The State of Network Security

Greg Young,
Research Vice President
Network Security
May 1, 2007

Gartner

Network Security Sea Change

- The network security market continues to be highly dynamic and subject to disruptive forces
- Your Dad's DMZ won't work for changing networks
- Enterprise security differs from the SMB
- New critical issues require actions be taken

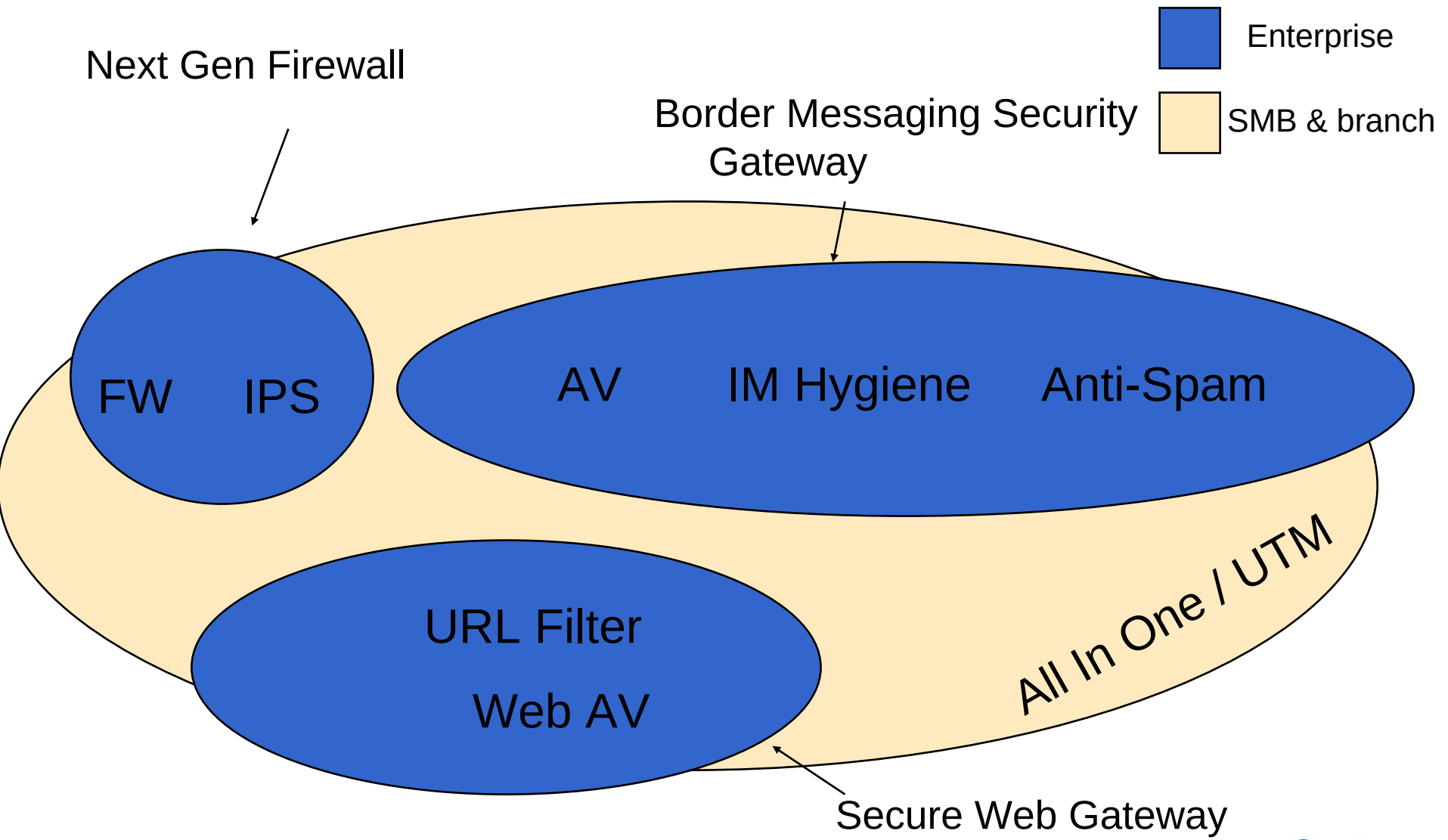
Defense in Depth and the "NxN" DMZ

- Complex applications require a more complex yet well-structured DMZ
- Death-spiral of increasing rules or ACLs
- Increased connection methods
- Protecting assets from the internal network
- Mobility of endpoints

