TippingPoint
a division of 3Com

# Evolution of Security: Network Intrusion Prevention

**Brett Hunter**
**bhunter@tippingpoint.com**

## TippingPoint – The Company

TippingPoint
a division of 3Com

- **The Proven Leader in Intrusion Prevention (Nasdaq: TPTI → COMS)**
  - Launched industry's first intrusion prevention solution, January 2002
  - Only Vendor Awarded NSS Gold for Intrusion Prevention, January 2004
- **Deep Domain Expertise and Experienced Management**
  - Networking, security and software knowledge from industry-leading companies such as Cisco, SANS, NetSpeed, Alcatel, IBM, Efficient & Motive
- **Best-of-breed Technology and Execution**
  - Tens of millions of dollars invested in core technology R&D
  - Solutions are built first for network performance, then security capabilities
  - Highly parallel, custom packet-processing ASIC technology
    - 10,000 Parallel Filters
    - Microsecond Latencies
  - Patent-pending technologies (10) that deliver unmatched performance

2

# Select TippingPoint Customers

TippingPoint
a division of 3Com




# TippingPoint Awards

TippingPoint
a division of 3Com

**SC Global Awards 2005 – Principal Awards**
TippingPoint was named the Best Security Solution in the 2005 SC Global Awards for the best overall solution for dealing with today's threats to information security and the protection of corporate information assets.

**SC Magazine Best Buy**
TippingPoint was selected by SC Magazine as a "Best Buy" in their group test of intrusion prevention products.

**Common Criteria Certification**
TippingPoint is the first Intrusion Prevention System (IPS) to obtain all four government-validated protection profiles: analyzer, sensor, scanner and system.

**Frost and Sullivan 2005 Network Security Infrastructure Protection Entrepreneurial Company of the Year**
TippingPoint was named the 2005 Network Security Infrastructure Protection Entrepreneurial Company of the Year by Frost & Sullivan.

**IDG Network Awards 2004 Winner**
TippingPoint is the winner of the "Network Protection Product of the Year" from IDG and TechWorld.com. The prestigious IDG awards recognize the very best in the industry and reward companies for innovative and effective use of networking technology.

**eWeek Labs Analyst's Choice Award**
TippingPoint's IPS ably handled both real and staged attacks on week Labs' test network, attached to the Internet for nearly a week.

**Information Security Magazine 2004 Product of the Year**
TippingPoint was selected by Information Security Magazine as "2004 Product of the Year" for Intrusion Prevention Systems.

**NSS Gold Award**
TippingPoint's Intrusion Prevention System is the first and only product to win the coveted NSS Gold Award in the IPS space.

**The Tolly Group "Up To Spec"**
Performance and security benchmark. TippingPoint's IPS demonstrated 100% security accuracy at 2 Gbps.

**SC Magazine Best Buy of 2004**
TippingPoint's was selected by SC Magazine as a "Best Buy in 2004" for intrusion prevention

**eWeek Excellence Award**
TippingPoint's Intrusion Prevention Systems received the "Enterprise Resource Protection" eWeek Excellence Award announced in the April 5, 2004 issue of eWeek Magazine.

**CompTIA "Best New Product"**
TippingPoint's Intrusion Prevention Systems were named "Best New Product" in the hardware category at the Executive Breakaway 2003 Conference hosted by CompTIA in Halifax, Canada.

**SANS "Trusted Tool"**
TippingPoint's Intrusion Prevention System has been selected as a "Trusted Tool" by the SANS Institute, the world's premier security research and training organization.

**InfoWorld 100**
University of Dayton, a TippingPoint customer, was recognized as a technological leader and awarded with the 'InfoWorld 100' for its advancements made through implementing TippingPoint's Intrusion Prevention Systems.

**University Business Magazine "Show Stopper" Award**
TippingPoint's Intrusion Prevention Systems were awarded the "Show-Stopper" at the 2003 Educause Conference in Anaheim, California.

