Proactive Approach to Cyber Security

Jeffrey Neo

Sales Director

HP Enterprise Security Products

Customers struggle to manage the security challenge

Today, security is a **board-level** agenda item

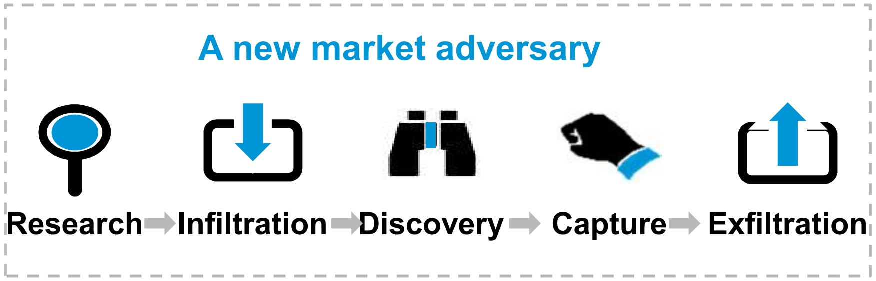
Trends driving security investments

Primary Challenges

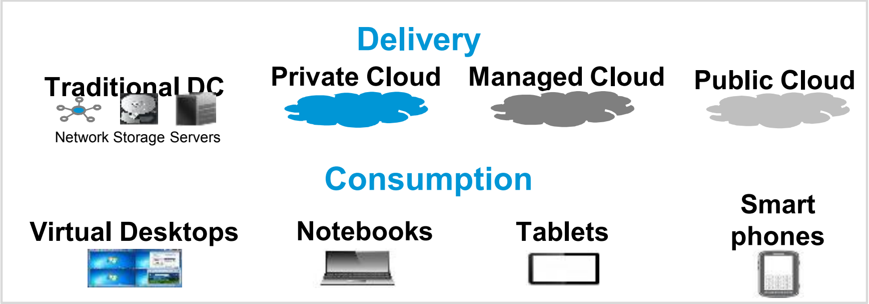
1 **Nature & Motivation of Attacks**
(Fame → fortune, market adversary)

2 **Transformation of Enterprise IT**
(Delivery and consumption changes)

3 **Regulatory Pressures**
(Increasing cost and complexity)



A new market adversary



Delivery

Consumption

Policies and regulations

Sarbanes-Oxley
Financial and Accounting Disclosure Information

PCI Security Standards Council™

Basel III

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

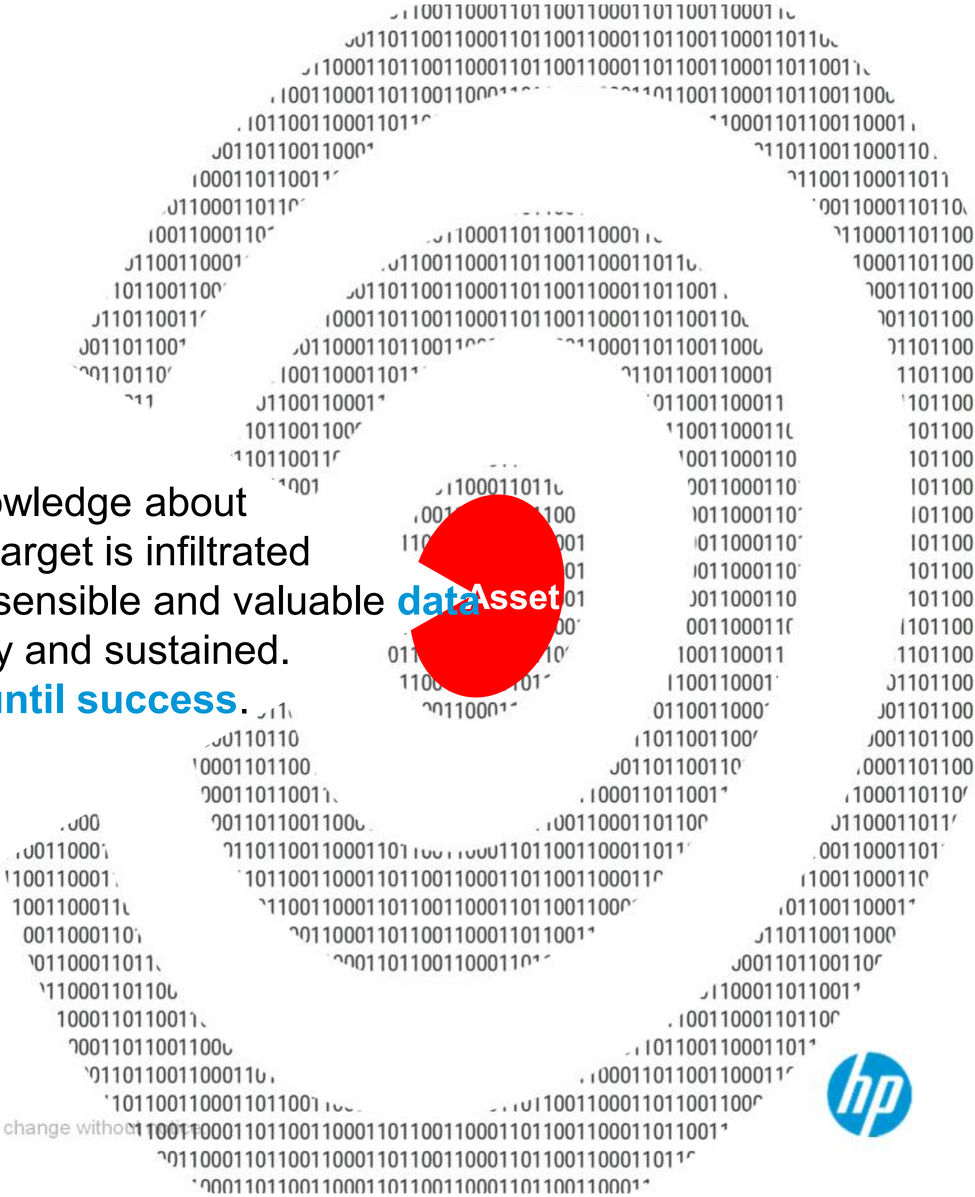
GLBA

DoD 8500.1

APT - Definition

Advanced Persistent Threat (APT)

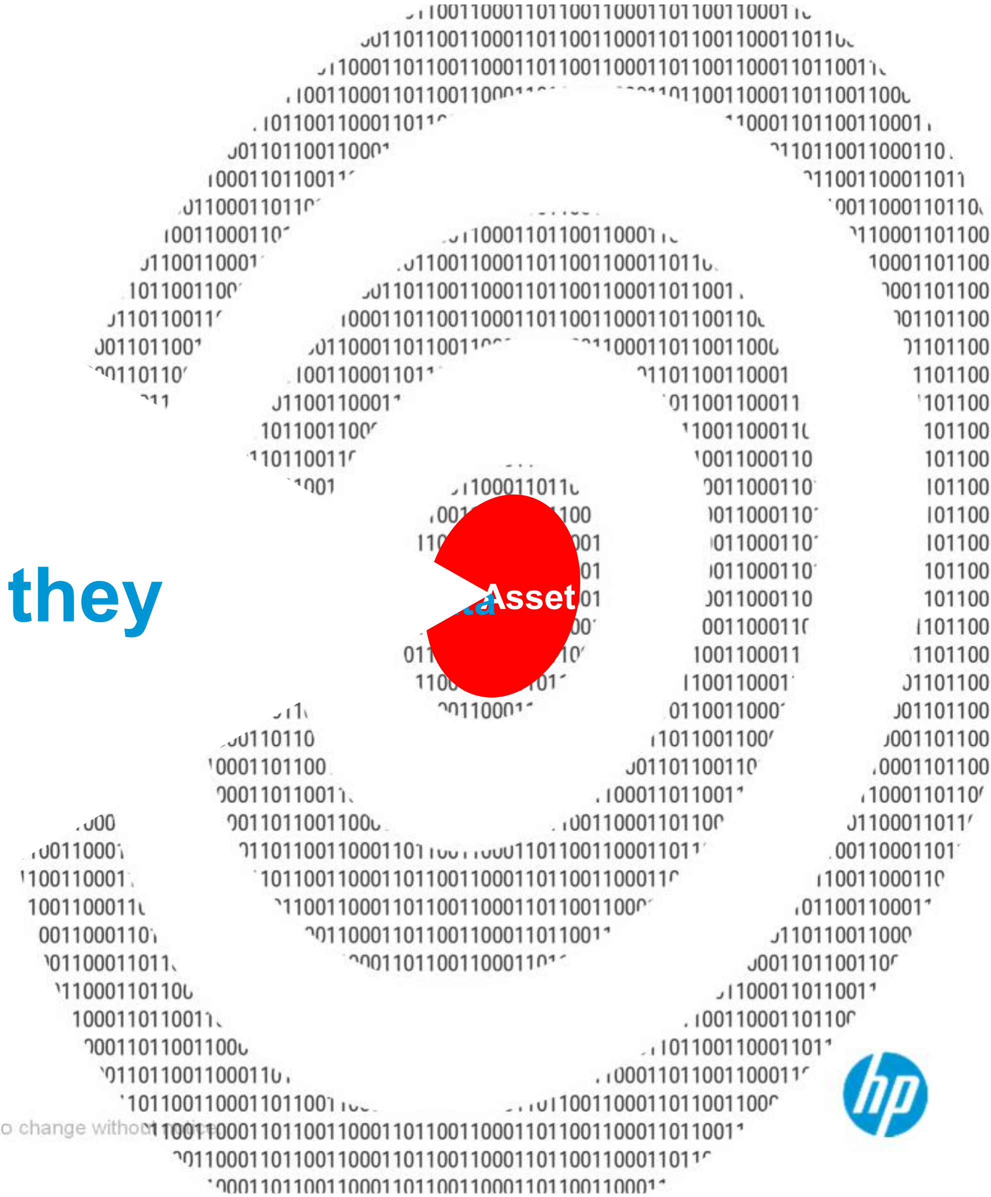
Well-funded and **skilled** attacker (teams) with profound knowledge about the **target** and a **long-term infiltration strategy**. Once the target is infiltrated the highest priority is to stay **covert** and **exfiltrate** as much sensible and valuable **data** as possible or to **damage** the target (organization) effectively and sustained. Due to the **high stakes** the attacker(s) will **keep on trying until success**.



