McAfee
An Intel Company

# Mucho Big Data y ¿La Seguridad para cuándo?

Juan Carlos Vázquez

Sales Systems Engineer, LTAM

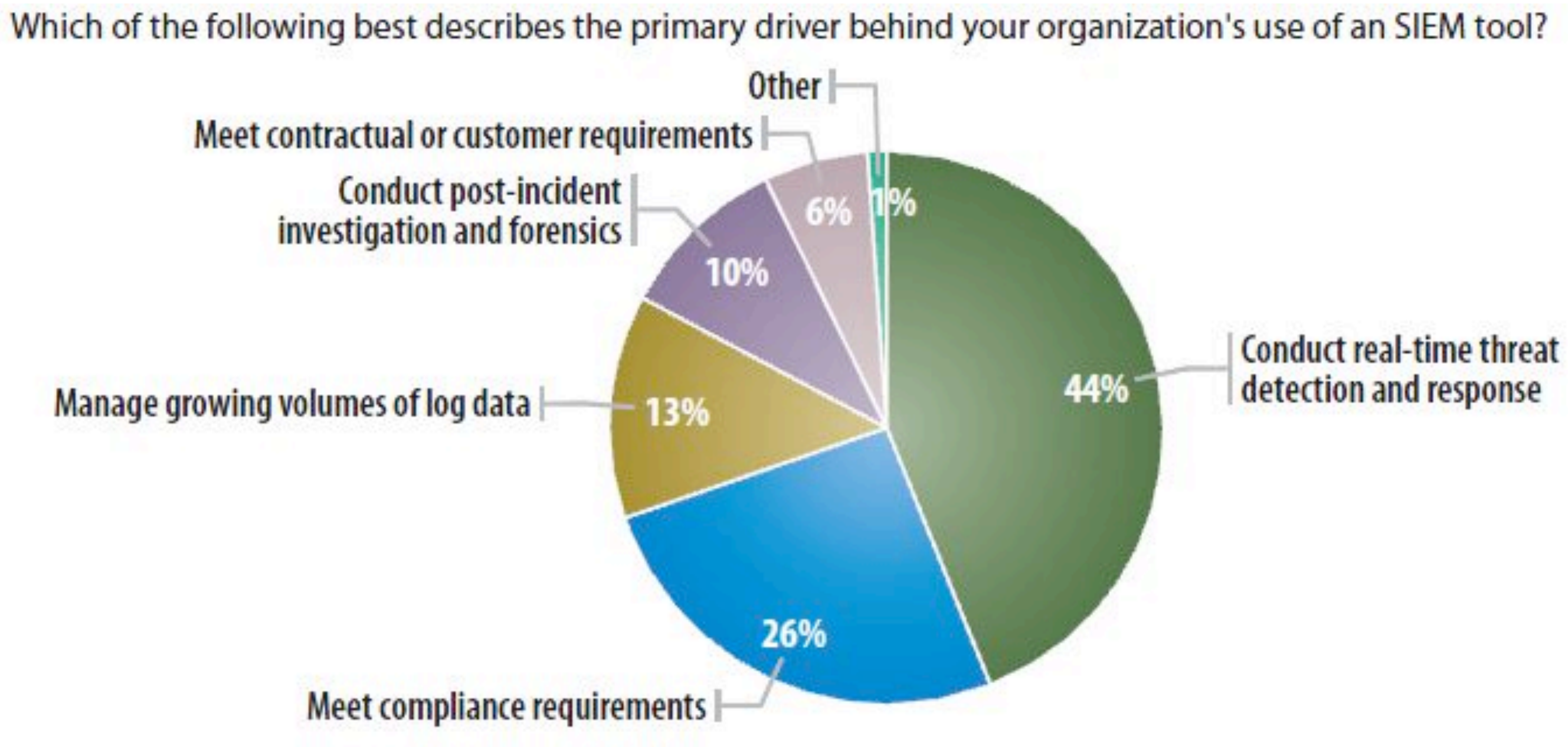
mayo 9, 2013

SAFE NEVER SLEEPS™

# Agenda

- Business Drivers
- Big Security Data
- GTI Integration
- SIEM Architecture & Offering
- Why McAfee
- Demo