## Recognized for Security Excellence

TippingPoint a division of 3Com

SC MAGAZINE GLOBAL AWARDS 2005 WINNER

# Best Security Solution 2005

- TippingPoint IPS Overall Winner in SC Global Awards
- Over 1,000 products nominated
- The world's leading awards program for the information security industry

### Additional Awards


5

## A day in the life of the security admin …

TippingPoint a division of 3Com

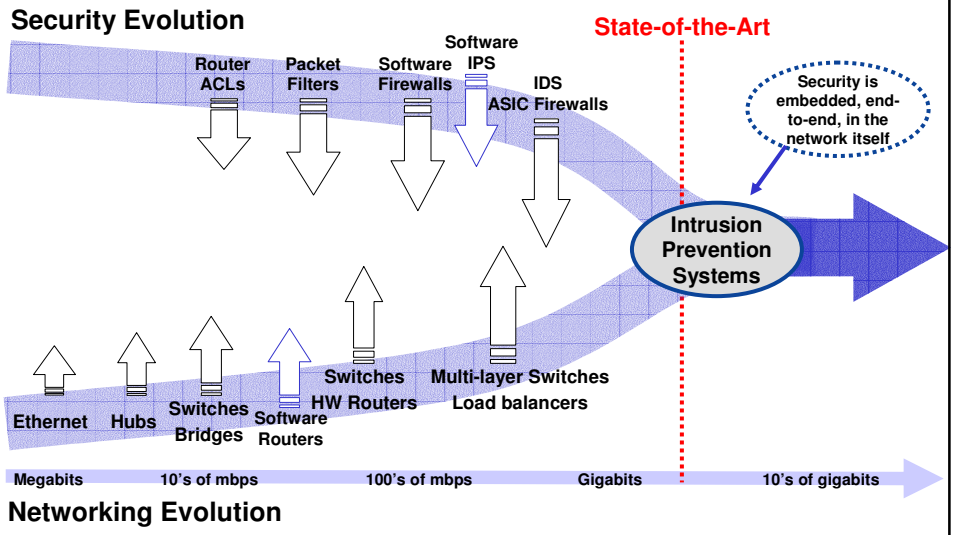
- Continuous hostile scans of your networks.
- Ever-present Internet background noise from older works.
- Attempts, internally as well as externally, to break into your hosts.
- Constant challenge to keep your website from being defaced.
- DDoS network flooding you and using all your bandwidth.
- Some of your internal systems are "owned" and are launching attacks against other companies (liability issues).
- Worms and viruses propagating behind your firewall from walk-ins, emails and file sharing.
- Other worms pummeling your external web servers.
- Spammers trying to use your mail server as a relay.
- Internal users trading sensitive material via P2P.
- Your DNS servers are being targeted and sometimes the root DNS servers are only reachable intermittently.

