

CavVelocitySM
SecureIP

CavalierTM
TELEPHONE &
TV


perimeter
eSecurityTM
Complete. On Demand. Affordable.

CavVelocity

SecureIP Security Services

April 2007



- 1 Perimeter Overview
- 2 The Problem
- 3 The SecureIP Solution
- 4 Features and Services
- 5 Question to ask and common objections



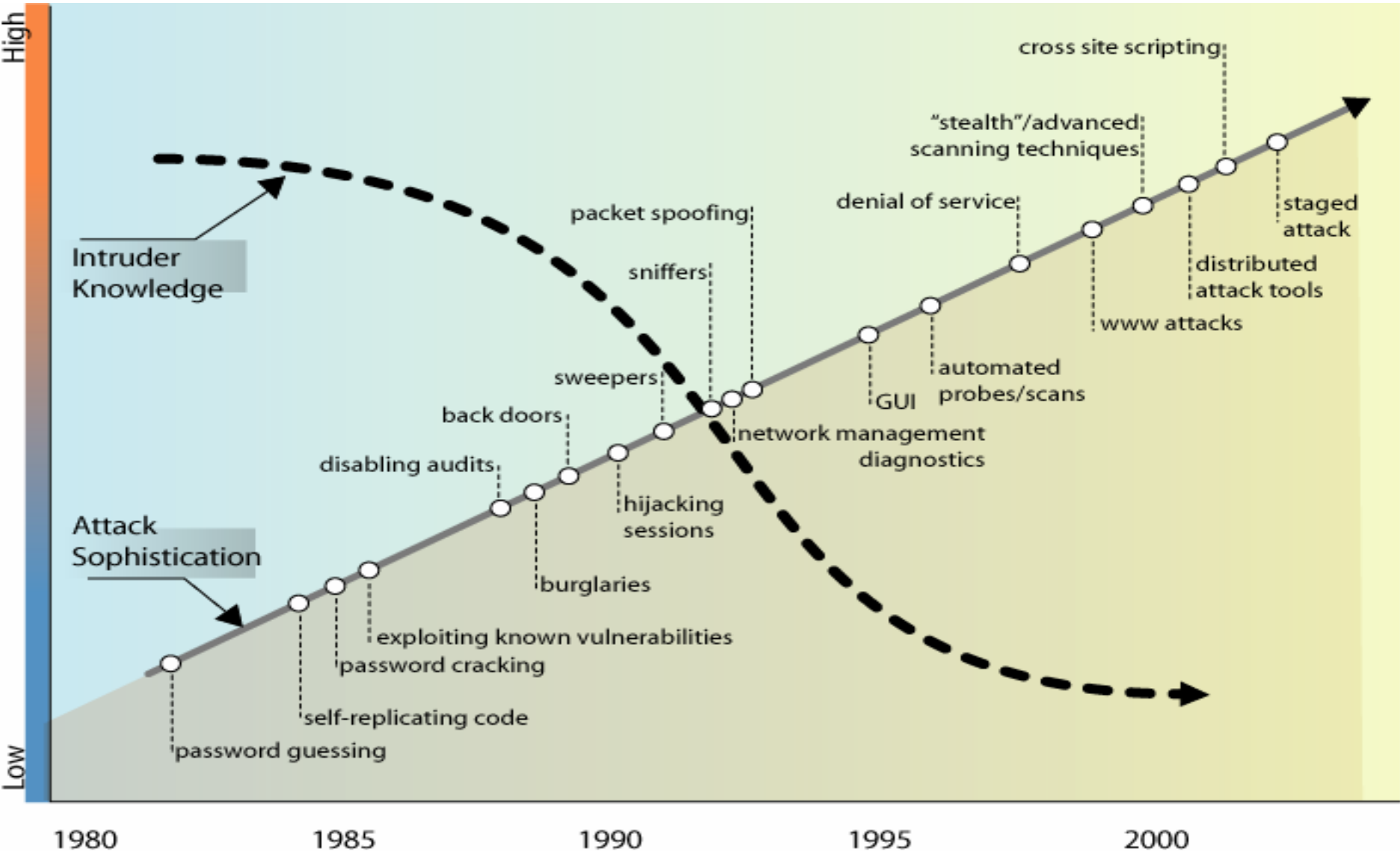
- **History:** Formed in 1999. Early focus on US Financial Industry
- **Market Leader:** Over 4,000 Clients (1,800+ Financial Institutions)
- **Nationwide Presence:** Staff of 170+ includes 100 in customer support/service, located in 7 Operation Centers and 3 Data Centers nationwide
- **Vendor Diligence:** 4 Years of Federal Financial Institutions Examination Council (FFIEC) Oversight/Audit; SAS 70 Type II Certification; Cybertrust TruSecure Certified Service Provider; Cisco Certified MSSP



Perimeter Command Center



Trends in Hacker Techniques



Now Days Anyone Can be a Hacker!

