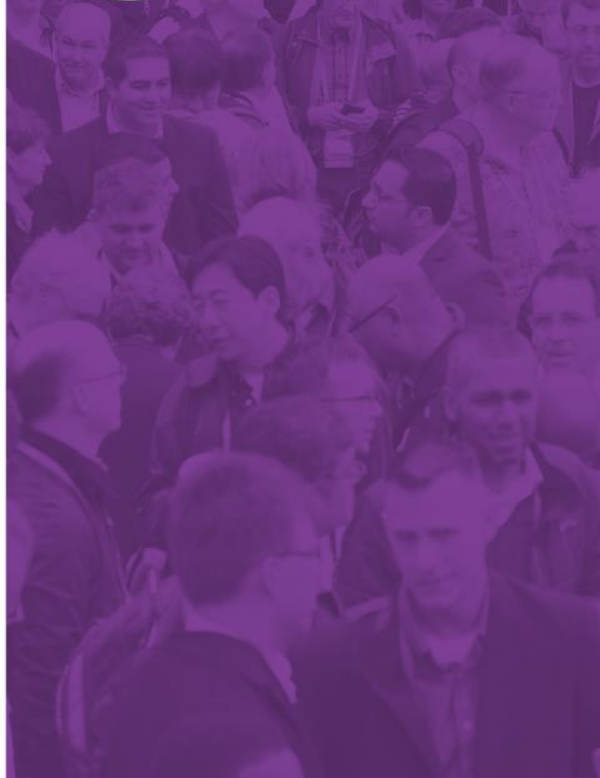
RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect



Session ID: TECH-R05

Next-Generation Endpoint Security Overview

Jon Oltsik
Senior Principal Analyst
ESG

#RSAC

Agenda

- Endpoint Security Defined
- What about antivirus?
- The next-generation endpoint security triggers
- Next-generation endpoint security market dichotomy
  - Prevention vs. Detection/Response crowd
- Recommendations and lessons learned

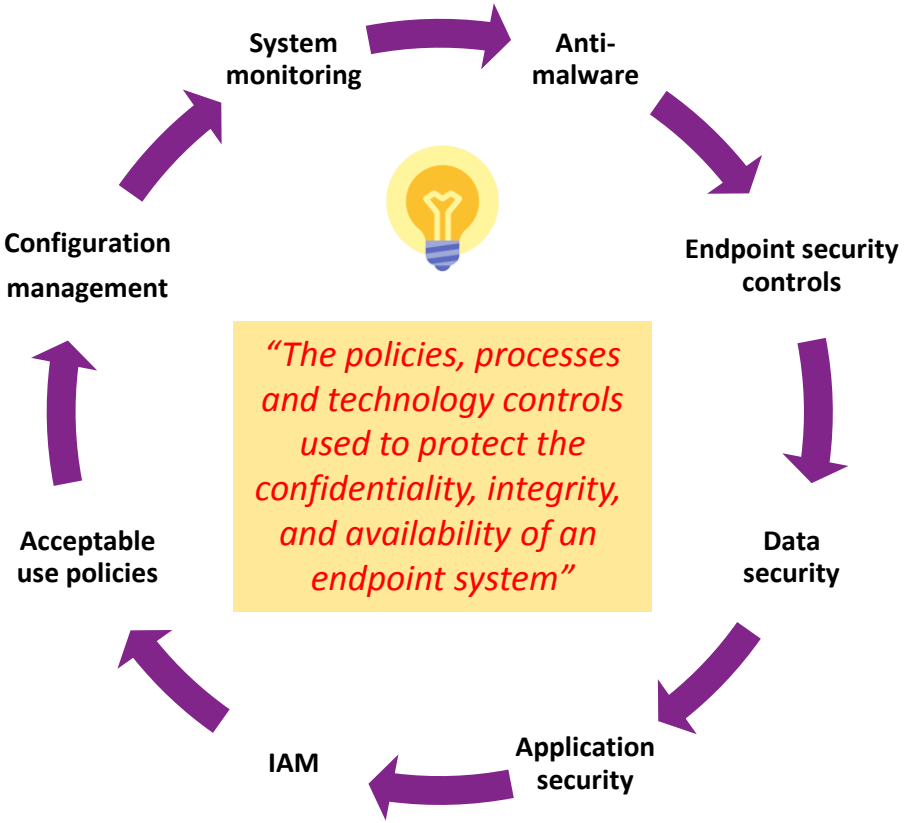
What Is An Endpoint?

