Banking on Better Email Security

Community bank blocks millions of malicious messages with Cisco

Executive Summary

Customer name
American National Bank

Industry
Financial Services

Location
Omaha, Nebraska

Employees
560

Challenges

- Bank is a highly attractive target for cyberattacks
- Email remains the #1 threat vector for corporations
- Bank's outsourced email security solution was ineffective

Solution

- Cisco® Email Security with Advanced Malware Protection (AMP)

Results

- Able to identify and neutralize the vast majority of email threats
- Over one million malicious messages blocked per month
- Drastically reduced security gaps

American National Bank is a mid-sized community bank headquartered in Omaha, Nebraska. It has 37 branches spread throughout Nebraska, Iowa, and Minnesota. Established in 1856, the bank has $3.7 billion in assets and approximately 560 employees. It prides itself on maintaining a very strong community presence, promoting charitable giving, and offering an open and supportive company culture.

To protect its customers, community, and company, a strong security strategy is non-negotiable for American National. Being a financial institution, it is a prime target for cyberattacks, many of which come in via email. Despite all of today's sophisticated attack vectors, email remains the #1 means of launching attacks on corporate infrastructure – and even the most technically savvy among us continue to fall victim.

> "Cisco Email Security is an invaluable asset for safeguarding our users, customers, and data."

Ben Brandt
Cybersecurity Engineer, American National Bank

An Underperforming Solution

Several years ago, most of American National's security solutions were outsourced and managed by third parties. However, its hosted email security solution lacked critical capabilities – providing limited whitelisting/blacklisting functionality, ineffective spam controls, a lack of SPF/DMARC validation options, and no Data Loss Prevention (DLP) technology. These deficiencies left the bank vulnerable to potential security risks including phishing attacks, email forgery, and data loss.

The bank therefore decided to bring its email security solution in house. After a thorough competitive analysis, it decided that the Cisco® Email Security Appliance would be the best solution in terms of both capability and cost.

Putting Strength Back in Security

With Cisco Email Security, organizations can stop attacks like phishing, business email compromise, ransomware, and spam from infiltrating their systems. They can also prevent their own users from inadvertently sending out infected or sensitive messages.

"We have been able to leverage many Cisco Email Security features to drastically reduce threats and security gaps," said Ben Brandt, cybersecurity engineer at American National Bank. According to Brandt, these capabilities include:

- **Data Loss Prevention –** American National has leveraged the many highly customizable DLP filters within Cisco Email Security to prevent sensitive data from accidentally leaving its network.
- **Spoof Detection –** SPF/DMARC validation allows the bank to identify and quarantine messages sent from non-approved mail servers.
- **Anti-Spam Filters –** According to Brandt, "Cisco offers a robust anti-spam solution that's both user friendly and easy to administer."
- **Advanced Malware Protection –** Cisco's Advanced Malware Protection (AMP) for Email Security allows organizations to protect against risky files.

Cisco Email Security also includes additional layers of protection including antivirus, encryption, URL analysis, sender reputation, and advanced authentication and access control. The backbone of this comprehensive solution is Cisco Talos, one of the world's largest threat intelligence organizations. According to Brandt, Cisco Email Security is also easy to implement and fine tune, quickly filling his company's email security gaps.

> "AMP has prevented countless malicious attachments from entering our network. This allows our security team to focus on bigger threats instead of chasing and remediating minor workstation infections."

Ben Brandt
Cybersecurity Engineer,
American National Bank

The Numbers Speak Volumes

“Cisco Email Security has allowed us to identify and neutralize the vast majority of email threats, ultimately protecting our users and customers,” said Brandt. These threats have ranged from infected documents and malicious executables, to phishing and ransomware campaigns.

Within a 30-day timeframe at American National Bank, Cisco Email Security:

Stopped	Identified and quarantined
1.2 million	89,000
threat/spam messages (82% of total email)	graymail messages (6.2% of total email)

“In the event that an infected message does make it through,” added Brandt, “the solution provides a wide array of filtering options that enable us to quickly block similar messages and avoid any further risk.”

“Cisco Email Security is highly effective at identifying and remediating threats, and is simple to implement and manage,” he continued. “It is the email security solution of choice for American National Bank.”

For more information

For more information on Cisco Email Security, go to: cisco.com/go/emailsecurity.

> “Cisco Email Security has drastically reduced our threats and security gaps.”

Ben Brandt
Cybersecurity Engineer,
American National Bank

> “The Cisco Email Security solution has proven to be reliable and consistent in detecting and preventing threats with low management overhead. It is a key component of the bank’s information security strategy.”

Tim Wilkinson
Vice President, Cybersecurity,
American National Bank