There Will Always Be a Perimeter

- Neither “All Network” nor “All Host” safeguards are feasible
- The edge changes and gets more complex but doesn’t go away
- Coordinated safeguard approach rather than a single safeguard

There Is No UTM for the Enterprise



Gartner

Firewall in the NIC

- Network group can always talk to a NIC card
- 4th Firewall tier in the NIC
- Silicon based firewalls are inexpensive and widely available
- A panic button

NAC Is Real, but the Market Is Fragmented and Immature

- Network Access Control
- Feasible but tactical
- Vista, Longhorn, 802.1x
- Over-hyped today
- Will become part of how we can secure networks
- Drop in appliances vs infrastructure upgrades

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Bradford Networks				x	
Caymas Systems		x			
Check Point Software Technologies			x		
Cisco Systems				x	
ConSentry Networks			x		
ForeScout			x		
InfoExpress			x		
Juniper Networks			x		
Lockdown Networks		x			
McAfee			x		
Mirage Networks			x		
Nevis Networks		x			
Sophos (Endforce)				x	
StillSecure				x	
Symantec				x	
Trend Micro		x			
Vernier Networks			x		

As of 1 February 2007

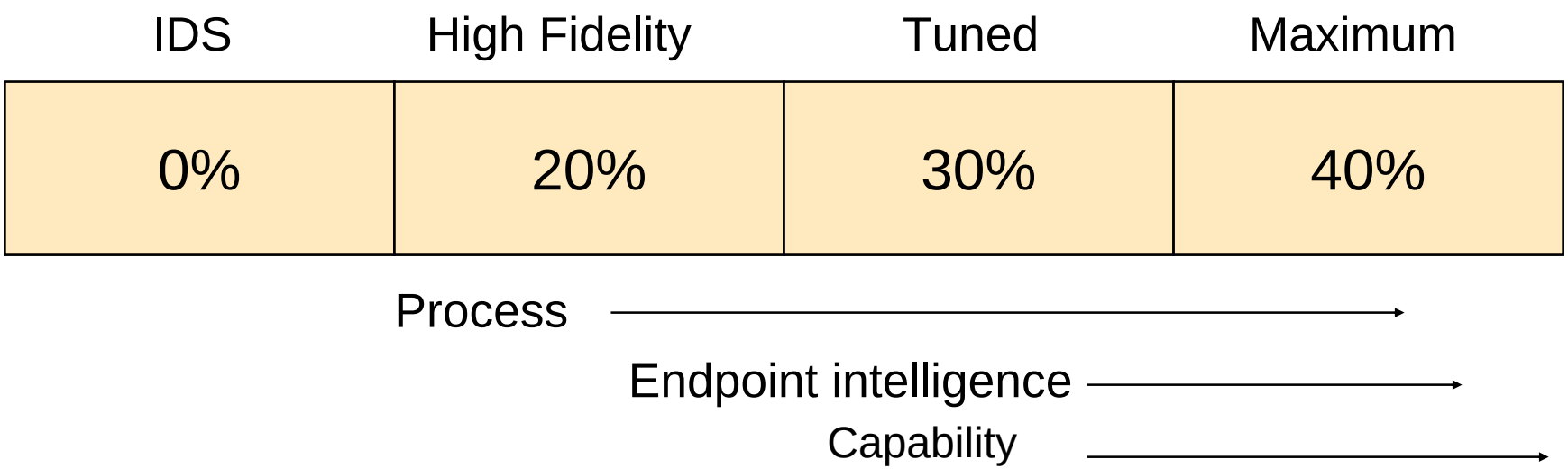
Source: Gartner (February 2007)

