

# Symantec Gateway Security

---

**Vikas Gupta**

**CISSP**

vgupta@hi-link.com

04-28-2005



# Agenda

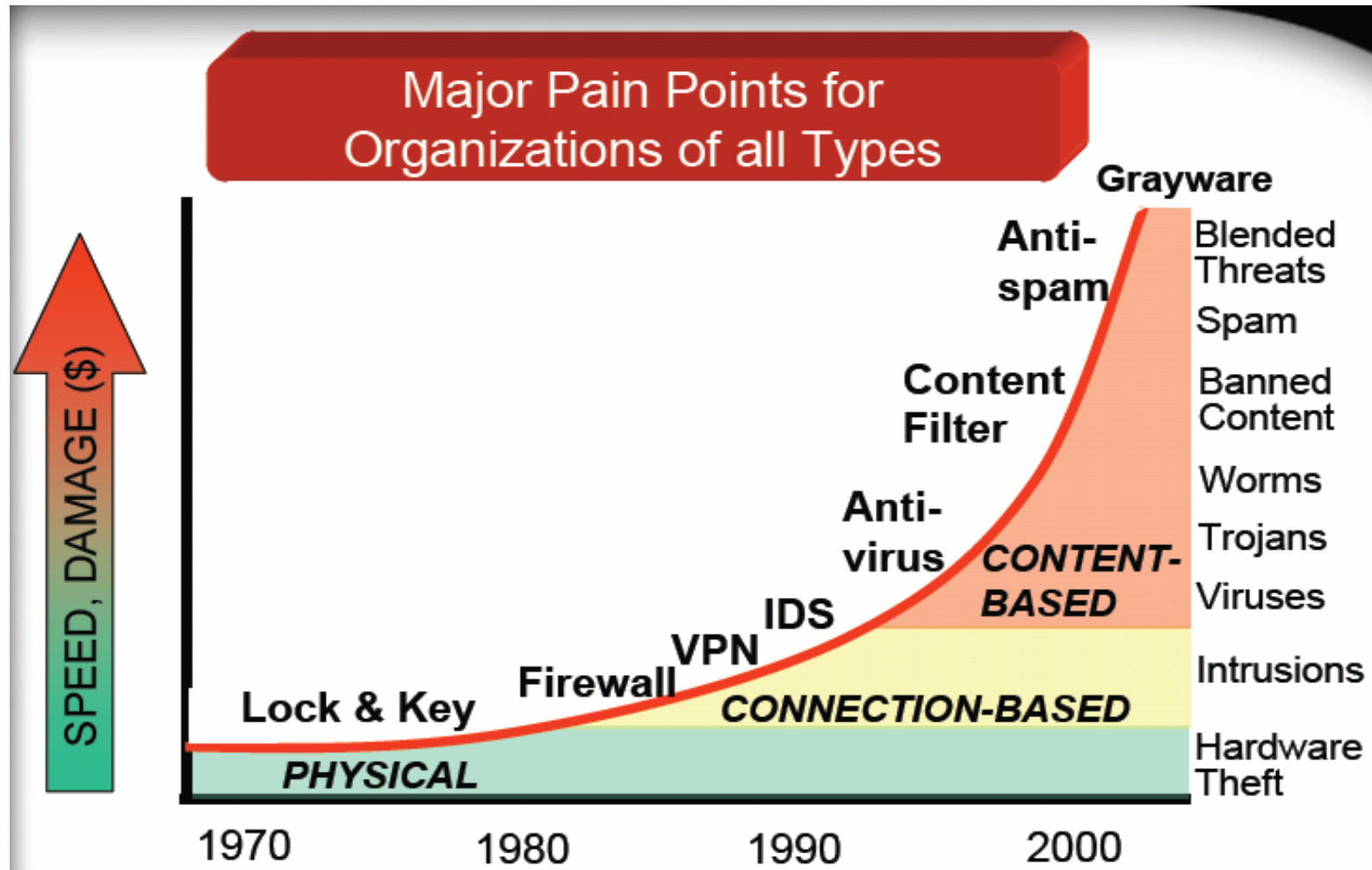
---

- ❖ Threat Ecosystem
- ❖ Unified Threat Management
- ❖ Where SGS 5400 fits in your environment