- Employees
- Former Employees/Contractors
- Vendors
- Customers and clients
- Competitors
- Professional Hackers
- Curious Crackers
- Terrorists
- Vandals
- Foreign Governments
- Industrial spies
- Organized crime



1. Internet is becoming increasingly crime ridden

(Source: CSI/FBI)

- Unauthorized access second greatest source of financial loss
 - 56% of companies report unauthorized use of computer systems
 - 48% of companies report they had between 1-5 computer system attacks last year
- Virus attacks continue to be source of greatest financial loss
 - Known computer viruses rose by 30,000 last year
 - Malware costs estimated at \$204 billion in 2005

2. SMB's Cannot Afford to Keep Up...

- Large companies can—so SMBs are target of choice
- Security spending cost per employee for large co. vs. SMB
 - \$126 vs. \$1,349 per employee per year

(Source: CSI/FBI)



Spyware and Trojans Horse Programs

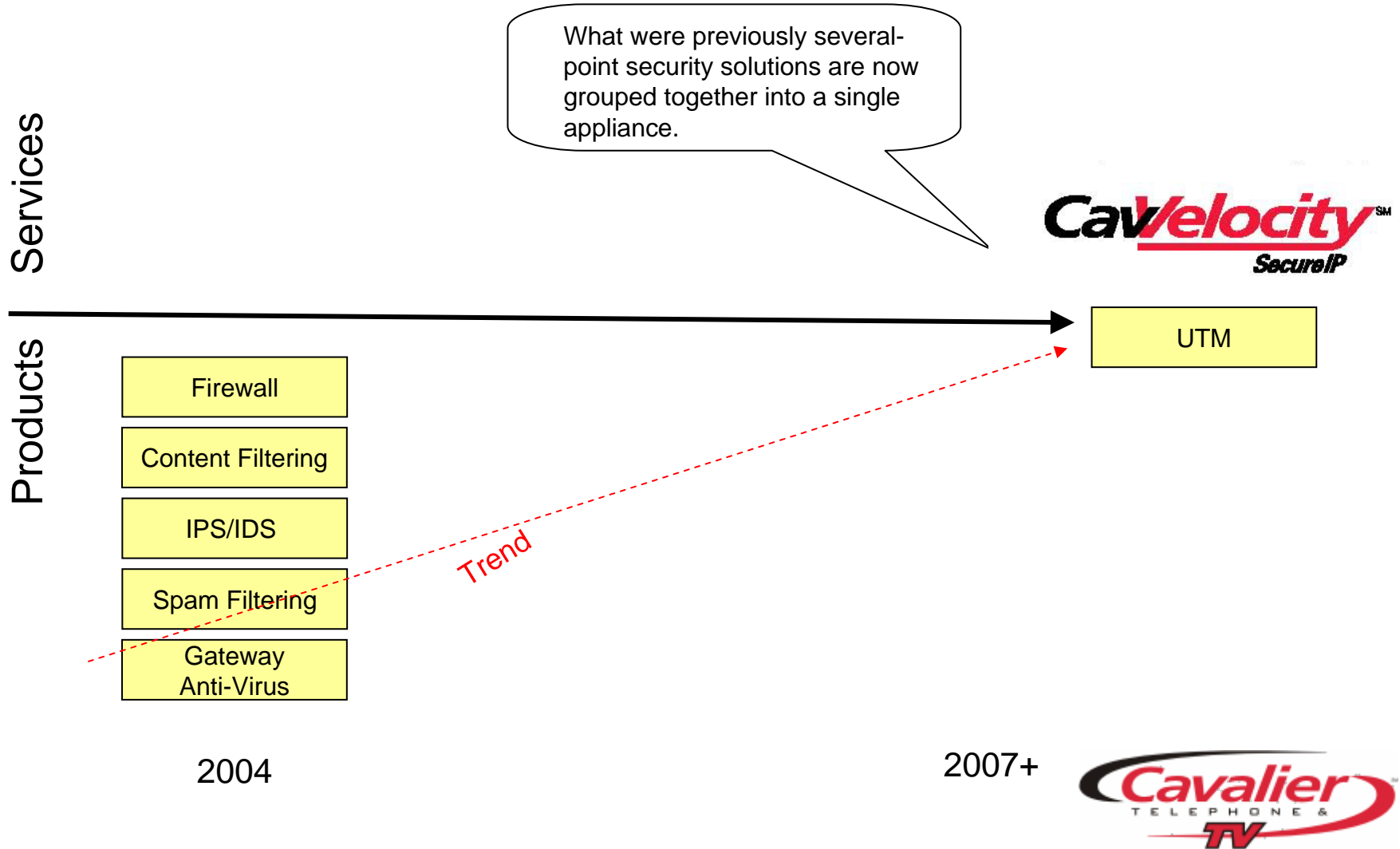


Spyware resides on approx. 90% of computer systems

www.webroot.com/stateofspyware



The UTM Progression



Source: Based on research conducted by Gartner Group.

What Do The Experts Say?

Gartner Quotes:

1. UTM's

“ *When compared with multiple-point solutions, the all-in-one security appliance provides excellent total cost of ownership, rack-space savings, and ease of use with single local interface. SMBs and branch office environments should consider all-in-one appliances rather than buying multiple single-function appliances.* ”

Network Security Platform Evolving Into Single Appliance Solution
by Greg Young, John Pescatore
Gartner Group, August 2005



What Do We Say?