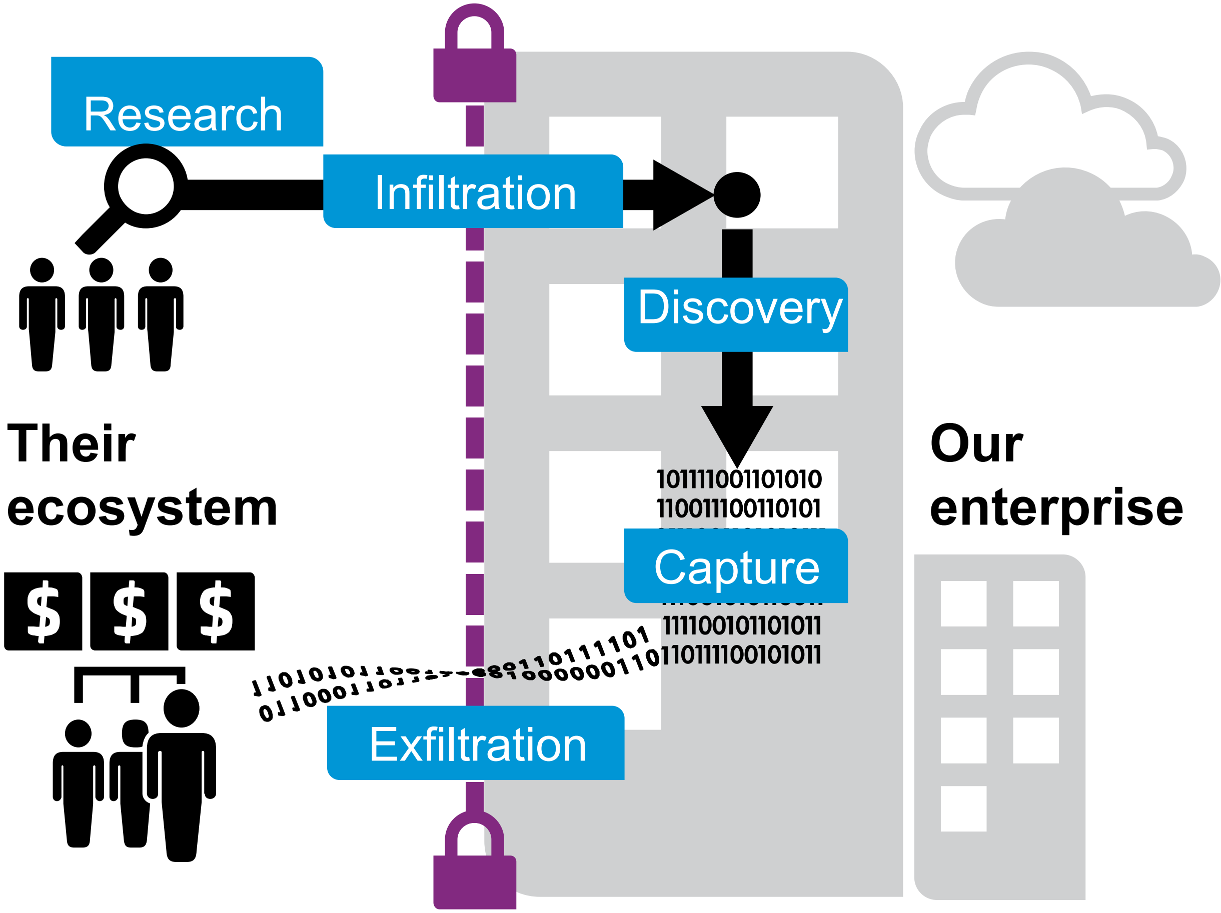
APT - Definition

Advanced Persistent Threat (APT)

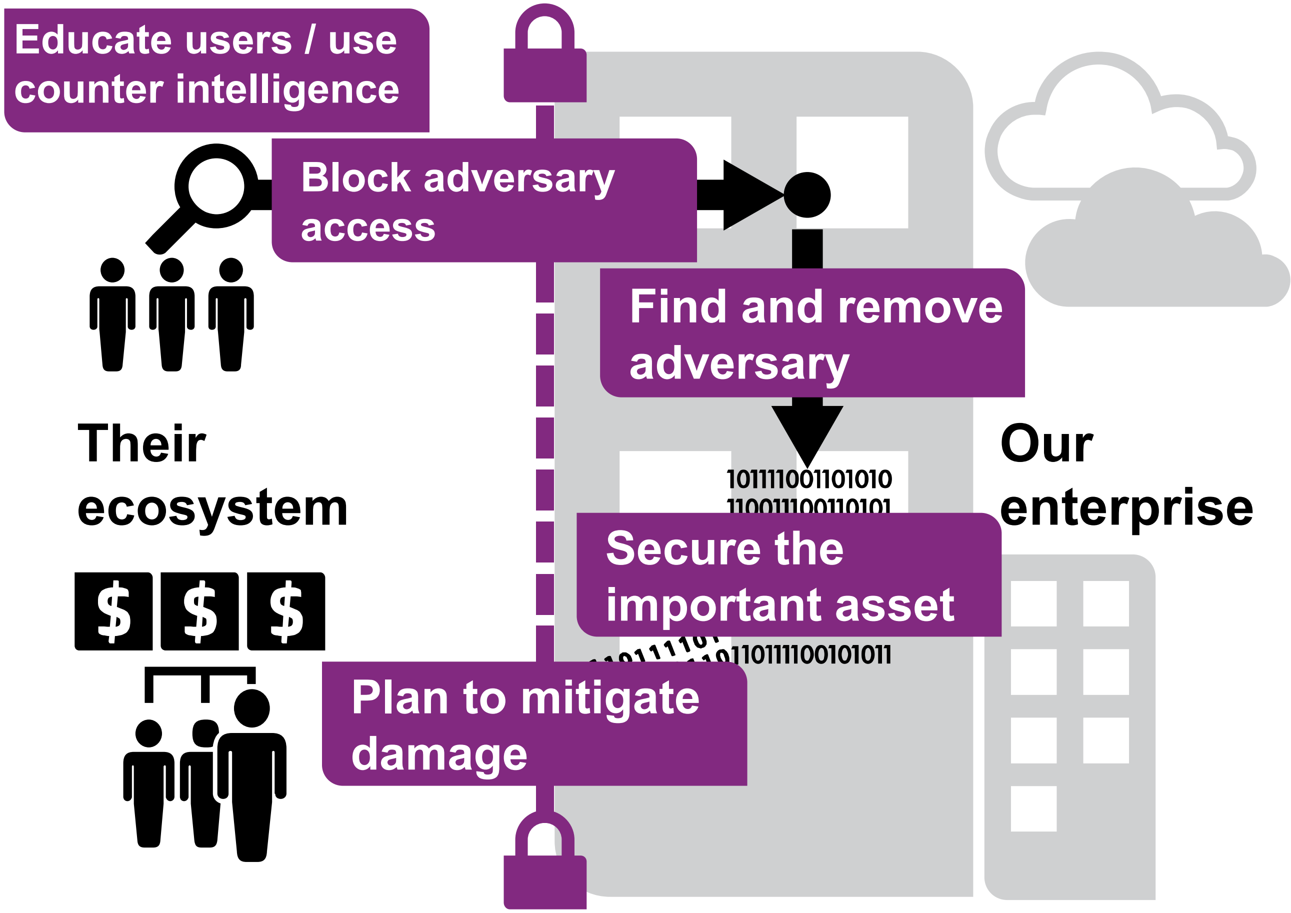
They will keep on trying until they succeed!



