



# Security on Demand

Solution with a Difference

# Threats: Types, Intent, Probability and Damage

Threats to the network resource could take various forms, viz.:

- Network Intrusion
- Denial of Service
- Need for URL/Content Filtering
- Adware and Spyware
- Key Loggers
- Rootkit
- DNS Poisoning
- Spam

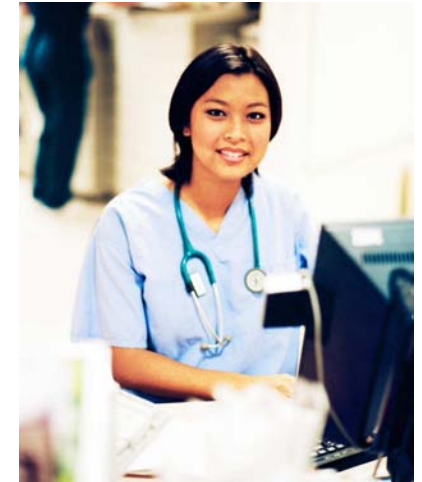
# Key issues : Healthcare

Healthcare organizations continually look to technology solutions to increase mobility and enhance productivity.

Key issues include :

- Ensuring the security of patient and financial information.
- Entry of viruses and worms into the networks through email
- Employee Internet Misuse – Access sites that may contain spyware/ adware, malicious code, all of which can compromise the integrity of systems and data.
- Illegal Access (Internal) - employees who may indulge in sharing unauthorized information on records of a famous patients, new drug, details of a patent pending technique etc.

Health Insurance Portability and Accountability Act (HIPAA) requires that all healthcare organizations protect sensitive client data, much of which can be illegally transferred by a simple keystroke.



# Solution for Healthcare

- The most suites solution would be easy-to-manage, flexible, and cost-effective security appliances to help healthcare ensure the security and reliability also ensures :
  - Firewall, Anti-virus and Intrusion prevention - deep packet inspection shields networks from outsiders such as hackers, trojans and worms.
  - Surf Protection – Content Filtering lets retailers provide employees with Internet access while blocking inappropriate or objectionable sites
  - Flexible policy setting control based on user, group network - Surgeons, Support staff, grade levels etc.
  - Spyware Protection - detects spyware and quarantine the infected files for immediate protection by blocking web pages and software downloads from websites.
  - Easy to Use / Minimum installation and management
  - Minimal administrative overhead – No IT specialist required

# Key issues : Education

**Internet has open new worlds to students of today to information; unfortunately, it has also made it easy to access inappropriate content and to utilize school/colleges networks for non educational pursuits.**

Key issues include :

- Access to inappropriate content by students
- Illegal Access or Intrusions into academic records and results
- Entry of viruses and worms into school/college networks
- Utilization of school/campus networks for illegal content download and sharing



CIPA requires educational institutions to operate "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors,"

*CIPA stand for Children's Internet Protection Act*

# Solution for Education

- The most suited solution would be a cost effective and comprehensive integrated appliance that provides critical security application in one platform and also ensures :
  - Easy to Use / Minimum installation and management
  - Conserve expensive bandwidth - Blocking of inappropriate content and peer-to-peer file sharing, instant messaging, to free up valuable bandwidth.
  - Flexible policy setting control based on user, group network - Faculty, student grade levels etc.
  - Scalability for easily accommodating more users.
  - Easy to budget (Predictable cost structure making it easy to budget)
  - Minimal administrative overhead – No IT specialist required

# Key issues : Retail & Hospitality

With the burgeoning e-commerce market, retailers have to ensure that their Internet infrastructure is secure and fool-proof.

Key issues include :

- Securing Front & Back office applications
  - Credit card processing (Internet based)
  - Corporate access to traveling employees
  - Customer/ Partner Loyalty Programs
- Protection from hacker attacks & Securing against valuable business and customer data against fraud
- Securing daily communication over the Net



# Solution for Retail & Hospitality

- The most suites solution would be easy-to-manage, flexible, and cost-effective security appliances to help retail organizations ensure the security and reliability also ensures :
  - Firewall, Anti-virus and Intrusion prevention - deep packet inspection shields networks from outsiders such as hackers, trojans and worms.
  - Virtual Private Networking (VPN) - provides secure communications over the Net to protect sensitive information transmitted across networks.
  - Surf Protection – Content Filtering lets retailers provide employees with Internet access while blocking inappropriate or objectionable sites. Also maximize employee productivity .
  - Easy to budget (Predictable cost structure making it easy to budget)
  - Scalability for easily accommodating more users.
  - Continuous security updates, Upgrades and Patches

# Key issues : Financial Institutions



**With the disturbing trends of phishing and online financial frauds, it is evident that financial services industry has become the most frequently targeted industry.**

Key Issues :

- Network Intrusion (External) : Without the access privileges, attempts to penetrate your network resources with malicious intent.
- Illegal Access (Internal) - employees who may indulge in sharing unauthorized information on passwords, credit card details etc.
- DNS Poisoning: The domain name server is duped so that it starts redirecting the traffic to another predetermined malafide destination.
- Phishing Scams: Phishers attempt to fraudulently acquire sensitive information, by masquerading as a trustworthy person/ business.
- Employee Internet Misuse – Access sites that may contain spyware/ adware, malicious code, all of which can compromise the integrity of systems and data.