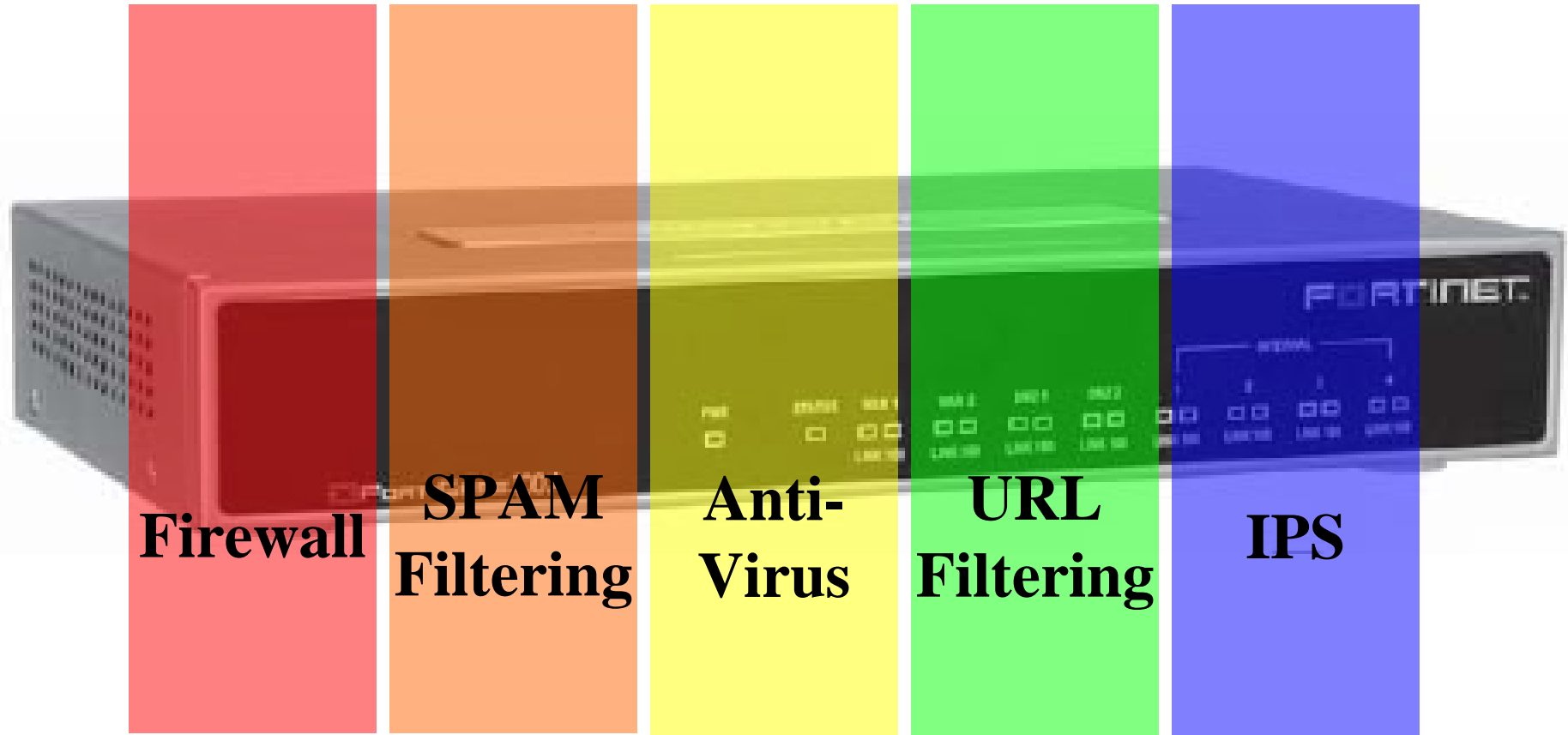


Purchasing security technologies like Intrusion Detection systems, Firewalls and Antivirus solutions and trying to “glue” them together to achieve “security” is tough work!

Perimeter Internetworking: Complete Network Security On Demand, No Assembly Required™



The SecureIP Device



- 1st Layer of Defense
- Port Lock and Unlocking
- Stateful Inspection
- Basic Attack Detection and Protection
- ICSA Certified
- Configuration, Updates, and changes handled by professional Internet security engineers



SPAM Filtering

- SMTP Support
- POP3 Support
- Extremely Low Cost
- High Catch Rate
- Other Solutions Cost
 - Onsite SPAM server - \$1,000 - \$5,000
 - Remote “relay” services - \$5 - \$25/month/user
 - Hardware server required for onsite



SPAM
Filtering

Gateway Anti-Virus



Anti-
Virus

- Why wait for viruses to get inside?
- Stop the Virus or Worm before it hits your network!
- AV Signature file updated hourly for 0-Day protection
- Compare costs to McAfee or other gateway AV server protection
 - Thousands of dollars each year + hardware costs
- ICSA Certified



Web Content Filtering

- Blocks employee access to unauthorized web sites
 - 56-Categories
 - Over 30-Million URLs
 - Best way to reduce spyware!
 - Reduce Liability & Enforce Policy
 - Compare to Websense or SurfControl
 - Normally \$1,500 - \$4,000/year



Web
Filtering



Intrusion Prevention System (IPS)

- Deep Packet Inspection
- Full Management
- 24x7 Monitoring
- Analysis by live security engineers
- Detect and stop hackers!
- Compare to other managed IPS services
 - \$1,000 - \$2,000/month