# Shifting from Compliance to Security

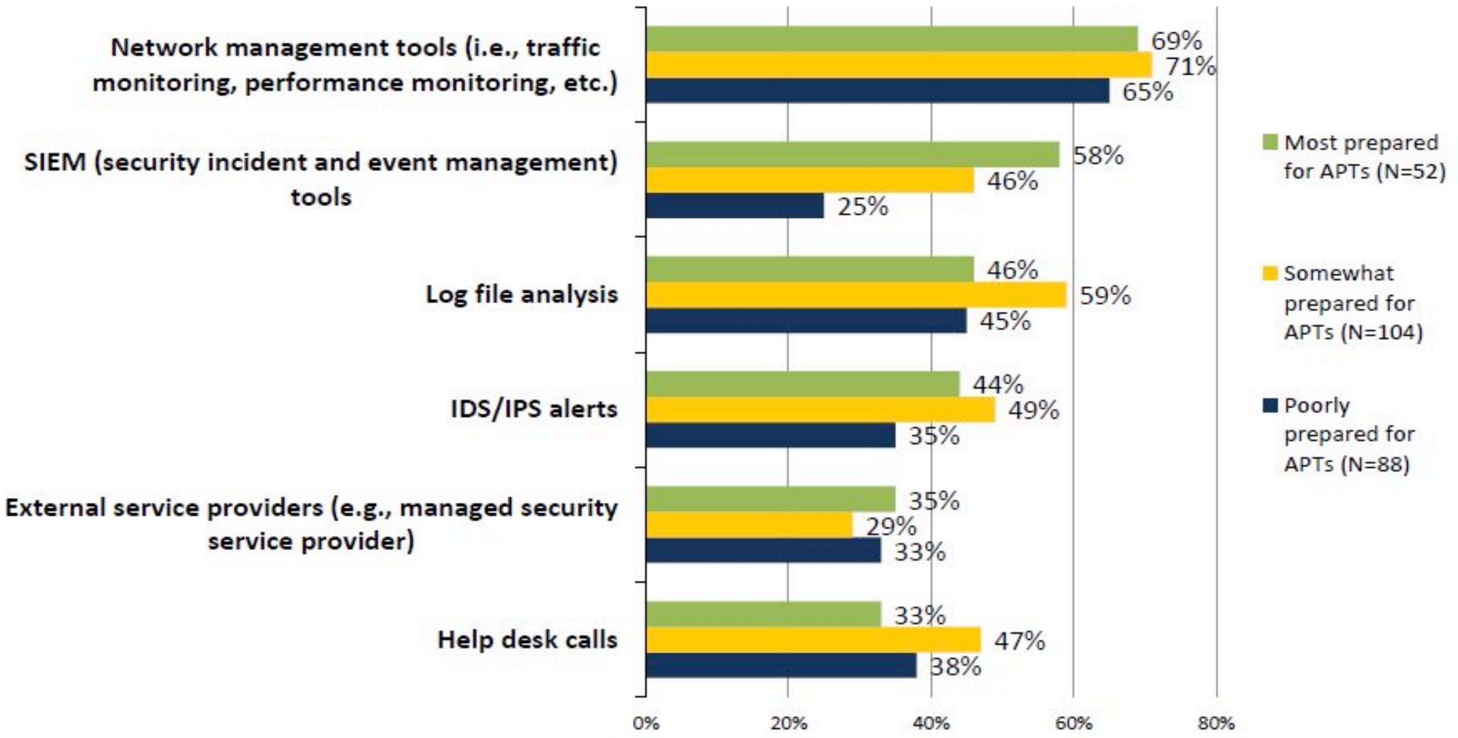


**Source:** *InformationWeek* 2012 Security Information and Event Management Vendor Evaluation Survey of 322 business technology professionals, April 2012

