



Case Study:

American Water

American Water makes Demarc Sentarus the Enterprise Intrusion Detection Solution of Choice

Introduction

American Water is the largest water resource organization in North America, founded in 1886. With annual revenues of more than \$2 billion, American Water owns or operates more than 800 water and waste water operations in the US, Canada and Puerto Rico. It owns or maintains 57,000 miles of main water distribution systems and 7,800 miles of sewer pipe lines.

Throughout its history, American Water has remained dedicated to innovation and best practices as evidenced by their technical and process innovation with the water industry and for their extensive capital investments in rehabilitation of infrastructure.

The Network

American Water operates in a complex IT environment through an enterprise level Wide Area Network, spanning the United States. The network connects hundreds of servers and thousands of Intel-based workstations. It provides the communications fabric for operations, partners and more than 9,000 employees to operate effectively. Adding to the system's complexity is a geographic footprint of the network linking hundreds of locations across the US using the latest in authentication and cryptography technology to extend secure remote access to Enterprise resources.

The Problem

After the terrorist attacks of 9/11, American Water took a serious look at its security efforts, including physical and IT security needs. The company knew it needed protection from both internal and external threats. One year later, American Water established a central security function under Bruce Larson combining physical and information security responsibilities with business continuity planning and corporate crisis management functions. All these functions were converged together with Corporate Health and Safety and Claims Management to form the Operational Risk Management Group.

Larson became responsible for the Security Programs in 2002 and brought valuable experience from previous work in the industry and with the federal government. American Water is keenly aware of the asymmetric threats facing US businesses and the water industry and the need to implement stronger security measures against the emerging threat of physical and information attacks by modern adversaries.

Industry:

- Utility

Organization:

- American Water
- Voorhees, New Jersey
- 9,000 employees

“Demarc is a world class player in enterprise level intrusion detection. Sentarus fills a vital role in our overall security strategy and we will continue to use Demarc solutions as we expand.

“Demarc’s Sentarus is the ideal choice in network intrusion detection specifically because of its flexibility in implementing rules, along with its ability to centrally manage multiple remote sensors across a large, geographically dispersed enterprise.”

*Bruce Larson
Director of Security
American Water*

As a foundational component of IT systems security, network intrusion detection at American Water needed to be both scalable and flexible in its management capabilities. In the search for a network intrusion detection system, Larson found that many systems came with pre-determined, inflexible rule sets or were limited in their ability to scale to the Enterprise requirements of American Water. With the scope and depth of their business processes, American Water needed a system that would be completely customizable and protect from the inside out — not just on the network perimeter.

“If you are monitoring an Internet gateway, it’s easy to use a set of general rules,” Larson said. “But when you are monitoring internal network traffic in a heterogeneous protocol environment like ours, you must have customizable rules that match your internal needs and processes.”

The Solution

American Water chose Demarc Sentarus for enterprise network intrusion detection. Sentarus Sensors were strategically placed in remote locations across the network. These sensors continuously feed data back to a central location for aggregated reporting and management. Larson puts it this way, “Demarc Sentarus is the ideal choice in network intrusion detection specifically because of its flexibility in implementing rules, along with its ability to centrally manage multiple remote sensors across a large, geographically dispersed enterprise.”

With Sentarus, American Water has been able to deploy a customized solution to get accurate actionable reporting, saving management time and resources.

“You must be able to develop customized rule sets that can differentiate false positives from significant security events; otherwise, you will be crying wolf and not be able to respond effectively,” Larson said. “With Demarc, the rule base can be specifically tuned to your network environment to reduce the number of false alarms.”

Today, American Water depends on Demarc Sentarus around the clock to alert them to and stop critical security breaches in near real time. As American Water grows and develops, Larson says Demarc has the capability to match that growth while continuing to provide enterprise level protection from the inside out.

The Benefits

As an integral component of risk management practices, American Water measures the value of security systems investment using a "Value Protection" calculation that compares the normal system Operating Cost to the potential impact to the business from an attack or service degradation of production Enterprise resources.

About Sentarus

The Sentarus product family enables customers to fully leverage their existing investments in IT security with an intelligent, multi-layered security solution. Our core Smart-Layered technology combines and correlates network and host-based event data to provide a contextual and easily understood view across your IT security environment.

About Demarc Security

Demarc Security, Inc. is an innovative, privately-held provider of powerful intrusion detection and prevention solutions (IDS/IPS). Demarc enables customers to cost-effectively protect their networks from both insider abuse and external attacks – addressing vulnerabilities that firewalls and other defenses do not.

Through this type of fiscal and operational analysis American Water developed a strong business case for the deployment of Demarc Sentarus across the Enterprise. This platform plays a significant role in reducing overall security risk, minimizing IT impact from security events and costs far less than competitive solutions.

“Demarc is not only effective from a product standpoint, but because of its flexibility we were able to deploy it rapidly,” Larson said. “Other systems can cost twice as much and take longer to configure to get the same level of security.”

Larson reports that localized Sentarus sensors utilizing Demarc Smart-Layered™ Technology and reporting back to a central management site is analogous to a physical home or business alarm system with sensors on doors, windows and other areas sending information back to a centralized panel for analytics.

As a result, American Water now has the ability to respond effectively to ongoing threats with real-time intervention, in spite of the wide distribution of its network.

“Demarc is a world class player in enterprise level intrusion detection,” Larson said. “Sentarus fills a vital role in our overall security strategy and we will continue to use Demarc solutions as we expand.”

For more information, please call 1-877-8-Demarc, or visit <http://www.demarc.com>.



Demarc Security, Inc.
6309 Carpinteria Avenue
Suite 200
Carpinteria, CA 93013

P: 805.566.3800
F: 805.456.2035
www.demarc.com