The Future of Network Defenses

Infrastructure, Content & Context

IBM Software

PCTY2010

Pulse Comes to You

Optimising the World's Infrastructure

Brian Moran

May 26, 2010

Three Phases of Technology Evolution

Context

Content

Infrastructure

Benn Konsynski
George S. Craft Professor of Information Systems & Operations Management
Goizueta Business School, Emory University

Technology Evolution: Historical Examples

Auto Industry

Infrastructure

Content

Context

Technology Evolution: Historical Examples

Internet

Context

Content

Infrastructure

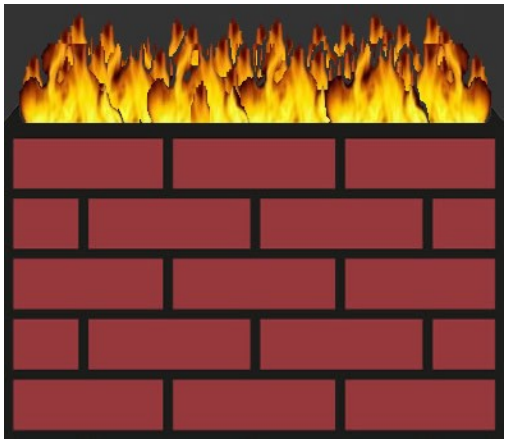
Key Lessons from Historical Examples

- Infrastructure and content never go away
  - Commoditization or Oligopolies (markets of 2-3 major vendors) limit opportunities for market-changing innovation in these areas
- Context allows users to get more value from infrastructure and content
  - To create real value, context must bring ***efficiency*** to the infrastructure and content
  - When most successful, contextual innovation becomes integrated into the infrastructure and content and may be a reason to upgrade the infrastructure. However, benefits must be greater than the costs to upgrade
  - There's always opportunity for innovation to bring greater context

Does network security follow this evolution?

What innovation improves network security – not with new point solutions, but with integration that makes infrastructure and content more efficient?