# SIEM as solution to detect CyberAttacks

McAfee
An Intel Company

## Sources Used to Determine if Organization is Experiencing a Cyber Attack, by Preparedness for APTs



ESG

# SEM + SIM = SIEM

## SIEM is the Evolution and Integration of Two Distinct Technologies

- Security Event Management (SEM)
  - Primarily focused on Collecting and Aggregating Security Events
- Security Information Management (SIM)
  - Primarily focused on the Enrichment, Normalization, and Correlation of Security Events

## Security Information & Event Management (SIEM) is a Set of Technologies for:

- Log Data Collection
- Correlation
- Aggregation
- Normalization
- Retention
- Analysis and Workflow

## Three Major Factors Driving the Majority of SIEM Implementations

1. Real-Time Threat Visibility
2. Security Operational Efficiency
3. Compliance and/or Log Management Requirements

# Security Connected Platform (SCP)

McAfee
An Intel Company

## NETWORK SECURITY

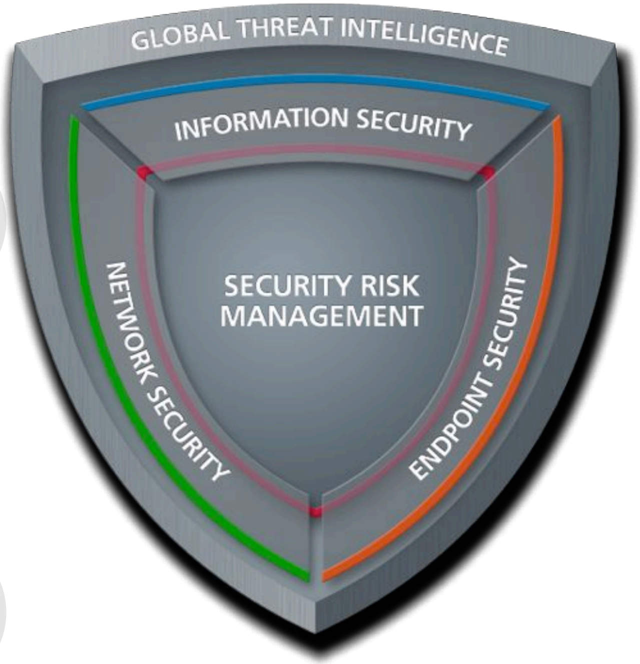
- High Assurance Firewall
- Network Intrusion Prevention
- Network Access Control
- Network Behavior Analysis

## INFORMATION SECURITY

- Email Security
- Web Security
- Data Loss Prevention
- Encryption
- Identity & Access Management
- API and Web Services Security

## SECURITY MANAGEMENT

- Security Operations Mgmt
- Policy Auditing & Management
- Vulnerability Management
- Risk Management/SIEM
- Compliance Management



## ENDPOINT SECURITY

- Malware Protection
- Device Encryption
- Application Whitelisting
- Desktop Firewall
- Device Control
- Email Protection
- Network Access Control
- Endpoint Web Protection
- Host Intrusion Protection
- Mobile Device Management

- Server & Database Protection
- Hardware Assisted Security
- Smartphone and Tablet Protection
- Virtual Machine and VDI Protection
- Embedded Device Protection

## PARTNER COMMUNITY

- Security Innovation Alliance
- McAfee Connected
- Global Strategic Alliance Partners

# The State of SIEM

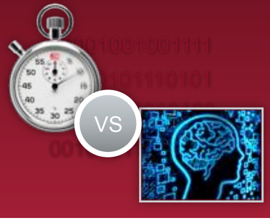
## SIEM Promise:

Turns Security Data Into Actionable Information

Provides an Intelligent Investigation Platform

Supports Management and Demonstration of Compliance

## Legacy SIEM REALITY:



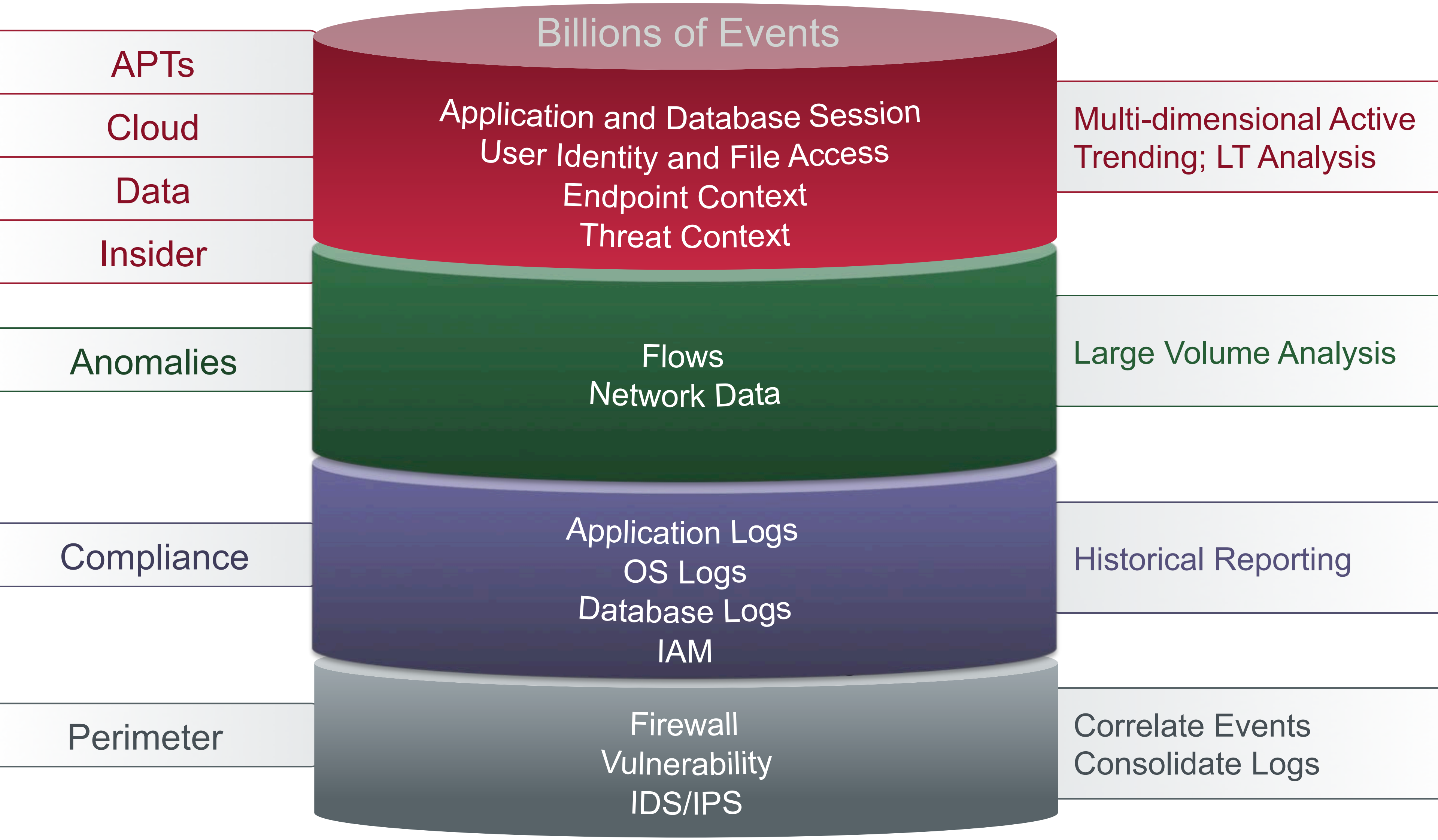
Antiquated Architectures Force Choices Between Time-to-Data and Intelligence

Events Alone Do Not Provide Enough Context to Combat Today's Threats

Complex Usability and Implementation Have Caused Costs To Skyrocket

# The Big Security Data Challenge: Lots and Lots of Data

McAfee
An Intel Company



# Big Data vs. Big Security Data

## Big Data:

Datasets whose size and variety is beyond the ability of typical database software to capture, store, manage & analyse.