Primary:
Windows PCs

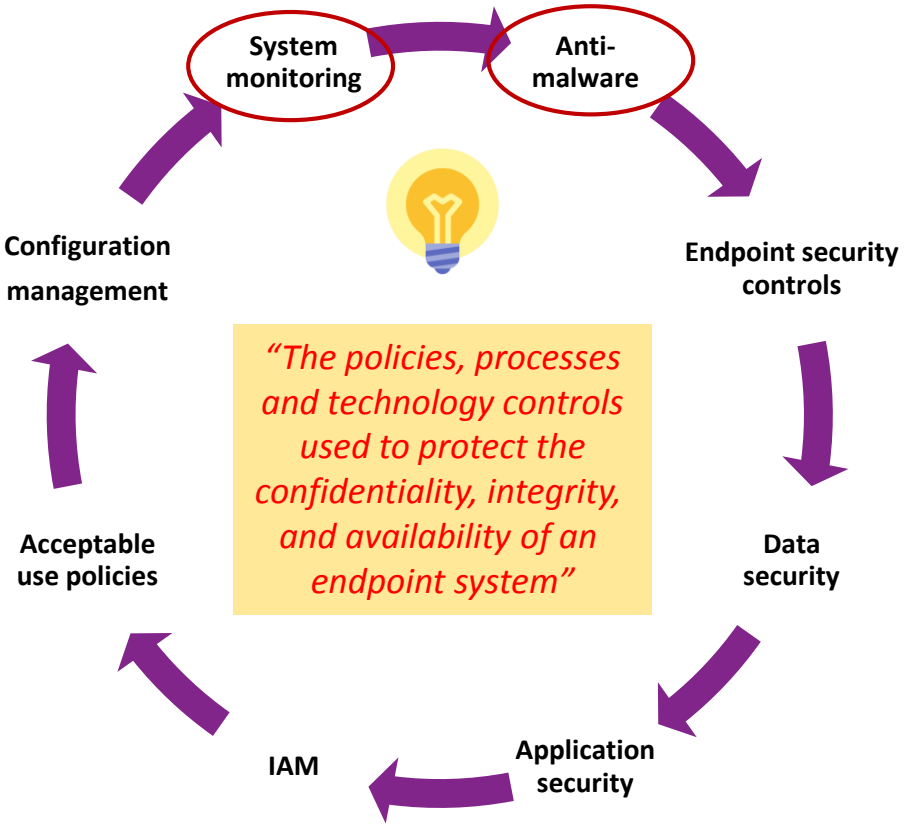
Secondary

Windows Server

What is Endpoint Security?



What is Endpoint Security?



What About AV?

- $5 billion to $7 billion WW market
- 95%+ penetration rate
- Historically dominated by 5 vendors
- History of usurping functionality
  - Application controls, anti-spyware/adware, full-disk encryption

Antivirus Myth and Reality

- AV is NOT a commodity product (nor is it “dead”)
- AV management is often delegated to IT operations groups
- AV is not always well maintained
- Advanced features:
  - Not well known or always used
  - Can have a substantial impact on system performance
  - Mixed results in terms of efficacy