# Current Security Trends

- ❖ Number of threats are increasing year over year - over 2600 new vulnerabilities documented in 2003
- ❖ Many new vulnerabilities are easy to exploit with code being made public for scripting
- ❖ Time of infection is now very fast requiring IT to react much faster
- ❖ Malicious Code which exposes confidential data has increased significantly
  - Blended attacks against Microsoft has increased
  - Microsoft attacks are getting smarter (IIS, IE, SQL, Outlook, Exchange etc.)
  - Linux is also becoming a platform target
  - Instant messaging and peer-to-peer code is rising
- ❖ The motive and intent is changing – moving from notoriety to financial gain with theft of financial and personal information

# How Threats Have Evolved

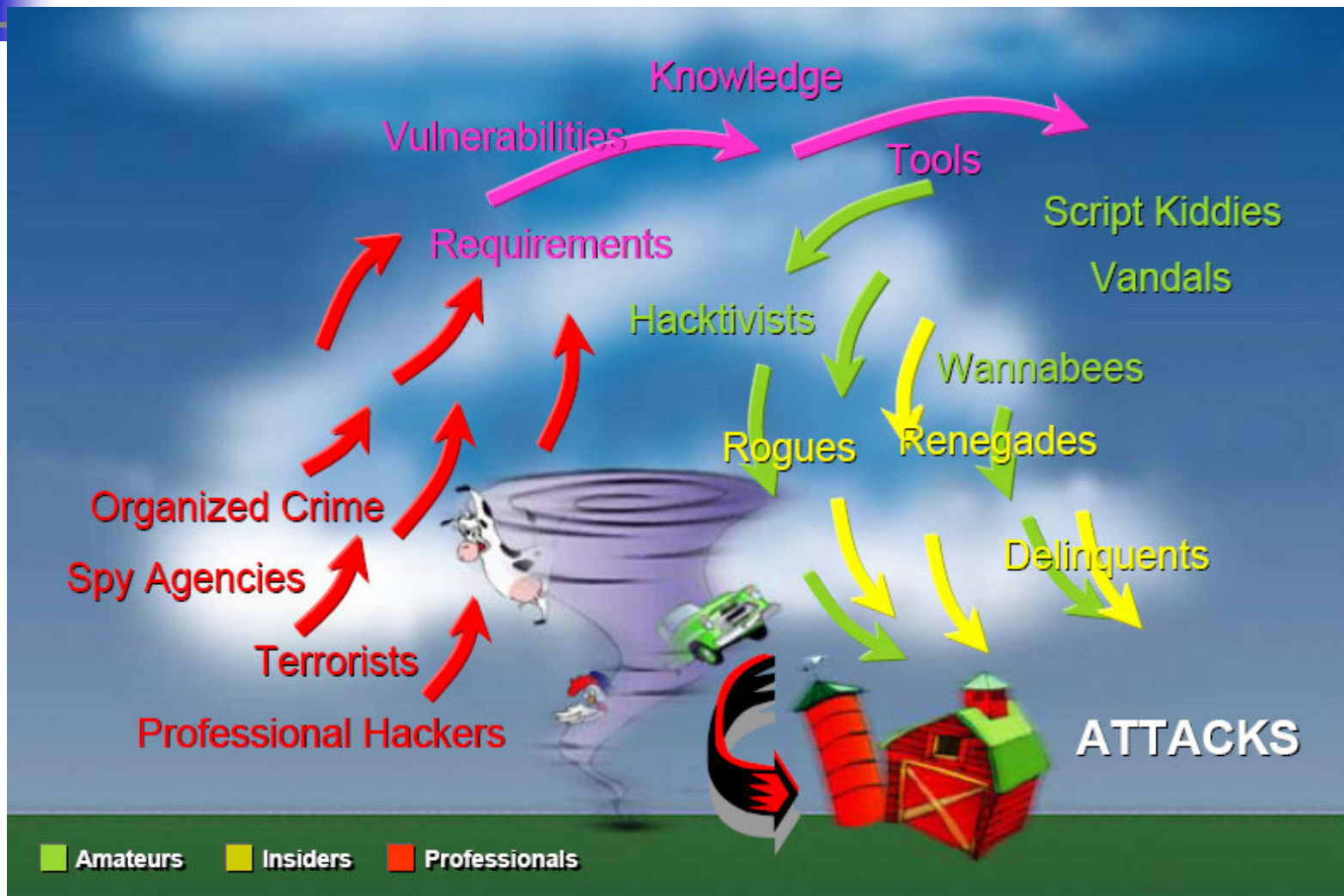


# Tactical Threat Components

---

- Malware (Virus, Worms & Trojans)
- Zombies
- Blended Threats
- SPAM
- Configuration Errors
- Application Vulnerabilities
- Automated Hacker tools and scripts
- Denial of Service
- Buffer overflows