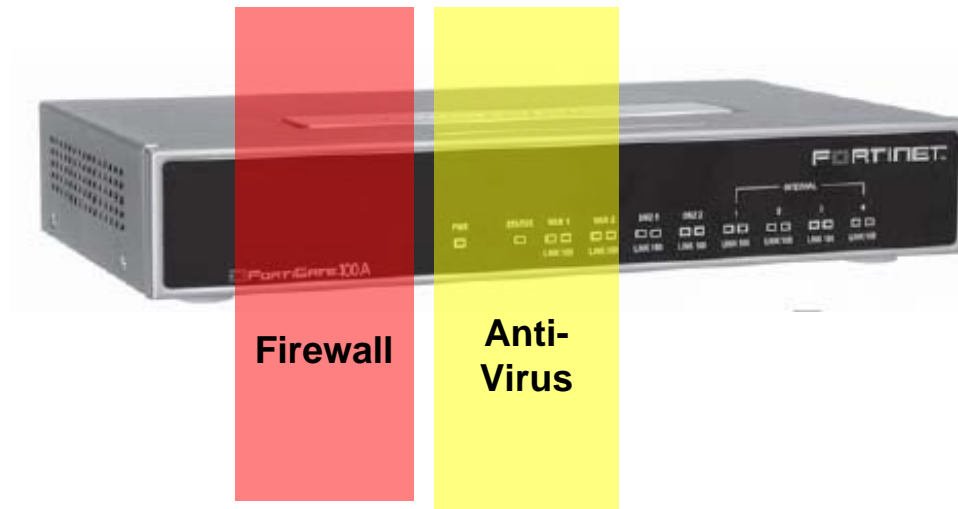
IPS



- **Firewall** An access control device that allows or blocks Internet traffic into the network.
- **Web Content Filtering** Monitors and restricts user access to the Internet.
- **SPAM Filtering** Blocks emails likely to be SPAM.
- **Anti-Virus** Scans for and removes Computer Viruses and Worms.