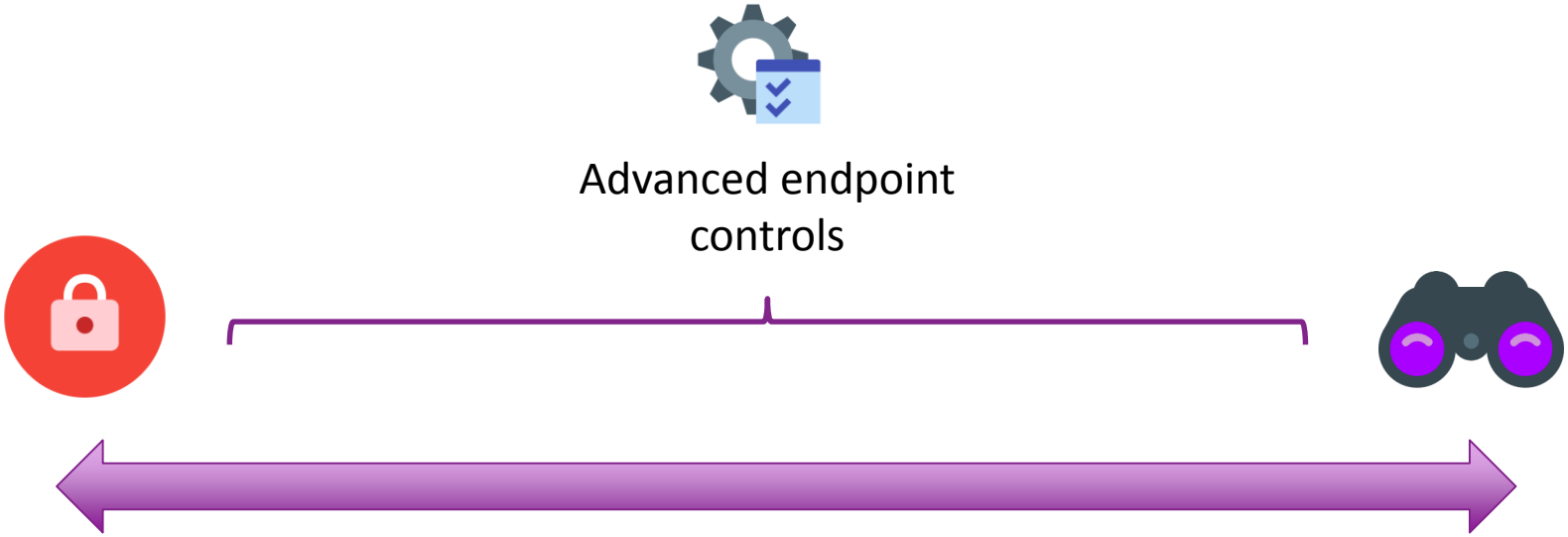
Endpoint Security Market

NG Endpoint Security Triggers

- Network compromise, cyber-attack, or data breach
- Time and resources necessary for system reimaging
- Cybersecurity quantum leap

