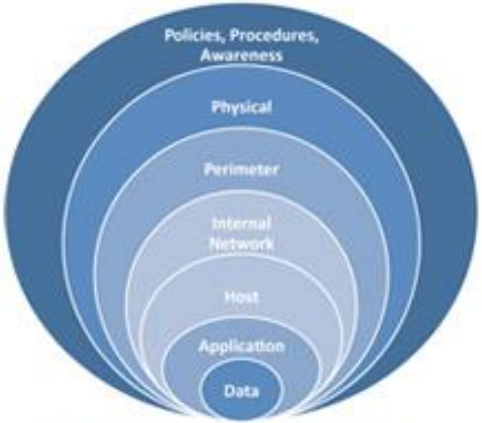
Managing Risk
Through Visibility

Arun George CISSP, CISM, CRISC, ITIL- F, 7799LA
Regional Manager – Solution Architects
Middle East, Mediterranean & Africa
Enterprise Security Group

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Best Practices in Security Architecture

- **Defense in Depth**



Layers of Defense in Depth

- **Multi-layer Security**
  - Perimeter Firewall & Core Firewall
  - Gateway Antivirus & desktop antivirus
  - Double authentication

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Back to the Basics

Risk = Asset value x Vulnerability x Threat/Exploit

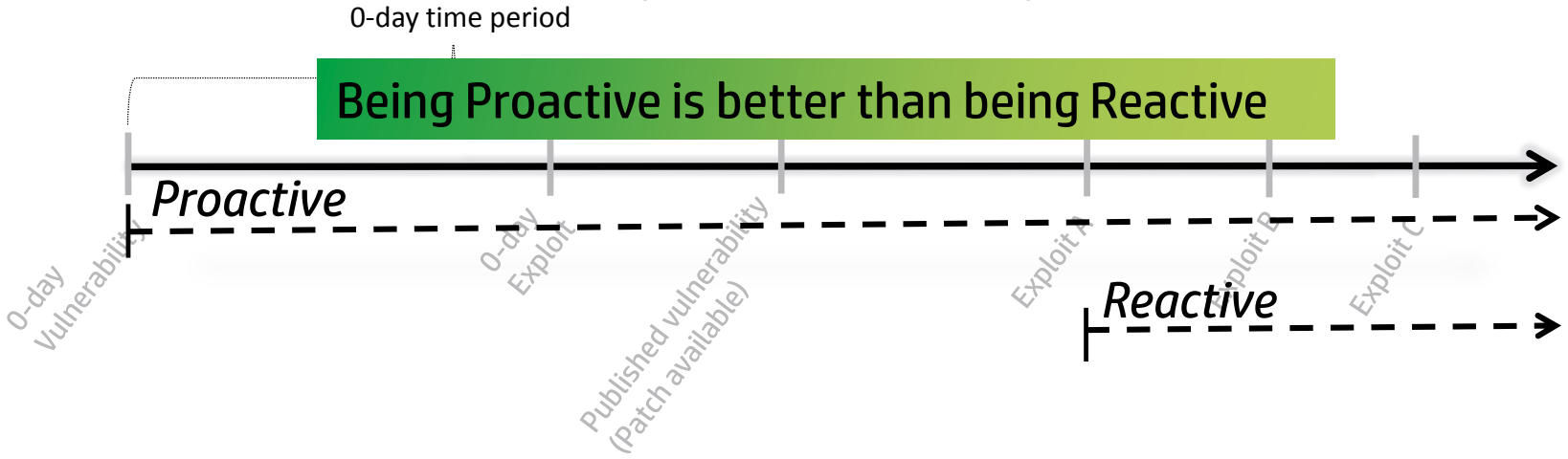
Term	Definition
Vulnerability	**Security flaw in a software program**
Exploit	**Attack on a vulnerability to:** • Gain unauthorized access • Create a denial of service

On a timeline plot, Vulnerability comes first. Exploit is released to abuse an already existing vulnerability.

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

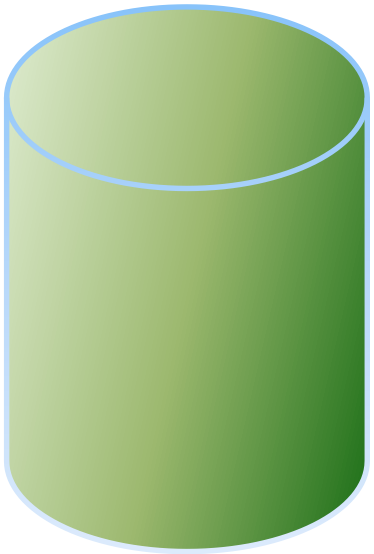
Attack Timeline

1) Vulnerability is discovered first, exploits are released later
2) Ratio of (Vulnerability: Exploits) is always (1:n), where n>1



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Classifying Security Technologies



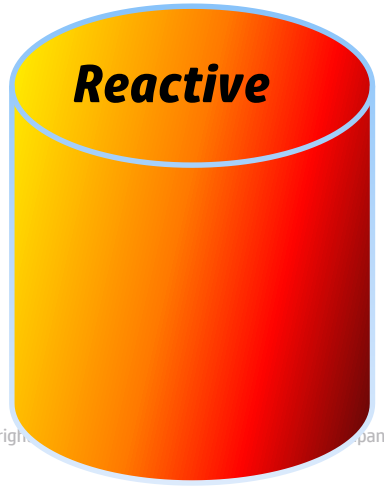
Luxury

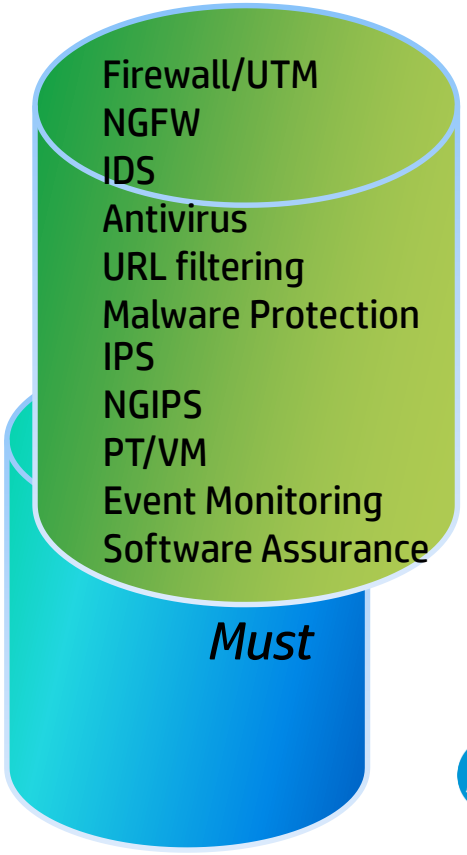
Firewall/UTM
NGFW
IDS
Antivirus
URL filtering
Malware Protection
IPS
NGIPS
PT/VM
Event monitoring
Software Assurance
SSO
IPAM

Must

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Classifying Security Technologies





© Copyrigh pany, L.P. The information contained herein is subject to change without notice.

