Lambda DSS Ltd

LAMBDA SENTINEL

THE ULTIMATE PRODUCT FOR MONITORING, ALERTING AND PREVENTING UNAUTHORIZED INFORMATION TRAFFIC IN OR OUT OF THE ENTERPRISE

SENTINEL

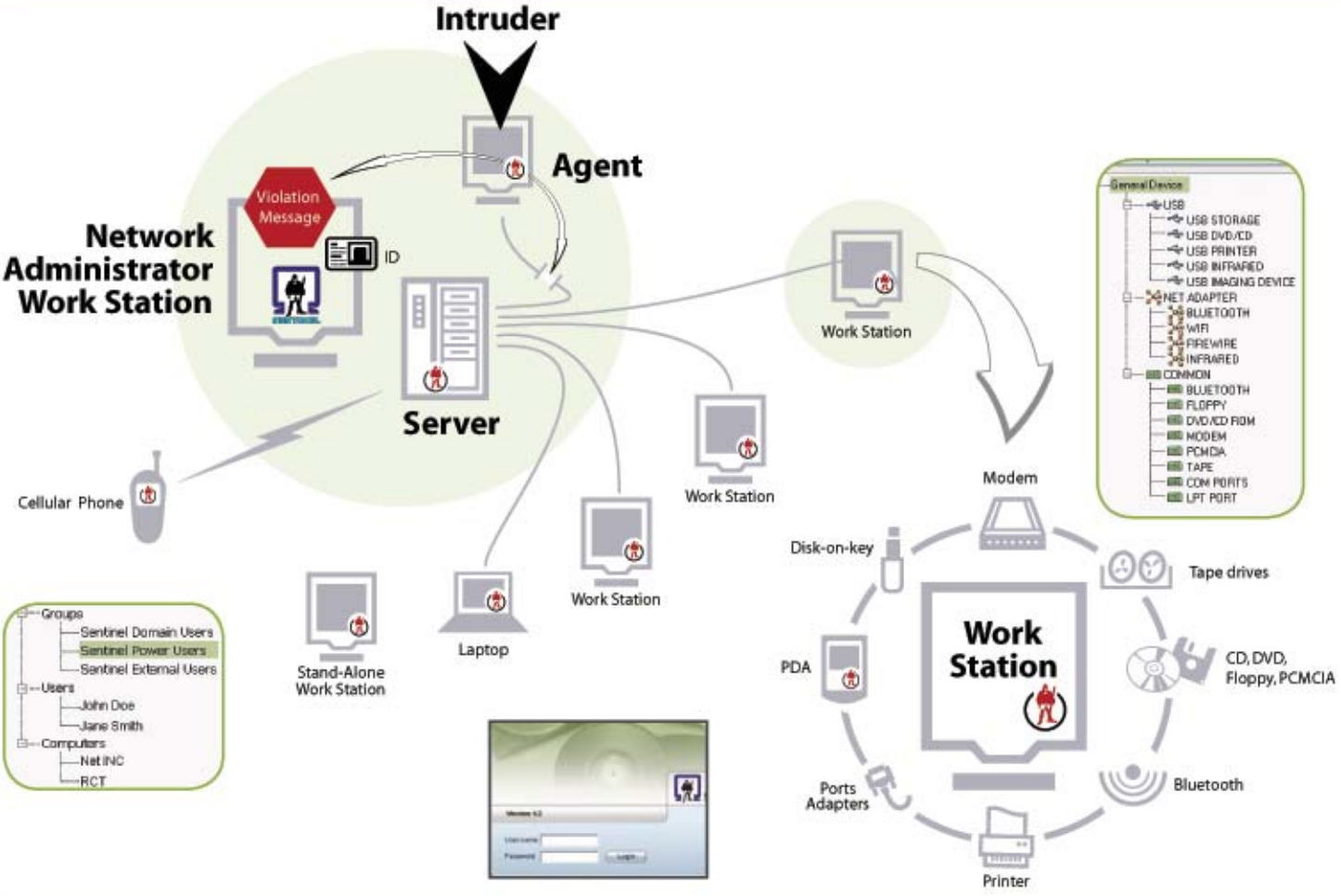
Lambda DSS Ltd • 9 Hamelacha St. Lod 71520, Israel
Tel: 972-8-9245775 • Fax: 972-8-9245815 • Email: info@lamda-sys.co.il

THE NEED

Information is one of the most valuable assets in commercial and defense enterprises. For several years, information security has been of highest priority in organizations worldwide, seeking to protect networks, computer groups, end user workstations, stand-alone computers, cellular and PDA devices, from potential security breaches.

Lambda Sentinel is intended to safeguard enterprise information from unauthorized data traffic by blocking unauthorized hardware devices according to very flexible, centrally-controlled authorization policies.

