



USE CASE: Carrier Defense against the new smart device landscape

As we watch the continued emergence of smart devices such as Smartphone's, Tablets and Netbooks into the mainstream carriers see the threats that accompany devices that act more like the common PC. Threats such as viruses, worm propagation, device scanning and man-in-the-middle attacks, just to name a few are becoming more of a concern as the devices become more intelligent and a necessity in our everyday lives.

Today's carrier's have addressed some of the problems by embracing network base defenses as well as making well-known commercially available anti-virus solutions to end user's. Solutions that are installed and maintained by the end-user, that were initially designed and architected for PC's.

Technical challenges and risks

There are several technical and business challenges that present themselves, with neither out weighing the other. Here are a couple of technical challenges and risks.

Technical challenge

From an end-point prospective the challenge is resource availability. Most devices such as Smart Phone's, Tablets and Netbooks, have a limited amount of resources available, resources which include CPU power and available memory for applications to be stored and run on. Resources that are predominately preserved for revenue generating applications, not for utilities such as anti-virus solution's which require additional resources due to their signature database. So one of the technical challenges faced by many carriers is how do you preserve the valuable resources and still protect the end-point, and the network. In addition there is a real risk in "Reacting" to a problem versus being "Proactive" this is inherent to using PC technology for the new smart device environment. The cause and effect here could be monumental.

The Risk

The risk in "*What to protect*" becomes a delicate problem, "Protect the network versus protecting the end-point". The network holds the biggest value so protection has been put in place for years and continues to be a priority. As for the end-point that is left in the hands of the end-user today, beyond some basic security features that have been in place since the first Smartphone shipped in 1993. But with the ever changing profile of devices and their capability valuable data now resides on the devices making them expensive targets. In addition the devices have become launching pads for a variety of threats including a carrier's own network. But a business risk also presents itself, and that is the cost of providing commercially available security protection by some of the well known companies. The business risk is profit degeneration due to basic support cost to the common user. A basic support call can relate to



several Dollars, Euros, Pounds, Yen's etc per call. A simple call such as "My device is telling me I have no virus is there anything I need to do?" or "How do I know if my antivirus solution is up to date?". The result is unnecessary cost.

Summing up the problem

So the problems that the carriers have been presented with the new smart devices are as follows:

- Limited resources on smart devices, prohibiting a commercially off the shelf anti-virus solution to be deployed as *a De facto standard* on certain smart devices.
- Reluctance to place one of the common end-point solutions on a device due to the additional support cost.
- Uncertainty in how to protect "New" threats, all actions taken today are "Reactions"
- Using PC "Type" solutions to protect SmartPhones Tablets and NetBooks.

How does Arxceo's solution help Carriers defend the new landscape?

The new landscape of devices present a much different problem to carriers then the days of the traditional cell phone.

Today with the carriers need to protect profit erosion and churn, yet deliver a product whereby the customer feels protected by doing the least amount of work.

Arxceo delivers some of the critical pieces that a carrier looks for:

- Defends against threats silently.
- Requires no user intervention for maintaining or installing. Therefore removes the possibility of support calls.
- Proactively defends against threats. Today we can no longer be reactive.
- Minimizes the amount of resources needed on a device therefore saving CPU cycles, memory and battery life.



- As a signature-less based solution Arxceo does not require the resources necessary to store signatures, therefore leaving precious resources available for revenue generating applications.
- One of first point rejections on for the network to threats.