HP Enterprise Security Products (ESP)

Market leading products and services

- Security Information and Event Management
- Log Management
- Application Security
- Network Security
- Data Protection
- Threat Research
- Security Services

One Team, One Vision

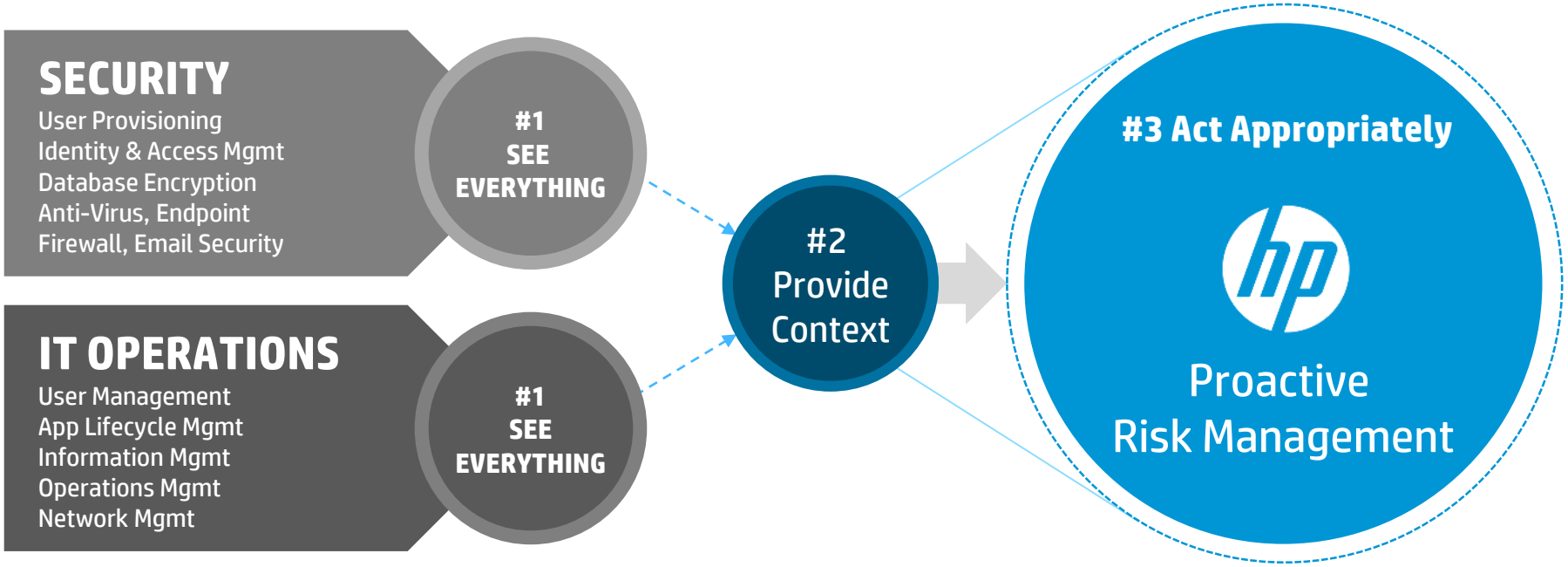
TippingPoint
DVLabs
ArcSight
VISTORM
FORTIFY
SPI DYNAMICS
secure. protect. inspect.
ATALLA

- **1,400 security professionals from ArcSight, Fortify and TippingPoint teams**
- **1,500 security professionals in HP Enterprise Security Services**
- **Top three security company by market share (leader in SIEM, Log Mgt, AppSec, Network Security)**