Gartner

IPS Primarily at the Edge and in Blocking Mode

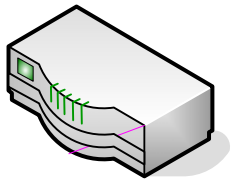
- IPS moves beyond threat signatures
- Endpoint and ‘extra-IPS’ intelligence
- A big market – forecast >$1B in 2007
- Deployments march inwards at critical points

Signatures In Blocking Mode

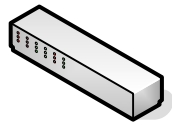


Gartner

The Need for a Separate Security Control Plane



Move packets

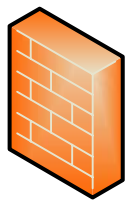


Dynamic

Asset

Vulnerabilities

Block packets



Secure Configuration

Kernalized and evaluated

$

There Is No Big Security Market Convergence

- Existing companies merge, get acquired, keep going, go under
- New threats and technology drive new markets and companies
- Markets evolve through the hype cycle
- Security and compliance markets grow

Network and Host Security Will Communicate but Not Become One

- Benefits
  - Buying center
  - Some efficiencies and early warning
- Problems
  - Signature enablement is a benefit
  - Operations and business knowledge across network/host boundary is limited

Encryption of MPLS and Internal Links Remains Niche

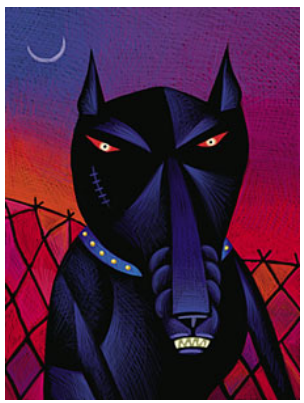
- Encryption is blinding WOC, IPS, NBA, firewalls
- High cost and disruption
- Drop in appliance approach from Cypheroptics, Cisco et al is most common approach
- Overlay approach from Cisco GET
- Quantum Crypto very niche until at least 2011

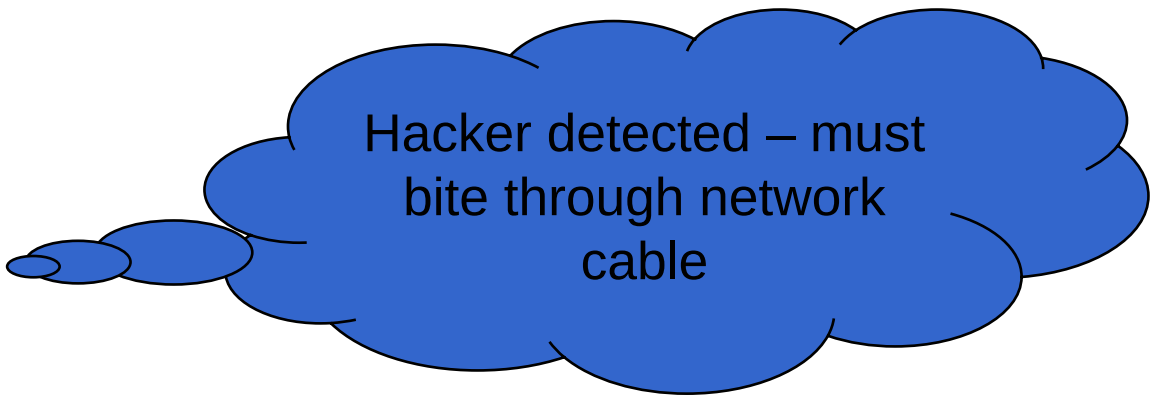
In The Cloud

- Non-Customer Premise Equipment (CPE)
- Moved easily into the cloud:
  - DDOS
  - email spam/av
  - FW
- More problematic:
  - IPS
  - CMF,
  - antiphish
- New pricing/availability

Physical Security and IT Security Are Not Converging

- Distinct buying and management centers
- Nexus is securing user content, including video and access control
- Pushed by vendors rather than requirements
- Physical security can disrupt ITSec





Recommendations

Gartner