# Threat Ecosystem



# Threats: Summary

---

- Worldwide problem
- Everyone connected to the Internet is a target
- Automated tools, blended threats, and worms increase exposure.
- Both external and internal attackers cause damage
- Customers may never know identity, intent, or execution of attacks

# Security Solutions

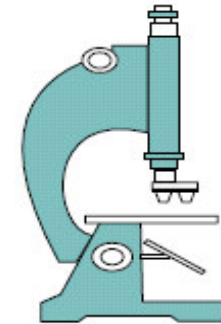
## Layered Security Infrastructure Tools



**Firewalls**



**Secure Content Management**



**VPN & Data Encryption**

**Authentication & Authorization**



**Intrusion Detection & Prevention**

# Security Appliances

- Firewall/VPN is the heart of security appliances
- Appliances now platform for almost all security applications
- Flexibility allows the customer to make the decision

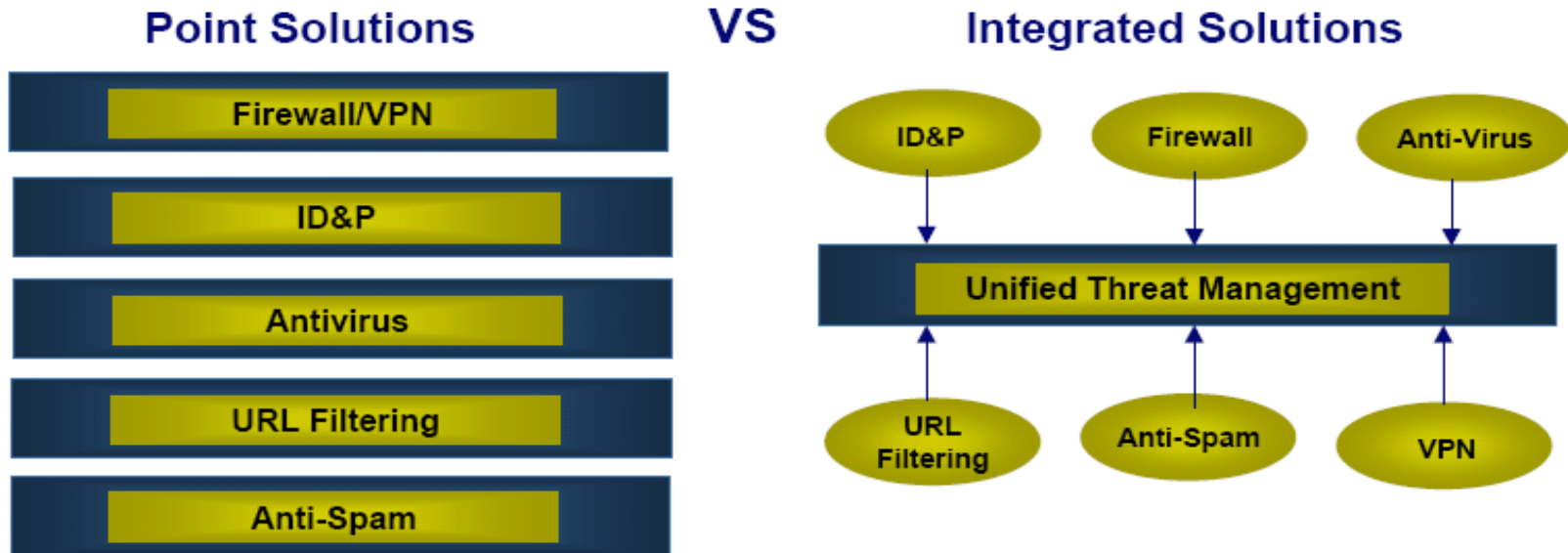
**By 2008, 80% of all security products will be delivered via an appliance!**

# Appliances Benefits

---

- Plug, Play and Forget
- Optimized Hardware – Performance
- Less operator interaction
- Troubleshooting Ease
- Reduced Cost and Complexity
- Simplified Management

# Security Appliances – Single-function VS Multi-function



# Unified Threat Management (UTM) Appliances

Qualification for UTM:

- ❖ **Network Firewall and VPN**
- ❖ **Network Intrusion Detection and Prevention**
- ❖ **Gateway Anti-virus**

All of the capabilities in the appliance need not be utilized, but the functions must exist inherently in the appliance.