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

We need a new way to reduce risk

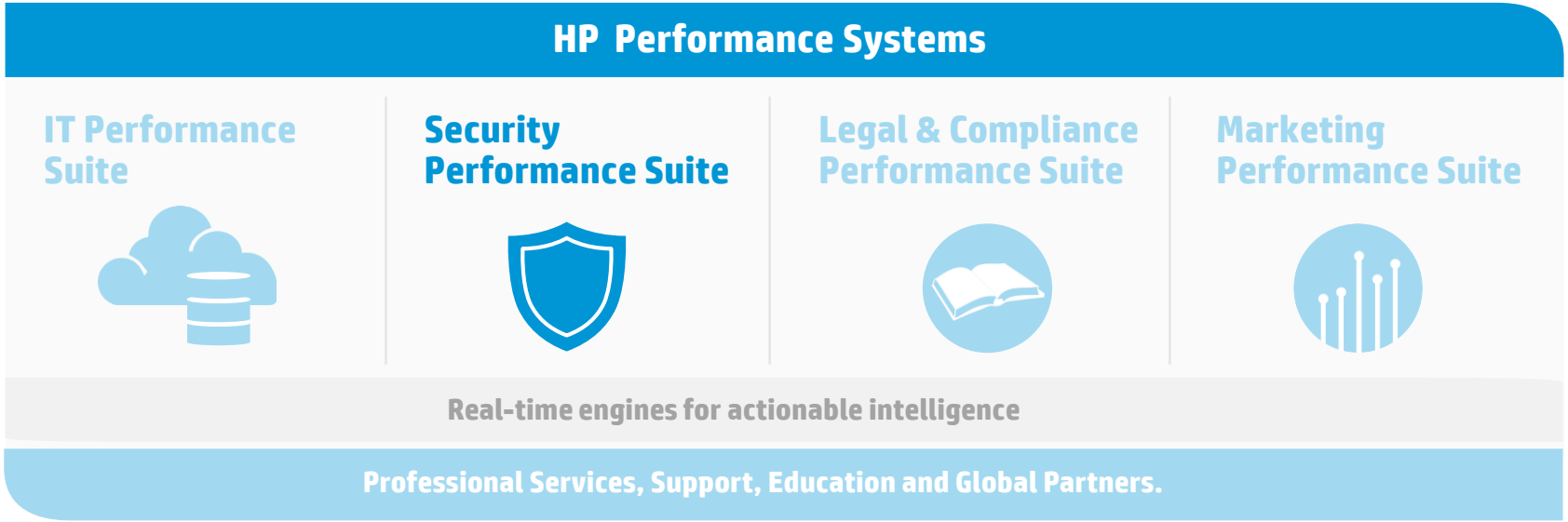
Proactive Risk Reduction



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Performance Systems

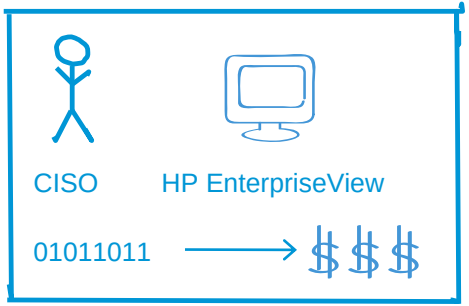
HP ESP – Where we fit



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Security Performance Suite

Risk ↓
Dev Costs ↓
Revenue ↑



Harden

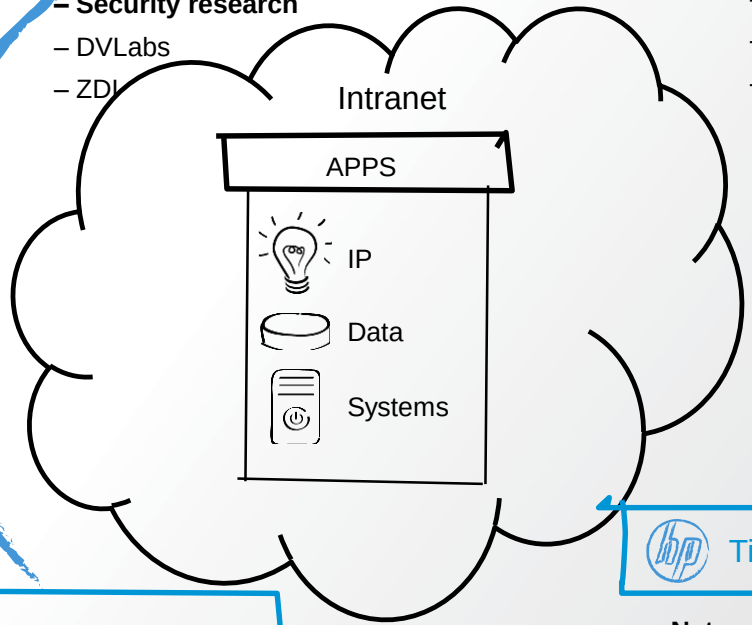
Intelligence

Protect

HP ESP

HPSR
- **Security research**
- DVLabs
- ZDI

Fortify
- **Application security**
- Vulnerabilities
- Development



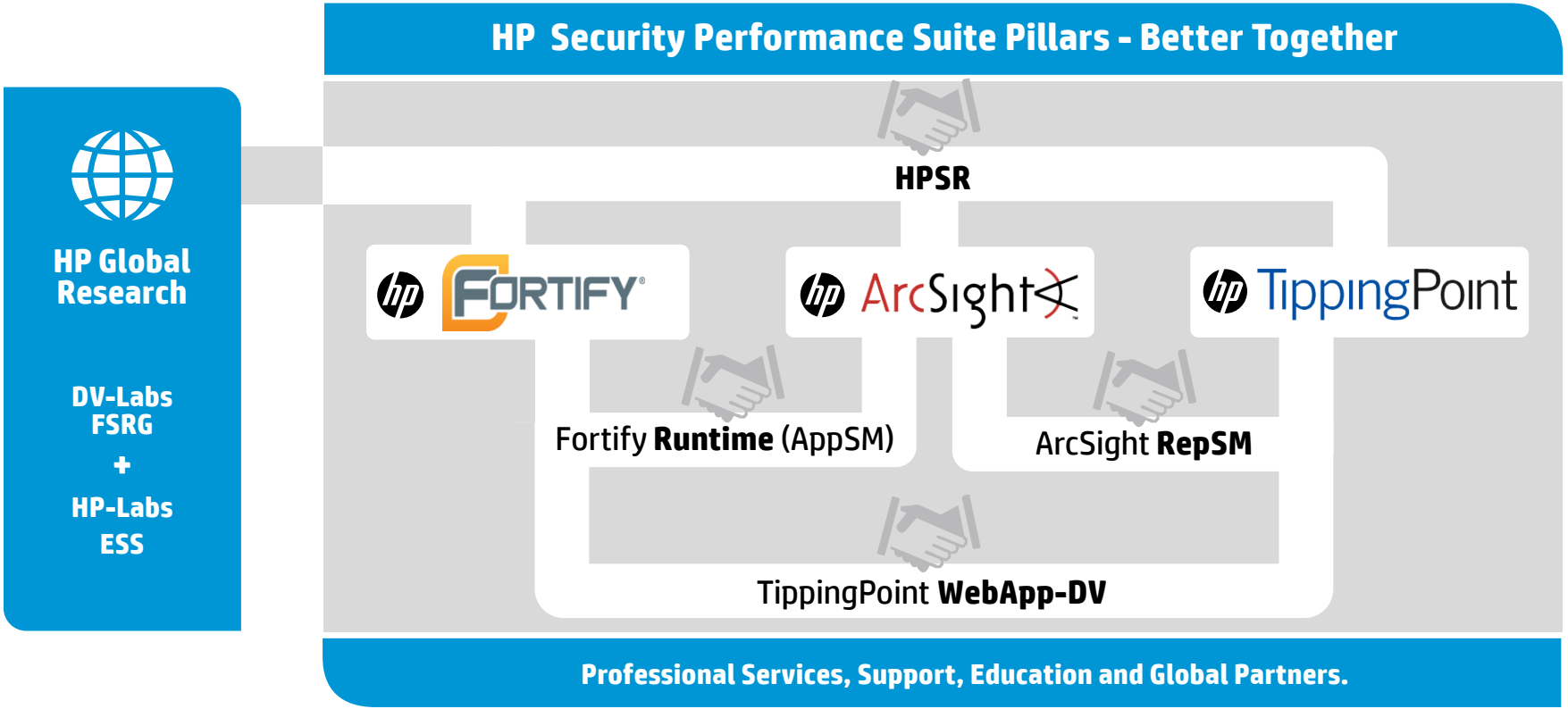
TippingPoint
- **Network Security**
- Scalable
- Predictive

ArcSight
- **Security Intelligence**
- Analyze
- Respond

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Better Together – Intra ESP

Security Performance Suite



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Web Application Protection

Adaptive Web Application Firewall (WAF) technology

What does it provide?