Context



Infrastructure

Firewalls

Content

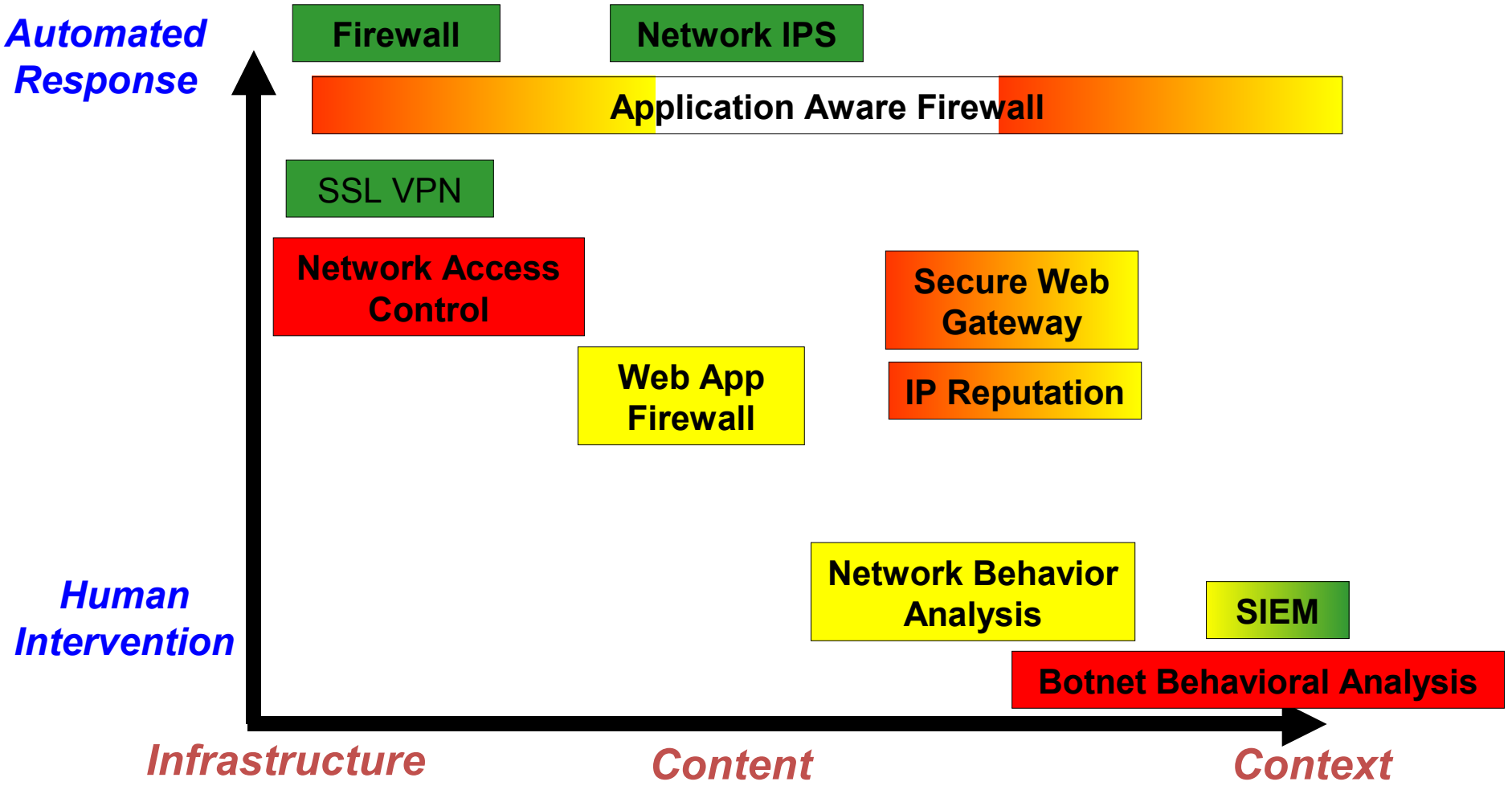
Network Intrusion Prevention Systems

Network security innovation (2003-2010)

- The industry continues to innovate, but few innovations have developed into network security “standards”
  - Require additional infrastructure; cost to manage greater than the benefits
  - Require manual intervention to apply contextual information and take action via existing infrastructure and content
- Notable exceptions to the above:
  - Government, Financial Institutions and high value Intellectual Property
  - Cyber warfare is real!
  - Organized crime exploits network & system vulnerabilities for financial gain
  - Management costs of point products are acceptable given the risks