Show16.exe

6

## Networking and Security Convergence Trends

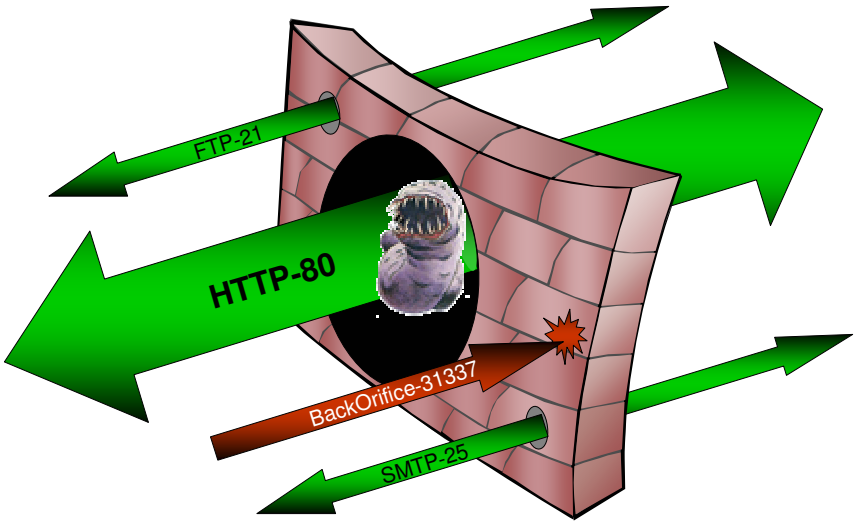
TippingPoint a division of 3Com




7

## Today's Firewall Holes

TippingPoint a division of 3Com

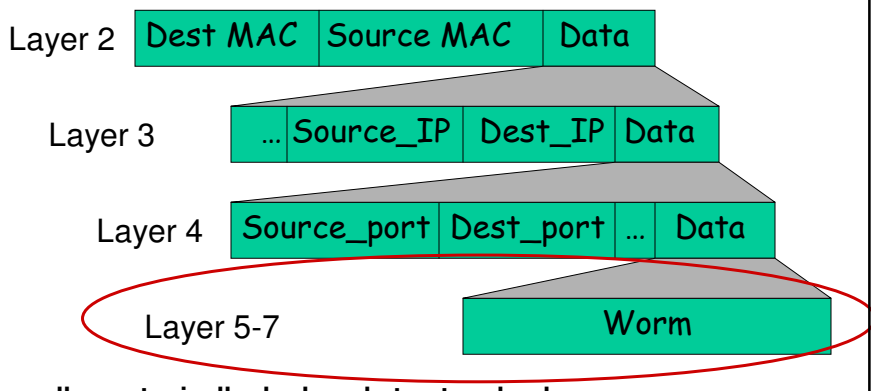



8

## Limitations of the Firewall

TippingPoint a division of 3Com

- **Firewalls enforce policy at layer 3 and 4**

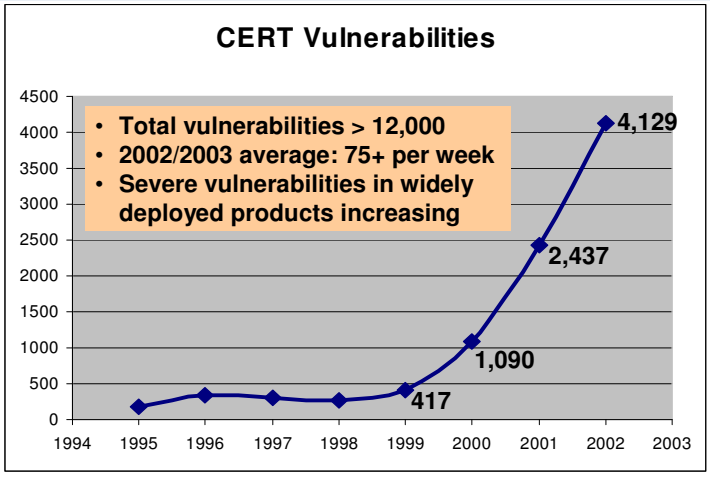



- **Firewalls are typically deployed at network edge**
  - But perimeter is eroding: wireless, VPN, laptops
  - Attacks that originate internally bypass the firewall

9

## Traditional Defenses: A Losing Battle
## Increasing Number of Vulnerabilities

TippingPoint a division of 3Com

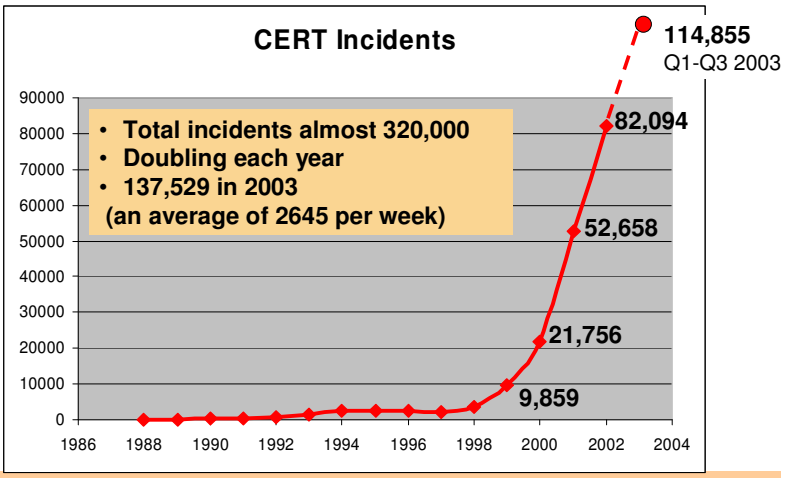



**# vulnerabilities x # systems = insurmountable task**

10

## Traditional Defenses: A Losing Battle
## Increasing Number of Attacks

TippingPoint a division of 3Com

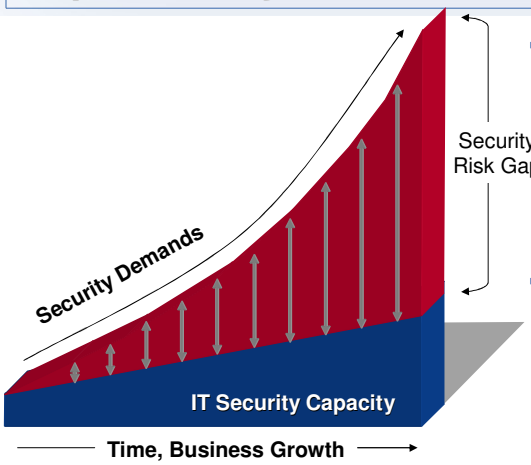



CERT Note: An incident may involve one site or hundreds (or even thousands) of sites. Also some incidents may involve ongoing activity for long periods of time

