems and hours to implement and manage these systems," said Thornell.

Security Product Integration

To Bremer, CounterACT is more than just network access control, and the Bank offers the following advice for other financial institutions looking to implement a NAC solution:

"The visibility and monitoring capability is as much of a win as the enforcement," advised Thornell. "Go big with policies in monitor mode, and you can really gain a significant amount of intelligence from the system, with little to no impact on the end user experience."

In the future, Bremer plans to expand ForeScout CounterACT into other areas in addition to monitoring user endpoints. The Bank plans to integrate more security solutions through the ControlFabric technology, including Tenable vulnerability scanning, corporate and guest wireless, mobile device management (MDM), VMware and RSA data loss prevention (DLP). The bank also plans to use an endpoint monitoring policy leveraging Windows Server Update Services (WSUS) to check for patch levels for reporting and manual remediation. They also intend to expand policy to enable direct updating and WSUS-enabled updates.

"The visibility we've achieved into our endpoints, and high level of security we've maintained has been invaluable," said Thornell. "ForeScout CounterACT delivered as soon as we plugged it in. The ability to see and manage over 4,000 endpoints is instrumental. We look forward to seeing continued benefits from our deployment."

Learn more at
www.ForeScout.com



ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1.866.377.8771
Tel (Intl) 1.408.213.3191
Support 1.708.237.6591
Fax 1.408.371.2284