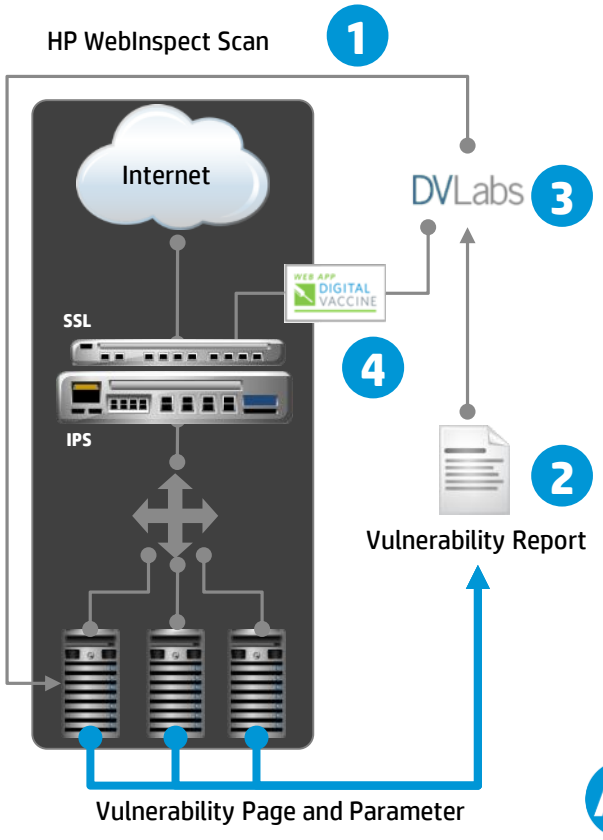
- Advanced web application scanning to uncover vulnerabilities combined with adaptive IPS response
- WebInspect information passed to WebAppDV to auto-generate IPS filters for virtual vulnerability patch

Features

- Inspection of encrypted and non-encrypted traffic (ideal for web commerce apps)
- Detailed vulnerability report of web applications
- Quick activation of vulnerability filters

Customer benefits

- Protection for custom and commercial web applications
- Elimination of tuning required by legacy WAFs



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Runtime Application Security

HP Application Security Monitor (AppSM)

What does it provide?

- Detection of standard threats quickly integrated with HP ArcSight ESM

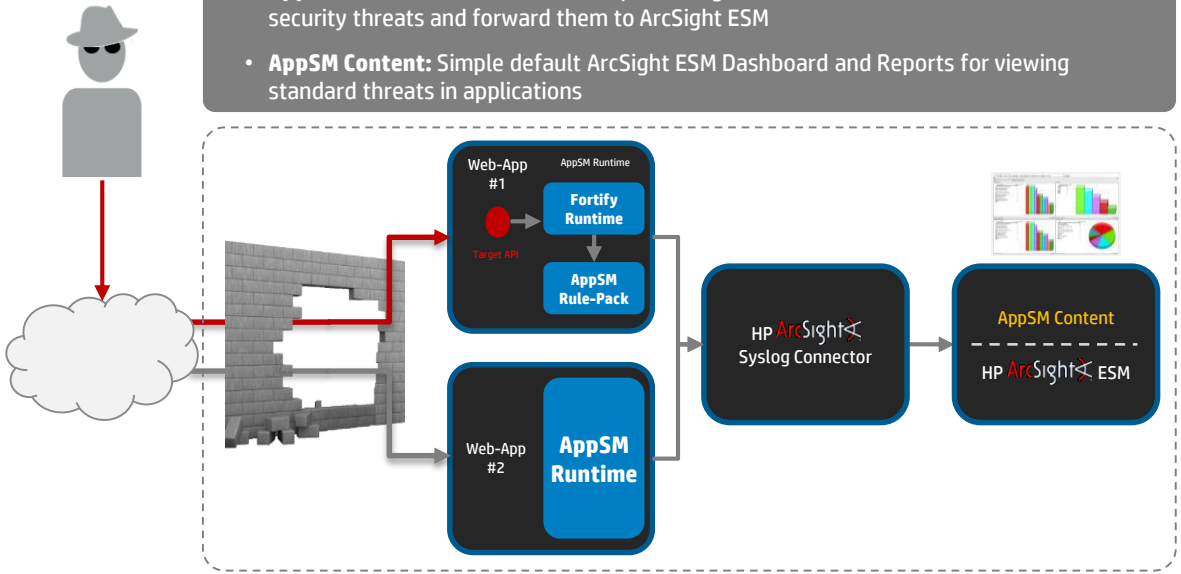
Features

- Malicious user behavior detected
- Events sent to real-time correlation engine
- Active response taken

Customer benefits

- Application monitoring for applications not instrumented to create security logs
- Leverage ESM investment to receive additional threat intelligence
- Default RTA rules pre-configured in connector

- **AppSM Runtime**: Default RTA rules pre-configured in connector to detect “standard” security threats and forward them to ArcSight ESM
- **AppSM Content:** Simple default ArcSight ESM Dashboard and Reports for viewing standard threats in applications



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Reputation-based Threat Intelligence

HP Reputation Security Monitor (RepSM)

What does it provide?

