CASE STUDY

REVENUE ASSURANCE

REDUCE REVENUE LOSS FROM THEFT OF SERVICE

Highlights:

1. Reduced revenue loss to less than one third of the industry average
2. Eliminated 88% of CPE firmware hacking instances over three months
3. Secured network with anti-roaming, advanced encryption, and dynamic configuration files
4. Enhanced subscriber QoE by eliminating fraudulent, high-bandwidth users

The Challenge

A major United States cable MSO with more than 5 million subscribers was experiencing significant annual revenue loss as a result of CPE fraud. Hackers exploited security weaknesses to fraudulently access services using cloned MAC addresses, hacked or unauthorized firmware, or fraudulent configuration files on a daily basis. As a result, the company was losing an estimated $US 1 million annually from service theft and CPE fraud.

Solution

Incognito offers an all-encompassing provisioning solution that enables broadband service providers to not only stop existing CPE fraud, but actually stop it from occurring in the future. The inclusion of standards-based and proprietary provisioning safeguards defends your network from cloning and bandwidth theft.

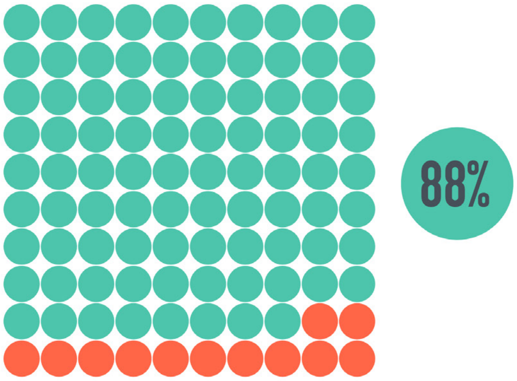
Service providers using this Revenue Assurance Solution on average reduce losses from the industry average of $1 per subscriber to less than one third. In addition to curtailing losses, restricting unauthorized network access and eliminating fraudulent top talkers boosts the quality of experience for legitimate customers and lowers wasted CAPEX spending in infrastructure upgrades.

Incognito safeguards include:

- Anti-roaming to prevent simultaneous and multiple leases on one device
- Advanced encryption for cable modem authorization and CPE IP limiting to restrict the number of IP addresses that can be allocated behind a cable modem
- Dynamically generated and single-use configuration files
- IP address and configuration file name verification
- DHCP Denial of Service (DoS) protection
- Historical records of potentially fraudulent devices
- Filtering to ignore legitimately duplicated devices
- Ability to immediately ban fraudulent devices from further access or restrict to a walled garden where they can no longer affect QoE for legitimate subscribers

Results

After applying these safeguards, the operator saw a dramatic decrease in the number of fraudulent devices. For just one CPE model, the instances of hacked firmware decreased from over 1800 to under 200 instances over a period of three months – an 88% reduction. As the operator continues to deploy these safeguards, they expect to see an even greater impact on the integrity of their network.



Tier 1 provider was able to eliminate hacked firmware by 88% after deploying advanced device provisioning security features from the Incognito revenue assurance solution.

THE INCOGNITO PHILOSOPHY

Broadband service providers worldwide use Incognito products to solve their device provisioning, network intelligence, resource management and service activation challenges. In addition to helping you increase operational efficiency and monetize IP-based services, Incognito also delivers:

Flexible Modular Solutions.

Get software solutions that fit your needs, not the other way around. Our extensive toolkits and expereinced integration experts ensure that you can easily integrate any Incognito solution into your existing systems.

Customer-Centric Approach.

Be heard. We listen to and take your suggestions seriously. That's why 80% of new product features are a direct result of customer feedback.

Support Services.

We're committed to your success. Our experienced professional services team can design custom solutions to suit your needs, while our support team is available 24/7 to answer your questions.

incognito®

Better Intelligence. Better Solutions. Better Experience.

SCHEDULE A CONSULTATION

email: solutions@incognito.com **web:** www.incognito.com