11

## The Security Risk Gap is Growing Exponentially

TippingPoint a division of 3Com



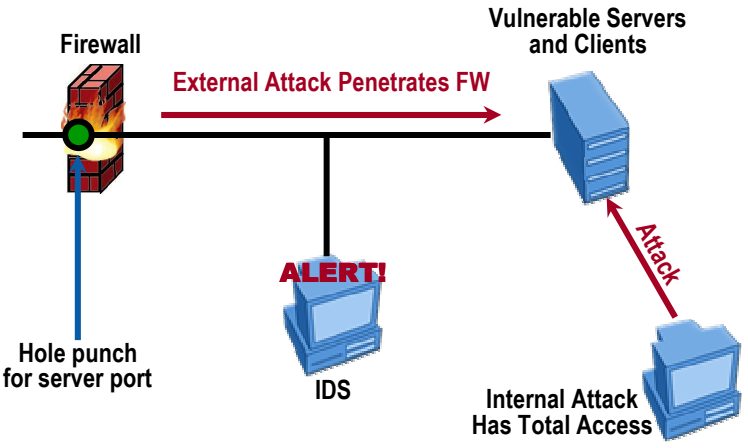

- New security demands exceed IT capacity
  - Increasing rate of new vulnerabilities
  - Decreasing time to patch them
  - Walk-in worms, e-mail attacks
  - Rogue applications "stealing" IT resources
- Traditional tools can't fully mitigate today's security challenge
  - *Perimeter* firewalls are porous (e.g. allow port 80) and can't handle the core
  - Comprehensive patching is impossible
  - Not all end-points under IT control

**Line speed Intrusion Prevention closes the gap**

12

## Traditional Defenses: Firewalls and Intrusion Detection Systems

TippingPoint a division of 3Com




**Traditional Defenses Miss 80% of All Attacks**

13

## Traditional Defenses: Firewalls and Intrusion Detection Systems

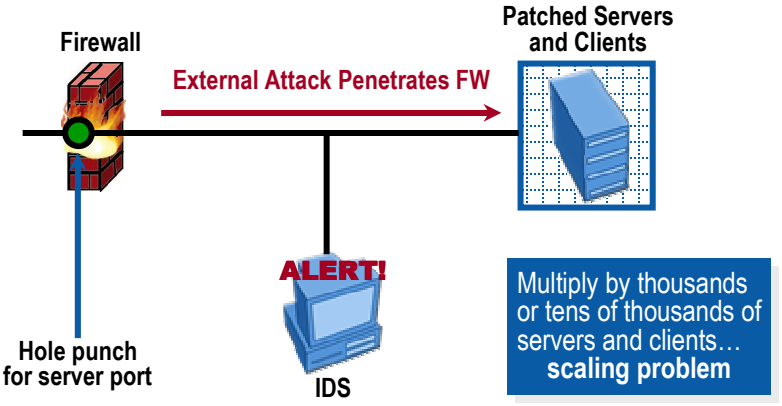
TippingPoint a division of 3Com

- **Firewall**
  - Excellent at blocking traffic to ports that are not offering public services
  - Poor at filtering attacks from traffic involving allowed services
  - Can't stop any attacks that come from the inside – 80% of the attacks
- **Intrusion Detection Systems (IDS)**
  - Excellent at detecting many types of network attacks
  - Poor at preventing attacks from succeeding

14

## Traditional Reaction: Patching Individual Systems…

TippingPoint a division of 3Com




**…But Can't Keep Up With All The Patches**

15

TippingPoint a division of 3Com

## Patching and Downtime Financial Impact

- **Cost to patch 5000 desktops exceeds $1 Million**
  - $234 average per patch  Yankee Group Enterprise Security survey, 2004
- **$1.2 Billion in lost productivity in first five days of Slammer**
- **Worldwide annual costs to businesses of all malicious code attacks were $1.8 billion in 1996; soared to $13.2 billion in 2001**
  - Horison Information Strategies, 2003

| Security Threats | Typical Impact per Incident |
|---|---|
| Virus | $24,000 |
| Denial of Service | $122,000 |
| Physical Theft or Destruction | $15,000 |
| Data Destruction | $350,000 |
| Theft of Proprietary Information | $4.5 million |
| Illegal system access - outsider | $225,000 |
| Unauthorized insider access | $60,000 |
| Installation/Use of Unauthorized Software or Hardware | $250,000 |
| Insider Abuse of Net Access / E-mail | $360,000 |
| Financial Fraud | $4.4 million |