- **Intrusion Prevention System** Looks inside incoming packets for exploits and Hacker Scripts



Client Can choose to Leverage Some or All of the SecureIP Services...



Once the Firewall is in place the client can add other services as needed.

Security Portal – What does it accomplish?

• FIRST TIME EVER....

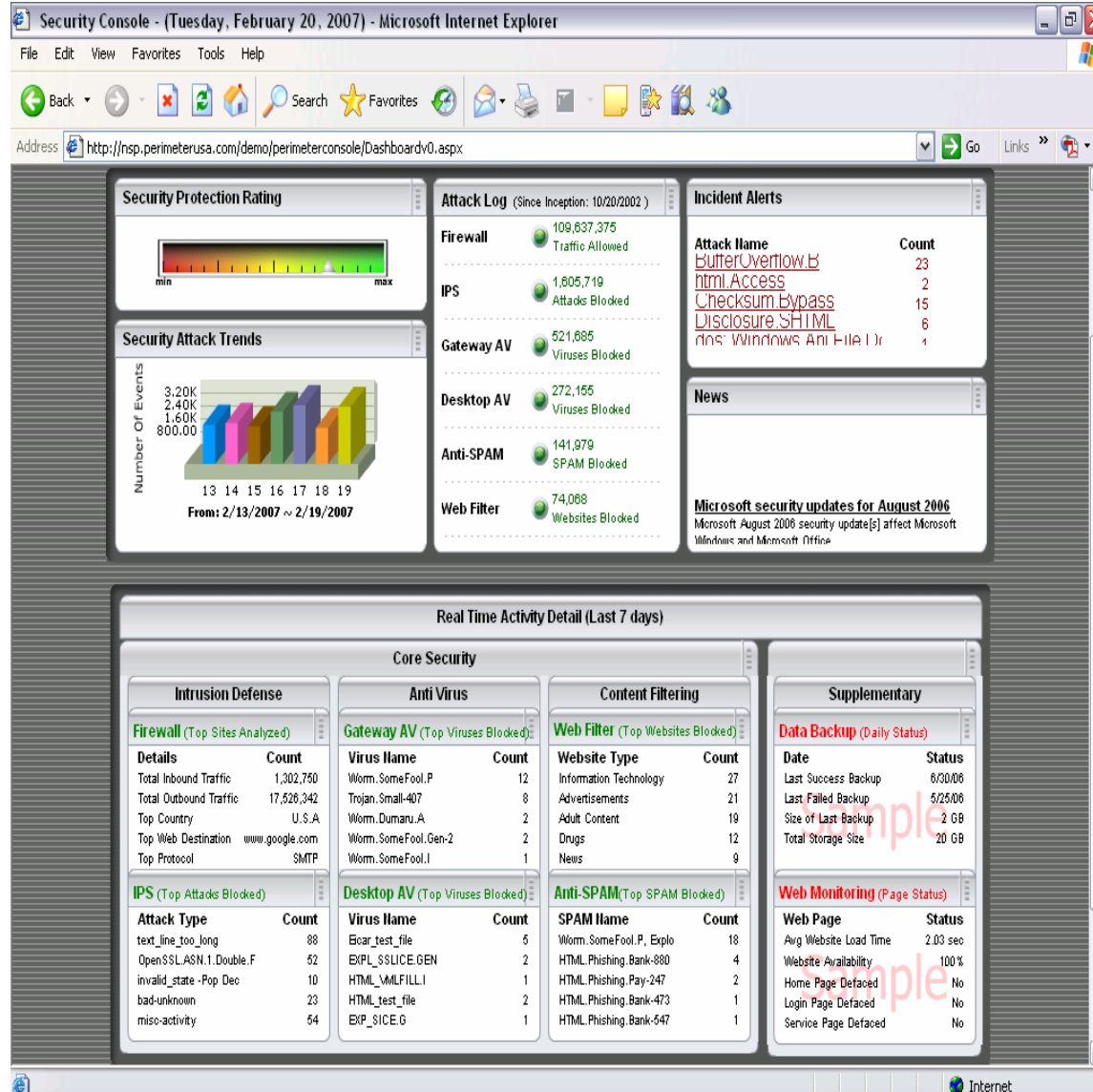
• Puts ALL important security technologies in one view

