CASE STUDY

KATALYST

MUNICIPAL CYBERSECURITY

Government

Business Challenges

- Security monitoring is not properly implemented
- Running old protocols to support legacy applications
- Different information security requirements for each department
- Firewalls with lists of passwords were obtainable

Business Opportunities

- General network security assessment
- Foresite's Reseller and client are working on plans for better data governance

Katalyst Solutions

- Training program
- Special policies for privileged access
- Removal of legacy protocols and applications
- Better network monitoring & detection

Background

Municipalities and governments often have IT and information security departments that are a generic city or county service. Each department had different security requirements. Many of the networks were old and had grown organically rather than by specific design.

Objectives

- Network segregation and ACLs to prevent unauthorized access

- Those responsible for data security must understand the risk of each type of regulated data

- Removal of legacy protocols and applications, and much better network monitoring & detection

- Training program is being put in place with special policies for privileged access

Solution

We performed a general network security assessment for the client. The consultant was able to access data without authentication, gain credentials, and set up a basic user account. Lists of passwords were also found during a basic user scan. The attempt for access was not quiet, yet Foresite was not detected, showing security monitoring was not properly implemented. The solution was to set up network segregation and ACLs to prevent unauthorized access. Additionally, we provided a training program from the staff to better understand security protocols and the risk of each type of regulated data.

Fully Implemented

Network monitoring & detection