The adversary ecosystem



Build capability to disrupt their ecosystem



Educate users / use counter intelligence

Block adversary access

Find and remove adversary

Secure the important asset

Plan to mitigate damage

Their ecosystem

Our enterprise

A new approach is needed

A risk-based, adversary-centric approach

Our strategy is to focus solutions around three areas

1. **Harden** the attack surface

2. **Improve** risk management and response

3. **Proactively protect** information assets

HP addresses three major capability weaknesses:

Harden the attack surface

Identify, improve and reduce the vulnerability profile of enterprise applications and systems

Improve risk remediation

Turn information to intelligence and more quickly see, find and stop known and unknown threats

Proactively protect information

Proactively find, understand and protect sensitive information across the enterprise

HP Enterprise Security Products

HP Security Technology

#1
#2
In all markets where we compete

HP Security SaaS

2.5B lines of code under SaaS subscription

HP ESP Customers

10000+ Customers

900+ Managed Security Services

New Technologies

35 Released in the last 12 months

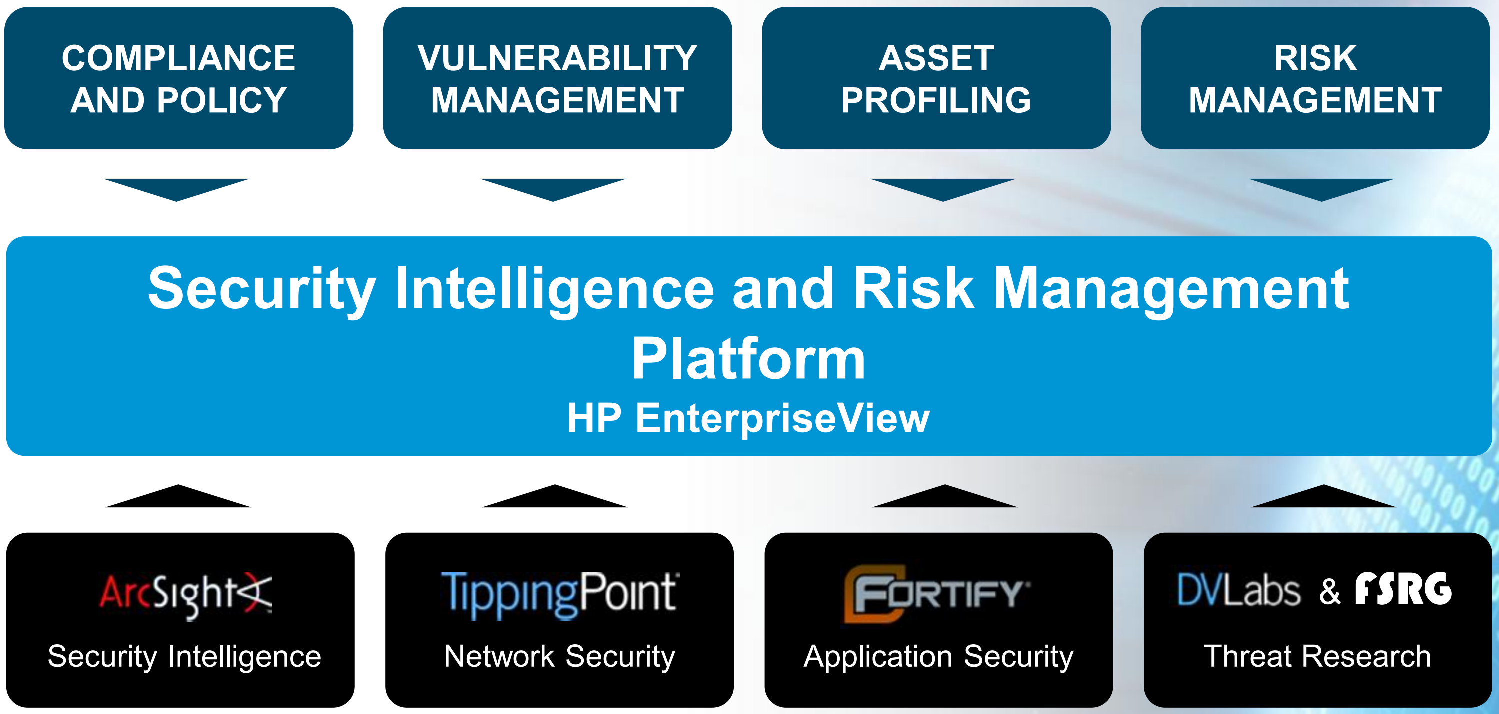
9 out of 10
Major banks

9 out of 10
Top software companies

10 of 10
Top telecoms

All Major Branches
US Department of Defense

A Security Intelligence and Risk Management platform



COMPLIANCE AND POLICY

VULNERABILITY MANAGEMENT

ASSET PROFILING

RISK MANAGEMENT

Security Intelligence and Risk Management Platform

HP EnterpriseView

ArcSight – Security Intelligence

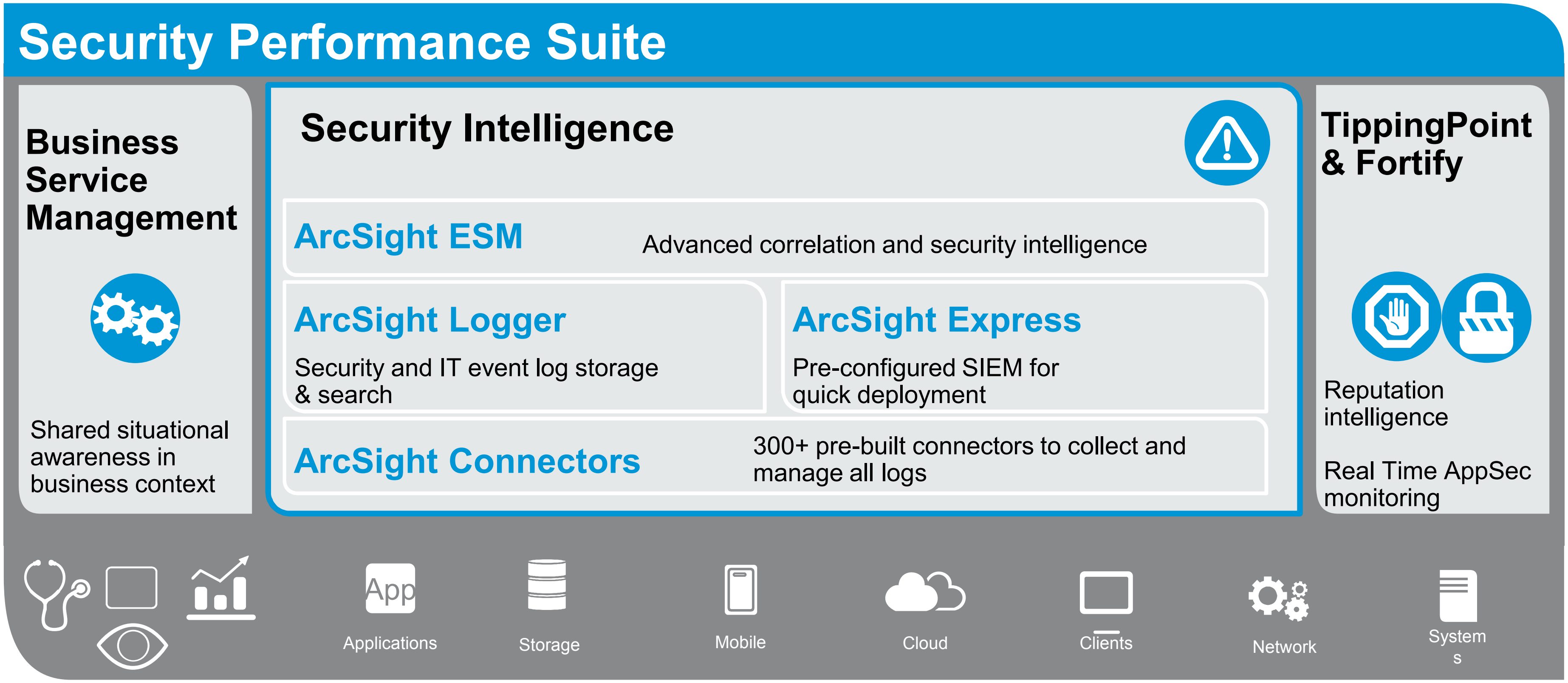
TippingPoint – Network Security

FORTIFY – Application Security

DVLabs & FSRG – Threat Research

Security Intelligence

Proactively detect and respond to threats and compliance breaches