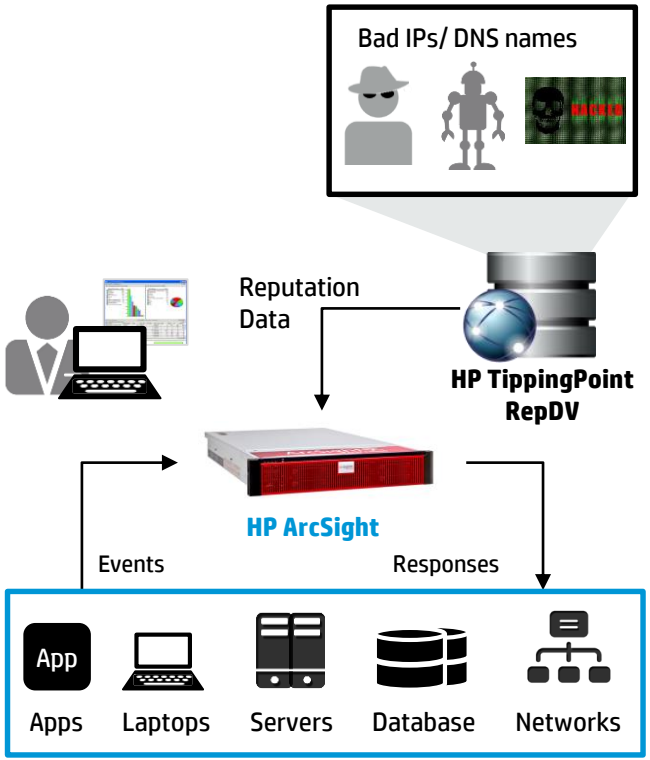
- Enables Security Operations to leverage global threat intelligence to detect and protect against APTs

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

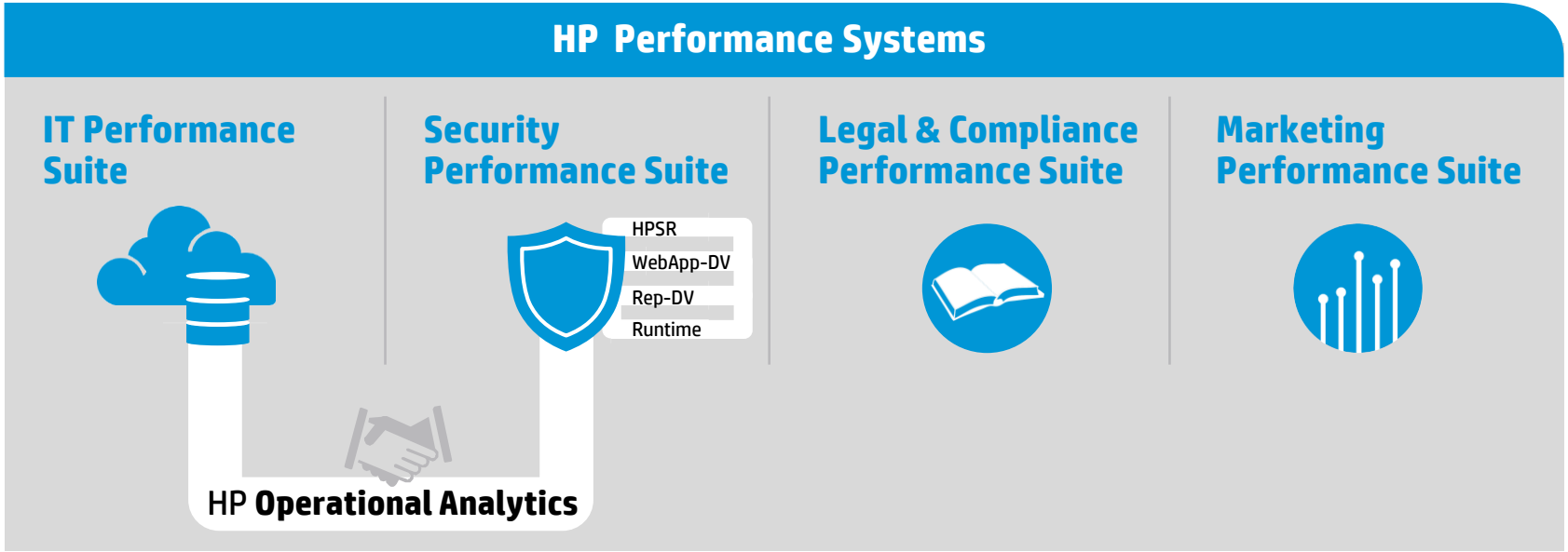
Customer Benefits

- 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



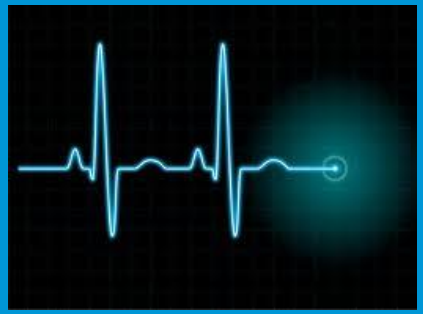
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Better Together – Inter ESP



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Event triage and Correlation