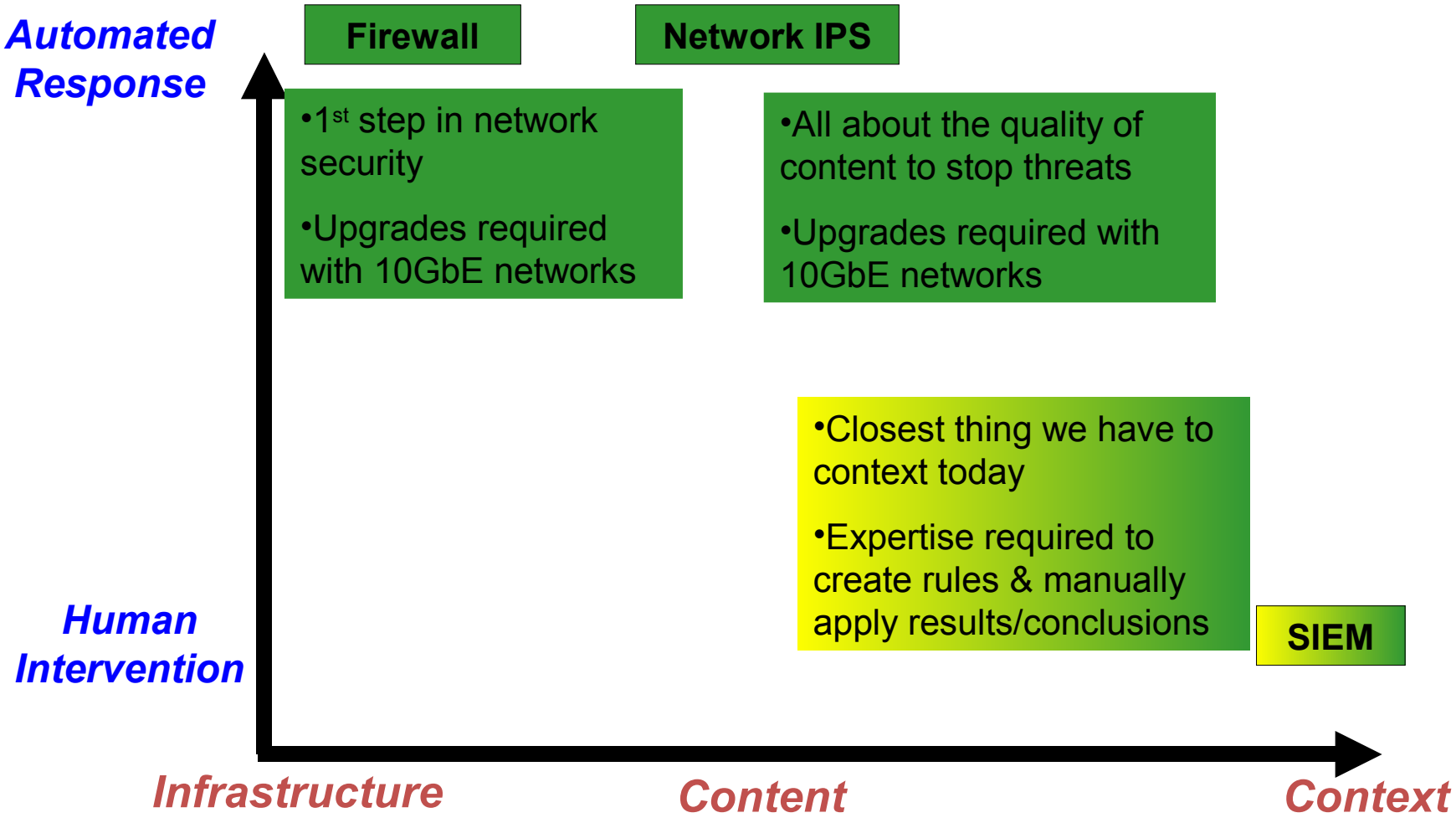
Market Adoption

Landscape of network security offerings today



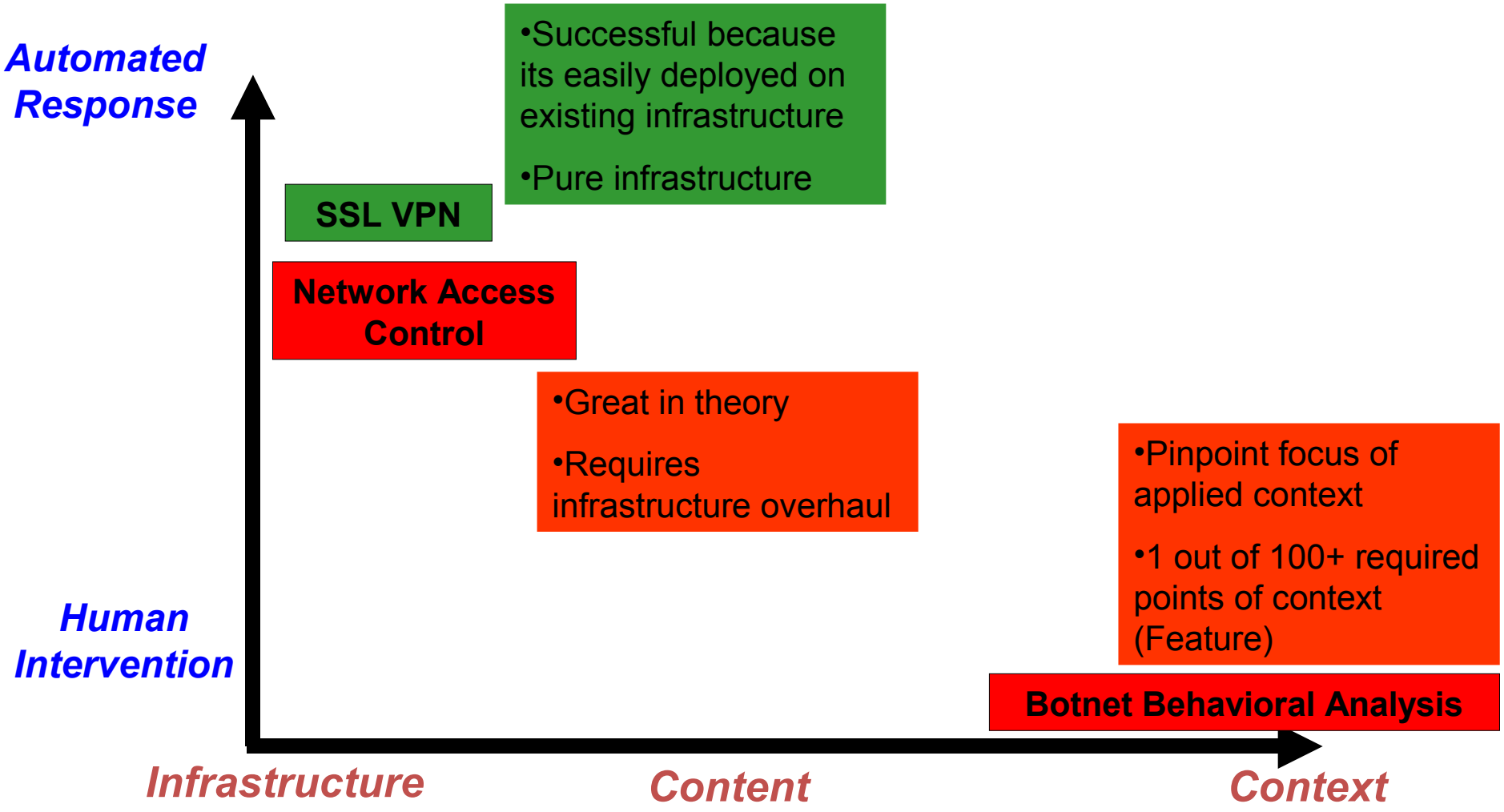
Market Adoption

Landscape of network security offerings



