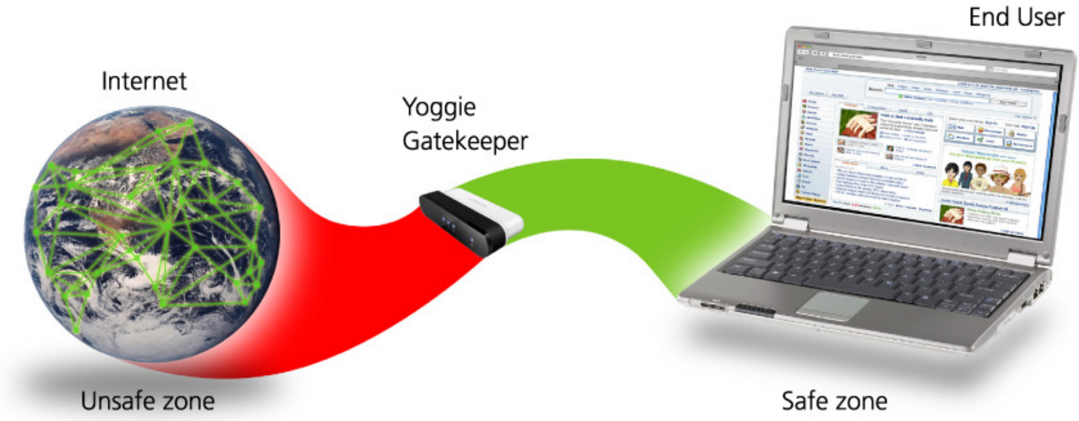
Executive Summary

YOGGIE™

Yoggie™ Security Systems

Executive Overview

September 2006



Yoggie. The Power To Be Free.

Our Mission

Provide traveling, remote and mobile laptop users with corporate-level security

The Challenge

When connecting to the Internet from within the corporate network, laptop users are protected by two lines of defense:

- The first line of defense is based on a comprehensive set of IT security appliances running secured and hardened Operating Systems, and security software including firewalls, Intrusion Prevention/Detection System, antivirus, antispyware, antispam, and content filtering, all of which are completely controlled by the respective corporate IT organization.
- The second line of defense is the personal firewall and antivirus software installed on the user's laptop and controlled by the user.

When these users connect their laptops to the Internet on the go (in hotel rooms, airport lounges, or wireless hot spots) they find themselves outside their corporate network connecting their laptops into the same physical infrastructure as other unknown connected users. As a result, they are left with only one line of defense – the laptop's firewall and antivirus software.

Instead of enjoying the advantages of a first line of defense (an integrated hardware and software solution offering robust security), remote users have to rely on the security offered by a software-only solution running on Windows. This significantly increases the exposure to risks due to the following reasons:

- **Operating System Inherent Vulnerabilities -** By definition, security software running on Windows is subject to inherent Windows vulnerabilities, effectively exposing personal firewall and antivirus applications to malicious content attacks.
- **Unknown Threats** – The security software can only defend against known threats. By the time these threats are added to the knowledge base, it may be too late
- **Immediate Damage -** Malicious content executes directly on the platform to be protected, rather than on a security appliance designed to filter the content and serve as a buffer.
- **Managing Security Level** – Making sure all the computers have installed the latest security updates and enforcing a unified security policy can be very difficult. When the computers themselves are at the frontline, these security weaknesses can be disastrous to the entire network. In other words, its "all or nothing", either the entire network is secured or nothing is secured.

These inherent weaknesses threaten the individual laptop and increases danger of infecting the enterprise's network when the laptops return to the corporate network. Consequently, many organizations adopt tough security policies prohibiting most wireless networking options (significantly limiting user productivity and remote computing freedom), or imposing strict, costly and difficult to enforce cleansing procedures for laptops that return from the “field”.

Enterprises face the challenge of solving the conflict between the mobility of the workforce and the inherent security risks by implementing a layered IT security solution based on two lines of defense.