- Cybersecurity cavalry to the rescue!
  - Needs and resource assessment

Endpoint Security Continuum

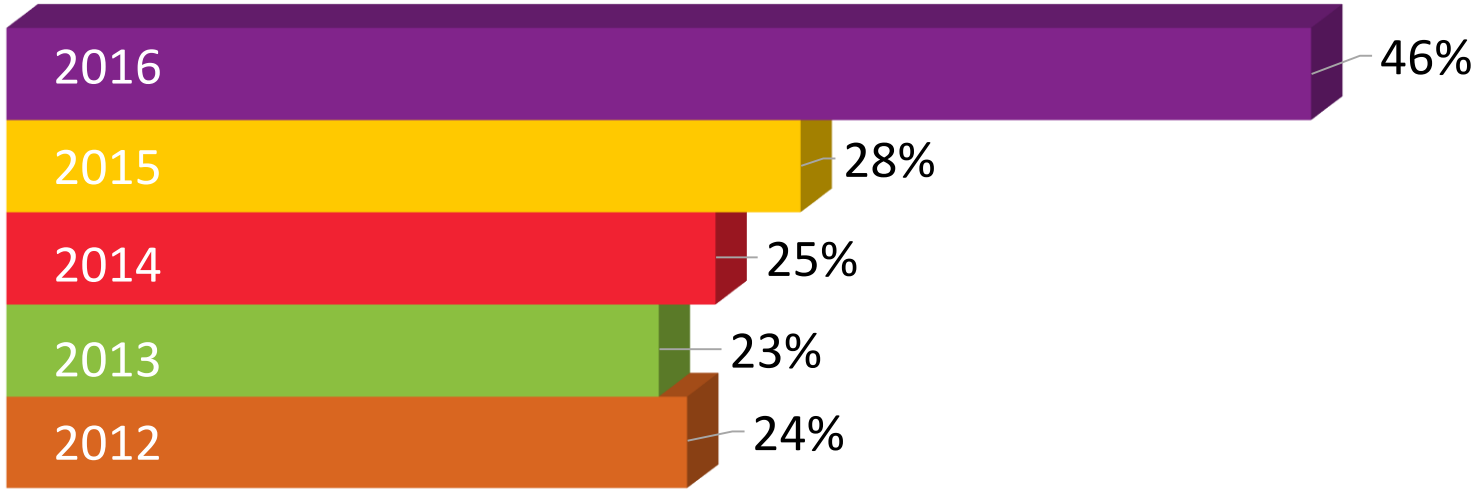


Endpoint Security Advanced Prevention

- "Hair-on-fire" problem
- Resource constraints
  - Staff size, skills, time
- Endpoint malware prevention may be one of several cybersecurity initiatives

Endpoint Security Advanced Prevention

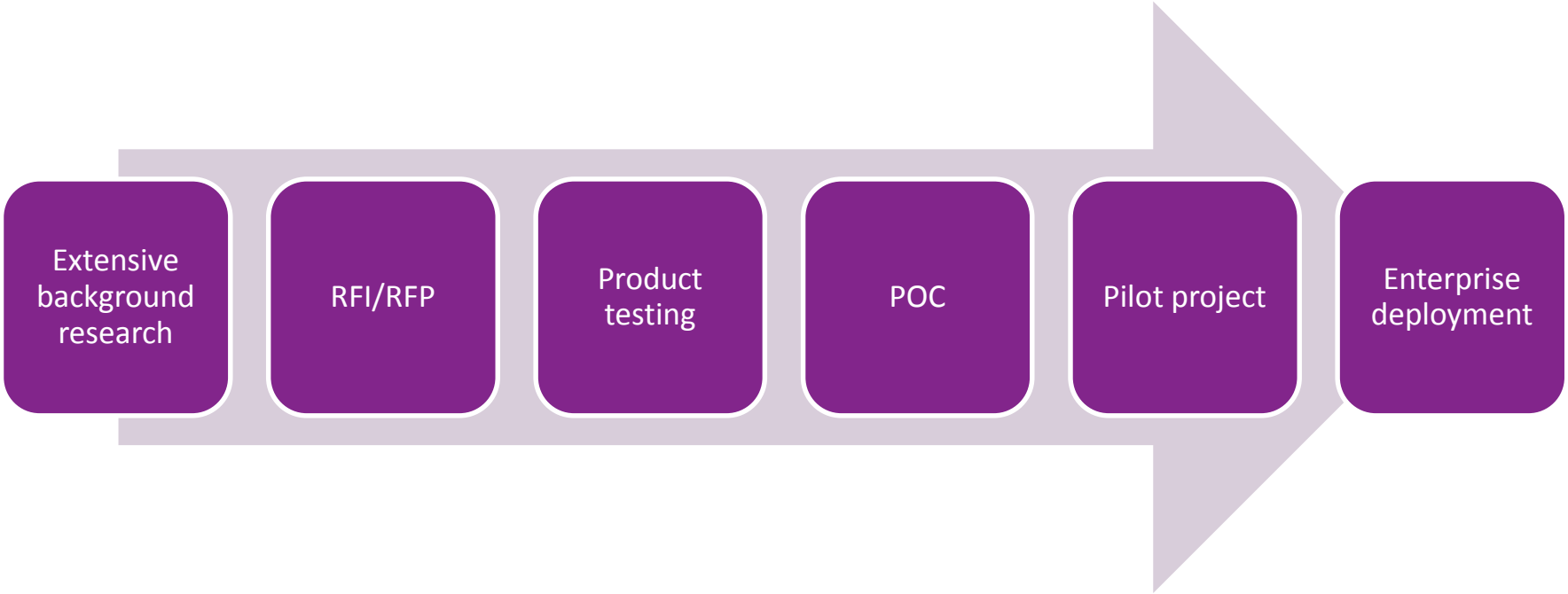
Problematic shortage of IT security skills



Advanced Prevention Products

- New types of algorithms
- Process isolation or sandboxing
- Behavioral heuristics
- Tight integration with threat intelligence

Procurement and Deployment



Observations

- Early stage products have obvious flaws
  - Extensive customer input into product roadmaps
- Scale and manageability are high priority requirements
- AV replacement is often part of strategy
- Enhancements may be required
  - Windows firewall, application controls, etc.

