CogniSafe Ltd.

CogniSafe Ltd
6 Gershon Shatz St.
Tel Aviv-Jaffa, 67017
Israel

Tel: 972-3-6241526
Mobile: 972-52-7907719
www.cognisafe.com

Mission:

Anti-social and criminal cyber activity in multi user environments is a major challenge, causing operators and vendors significant monetary and security damage. CogniSafe develops the next generation cyber security platform for network users and solution providers. Based on semantic technology, CogniSafe's solution detects and handles a variety of threats on network and end user assets.

The Problem:

The explosive growth in the internet in general, and in network access applications generates massive amounts of information at all times. Many end points (Millions) can access the network simultaneously and generate huge amounts of information. The challenge is to introduce a solution that can overcome the following hurdles:

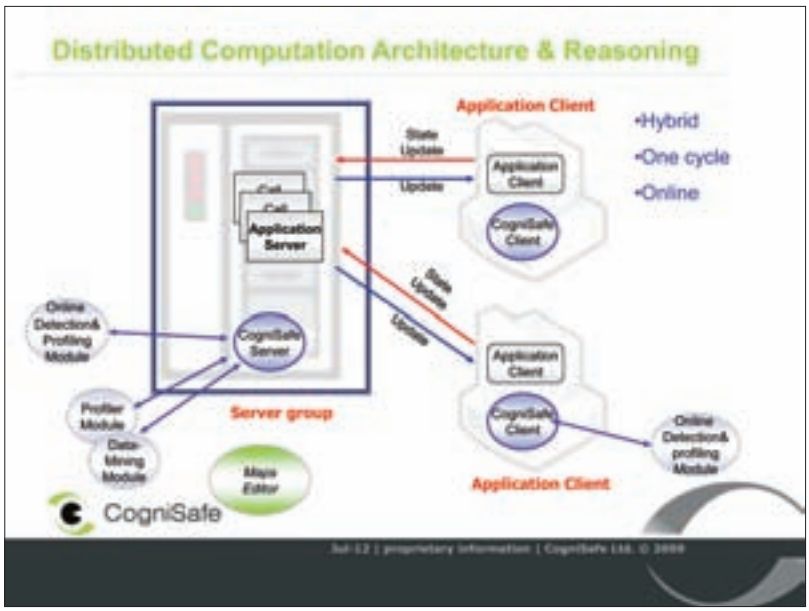
- Traffic is very expensive (bottle neck)
- The environment in constantly changing
- The threat is constantly changing
- The threat is a combination of several low signature changes

The Solution:

The CogniSafe Platform is based on recent advances in Semantic technology. This technology makes it possible to build modules that imitate human thinking/behavior: The technology is:

- **Cognitive:** Situation aware, capable of learning and reasoning about known and unknown environments and applications; can define and identify new unknown threats and cheats;
- **Autonomous:** Can automatically respond to new threats by creating the needed rule/knowledge.
- **Distributes knowledge:** The technology is well suited for distribution/ exchange of the knowledge.

As a result, CogniSafe behavior analysis, using application-user context and auto-learning is capable of giving a complete answer to cyber threats.
The solution includes a generic cross-application layer as the first layer of protection complemented with an optional application specific layer. This architecture offers reduced costs for updates, new threat handling and support of new applications.



Value Proposition

- Detecting abnormal activity at the remote endpoint (such as: "entering" applications outside user's occupation or personal profile and/or norms)
- Generic Protection against a variety of application threats, without any prior knowledge about the specific application. For example Detecting database abuse (e.g. destruction, unauthorized replication, erasing, etc) at the remote endpoint
- Identifying Bots, operating on a specific application or accessing specific resource/s.
- Building a Bot profile in its specific environment to identify unusual behavior – essentially protecting the Bot itself (e.g. a Bot, in this case, can be a mechanical sensor, or a camera).
- Continuously build and update profile for a specific application.
- Online detection:
  - Unusual behavior
  - Wrong behavior
  - Lack of knowledge – User Experience