abusix | telenor

Case Study: Telenor

Telenor Norway Uses Abusix's AbuseHQ to Improve Its Ability to Handle Increasing Network Abuse

Industry
- Telecommunications Service Provider

Background
- Telenor's wholly owned Norwegian mobile operation is the country's leading telecommunications operator.
- Telenor Norway serves both consumers and business customers and strives to maintain the highest level of network service quality.

Challenges
- With its success, Telenor Norway experienced a significant rise in network abuse, jeopardizing the company's service performance.
- Their abuse specialists were being overwhelmed with mundane response and mitigation tasks on an almost daily basis.

Solution
- Telenor Norway chose Abusix's AbuseHQ as the foundation for its efforts to combat network security issues.
- They use AbuseHQ as their network abuse command center.

Results
- AbuseHQ helped Telenor Norway quickly integrate their abuse handling processes into their SOC, speeding mitigation and if necessary, the shut down of compromised customer machines before they can inflict significant damage.
- Automated response allows them to ensure customer privacy and to react quickly, helps them maintain a safe Telenor network environment and contributes to a more secure Internet.
- Using AbuseHQ Telenor's abuse specialists are able to focus on the highest priority and most complex network security issues, while leaving the handling of vast quantity of cases to AbuseHQ.

The Customer

Telenor Norway is Norway's number one supplier of telecommunications and data services. As a flagship division of Telenor Group, a $17 billion (2013 revenues) global leader in mobile communications, Telenor Norway serves both consumers and business customers and strives to maintain the highest level of network service quality.

The Situation

With its success, however, Telenor Norway has experienced a significant rise in network abuse, jeopardizing the company's service performance. Vegar Åsmul, the security analyst responsible for Telenor Norway's Abuse Response Team, said, "As abuse increased on our networks, we realized that we needed to take a smarter approach. Our abuse specialists were being overwhelmed with mundane response and mitigation tasks on an almost daily basis. Continually adding resources wasn't a viable option. We needed a better solution."

50%
Reduction in Workload

3X
More Cases Handled

The Solution

After evaluating several alternatives, Telenor Norway chose Abusix's AbuseHQ as the foundation for its efforts to combat network security issues. Åsmul, Telenor's abuse response leader, said, "AbuseHQ is our network abuse command center. AbuseHQ helped us quickly integrate our abuse and security handling processes into the Telenor Norway SOC. Now we have a continuous and comprehensive perspective on both current and historical abuse and subscriber security activity."

THE PROBLEM	THE SOLUTION	THE RESULTS
Rising Abuse Cases	Flexible playbook rules	50% Reduction in Workload
Lack of Efficiency	Automation for faster case handling	3X More Handled Cases
Inability to Prioritize	Feedback loops for continuous improvement	Zero Open Abuse Cases

The Results

AbuseHQ not only provides a better view into the company's own network abuse activity and subscriber security issues, it aggregates and analyzes massive amounts of data from a wide variety of external and internal sources, including Abusix's proprietary data ecosystem, third-party providers, and internal security systems, to automate the correlation of incidents and IP addresses. This allows Telenor Norway to shut down compromised customer machines before they can inflict significant damage. "Automated response means we can react quickly to ensure customer privacy and security. This helps us maintain a safe Telenor network environment and contributes to a more secure Internet. That makes me feel pretty good," said, Åsmul.

What's more, AbuseHQ's process automation is flexible and easy. AbuseHQ lets Telenor Norway define automated subscriber abuse and security response processes based on the most appropriate parameters and its intimate knowledge of its customers. "AbuseHQ has reduced the amount of malicious traffic leaving our network. Now our abuse specialists can focus on the highest priority and most complex network security issues, while leaving the vast quantity of cases to AbuseHQ," said Åsmul.

AbuseHQ has increased Telenor Norway's abuse response productivity, allowing the company to respond to more abuse and security issues with better efficiency and effectiveness than ever before. "AbuseHQ is a fundamental piece of our network security infrastructure. It helps us maintain a strong network reputation and stable operations, while keeping our customers satisfied and secure. We couldn't be happier with AbuseHQ," exclaimed Vegar Åsmul.

telenor

"AbuseHQ is our network abuse command center. AbuseHQ helped us quickly integrate our abuse handling processes into the Telenor Norway SOC. Now we have a continuous and comprehensive perspective on both current and historical abuse activity."

- Vegar Åsmul