Log Management

Operational Analytics

Understand the health and performance of IT

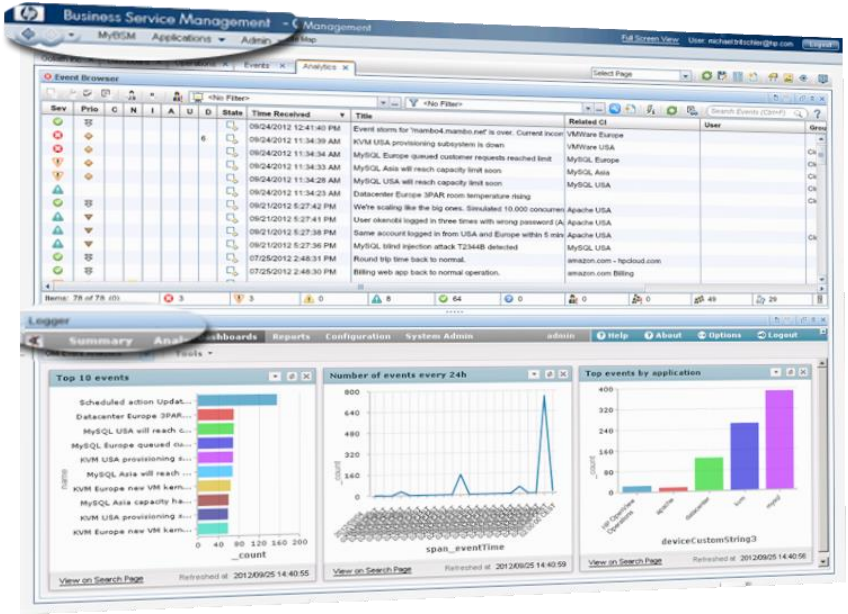
Understand logs and raw data across IT

Better insight and business context

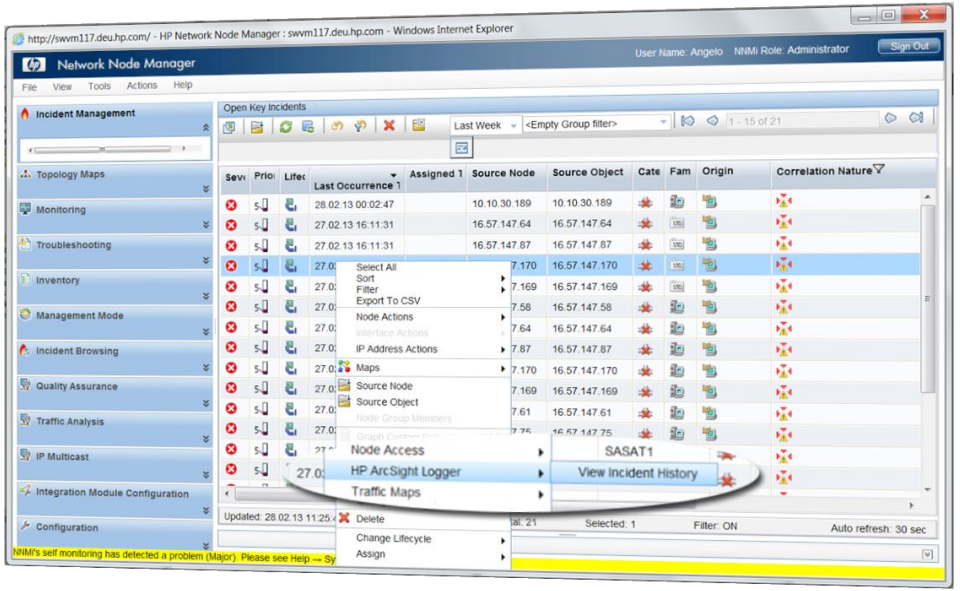
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Event Analytics: Insight from the logs and events

‘Mine’ the historical events and logs for patterns, resolutions etc.