Security Performance Suite

Business Service Management

Shared situational awareness in business context

Security Intelligence

ArcSight ESM Advanced correlation and security intelligence

ArcSight Logger Security and IT event log storage & search

ArcSight Express Pre-configured SIEM for quick deployment

ArcSight Connectors 300+ pre-built connectors to collect and manage all logs

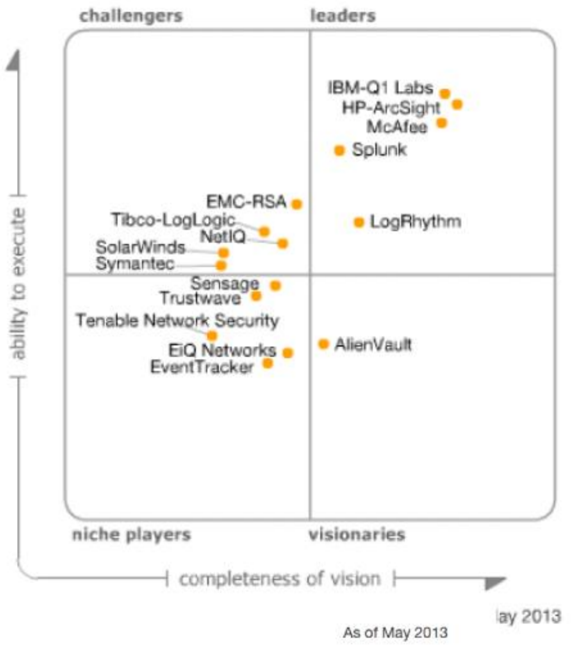
TippingPoint & Fortify

Reputation intelligence

Real Time AppSec monitoring

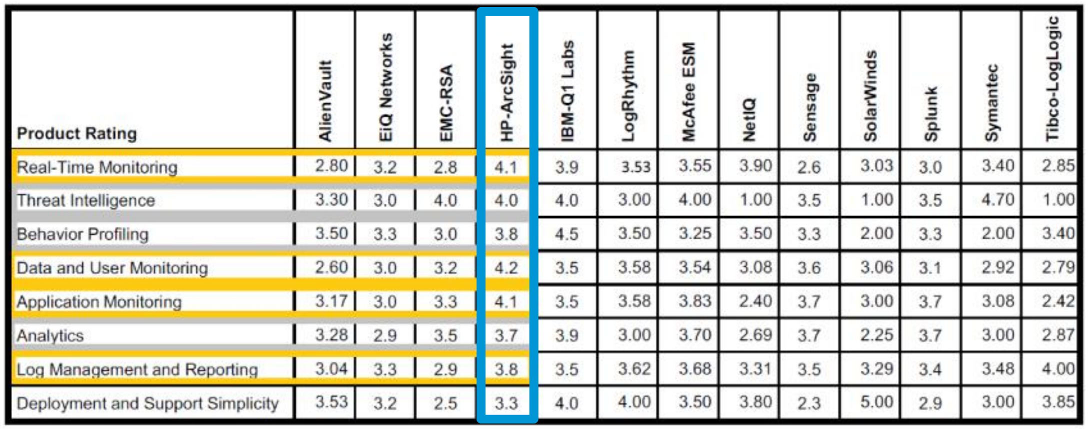
Gartner SIEM MQ 2013

- HP ArcSight has moved **UP and to the RIGHT**
- A **LEADER for 10 consecutive years,** while others have appeared and disappeared
- The **most visionary product** in the Gartner MQ
- Gartner recognizes **HP's vision through ops-analytics**, integrating SIEM and IT Ops
- We are **#1 in 4, #2 in 3** of the 8 categories in meeting customer's SIEM requirements no other vendor is #1 in more than 2 categories



Product Rating on Critical Capabilities

As of May 2013

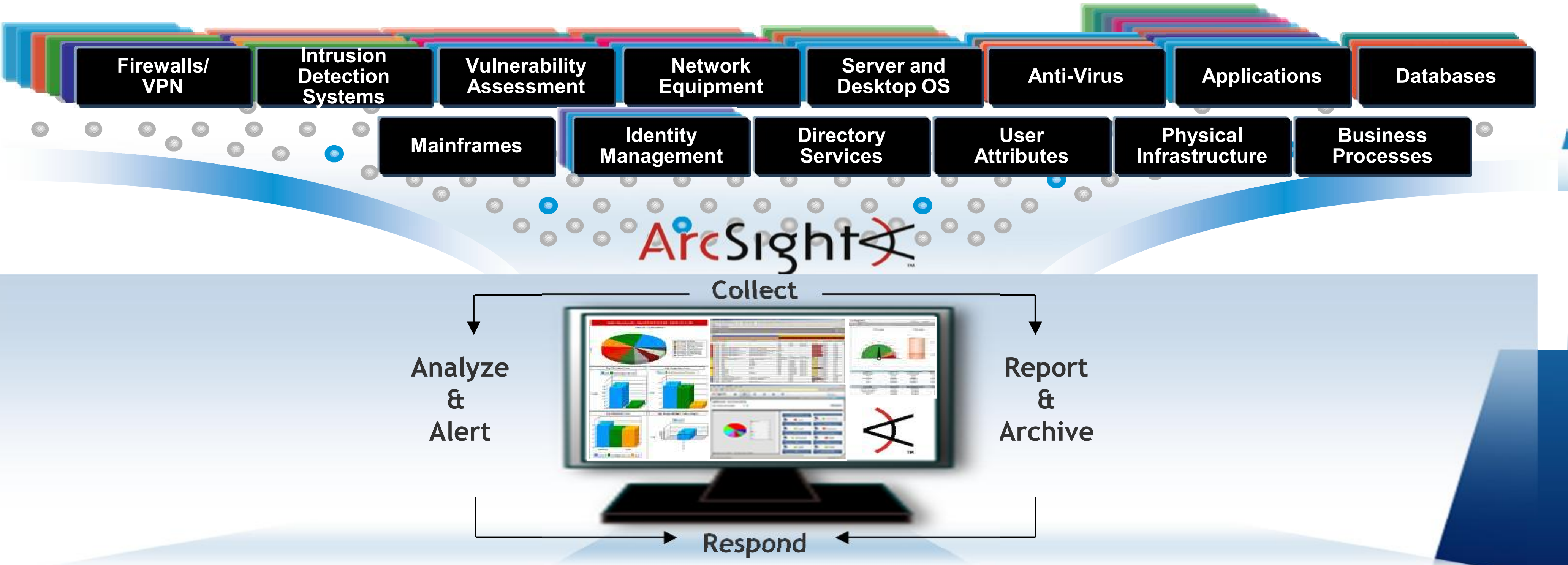


Product Rating	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Real-Time Monitoring	2.80	3.2	2.8	4.1	3.9	3.53	3.55	3.90	2.6	3.03	3.0	3.40	2.85
Threat Intelligence	3.30	3.0	4.0	4.0	4.0	3.00	4.00	1.00	3.5	1.00	3.5	4.70	1.00
Behavior Profiling	3.50	3.3	3.0	3.8	4.5	3.50	3.25	3.50	3.3	2.00	3.3	2.00	3.40
Data and User Monitoring	2.60	3.0	3.2	4.2	3.5	3.58	3.54	3.08	3.6	3.06	3.1	2.92	2.79
Application Monitoring	3.17	3.0	3.3	4.1	3.5	3.58	3.83	2.40	3.7	3.00	3.7	3.08	2.42
Analytics	3.28	2.9	3.5	3.7	3.9	3.00	3.70	2.69	3.7	2.25	3.7	3.00	2.87
Log Management and Reporting	3.04	3.3	2.9	3.8	3.5	3.62	3.68	3.31	3.5	3.29	3.4	3.48	4.00
Deployment and Support Simplicity	3.53	3.2	2.5	3.3	4.0	4.00	3.50	3.80	2.3	5.00	2.9	3.00	3.85