To provide corporate-grade security IT security solutions must support:

- A layered security architecture with increased capacity for processing threats
- At least two complementary lines of defense
- A physical separation between the two lines of defense to establish a de facto "demilitarized zone"

The Yoggie Solution

The Yoggie Gatekeeper is an integrated hardware and software solution, which is in fact a miniature and mobile version of the IT security devices implemented as the enterprise's first line of defense.

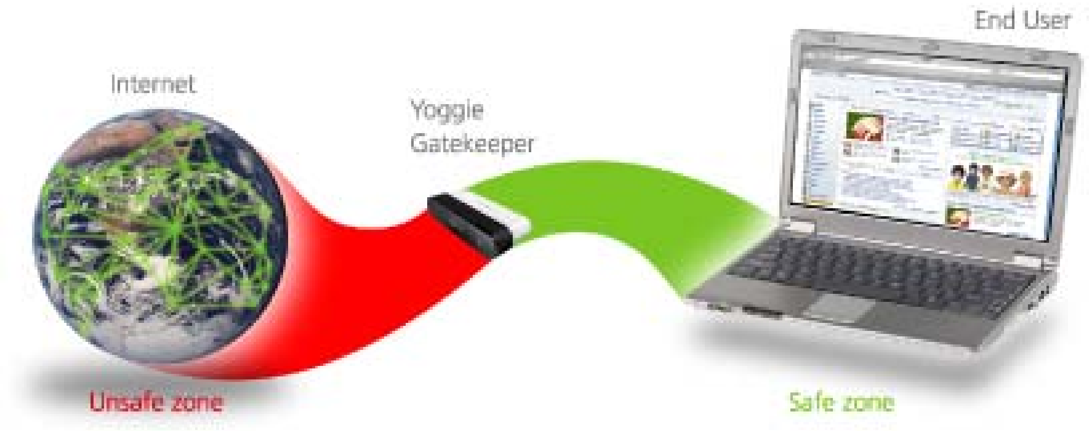
The Yoggie Gatekeeper connects to the laptop's USB port or optional RJ-45 connection to effectively:

- Isolate the physical layer, concealing the laptop’s network connection and IP address
- Clean traffic of any virus, Trojans, spyware, worms and other Internet attacks before they penetrate the laptop

Yoggie Gatekeeper allocates a dedicated IP address to the laptop while obtaining a dynamic IP address from the router, concealing the “real” IP address identity from the outside world. These and other features make the Yoggie Gatekeeper easy to use and transparent to the user.

The device is fully managed by the Yoggie Management Server, installed at the enterprise’s IT communication room or cabinet, allowing central IT control and policy enforcement over roaming laptops. At the same time, end users benefit from a transparent ‘connect and forget’ solution, which provides them with corporate-level security while allowing maximum productivity from their laptops.

Yoggie Gatekeeper is the first solution on the market that settles the ownership conflict between the IT managers and their end-users, providing a specific solution for each party: retained control, enforcement, and corporate-level security for the IT organization; and the freedom to pursue the most versatile and productive forms of remote and mobile networking for users.