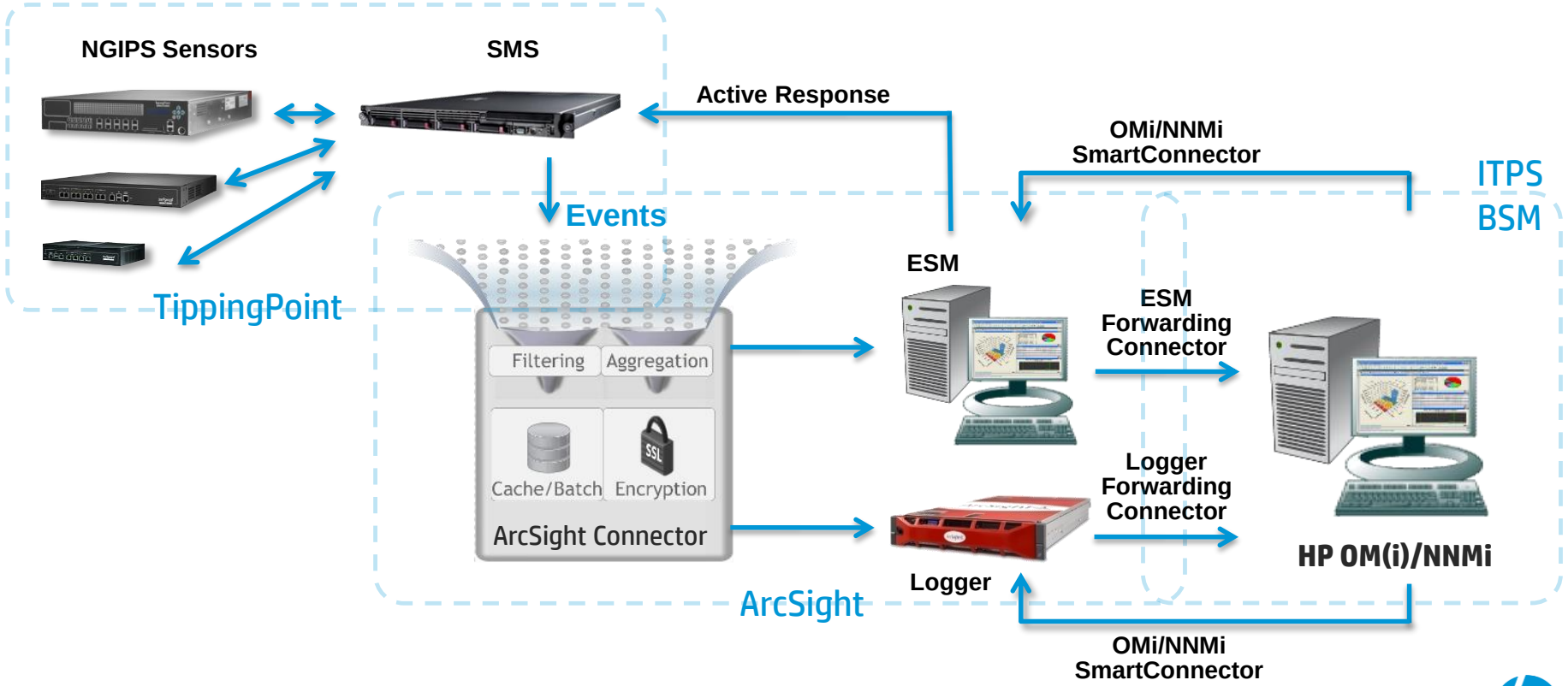
BSM ⟷ Logger



OMi/NNMi ⟷ Logger

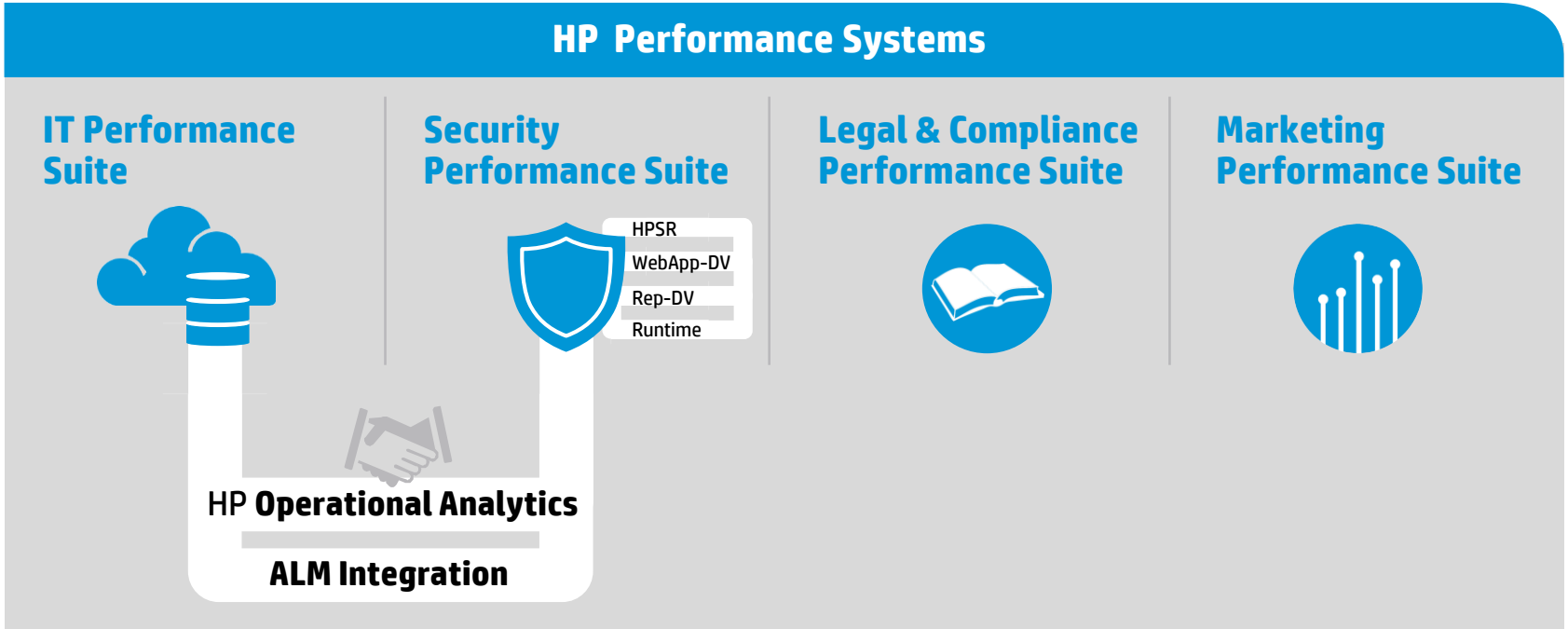
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Operational Analytics



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Better Together – Inter ESP



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Critical success factors for APPS initiatives

Will the App PERFORM ?

Many factors impact the real life performance of application performance . Performance degradation is often primary cause of failure for application initiatives.

Will the App FUNCTION ?

Applications has to behave as per the intend they were built for.

Failure to function properly is not only a satisfaction issue but is also a security concern.

Will the App BE SECURE ?

Certain practices of coding can introduce vulnerabilities. Unsecure coding practices can reveal serious threat. Code level and application level security testing is a proactive preventive solution for application security.

Will lifecycle BE MANAGED?

Application creation is not limited to coding but is a broader set of activities that needs to be governed. This level of control will not only ensure the service quality and lowering failure costs but also make sure the best practice is sustainable.

Ability to address all the challenges are critical for success.

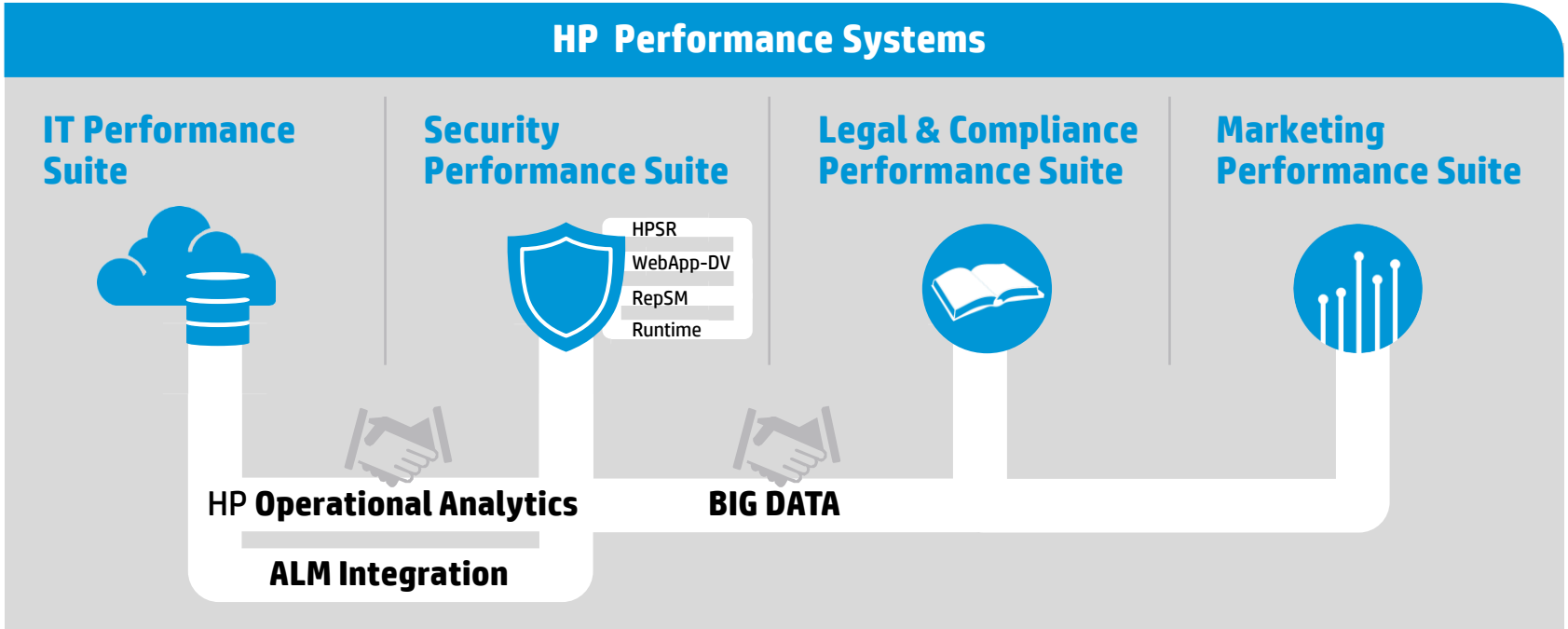
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Solutions

Will the App PERFORM ?	Will the App FUNCTION ?	Will the App BE SECURE?	Will lifecycle BE MANAGED?
Performance Assurance	**Functionality Assurance**	**Security Assurance**	**Management**
HP Load Runner	Manual : Sprinter	Fortify Software Security Center	Test Management
HP Performance Center	Automation: UFT & BPT	Fortify Static Code Analyzer	Application Lifecycle Management
Mobile: Mobile Performance V.	Acceleration: Turnkey	WebInspect	
	Mobile: UFT Mobile	Fortify-on-Demand	
	Virtualization: SV		
Performance testing of applications by simulating load conditions	Manual test tools and Automated functionality testing of applications	Security testing and code security analysis of the applications	Governance and management of the testing process and development process ; from planning through development , testing, operations till retirement.