HP/ArcSight

#1	#2

HP ArcSight: Centralized Threat and Risk Management



Firewalls/ VPN

Intrusion Detection Systems

Vulnerability Assessment

Network Equipment

Server and Desktop OS

Anti-Virus

Applications

Databases

Mainframes

Identity Management

Directory Services

User Attributes

Physical Infrastructure

Business Processes

ArcSight

Collect

Analyze & Alert

Report & Archive

Respond

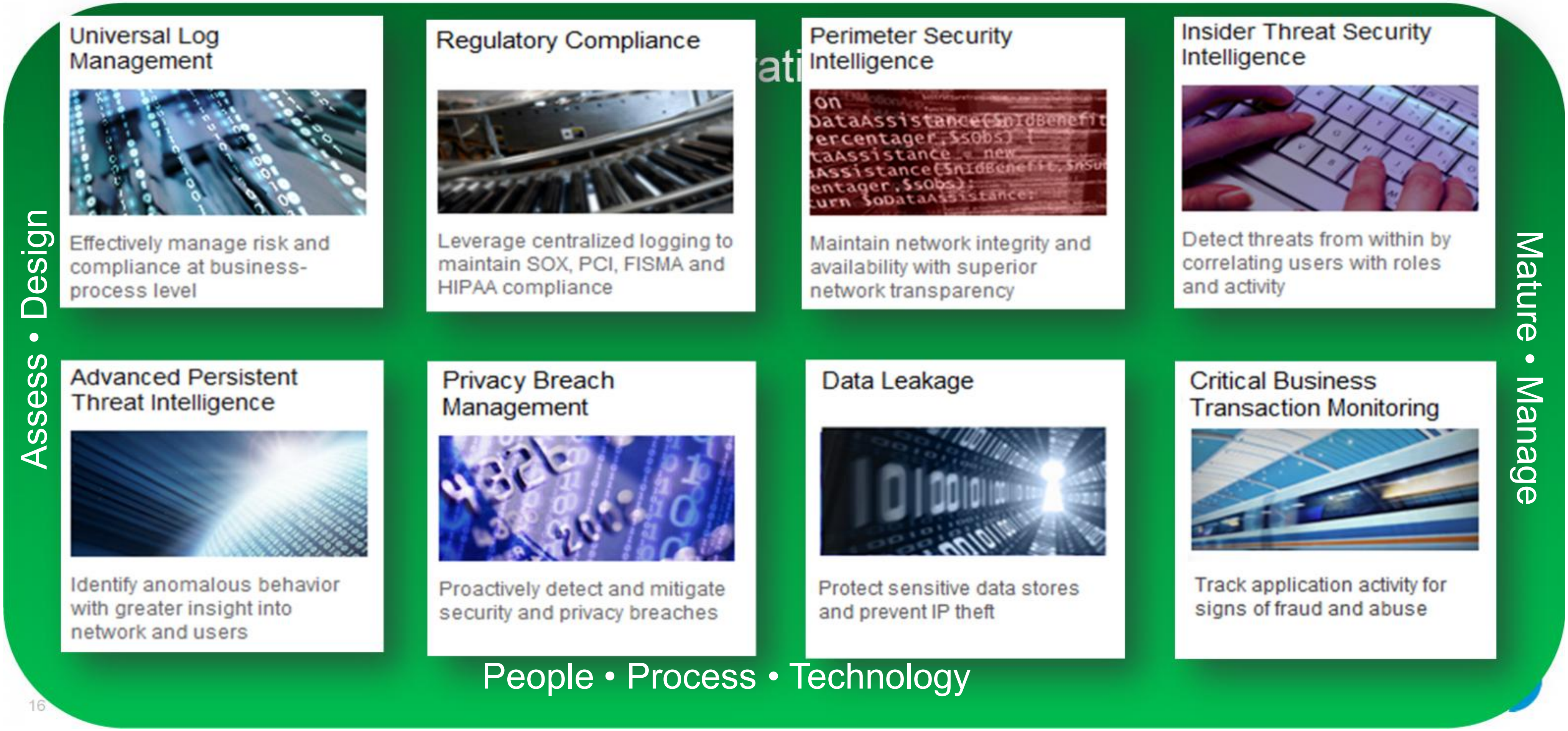
Address… Security Threats

Monitor… Compliance Controls

Ensure… Business Continuity

Security Intelligence Solutions

*A **Use Case Approach** to Solving Common Business Challenges*



Assess • Design

Universal Log Management

Effectively manage risk and compliance at business-process level

Regulatory Compliance

Leverage centralized logging to maintain SOX, PCI, FISMA and HIPAA compliance

Perimeter Security Intelligence

Maintain network integrity and availability with superior network transparency

Insider Threat Security Intelligence

Detect threats from within by correlating users with roles and activity

Advanced Persistent Threat Intelligence

Identify anomalous behavior with greater insight into network and users

Privacy Breach Management

Proactively detect and mitigate security and privacy breaches

Data Leakage

Protect sensitive data stores and prevent IP theft

Critical Business Transaction Monitoring

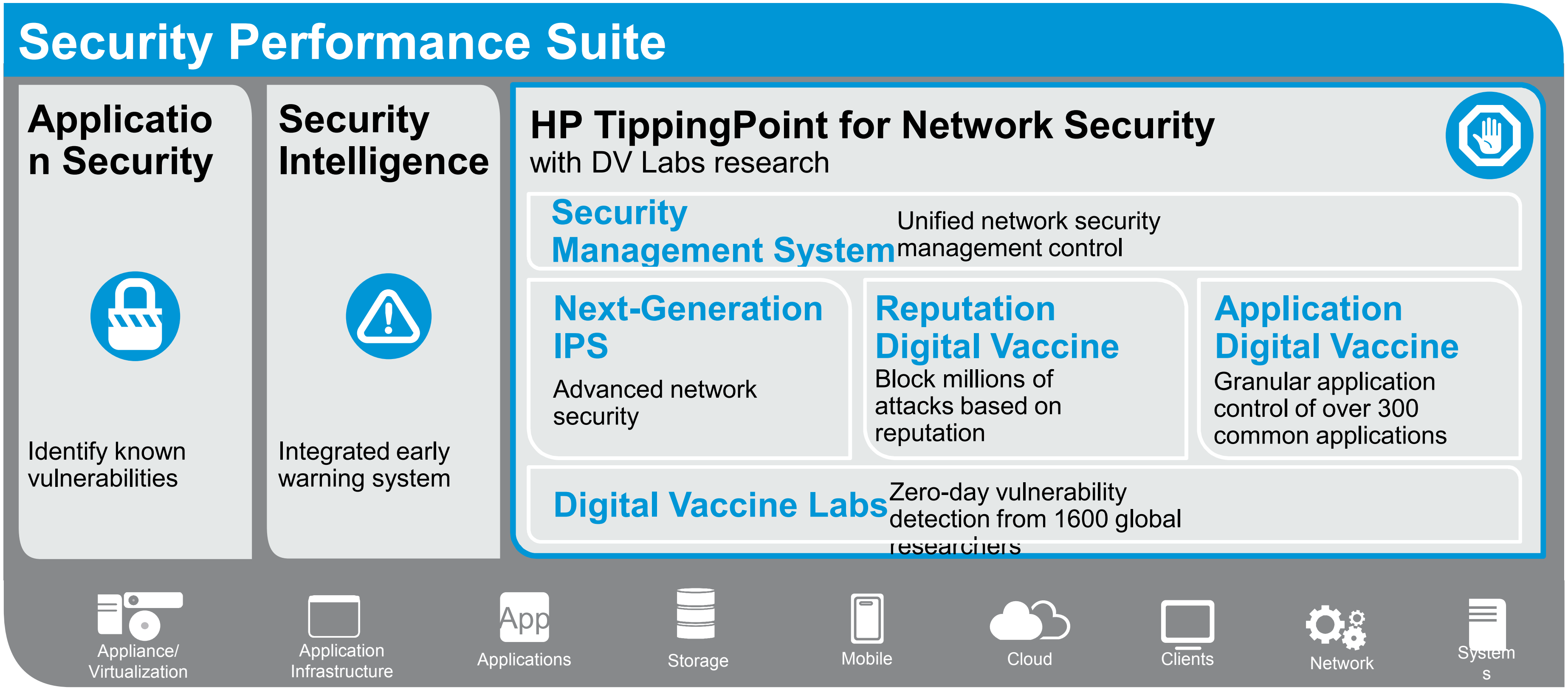
Track application activity for signs of fraud and abuse

Mature • Manage

People • Process • Technology

Network Security

Proactive next generation network security



Security Performance Suite

Application Security

Identify known vulnerabilities

Security Intelligence

Integrated early warning system

HP TippingPoint for Network Security

with DV Labs research

Security Management System Unified network security management control

Next-Generation IPS
Advanced network security

Reputation Digital Vaccine
Block millions of attacks based on reputation

Application Digital Vaccine
Granular application control of over 300 common applications

Digital Vaccine Labs Zero-day vulnerability detection from 1600 global researchers

Introducing the NX Platform NGIPS

Advanced Protection Against Advanced Threats

- Highest Port Density available on the market today
  - 24 x 1G segments
  - 16 x 10G segments
  - 4 x 40G segments
- Improved performance capabilities
- Swappable I/O modules
- Multiple performance options (3Gbps to 20Gbps)
- Installs quickly for seamless in-line threat protection
- Supports multiple security services:
  - Reputation Digital Vaccine
  - Web Application Digital Vaccine
  - Application Digital Vaccine
  - DV Toolkit
  - ThreatlLinQ portal