*Estimated security impacts per incident for various internal and external security issues – Source: Alinean – 2003*

16

# Traditional Defenses: A Losing Battle
# Auto-Propagating Worm Technology

TippingPoint a division of 3Com

**Initial Compromise Rate**

| | |
|---|---|
| Code Red | 1.8 hosts / hour |
| Slammer | 420 hosts / hour |

**Infected Population Doubling Time**

| | |
|---|---|
| Code Red | 37 minutes |
| Slammer | 8.5 seconds |

**Single Host Scanning Rate**

| | |
|---|---|
| Code Red | 11 probes / sec |
| Slammer | 26,000 probes / sec |

**Vulnerable Population Saturation Time**

| | |
|---|---|
| Code Red | 24 hours |
| Slammer | 30 minutes |

**Time it takes to compromise every host that is exposed and vulnerable**

17

# July 19, 2001: Code Red II

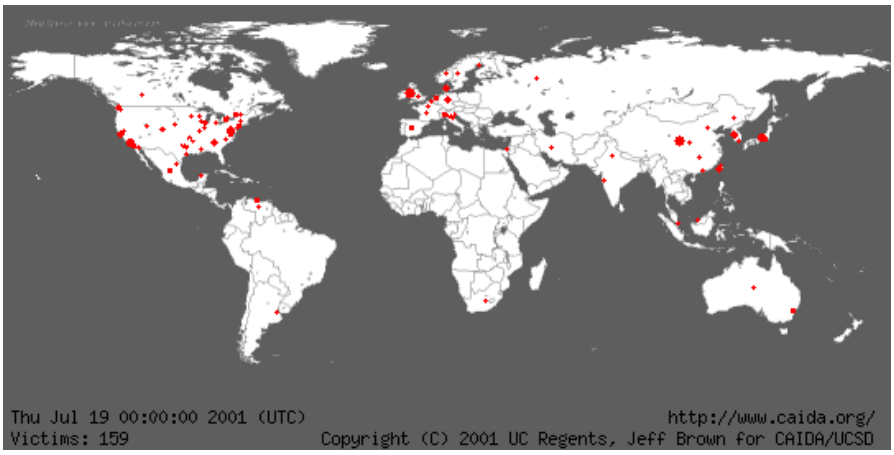
TippingPoint a division of 3Com

- Estimated cost: $2.6 billion
- Peak infection rate: 2K hosts per minute


18

## The Spread of Code Red II

TippingPoint a division of 3Com




19

## January 25, 2003: Sapphire/Slammer

TippingPoint a division of 3Com

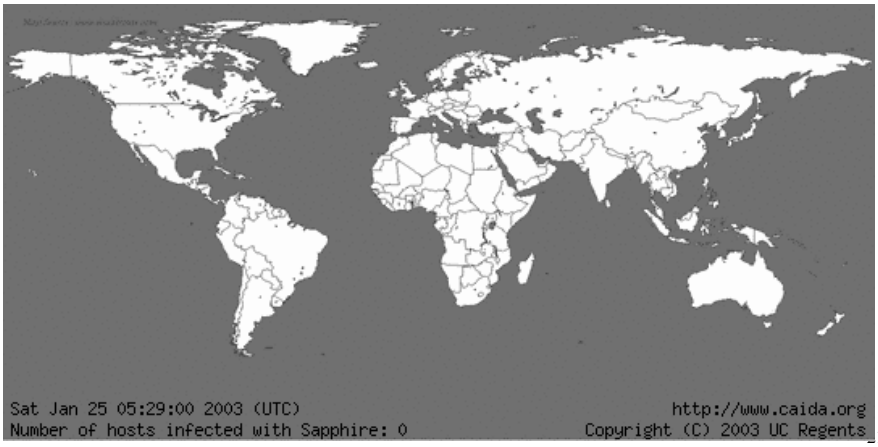
- Attacked buffer overflow vulnerability in MSSQL
- Single 376 byte UDP packet to port 1434


20

## Spread of Slammer/Sapphire

TippingPoint a division of 3Com

- Doubled in size every 8.5 seconds
- Infected 90% of vulnerable hosts in 10 minutes




21

## IPS Coming of Age

TippingPoint a division of 3Com

2002

- TippingPoint announces IPS *January 2002*
- Onesecure announces IDP-100 *February 2002*
- Intruvert announces Intrushield *May 2002*
- Netscreen acquires Onesecure ($40M) *August 2002*