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

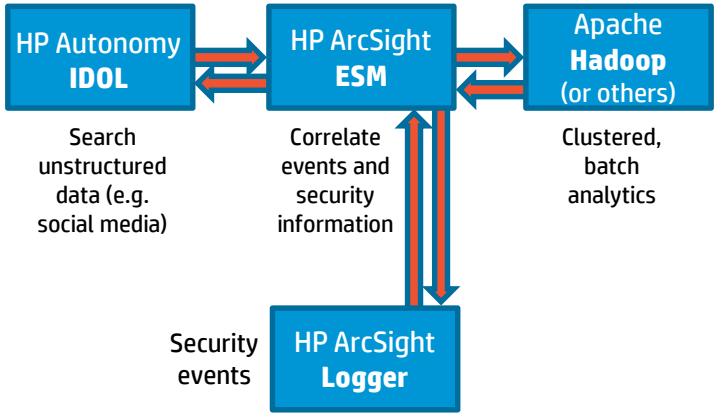
Better Together – Inter ESP



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ArcSight and Autonomy/Hadoop Integration

Big Security using Big Data



Features

- HP Arcsight + Autonomy IDOL for meaning/context based analytics
- HP ArcSight + Hadoop for the power of Big Data analytics
- Power of CORR engine for fast collection, efficient storage and fast analysis
- Sentiment and intent analysis on internal and external users

Problem it solves

Big data – Big analytics – Big Security

- Leverage big data for big security
- Gain insight like never before

Customer benefits

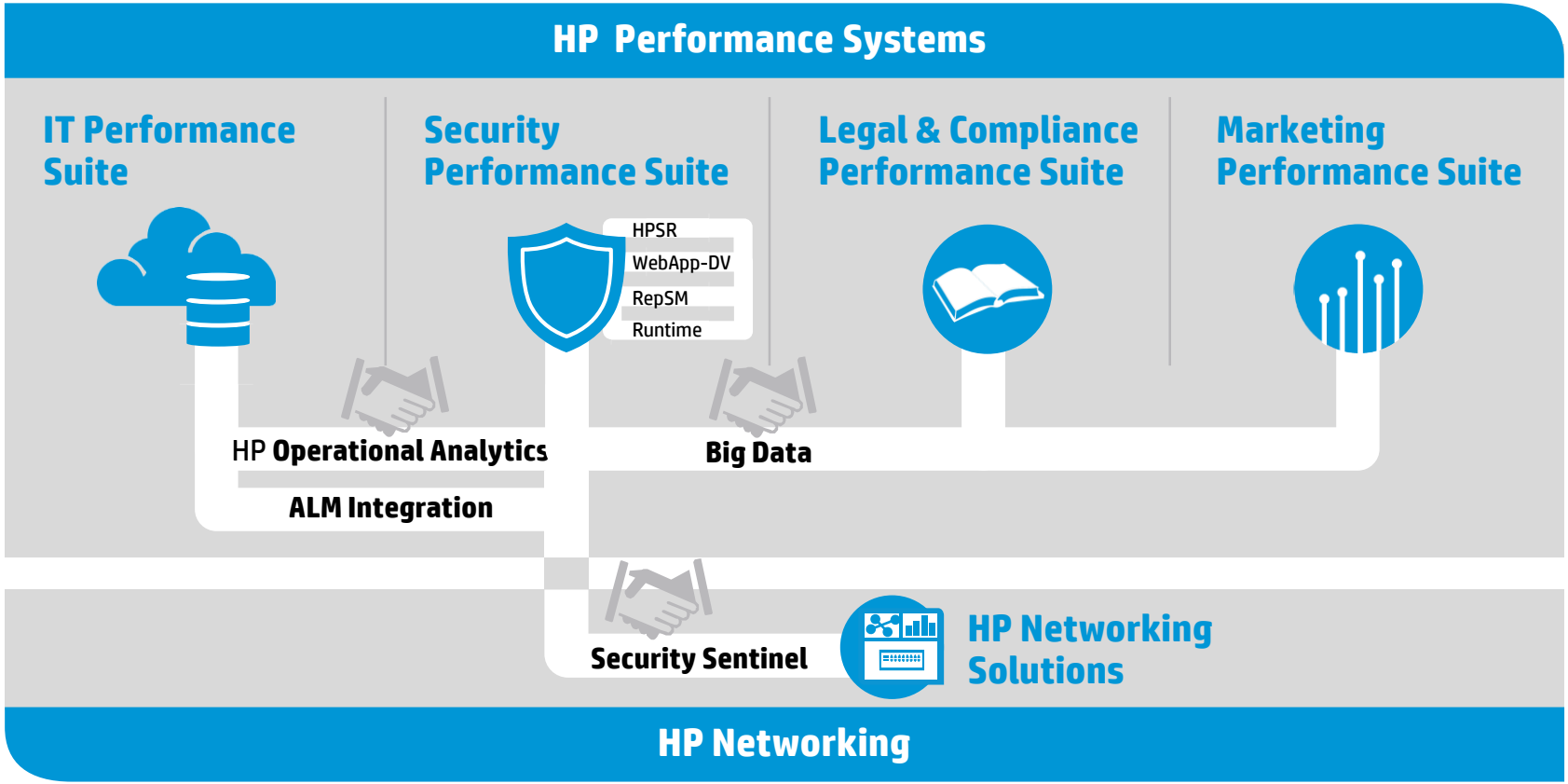
- Effectively monitor data in motion
  - IP, sensitive information, customer data
  - Email, social media, file transfers
- Identify & respond to potential data losses
- Reduce exposures and business risk
- Added ROI from Big Data investments

Why HP?

- Advanced automated analytics
- Large vocabulary of operations for out of the box analysis
- World leading filtering technology to get to all information
- Proven success in all verticals and industries

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Better Together – Inter ESP



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Thank you

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.