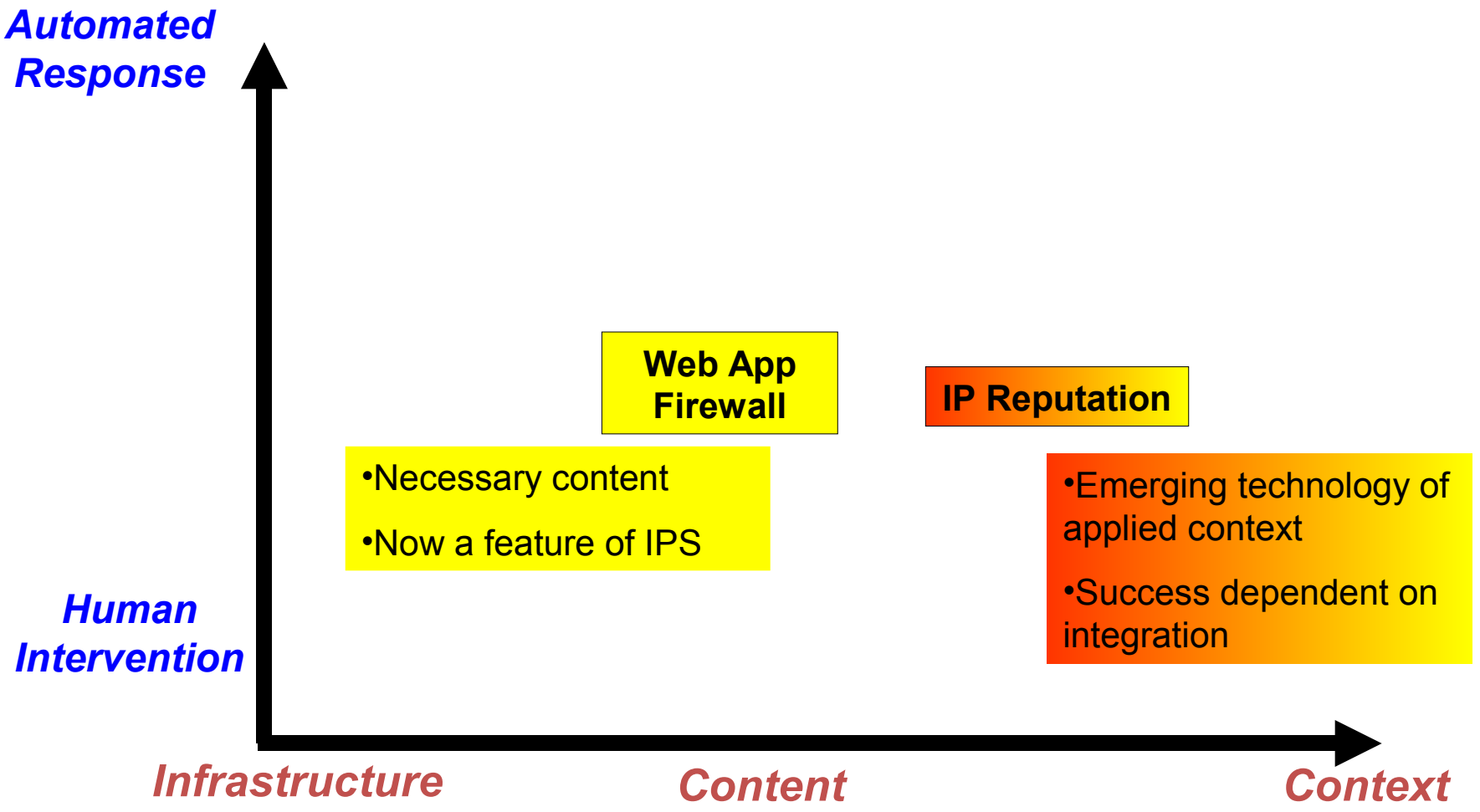
Market Adoption

Landscape of network security offerings



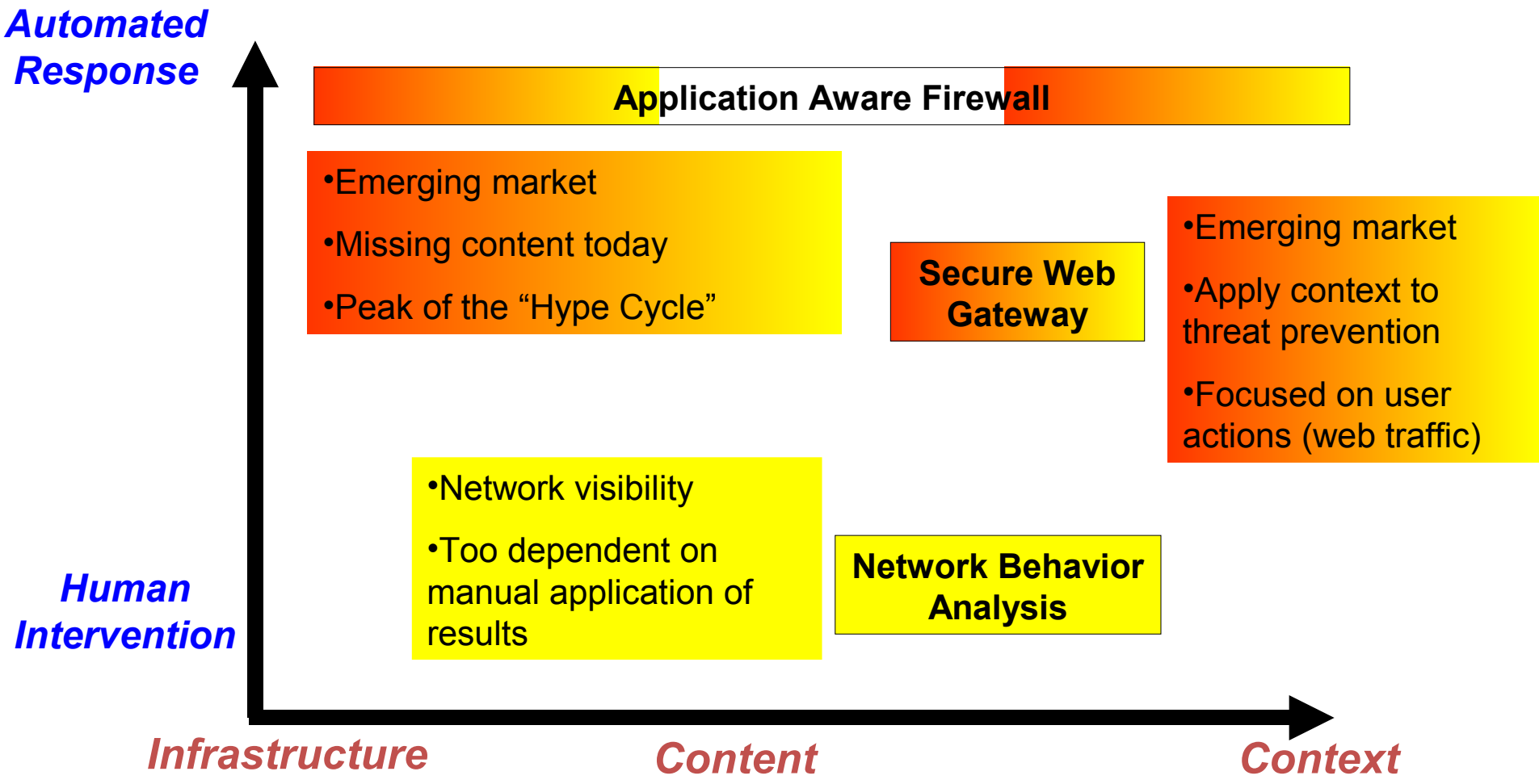
Market Adoption

Landscape of network security offerings