2003

- McAfee acquires Intruvert ($100M) *April 2003*
- Gartner's "IDS is Dead" proclamation *June 2003*

Cyber-attacks became far more widespread, damaging, *August 2003*

Example: Blaster, Nachi, Sobig, MyDoom, Beagle…

- ISS announces Proventia G Series *November 2003*
- NSS Group test results *January 2004*

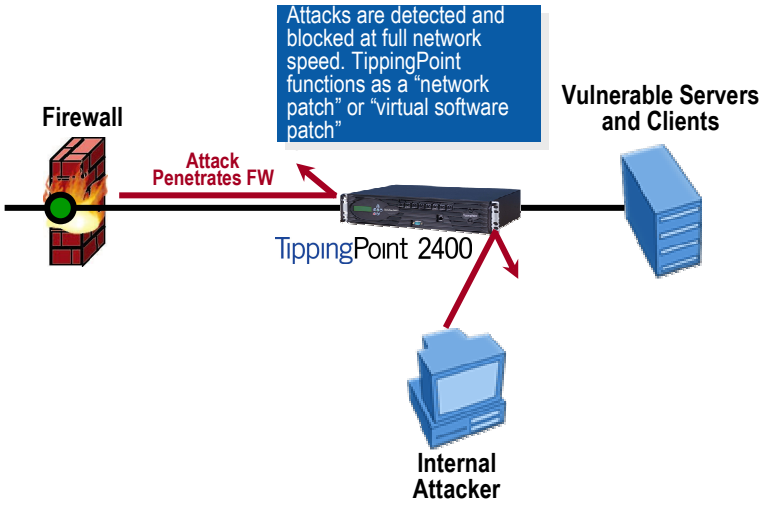
2004

- Checkpoint announces InterSpect *January 2004*
- Juniper acquires Netscreen ($4B) *February 2004*
- Cisco acquires Riverhead ($39M) *March 2004*
- Symantec releases 7100 product line *July 2004*

22

# Advanced Security Breakthrough: Intrusion Prevention System (IPS)

TippingPoint a division of 3Com

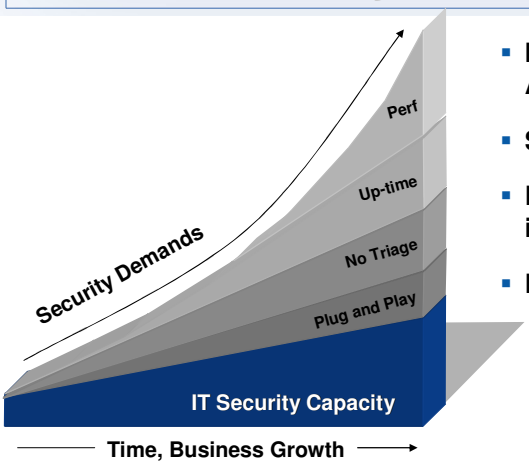



**Stops All Attacks Before They Can Do Damage**

23

# TippingPoint Closes the Security Risk Gap

TippingPoint a division of 3Com




- **Network Performance is Accelerated**
- **System Up-time is Maximized**
- **Emergency Patching Triage is Eliminated**
- **Plug-and-Play Operation**
  - No tuning required

**Business Continuity is assured and the cost of security operations is reduced**

24

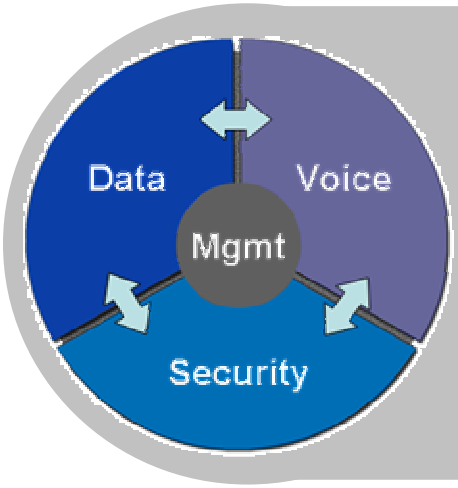
TippingPoint
a division of 3Com

# 3Com Security Strategy

**March 2005**

## 3Com's Secure, Converged Networking

TippingPoint
a division of 3Com




**Secure Network**
- Overlaid or Embedded Security
- Adaptive and Dynamic Protection
- Automatic and Centrally Manageable

**Converged Network**
- Resilient Multi-service Network
- Synergy between infrastructure elements
- Edge-to-Core Coverage
- Wired and wireless

