

American Water Saves Over One Million Dollars Fighting Malware Threats

Customer

American Water is the largest water resources provider in North America. American Water is a subsidiary of RWE AG's water division, which includes London-based Thames Water.

Challenge

While American Water had implemented network intrusion detection systems (NIDS), firewalls, and had segmented their network, the impact of a worm attack made it clear that there were limitations to those safeguards. The security team needed a solution that would not only detect worms, but could give them network-wide visibility and provide proactive network intervention to protect and secure the network.

Solution

Using American Water's existing infrastructure, the Arbor Peakflow® X deployment required no network redesign or disruption in traffic. Arbor Peakflow X immediately provided the IT security team with real-time visibility into the enterprise network to identify and mitigate any network anomalies.

Results

With Arbor Peakflow X, American Water has realized significant savings in time, money and productivity. Malware clean-up costs decreased and they eliminated the need for top level security to be on hand 24/7—a savings of approximately \$1 million over two years.

Detecting Threats Impacting the Internal Network

For American Water and their 9,000 employees, providing high-quality water and services to 18 million people in 29 states and three Canadian provinces, and protecting the country's water supplies is something the company takes very seriously. The security of the company's network is tightly integrated into securing the company's water services and their operational risk management goal to implement active and effective risk controls.

American Water assembled a core team of IT security experts responsible for driving security initiatives across the company. The team built a well-protected network and incorporated solid components for proper network security. While implementing a broad spectrum of network intrusion detection systems (IDS), firewalls, and segmenting the network, the IT team realized the limitations of signature-based detection and protection systems and determined that a relational anomaly detection system was necessary for their layered protection strategy; Network Behavioral Analysis (NBA) technologies and active network response was a priority.

"We lacked the technology to detect and classify zero-day worms, insider misuse and other threats impacting our internal network," said Bruce Larson, security director at American Water. This became abundantly clear when the company was infected by a worm on a Friday afternoon that forced the top level security engineers to spend considerable amounts of time responding to the event, which continued into the weekend. "Valuable time and productivity was wasted. It was clear that a relational-based anomaly detection solution that would provide network-wide visibility, and detect worms and other internal threats in real-time would enable the IT team to proactively defend and secure the network," said Larson.

The American Water network security managers also determined that the technology would need to complement existing security components. This was not something they could get out of a traditional IPS security solution.

Arbor Peakflow X Protects American Water's Internal Network

After surveying the security landscape market and examining new security technologies that focused on protecting the internal corporate network, the IT management team chose Arbor Peakflow X.

"Arbor Peakflow X offered American Water the essential components to round out our enterprise-wide security solution, and protect American Water's internal networks from insider misuse, spyware, phishing, zero-day attacks and propagating worms," said Larson. "Because Arbor Peakflow X can be deployed in a non-invasive manner, deployment did not require any network redesign and did not disrupt network traffic."

“Arbor Peakflow X offered American Water the essential components to round out our enterprise-wide security solution, and protect American Water’s internal networks from insider misuse, spyware, phishing, zero-day attacks and propagating worms,” said Larson. “Because Arbor Peakflow X can be deployed in a non-invasive manner, deployment did not require any network redesign and did not disrupt network traffic.”

Bruce Larson, security director,
American Water

Considerable Savings in Time, Money and Productivity

Today, the American Water security team can detect and mitigate worms with Arbor Peakflow X, saving valuable time and money. In addition, Arbor Peakflow X has armed the IT team with full network-wide visibility, enabling them to proactively secure the network.

While duties are segmented across the IT team, each and every team member relies on Arbor Peakflow X. The team leverages Arbor Peakflow X daily; it is an indispensable asset to their overall security strategy and supports the corporate operational risk management goals.

Arbor Peakflow X provides top level engineers network-wide visibility into the enterprise network and enables the IT team to identify and mitigate any network anomalies—saving American Water considerable time, money and productivity. The security team is no longer faced with network interruptions due to worm attacks or potential insider misuse. Arbor Peakflow X provides an instant automated response to threats by locking down segments of the network to prevent the spread of worms and other cyber threats—reducing downtime and clean-up costs.

Looking to the future, the flexibility of Arbor Peakflow X’s anomaly detection will enable American Water to adapt their detection platforms to emergent network technologies and standards such as IP V6 and MPLS. With continued growth and integration with their business partners and customers, the power of Arbor Peakflow X will allow the IT team to defend their network from rapidly emerging threats. Arbor Peakflow X will increasingly play a pivotal role in American Water’s information security portfolio and will replace rule-based systems.

“Arbor Peakflow X’s powerful enterprise capabilities has given the American Water security team the ability to detect, analyze and mitigate threats in real-time and allowed us to realize savings of over \$1 million in two years in operational expenses due to vastly reduced response and recovery efforts from malicious threats to our network,” said Larson.



Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824
Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 208 622 3108

Asia Pacific

T +65 6327 7152

www.arbornetworks.com

About Arbor Networks

Arbor Networks is a leading provider of secure service control solutions for global business networks. Its customers include over 70 percent of the world’s ISPs and many large enterprises. Arbor solutions deliver best-in-class network security and visibility, along with the power to improve profitability by deploying differentiated, revenue-generating services. By employing flow-based and deep packet inspection (DPI) technologies, Arbor solutions measure and protect the entire network—from the network core to the broadband edge. Arbor also maintains the world’s first globally scoped threat analysis network—ATLAS—which uses technology embedded in the world’s largest ISP networks to sense and report on comprehensive worldwide threat intelligence.

Copyright ©1999-2009 Arbor Networks, Inc.
All rights reserved. Arbor Networks, the Arbor Networks logo, Peakflow, ArbOS and ATLAS are all trademarks of Arbor Networks, Inc.
All other brands may be the trademarks of their respective owners.