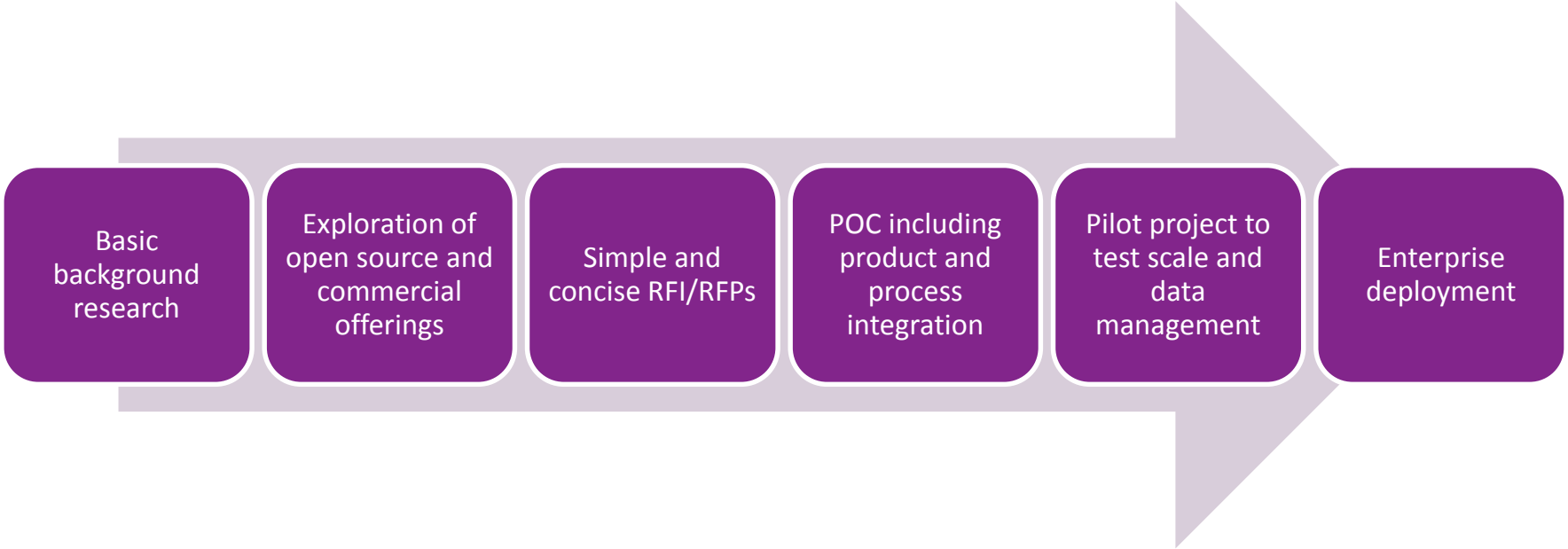
Advanced Detection and Response

- Progressive skills and resources
- Strong relationships with existing AV vendor
- Not hung up on endpoint agents
- Broad approach to anti-malware based upon data analytics
  - Network sandbox, threat intelligence, open source tools, custom rules, etc.
- Focus on IR automation and orchestration

Advanced Detection and Response Products

- Data collection- and analytics-centric
  - Windows logs, system activities, forensic capture, etc.
- Various requirements for endpoint data collection
  - Polling, trigger-based, local collection, central collection, etc.
  - Trend toward real-time continuous collection and visibility
- Product GUI and analytics may or may not be important

Procurement and Deployment



Observations

- Very demanding user base
- Best-of-breed mentality
- Customers will likely
  - Demand product customization and enhancements from vendors from the start
  - Want to use products to create (and even distribute) custom remediation rule sets
- “Big brother” issues

Further Analysis

- Continuum will continue
- Rip-and-replace mindset
- Possible extensions for data security and insider threat
- Cloud-based control plane?
- Endpoint security and patching

Action Items

- Assessment
  - Existing AV, malware, malicious network traffic, skill sets…
- Requirements definition
  - Comprehensive security requirements
  - IT and business requirements
  - Technical requirements
- Research and evaluation
  - Cast a wide net but maintain a focused search
- Plan for the long-term