✓ Contains a “Security Dashboard”

• Provides Context with multiple services viewed

• Encourages Client Interaction

✓ Outcome: Client buys more services



1. **Complete = Technology + Integration + 24/7 Staff**

- Customer no longer has to worry about:
 - Technology Review
 - Technology Purchase
 - Technology Integration
 - Dedicated Security Staff
 - Technology Upgrade Costs

2. **Easy to Deploy/Add New Services**

- For Customers With Basic Firewall, Optional Services Can Be Added Within Days
- Additional New Services Will Be Rolled Out Regularly



1. Differentiation at Point of Sale

- Get More Appointments
- Security is topical and high concept
- Offering a “Secure” Pipe sets you apart from the others

- Better Chance of Closing Deals
 - 50% increase Closing Ratios
 - With OR without security sale
 (“If you offer it, you must be secure....”) The Halo Effect

2. Maximize Revenue Potential and Increase Stickiness



1. Anyone connected to the Internet
2. Anyone doing business on the Internet
3. Key Industries
 - Financial Services (banks, brokers, insurance)
 - Healthcare (hospitals, clinics, doctor practices)
 - Professional organizations (legal, accounting, engineering, architects)
 - Government (local, state, federal)
 - Education (schools, learning centers)



Questions to Ask

- **Firewall** – Do you have a lock on your front door to the Internet?
 - How old is your Firewall?
 - Who is monitoring your security at nights? Or on the Weekends?

- **Web Content Filtering** – Are your employees “surfing” while at work?

- **SPAM** – Have you noticed/been bothered by the recent increase in SPAM?

- **Anti-Virus (AV)** – Are you comfortable with your current level of AV protection?
 - Gateway AV – Why would you wait until viruses get inside your network?
 - System AV – Do you have the most recent virus updates? Do you know?

- **IPS** – What would a Major security breach do to your business?



Common Objections

1. I don't need security.

- More likely to get information stolen or destroyed through your Internet connection than you are through an actual physical break into your building (Do you protect front door?).
- Typical companies have between 1,500 – 3,000 unauthorized access attempts daily.

2. I already have a firewall that was installed last year OR I can easily buy one.

- What about ALL of the other security services?
- Does it alert you if your network is attacked or compromised?
- Are you aware that after 5-10 days most firewalls are useless without constant updates/tuning?

3. I already have an IT staff managing security.

- Are you staffed on a 24/7 basis?
- Are they “dedicated” to security?
- Would these staff members be more productive working on better ways to run the business than trying to manage your growing security concerns?



Common Objections

4. Why should I trust you with my security?

- Our Partner's Security System secures over 4,000 networks.
- Our Partner's Security System now services over 10% of the US Financial Industry and has undergone multiple Federal Agency and third party audits and reviews.

5. We do not have an e-commerce web site or transact any business over the internet.

- Are you connected to the Internet? Then you are still vulnerable.

6. We have desktop AV on all of our PCs and we use AOL for our email.

- Do you know if your desktop AV is up-to-date?
- Do you care if malicious software is being sent all over your network, including to your servers and end users, before it is detected?

7. We are such a small company, nobody would want to attack us.

- Large companies can better keep up with security, so SMBs are best target.
- Hackers typically attack the easiest targets.



Common Objections

8. None of my other peers in business have managed security.

- Current statistic suggest strongly that all SMBs need protection.
- Will your peers accept the liability when something BAD happens to YOUR NETWORK?
- Aren't you concerned about YOUR security and protecting YOUR assets?
- It's just a matter of time....

9. There is just so much out there, why bother?

- Certainly a lot to consider and evaluate; that's why an "on demand" single source provider would be helpful
- Would you not put locks on the doors of your house just because there was too much crime?



QUESTIONS AND ANSWERS