Optional capabilities include URL filtering, traffic shaping, routing, anti-spam, and others.

# Unified Threat Management (UTM) Appliance Benefits

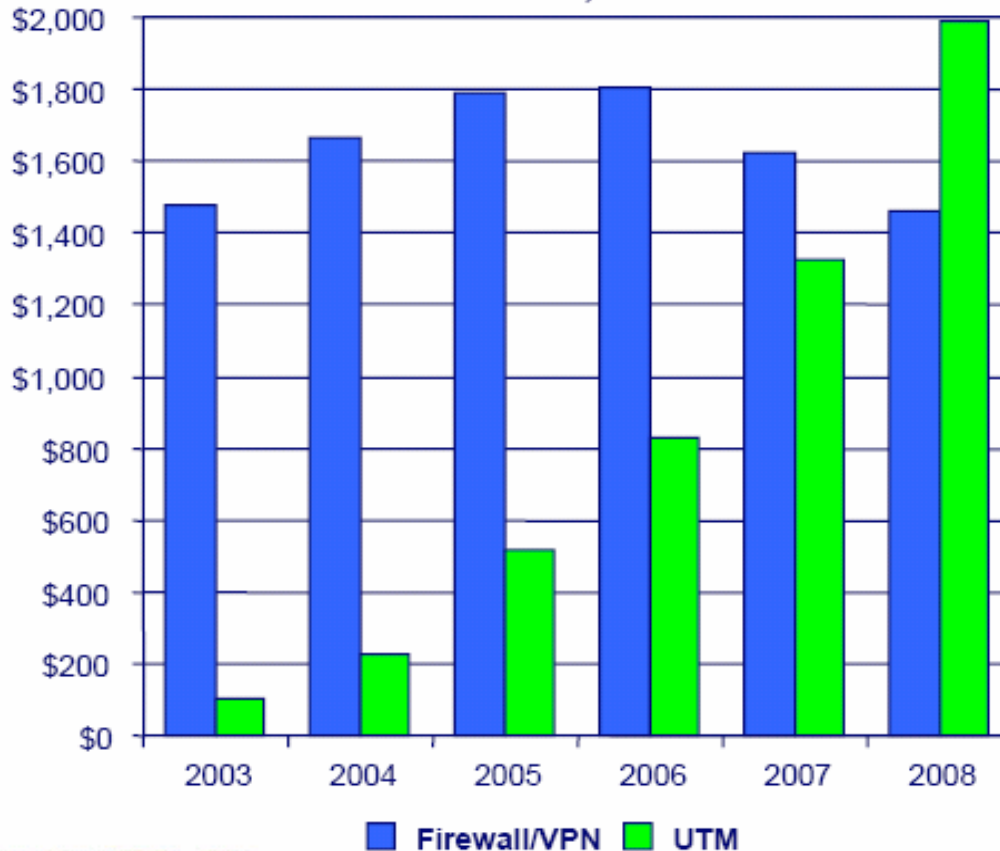
- Reduced Complexity
  - Integration
  - Vendor and Product Selection
  - Support and Management
- Combined Protection
- Flexibility
- Scalability
- Further Reduced Costs

**Customers have multiple options with UTM**



# The Future of the Worldwide Security Appliance Market

Worldwide Firewall/VPN & UTM Appliance Market Forecasts, 2003-2008



## The Worldwide UTM Appliance Market:

- Will increase at a 80.1% CAGR between 2003-2008
- Will reach \$1.99 billion in 2008
- Will exceed the firewall/VPN appliance market by 2008

**CAGR – Compound Annual Growth Rate**

# Where Symantec Gateway Security fits

---

- ❖ Protects networks at the connection to the internet or different subnets
- ❖ Meets the performance requirements of any size organization
- ❖ Simplifies the task of managing network security
- ❖ Combines full inspection firewall with intrusion prevention and detection, virus protection, URL-based content filtering, anti-spam, VPN

# Q&A