# Solution for Financial Institutions



- The most suites solution would be easy-to-manage, flexible, and cost-effective security appliances to help financial organizations ensure the security and reliability also ensures :
  - Firewall, Anti-virus and Intrusion prevention - deep packet inspection shields networks from outsiders such as hackers, trojans and worms.
  - Spam Protection - scans inbound email messages, whose score exceeds thresholds set by the administrator are dropped, returned to the sender, passed to the recipient with a warning, or quarantined.
  - Surf Protection – Blocking inappropriate or objectionable sites. Make employees efficient and productive
  - Spyware Protection - detects spyware, quarantine the infected files by blocking web pages and software downloads from websites.
  - Flexible policy setting control based on user, group network - Surgeons, Support staff, grade levels etc.
  - Scalability for easily accommodating more users.
  - Continuous security updates, Upgrades and Patches

# About Syntensia



- Syntensia AB, a European company headquartered in Stockholm, Sweden is a pioneer in Security on-demand solution sold on subscription basis.
- The name Syntensia:
  - Tensia- Latin way of writing Tension
  - Syn- Sin, which is without in Spanish
  - **Syntensia - Without Tension**
- Syntensia's White Knight appliance is the most cost- effective, comprehensive and efficient network security solution that protects organizations from common security threats from Internet
- White Knight is a hardware based appliance that integrates the seven crucial security check points - Firewall, VPN, Intrusion Protection, Anti-Virus, Spam Elimination, Surf Protection and Spyware Guarding in one management platform.

# White Knight Appliance



- Plug and Play Appliance
- Single Appliance for all Network Security
- Web Management for all features
- Easy to Install and Configure
- No need of specialist staff
- No additional need for security appliances



# White Knight Security Features



Firewall	<ul style="list-style-type: none"> <li>Stateful Inspection Firewall</li> <li>Secure embedded Operating System</li> <li>Integrated Purpose built Firewall and VPN</li> <li>DOS and DDOS Protection</li> <li>Transparent Firewall</li> <li>Support Dynamic and Static NAT</li> </ul>
VPN	<ul style="list-style-type: none"> <li>IPSec</li> <li>PPTP</li> <li>Integrated VPN site to site and client to site</li> </ul>
AV/IDP	<ul style="list-style-type: none"> <li>Embedded Antivirus Protection for Gateway</li> <li>Virus, Worm, Trojan, Backdoor, Buffer Overflow, and port scan protection</li> <li>P2P, IM, Web attack protection</li> <li>Automatic scheduling signatures update</li> </ul>
Anti Spam	<ul style="list-style-type: none"> <li>Spam, phishing prevention</li> <li>Configurable white and black lists</li> <li>SMTP, POP3 support</li> <li>External Spam database</li> </ul>
Content Filtering	<ul style="list-style-type: none"> <li>Web based blocking by URL keyword</li> <li>External database content filtering</li> <li>Java/ActiveX/cookie/News blocking</li> </ul>
Additional features and functionalities	<ul style="list-style-type: none"> <li>System Admin</li> <li>Centralized Web based administration on https</li> <li>Remote Management via Telnet or Web</li> <li>Monitoring</li> <li>Centralized logs</li> <li>Attack alert</li> <li>System Status Monitoring</li> <li>Syslog</li> </ul>

Security Features	<ul style="list-style-type: none"> <li>IKE keepalive is supported that allows the devices to detect a dead remote peer for IPSEC redundancy</li> <li>The software on the firewall supports online software reconfiguration to ensure that changes made to a firewall configuration take place with immediate effect</li> <li>Intelligent environmental design to ensure low failure rates due to environmental conditions</li> <li>Link and activity indicators</li> <li>Stateful Firewall</li> <li>Intrusion Prevention</li> <li>Spam Prevention</li> <li>URLFiltering</li> </ul>
Supports Following Software Features	<ul style="list-style-type: none"> <li>DHCP server</li> <li>Static and Dynamic Network Address Translation</li> </ul>
Management	<ul style="list-style-type: none"> <li>Real-time alerting and notification features and syslog support</li> </ul>
Firewalling Features	<ul style="list-style-type: none"> <li>Supports Application/Protocol Inspection Engines</li> <li>Supports Multizone Access controls like DMZs</li> </ul>

# Security on Demand Advantages




- Uniquely delivers tested and quality-controlled features
- Updates, and upgrades in real-time.
- Rapid innovation and trusted delivery
- Unequaled value our customers have come to expect.
- Has pioneered this model to give you low-cost, high-value technology as it's developed

# Which companies could use the Syntensia ?

- Everyone having IT systems.
  - Healthcare
  - Retail and Hospitality
  - Financial Institutions
  - Manufacturing
  - Traditional Industry
  - Academia and more...



# Syntensia's White Knight is

- 
- An all-in-one Security Solution
  - Plug and Play
  - Proven, reliable solution at affordable cost
  - Easy to budget (only OPEX)
  - An **Always** Updated Solution
  - Offers easy access and management
  - No need to hire specialist staff
  - Freedom to re-evaluate the solution (Pay as you go)
  - Offers 24 X 7 Support



Thank You