Customer Success Story

The Company
This energy and utility company is a family-owned business founded in the 1950’s. The company markets petroleum products and is a wholesale distributor of automotive parts and tires, as well as HVAC Equipment and supplies. The organizations’ roots is in terminal operations and the distribution of petroleum products such as gasoline and diesel fuel. Over the years, it has diversified its interests.

The Challenge
In the mid-90’s, the business hired its Network Administrator. At that time, the privately held company had just two servers with fifteen employees on its network. Over the past decade, the network has seen tremendous growth, and now has over 350 people and 30 servers on its network. The Network Admin is responsible for both managing and securing the company’s entire network.

Solution Summary
To ensure the network infrastructure is as secure as possible, the Network Administrator realized early on that he would need to understand the actual network risk posed by specific vulnerabilities, and to determine if the security investments were actually detecting and preventing attacks. “Hardware can be replaced, data can’t,” he said. “We want to do everything within reason to protect our information.” He was concerned that as his company increased its web presence, people were going to be “gunning” for them. “We have lots of scanning being done and lots of people hitting the outside of our network.” This concern led the Network Admin to proactively engage with consultants to do penetration testing on organizations’ network. From his experience, he knew that this form of testing would give him the most accurate view possible of the real risks to the network.

Unfortunately, as the Network Administrator points out, results from consultants are often inconsistent. “There are many people with questionable skills willing to come in and charge you a lot of money to run a penetration test. However, due to the disparate tools the consultants use we had trouble comparing the results from one test to the next and the results we saw were more dependent on the skill of the tester, than the quality of the product.” He felt the best course of action would be for the business to conduct and own the penetration testing process themselves.

“We wanted to know what tools people were using to do penetration testing, and we saw everything from home grown tools and exploits, freeware and a host of other options that required a significant level of knowledge to use effectively,” the Network Admin recalls. “I’m a network administrator, and everything we came across required too much expertise. I know my network and I know where critical parts are. I just needed something to help me test it easily and efficiently.” The challenge would be to find a cost-effective, easy-to-use product that allowed him to perform regular penetration testing.

“WITHOUT CORE IMPACT IT WOULD HAVE BEEN IMPOSSIBLE TO INTEGRATE PENETRATION TESTING INTO OUR SECURITY PROCESS. OTHER TOOLS REQUIRE TOO MUCH EXPERTISE, AREN’T SAFE TO RUN ON LIVE NETWORKS, AND DELIVER QUESTIONABLE RESULTS.”
The Solution

Ultimately, the organization turned to CORE Security and selected its product, CORE Impact Pro, the first comprehensive penetration testing product for assessing specific information security threats to an organization. The product enabled them to replace the inconsistent, outsourced penetration testing they had previously used with a professional, state-of-the-art, automated penetration testing product. CORE Impact allows the Network Administrator to safely exploit vulnerabilities in his network, replicating the kinds of access an intruder could achieve, and revealing actual paths of attacks that needed to be remediated. By automating the previously outsourced and expensive penetration testing process, CORE Impact helps improve the company’s security while reducing costs.

The Result

The Network Administrator now uses CORE Impact regularly, once a quarter, whenever there is a major vulnerability announcement and in conjunction with their year-end audit. “We manually patch everything, so Impact helps me prioritize and manage my vulnerabilities more effectively. With Impact, we are able to validate the existence of vulnerabilities, to find out if they are exploitable and what information might be exposed.”

Furthermore, the Network Admin is able to eliminate wasted efforts on false positive results from other security products and test all his patches to be sure they are deployed correctly. “Thanks to CORE Impact, I can prove that the technologies, polices and systems I have put in place are actually securing my network.”

“ONLY WITH CORE IMPACT CAN YOU CONFIRM WHAT THE REAL RISK IS TO YOUR NETWORK RESOURCES.”