**Customer Benefits**
- Business Continuity
- Capital Efficiency and Cost Reduction
- Corporate Control and Visibility

26

## VoIP Security

TippingPoint a division of 3Com

- **Committed to establish ourselves as leading authority on VoIP security**
  - VoIP Security Alliance
  - Comprehensive VoIP Security Filters
- **Launched VoIP Security Alliance (VoIPSA)**
  - Mission: To drive the confidence in and propagation of VoIP through collaborative research, testing and education of the industry's telecom, cable, VoIP, and security providers.
  - 50+ members: 3Com, Alcatel, Avaya, Qwest, Siemens, SANS Institute, Tenable, ATT, SBC, Nortel, Verizon, Agilent, Fidelity, Cable & Wireless, Accenture
- **VoIP infrastructure prone to the same cyber threats that plague data networks today**
- **In addition to traditional network security and availability concerns, there are also a plethora of new VoIP protocols that have yet to undergo detailed security analysis and scrutiny.**
- **TippingPoint's Intrusion Prevention filters protects networks against the known cyber threats as well as the future VoIP specific vulnerabilities and threats that will begin to emerge.**
  - Existing filter set protects against set of H.323 and SIP vulnerabilities
  - Offer extended VoIP protection coincident with Threat Suppression Engine (TSE) 2.0.

27

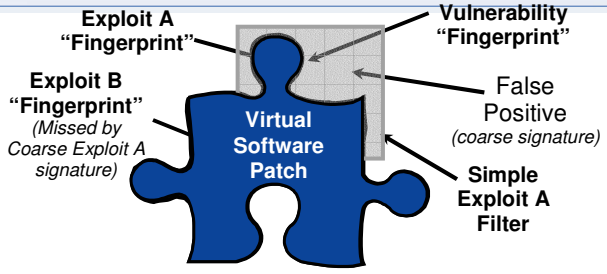
## TippingPoint's IPS

TippingPoint a division of 3Com

| Attribute | Value |
|---|---|
| Purpose-Built Custom ASIC Hardware Platform | Extensible Platform for Uncompromising Security and Networking |
| 50Mb – 5Gb Performance | Scalable Solutions for Perimeter and Internal Protection |
| Switch-Like Latency | Inline Network Deployment Without Impacting Network Performance |
| Inline Attack Blocking | Effective Proactive Attack Termination |
| Recommended Settings | Automatic Security, both out of the box and ongoing |
| Bandwidth Management | Network Performance Protection |
| Complete Filtering Methods | Accurate and Comprehensive Attack Filtering |
| Advanced DoS Protection | Protection for Evolving DDoS Attacks; Using SYN Proxy and Connection Rate Limiters |
| VoIP Security | Protects Against VoIP Threats |
| Spyware Protection | Secures business and employee information; Protects bandwidth |

28

# Application Protection – A Virtual Software Patch

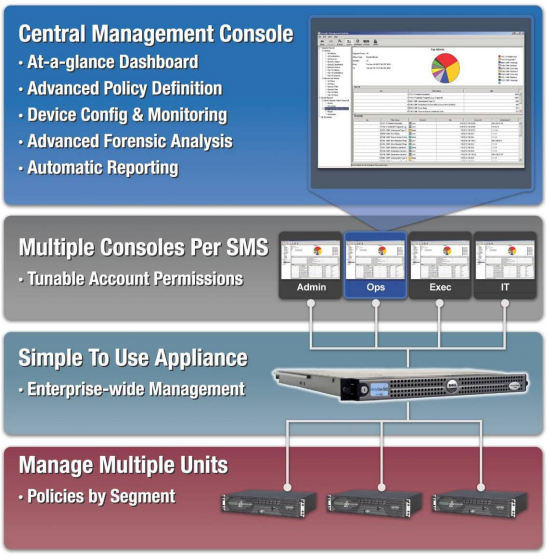



- A vulnerability is a security flaw in a software program.
- An exploit is a program that takes advantage of a security flaw to gain unauthorized access to a vulnerable system.
- Simple Exploit Filters are written only to a specific exploit.
  - Filter developers are forced to basic implementations because of engine performance limitations.
  - Result: missed attacks, false positives and continued vulnerability risk.
- TippingPoint's Vulnerability Filters act as a Virtual Software Patch and cover the entire vulnerability.