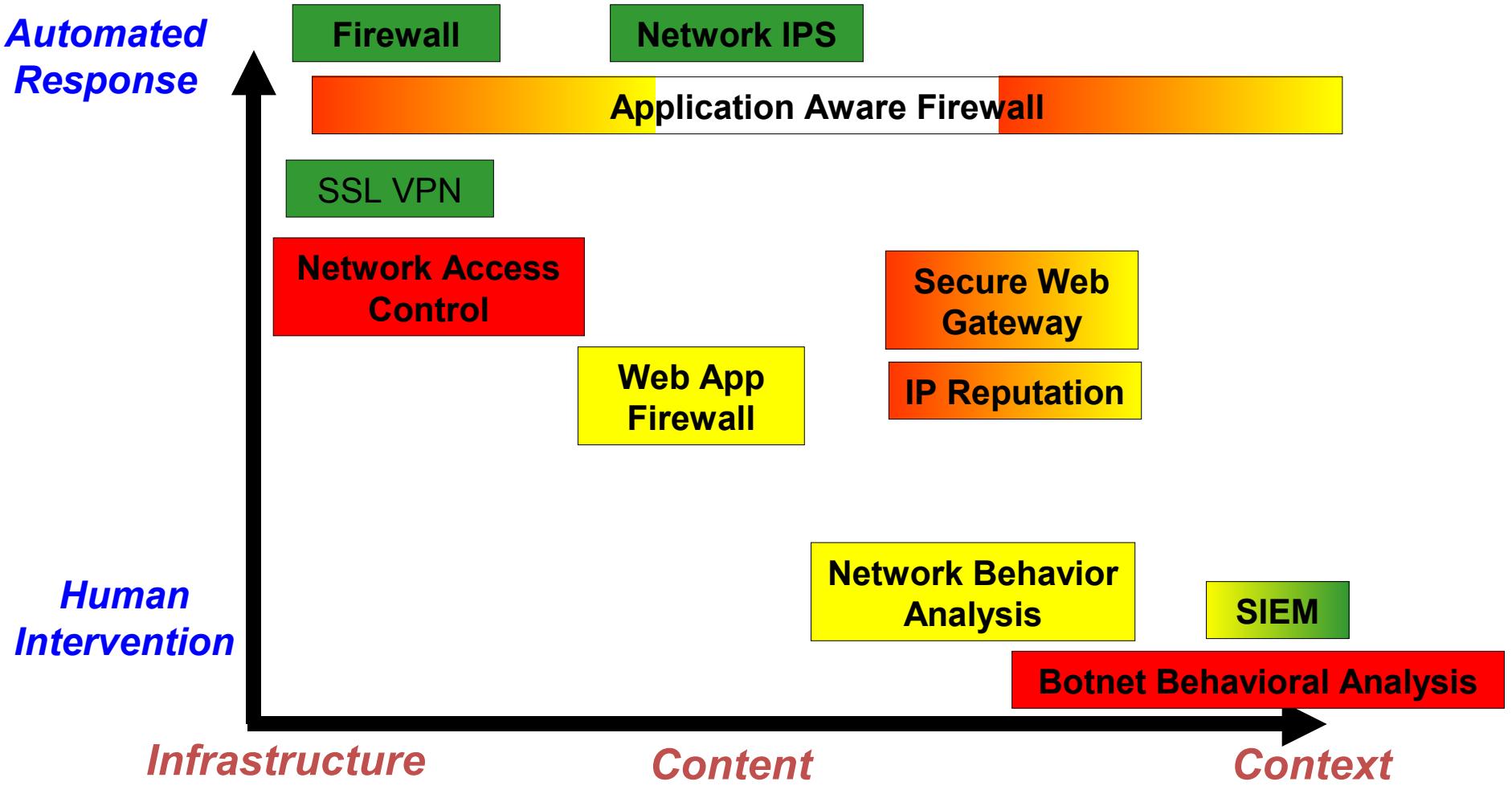
Market Adoption

Landscape of network security offerings



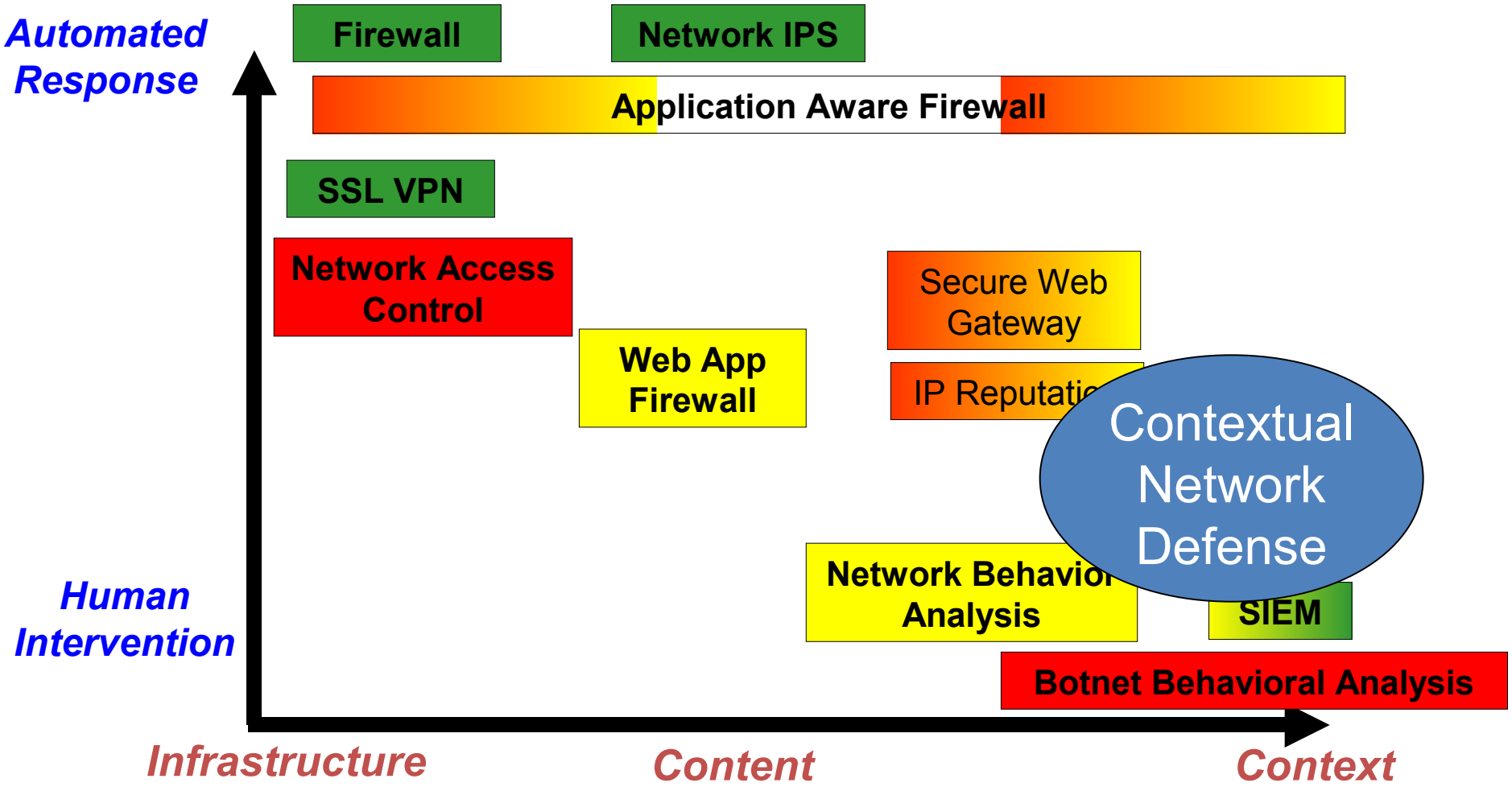
Market Adoption

Landscape of network security offerings



Market Adoption

Landscape of network security offerings



How can context improve network defenses?

- Understand the gray areas
  - Reduce reliance on white/black lists
- Move beyond baselines
  - Automated actions based on the identifications of the unusual
- Enforce risk profiles where all users are not equal
- Consolidate infrastructure, content and context while still meeting the needs of large enterprises

IBM Software

PCTY2010

Pulse Comes to You