Information security has become a major concern for government and commercial entities, especially after 9/11 events. The threat has vastly intensified with the widespread use of small, portable devices, characterized by very large data storage capacity and by physical or wireless connections. These easy-to-use and universal devices strongly increase the danger of data and IP breaches, demanding minimal skill and effort from the malevolent insider or intruder.



THE SOLUTION

Lambda Sentinel has been developed by information security specialists, having years of relevant experience, so as to cope with this vulnerability and ensure compliance with privacy mandates worldwide.

Lambda Sentinel monitors, alerts, and prevents unauthorized information traffic in or out of the enterprise. Its focus is to block and report any unauthorized hook-up of devices that can transfer information. The tool applies to all desktop and laptop computers, cellular and PDA devices in the organization.

The next Sentinel generation will be able to perform its job at the file level (in addition to the device level), enabling monitoring and blocking of specific and tagged information.

Lambda Sentinel, offered by Lambda DSS is a highly effective and very affordable solution, performing a comprehensive range of functions.

THIS IS HOW LAMBDA SENTINEL WORKS:

- **Lambda Sentinel** runs as a central application on a common computer (not necessitating a server), automatically and transparently activating agents on the networks' workstations, cellular and PDA devices. These agents are dormant, and are automatically activated only upon hook-up of unauthorized devices.

- It applies site-specified centrally-controlled authorization policies, that can be modified in real time.

- **Lambda Sentinel** prevents unauthorized two-way data traffic by blocking a wide variety of external and/or internal devices, such as:
  - USB devices (disk-on-key, camera, printer, scanner, etc')
  - Bluetooth devices
  - CDs, DVDs, floppy drives
  - Infrared devices
  - Tape drives
  - Modems, network adapters, PCMCIA adapters
  - Ports (com & LPT)
  - Printers
  - Others

- When connecting an unauthorized external device, the following sequence of actions is initiated:
  - **At the administrator monitoring console**
    A pop-up message is displayed and (optionally) a mail message is sent to the Network Administrator, indicating the violating workstation/device, user ID and applied policy.
  - **At the violating workstation or portable device**
    A pop-up message is displayed to the user (optional); A reaction is enforced according to the authorization policy scheme for the specific case (for example: block the user interface, shut off the environment, or other reactive measures)
  - **At both stations**
    All events are logged and time-tagged
  - **Networked and Stand-Alone Operations**
    Separate authorization definitions can be applied for networked and stand-alone (not connected) configurations

- Immunity to Tampering and Circumvention
  - Software files and processes are hidden to the user, making the tool immune to "kill" or un-install attempts
  - If located, any attempt to delete **Lambda Sentinel**'s processes will fail. The program will automatically re-load itself

LAMBDA SENTINEL OFFERS SIGNIFICANT ADVANTAGES TO ITS USERS

- A comprehensive breadth of capabilities in one product, as compared with other tools offering only limited capabilities
- The installation of **Lambda Sentinel** components is smooth and effortless, smoothly integrating into the organization's existing Active Directory.
- Operation requires minimal memory consumption and CPU load.
- **Lambda Sentinel** offers a very robust mechanism against circumvention attempts.

The Company

Our mission is to become one of the leading providers of enterprise Information Security software products.

The senior team at **Lambda DSS** consists of very experienced professional engineers and business development personnel, coming from the Defense, IT and Telecom industries, with profound expertise and know-how in development of data security products and markets.

Lambda DSS is focused on software security products that will complement each other as well as existing security products in the marketplace and will create a suite of products for safeguarding the enterprise information assets.

Lambda Sentinel is **Lambda**'s leading security product, offering the organization a comprehensive, cost-effective and easy-to-install solution. Its main markets consist of defense industries and commercial organizations such as banks, insurance companies, healthcare organizations, credit card companies, pharmaceutical companies, and communication companies where the loss of sensitive information assets or intellectual property would have grave consequences.

Lambda Sentinel Key Features

- Comprehensive safeguarding tool spanning all potential enterprise leak sources (computers, cellular phones, PDA devices etc')
- Operates in Windows 2000 and later environments for desktops/laptops, Symbian/Microsoft for cellular phones, Palm or other for PDAs, and NOVELL/ WINDOWS NT for the Network servers
- Very easy remote and "silent" installation using SMS tool or equivalent. Installation files (management software and clients) are of minimal size
- Monitors and blocks unauthorized external devices
- Neutralizes permanent/internal devices (such as CDs, floppy drives, com, etc.)
- Sends a violation message to the network administrator (including mail)
- Operates on stand-alone PC/Laptop computers disconnected from the network
- Manages user authorization using Active Directory or similar program
- Policy Control for specific devices – "White list"
- Changes of authorization or set-up of new users is done in real time
- All events are logged locally and at the managing software computer
- Immune to tampering and circumvention attempts