



GOVERNMENT AGENCY

The following example describes the situation we encountered at a government agency.

The network infrastructure and operation is outsourced to a global service provider. The heterogeneous infrastructure consists of thousands of servers, hundreds of routers and switches, dozens of firewalls, IDS, IPS, and network behavior analysis and log aggregation products.

RazorThreat installed the TAC software on an existing Linux server within their network and collected the previous day's security and network logs and real-time flow data. Within 30 minutes of this data being analyzed by the TAC it identified the following threats on their network.

1. A bot that was sending credit card information to a foreign country
2. Sensitive information traveling unencrypted in non-secured areas

These findings represent targeted, financially motivated external attacks and internal breakdowns in operations and management. Each of these catastrophic threats went undetected by the numerous perimeter and point solutions they had installed. The reason they were undetected is because their existing systems are not designed to find zero-day, individually targeted attacks.

The TAC enabled this government agency to identify and eliminate these threats to their agency. On an on-going basis the TAC provides them with a second order analysis of all of the data passing through their existing network infrastructure making their environment substantially more secure and improving the overall performance of their other security devices.