Technology

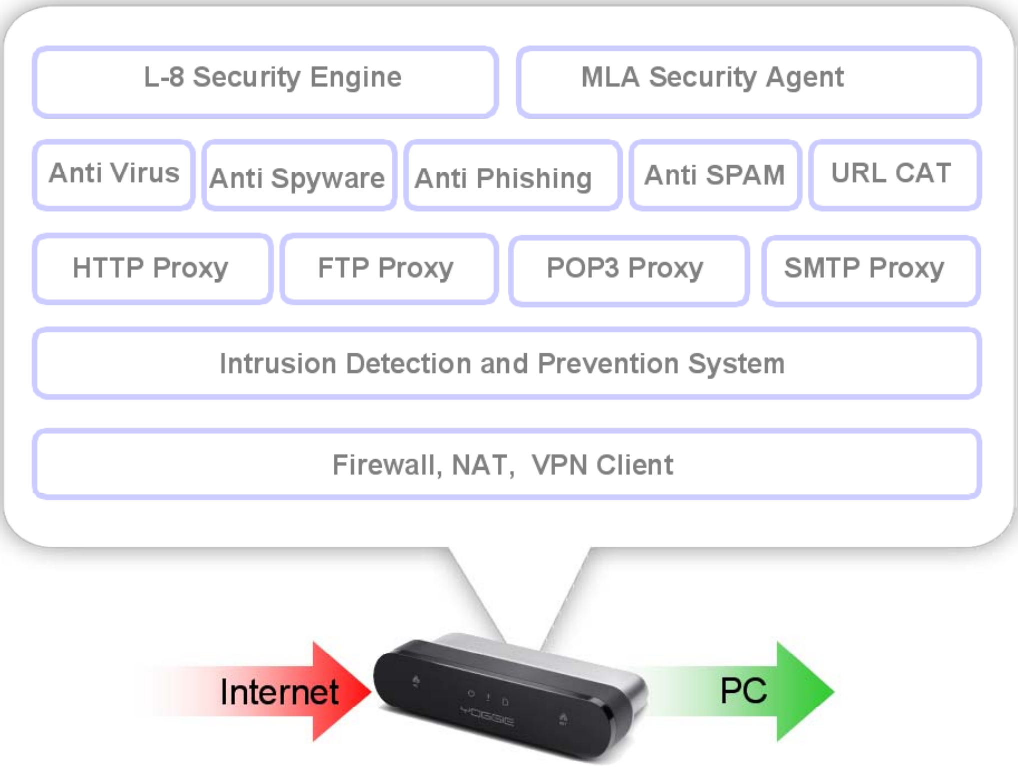
The Yoggie Gatekeeper is a multi-patented solution consisting of a powerful, miniature, embedded Linux-based computer and a robust set of security applications. It includes the following components:

- Intel PXA 270 416-624 MHz processor
- 64 MB/128 MB SDRAM
- 64 MB/128 MB Flash
- 4 MB secured Flash
- 2 x 10/100 Mbps network interfaces
- USB on the go
- SD memory slot
- Power management

Security Applications

All-In-One Security Solution:

- **Multi-Layer Security Agent™**
- **Layer-8 Security Engine ™**
- **URL Categorization & Filtering**
- **Anti Spam**
- **Anti Phishing**
- **Antispyware**
- **Antivirus**
- **Transparent Email Proxies (POP3; SMTP)**
- **Transparent Web Proxies (HTTP; FTP)**
- **Intrusion Detection System / Intrusion Prevention System**
- **VPN Client**
- **Stateful Inspection Firewall**



Yoggie Management Server

The Yoggie Management Server is a Pentium IV-based appliance installed in the IT communication room or cabinet. It manages the fleet of traveling Yoggie Gatekeeper devices, providing security policy updates, signatures, and rule-base updates, while obtaining local logs and events from every Yoggie Gatekeeper. This allows IT personnel to manage the security policies of all traveling, remote and mobile users from a web-based management console. At the same time, they can consistently enforce corporate-level security throughout the organization's network at all times.

About the Founder

Shlomo Touboul is a serial entrepreneur with a strong track record in the technology sector. He started his career by founding Shany Computers, where he was the inventor and patent holder of "Remote End User Application Management". During his time as the head of the Intel Network Management's Business Unit, he was responsible for $135M in revenues and 300 employees. In 1996, he founded and served as CEO of Finjan Software. At Finjan, he invented Behavior Blocking technologies to combat new and unknown Viruses, Spyware, Malware etc, with 5 issued patents since 1996. From 1999 – 2001, he founded and served as CEO of Runway, an internet startup incubator and Runway Telecom Venture Partner, a seed stage VC (joint venture with Alcatel). He was then called upon by the Finjan's Board of Directors to turn around Finjan Software: from near bankruptcy (2001) to a world-wide leader in the behavior blocking security appliance market, acquired strategic investments from Cisco, Microsoft and a unique patent licensing contract with Microsoft. In October, 2005, he founded and is the CEO of Yoggie Security Systems – the home of Yoggie.