29

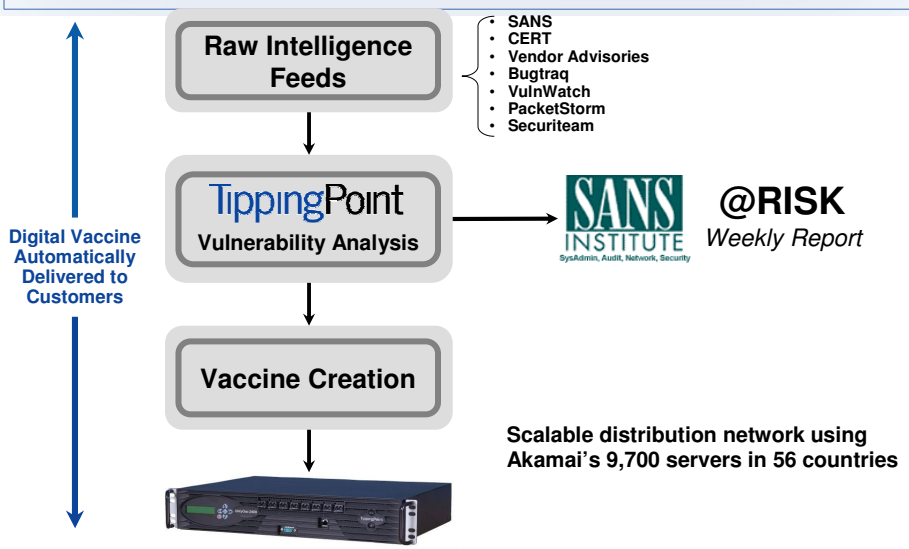
# TippingPoint Security Management System

- Hardware is included with SMS purchase and software is pre-installed
- Installation Ease
- Scalable
- Enterprise-wide security policy management
  - Port-by-port policy
  - Device-by-device policy



## Automatic Digital Vaccine

TippingPoint a division of 3Com

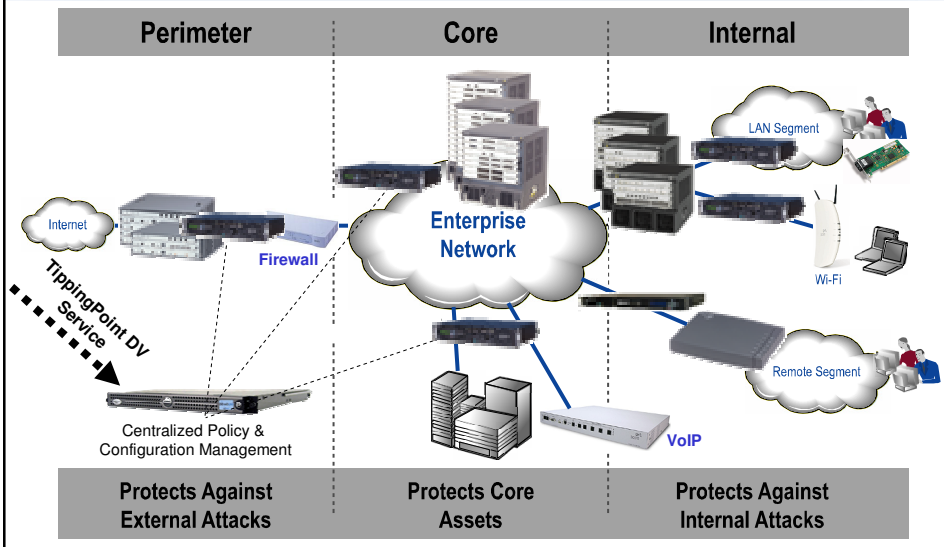



Scalable distribution network using Akamai's 9,700 servers in 56 countries

31

## Edge to Core Protection

TippingPoint a division of 3Com




32

## TippingPoint Product Line

TippingPoint
a division of 3Com

**TippingPoint 50**
50 Mbps
1x10/100/1000
Copper

**TippingPoint 100E**
100 Mbps
1x10/100/1000
Copper

**TippingPoint 200**
200 Mbps
2x10/100/1000
Copper

**TippingPoint 400**
400 Mbps
4x10/100/1000
Copper/Fiber

**TippingPoint 1200**
1.2 Gbps
4x10/100/1000
Copper/Fiber

**TippingPoint 2400**
2.0 Gbps
4x10/100/1000
Copper/Fiber

**TippingPoint 5000E**
5.0 Gbps
4x10/100/1000
Copper/Fiber

**TippingPoint SMS**
Security
Management
System

33

TippingPoint
a division of 3Com

## Thank You For Attending

**Brett Hunter**
**bhunter@tippingpoint.com**