HP TippingPoint NX Series

Agile NGIPS Adapts to Prevent Future Attacks

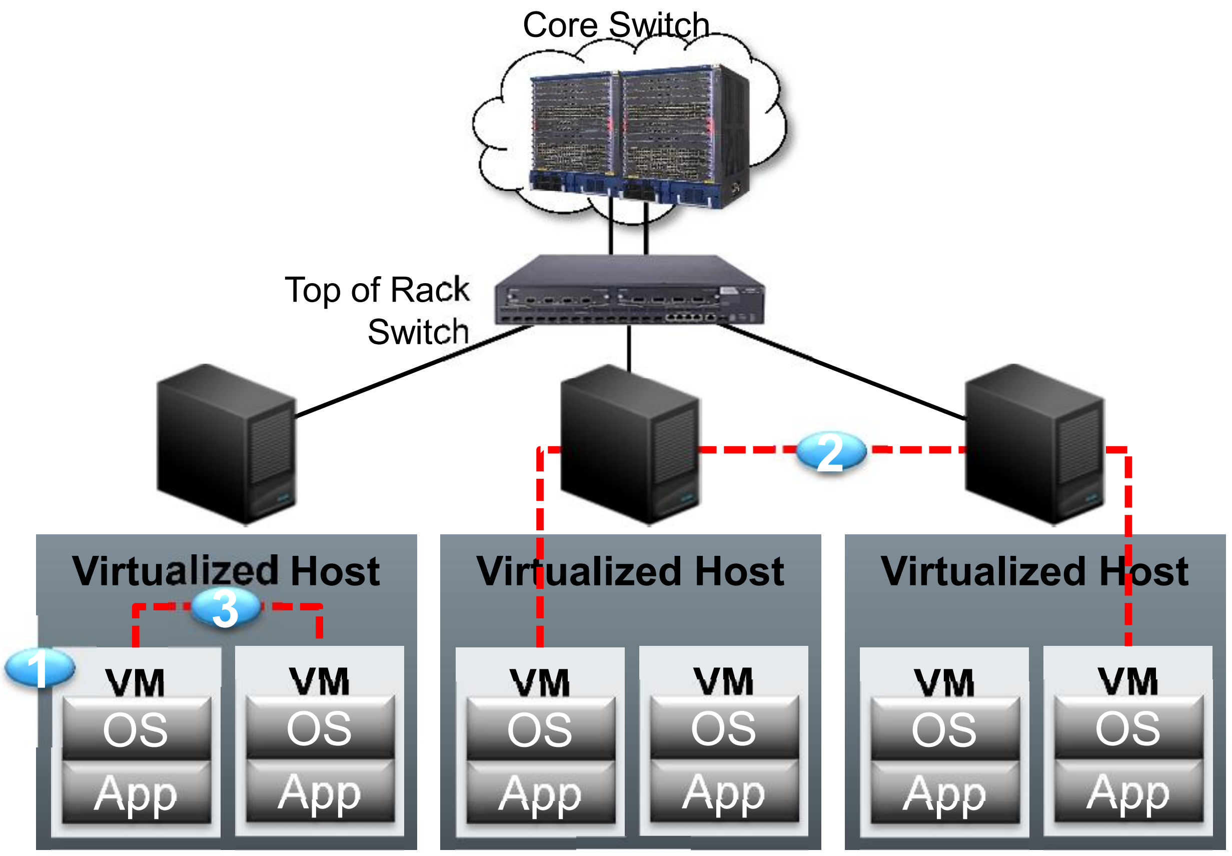
The Virtual Network Visibility Gap

1
- **Hypervisor Security**
  - Are mission critical
  - Can’t be secured with virtual IPS
  - Patches must be immediate

2
- **Host to Host Threats**
  - Can’t deploy IPS in front of every server
  - Also Need VM to Host security

3
- **VM to VM Threats**
  - Virtual trust zones
  - Traffic does not enter the physical network for inspection
  - A victim VM can attack other VMs

4
- **VM Mobility**
  - vMotion launches VMs in separate sites for DR or other purposes
  - Physical IPS options are cost prohibitive for these uses



4 **VMs moved to separate site**

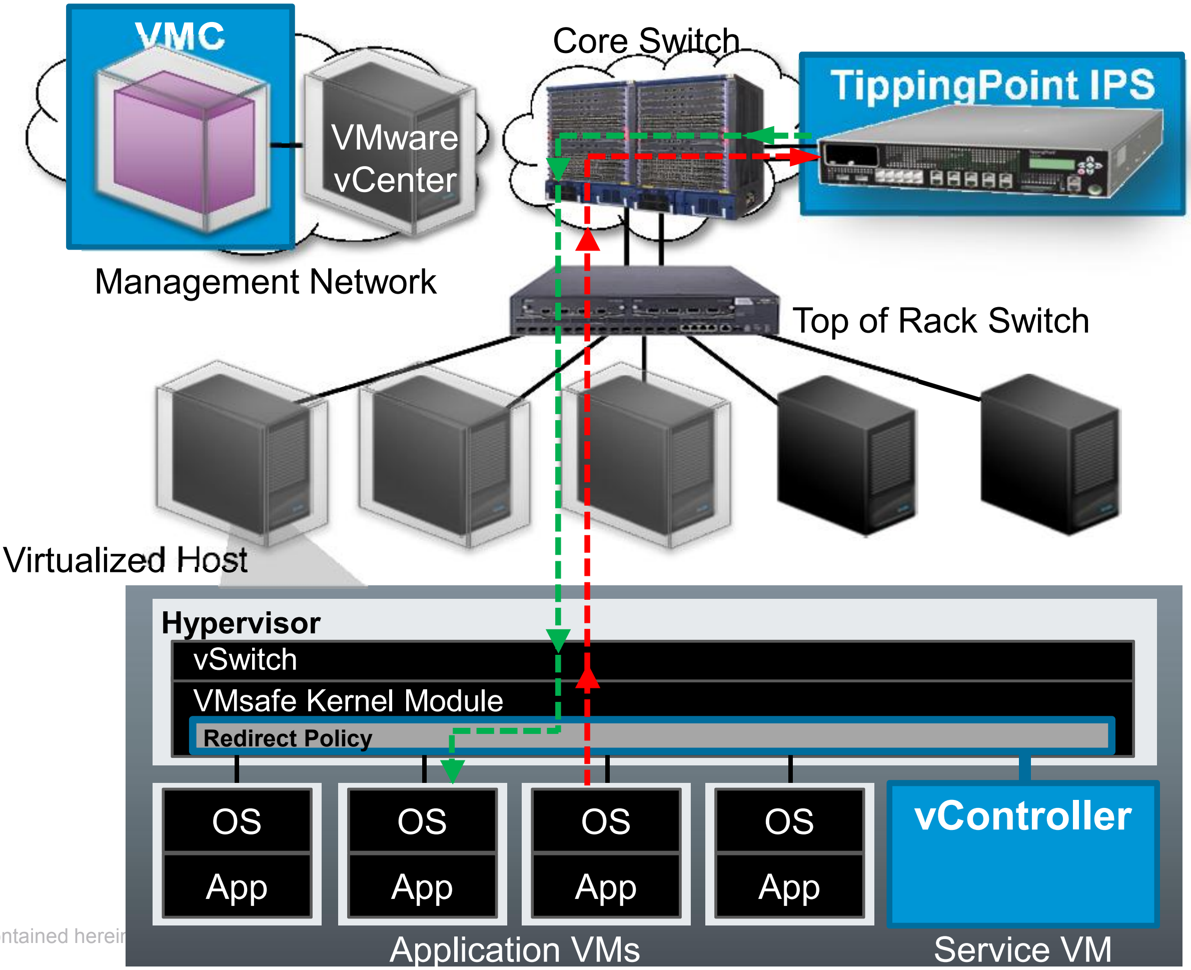
Secure Virtualization FrameWork (SVF)

- **What's Included**
  - IPS Platform
  - Virtual Controller (vController)
  - SMS / Virtual Management Center (vMC)

- **Securing Virtualization DC security solution**
  - Single, purpose-built DC security solution

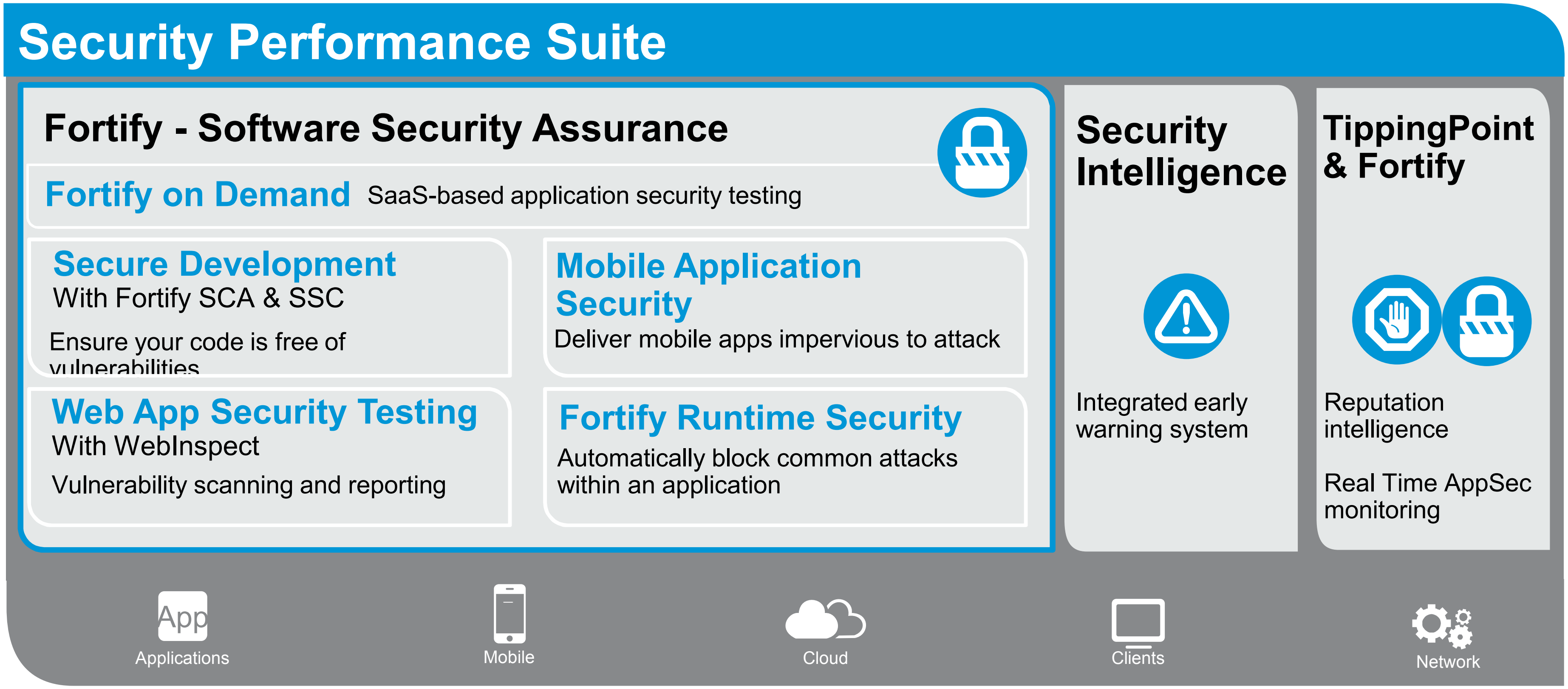
- **Extend IPS solution into the virtual DC**
  - Leverage previous IPS investments

