Will The Real Next Generation Security Please Stand Up?

John Pescatore
Director, SANS Emerging Security Trends
Moore’s Law and Next Generation Security

- Security products have to obey Moore’s Law:
  - If a product doesn’t address new threats, the price should drop dramatically.
  - To maintain pricing, security products need to do more with each new generation.
- Get more efficient at dealing with old threats, more effective at dealing with new threats.
- There really is no need for a new name for every new device that deals with threats.
A Brief History of Threats and Detection/Prevention

Peaceful Mainframe Days

1985
- Morris Worm
- Macro Virus
- Melissa E-Mail Worm

1995
- Code Red/Nimda
- Slammer/Blaster
- Phishing
- Botnets/Rootkits

2005
- Advanced Targeted Attacks
- Advanced Threat Prevention

2015
- Cybercrime as a Service
- Virtualization Attacks
- Peer-to-Peer Wireless Attacks
- Cascading Impacts
- Quantum Computing Attacks

Today
- IDS/IPS/NGFW
- Advanced Threat Prevention
- Botnets/Rootkits
- Slammer/Blaster
- Code Red/Nimda
The Evolution of NetSec Platforms

- Intrusion Detection/Prevention
- Secure Message Gateway
- Secure Web Gateway
- Firewall
The Evolution of NetSec Platforms

- Intrusion Detection/Prevention
- Secure Message Gateway
- Secure Web Gateway
- Next-Generation Firewall
The Evolution of NetSec Platforms

- Next-Generation IDS/IPS
- Secure Message Gateway
- Secure Web Gateway
- Next-Generation Firewall

Adv. Threat Detection
Services View

- Next-Generation IDS/IPS
- Secure Message Gateway
- Secure Web Gateway
- Next-Generation Firewall
- SIEM, EPP

Forensics/IR

STA, STH

Net Sec

Pen Test, App Attack
Our Panel

- Tom Hartig, Security Engineer, Check Point Software Technologies
- Justin Kallhoff, CEO, Infogressive, Inc.
- Ryan Petersen, FishNet Security