



QVISION™ Reveals Threats to Critical Systems at a Fortune 500 Financial Institution

Company at-a-glance:

- Fortune 500 financial institution. Through various subsidiaries the company provides credit cards, mortgage banking, insurance, brokerage and capital markets services.
- Network supports several thousand employees and over 10,000 banking transactions a day.
- Security program includes firewalls, VPN, IDS

“Within 30 minutes of installing QVISION, their network administrators were able to identify misuse and illegal file sharing activity on their network that they were previously unaware of.”

*Dwight Spencer
Q1 Labs Lead Developer*



QVISION provided verification of network misuse and abuse which enabled swift and appropriate response.

The Situation

The smooth flow of business often relies on the effectiveness of computer networks. Any congestion on the network can mean trouble for a company. So, when a major financial institution realized its bandwidth was being drained by unidentified traffic on the network, it had to act.

To counter the overload of traffic, the company separated its networks by firewall and router rules to prevent communication between networks that had no reason to interact. The problem was that there was periodic communication between several networks for the purpose of data backup. As a result they were unable to locate the source of the problem.

In addition, the organization had developed security policies and they were firmly in place, but there was no way to test or enforce them.

The Solution – What they found

The network engineers weren't convinced that there were any immediate threats to the network. But within half an hour of deploying QVISION, they discovered three areas of concern – an extensive amount of peer-to-peer file-sharing activity on the banking transaction server, online gaming servers which made the network vulnerable by opening the network to unauthorized users, and several pop email and spam relay servers. Much of this activity, unfortunately, was originating from internal sources within the IT area.

After running QVISION for several days, the network administrator saw spikes of traffic from the backup system and the primary network. By viewing this traffic through QVISION, the network administrator was able to immediately identify it as anomalous traffic. After a bit of investigation, he discovered that a sophisticated and intentional attack had been made upon the company's systems over a period of months. A machine adjacent to the backup servers had poisoned the ARP cache on a router and was spoofing the traffic.

The company took immediate action by isolating its backup servers, adding a firewall rule-set based on time of day, and developing methods to detect and protect their routers from ARP poisoning.

The Result

By installing QVISION, the financial institution was able to quickly identify both internal misuse and external threats to its network and take appropriate measures before significant enterprise system compromises had occurred.



Security policies were updated and can now be effectively enforced. Administrators were able to pinpoint and shut down the internal perpetrators. The external attack could have opened access to critical financial and customer data, thereby corroding the company's reputation and customer confidence. The company now has the capability to proactively protect its assets against attacks and network misuse.