- **Flexibly Inspect Data in Both the Physical and Virtual DC**



Application Security

Mitigate security risk posed by weak & vulnerable software



Security Performance Suite

Fortify - Software Security Assurance

Fortify on Demand SaaS-based application security testing

Secure Development
With Fortify SCA & SSC
Ensure your code is free of vulnerabilities

Mobile Application Security
Deliver mobile apps impervious to attack

Web App Security Testing
With WebInspect
Vulnerability scanning and reporting

Fortify Runtime Security
Automatically block common attacks within an application

Security Intelligence

Integrated early warning system

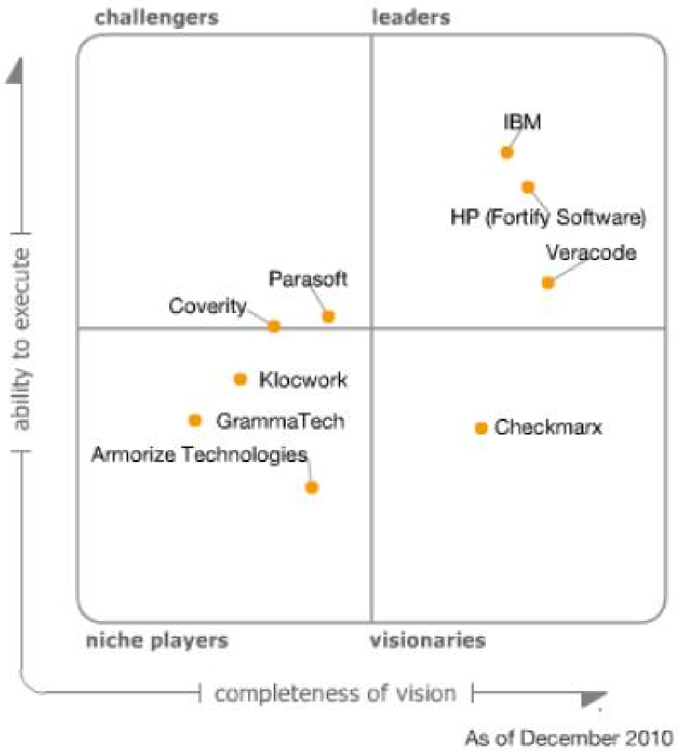
TippingPoint & Fortify

Reputation intelligence

Real Time AppSec monitoring

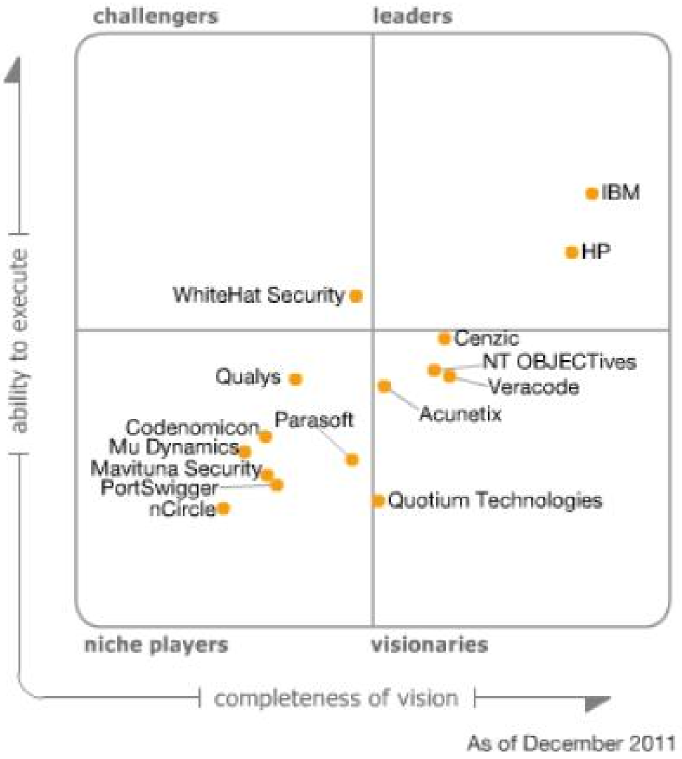
Fortify Competitive Position

Static Analysis MQ



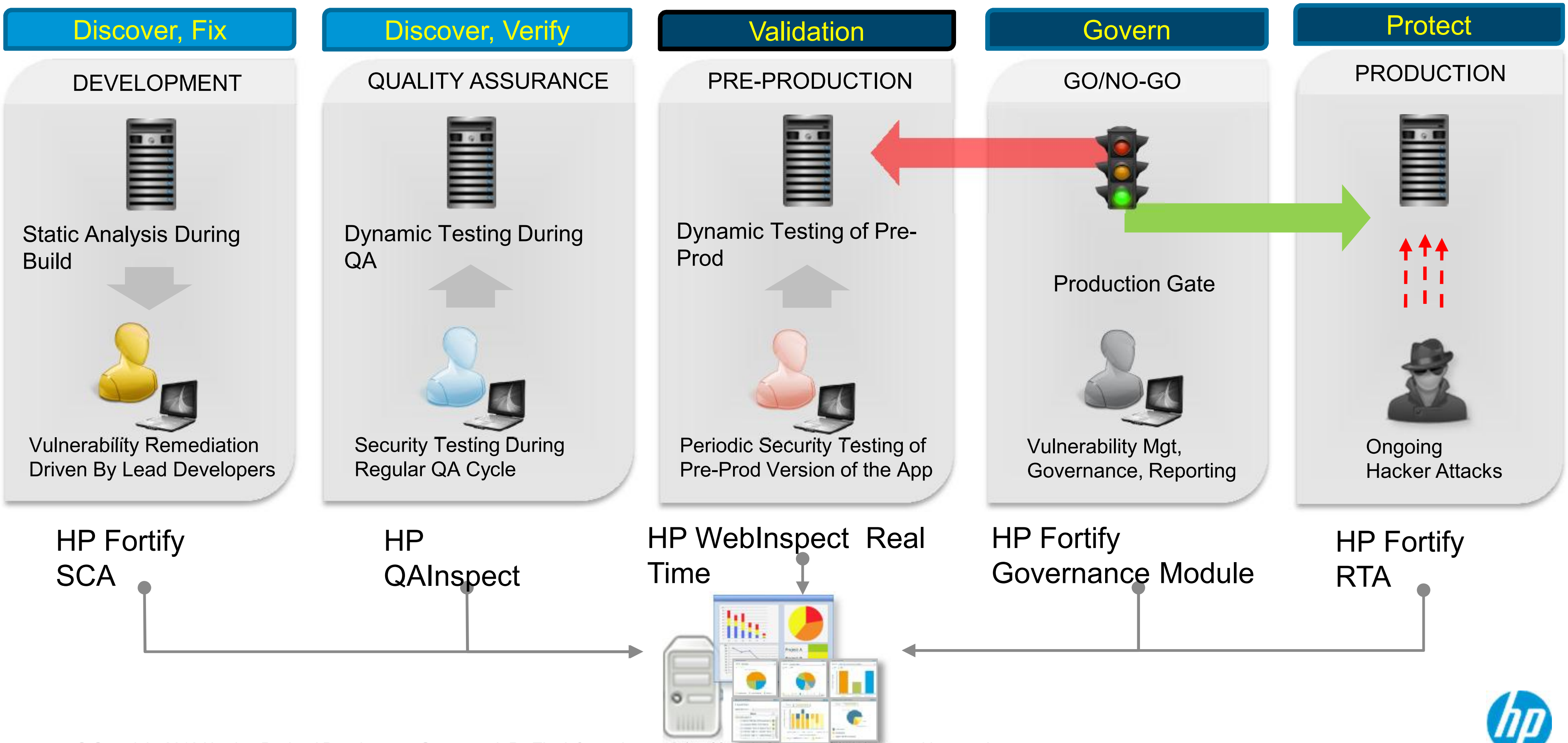
As of December 2010

Dynamic Analysis MQ



As of December 2011

Secure Software Assessment Technologies



Discover, Fix

DEVELOPMENT

Static Analysis During Build

Vulnerability Remediation Driven By Lead Developers

HP Fortify SCA

Discover, Verify

QUALITY ASSURANCE

Dynamic Testing During QA

Security Testing During Regular QA Cycle

HP QAInspect

Validation

PRE-PRODUCTION

Dynamic Testing of Pre-Prod

Periodic Security Testing of Pre-Prod Version of the App

HP WebInspect Real Time

Govern

GO/NO-GO

Production Gate

Vulnerability Mgt, Governance, Reporting

HP Fortify Governance Module

Protect

PRODUCTION

Ongoing Hacker Attacks

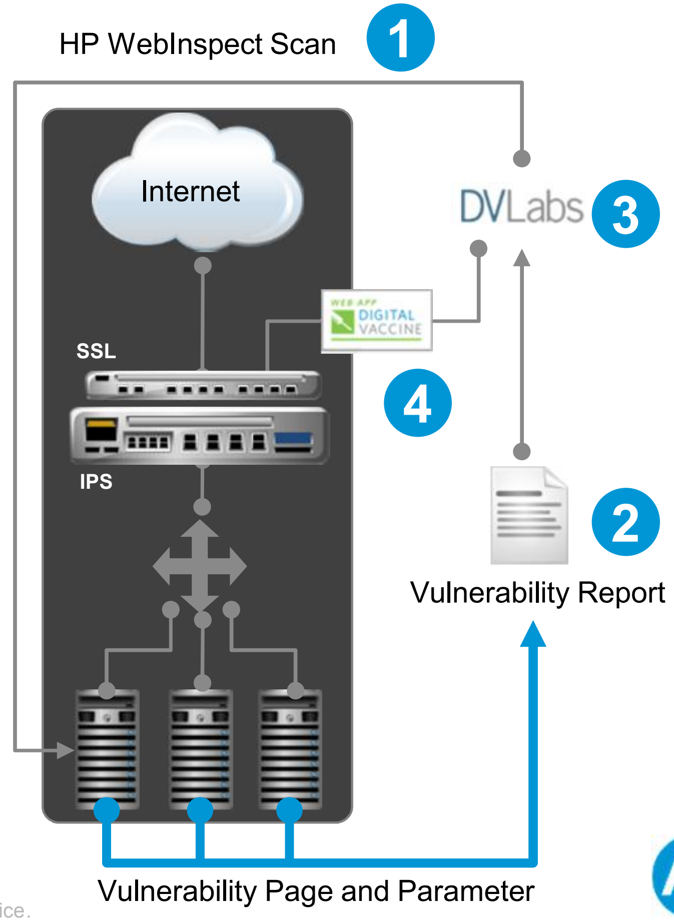
HP Fortify RTA

HP Software Security Centre

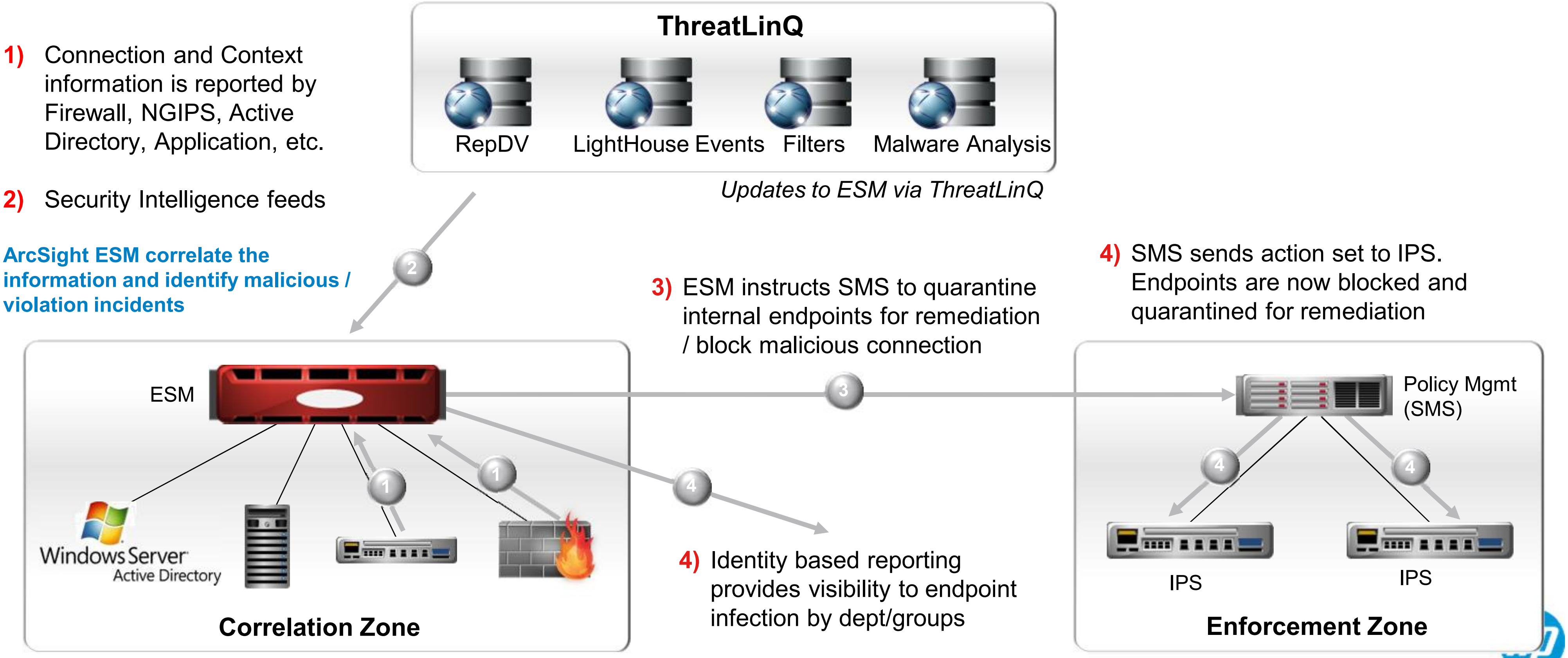
Proactive Web Application Protection

How does it work?

1. **HP WebInspect scans for potential security risks**
2. **Assess vulnerability threat report**
3. **Create customized application protection filters**
4. **Manage exposure with TippingPoint IPS**



Proactive Attack Remediation



1) Connection and Context information is reported by Firewall, NGIPS, Active Directory, Application, etc.

2) Security Intelligence feeds

ArcSight ESM correlate the information and identify malicious / violation incidents

3) ESM instructs SMS to quarantine internal endpoints for remediation / block malicious connection

4) SMS sends action set to IPS. Endpoints are now blocked and quarantined for remediation

4) Identity based reporting provides visibility to endpoint infection by dept/groups

Updates to ESM via ThreatLinQ

Reputation-based Threat Intelligence

HP Reputation Security Monitor (RepSM)

What does it provide?

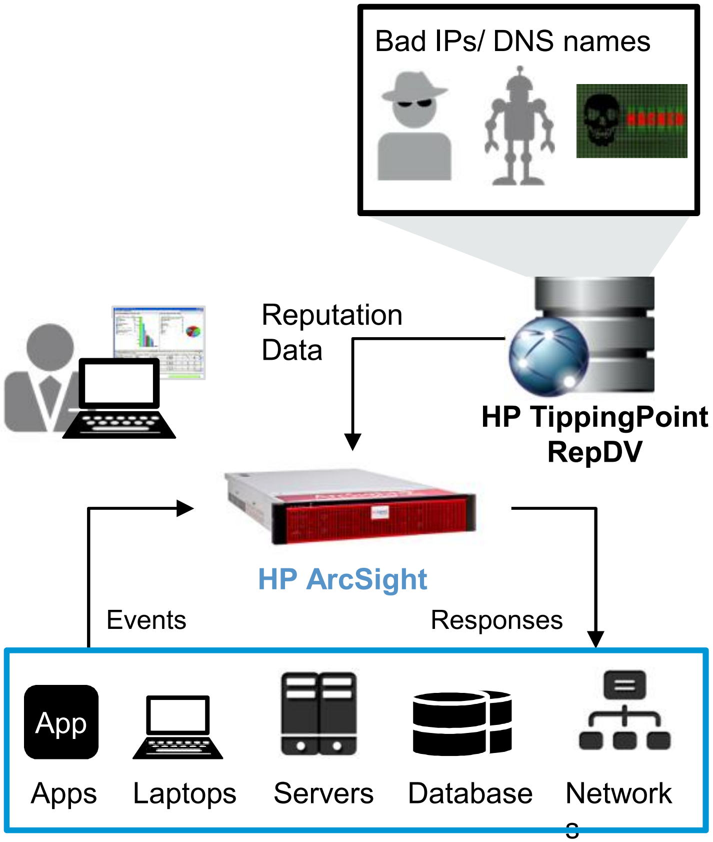
- Enables Security Operations to leverage global threat intelligence to detect and protect against APTs

Features

- Submissions from global security community
- Intelligence fed to SIEM for real-time correlation
- Active response taken in response to malicious activity
- Detects and prioritizes advanced persistent threats (APTs) through correlation of suspicious enterprise-wide activity
- Enables security operations to respond to unknown attacks with manual or automated actions

Customer Benefits

- Identifies APTs that go undetected by signature-based security controls
- Enables security operations to respond to unknown attacks with manual or automated actions
- Improves efficiency of SOC, by reducing false-positives using correlation



Thank You!

jneo@hp.com , +65 9177 3397