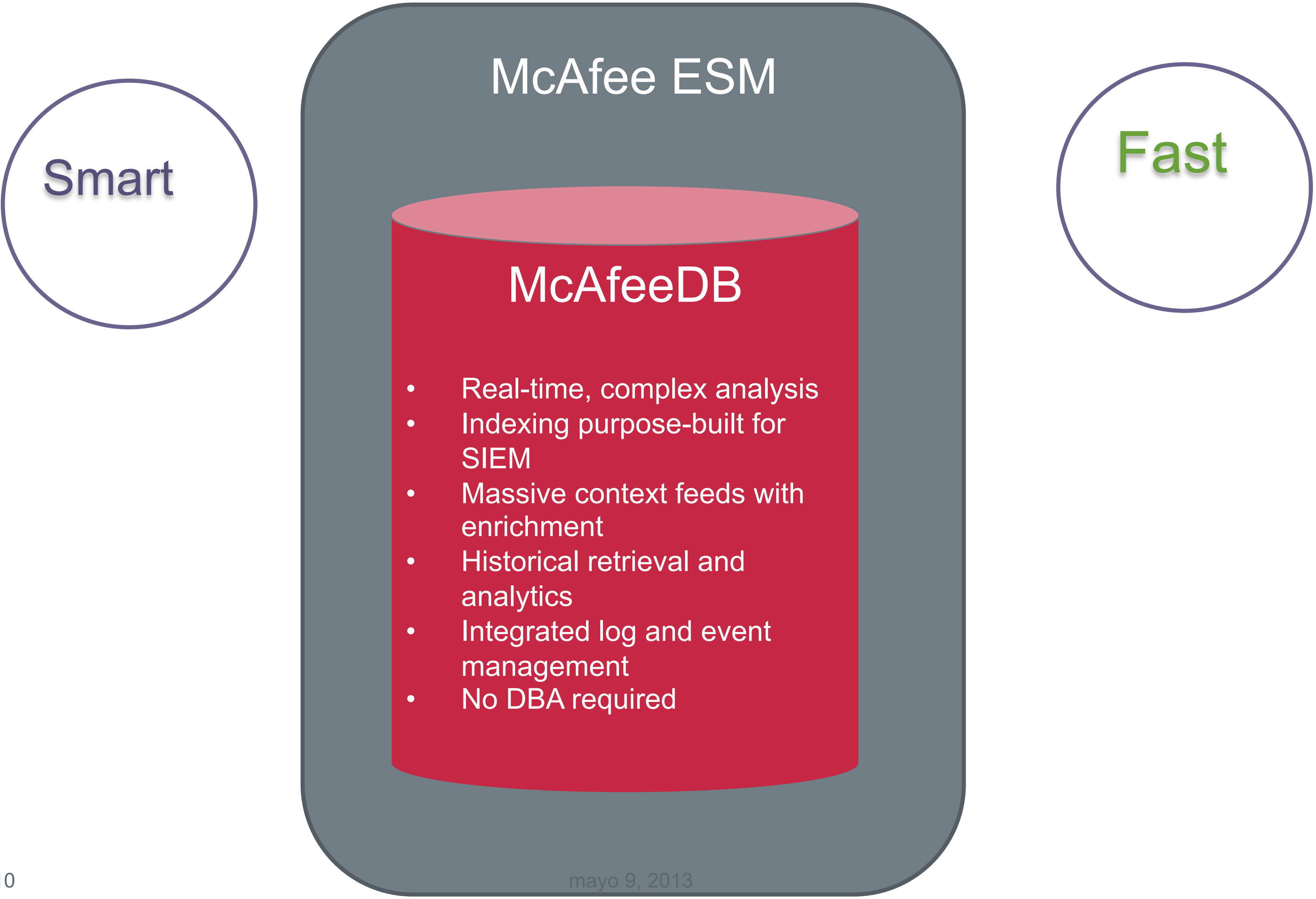
## Big SECURITY Data:

Understanding security data as big data.

- How do I gather security context?
- How do I manage big security information?
- How do I make security information management work?

- Size of security data doubling annually
- Advanced threats demand collecting more data
- Legacy data management approaches failing
- SIEM use shifting from compliance to security

# McAfee Starts at the Core



Smart

McAfee ESM

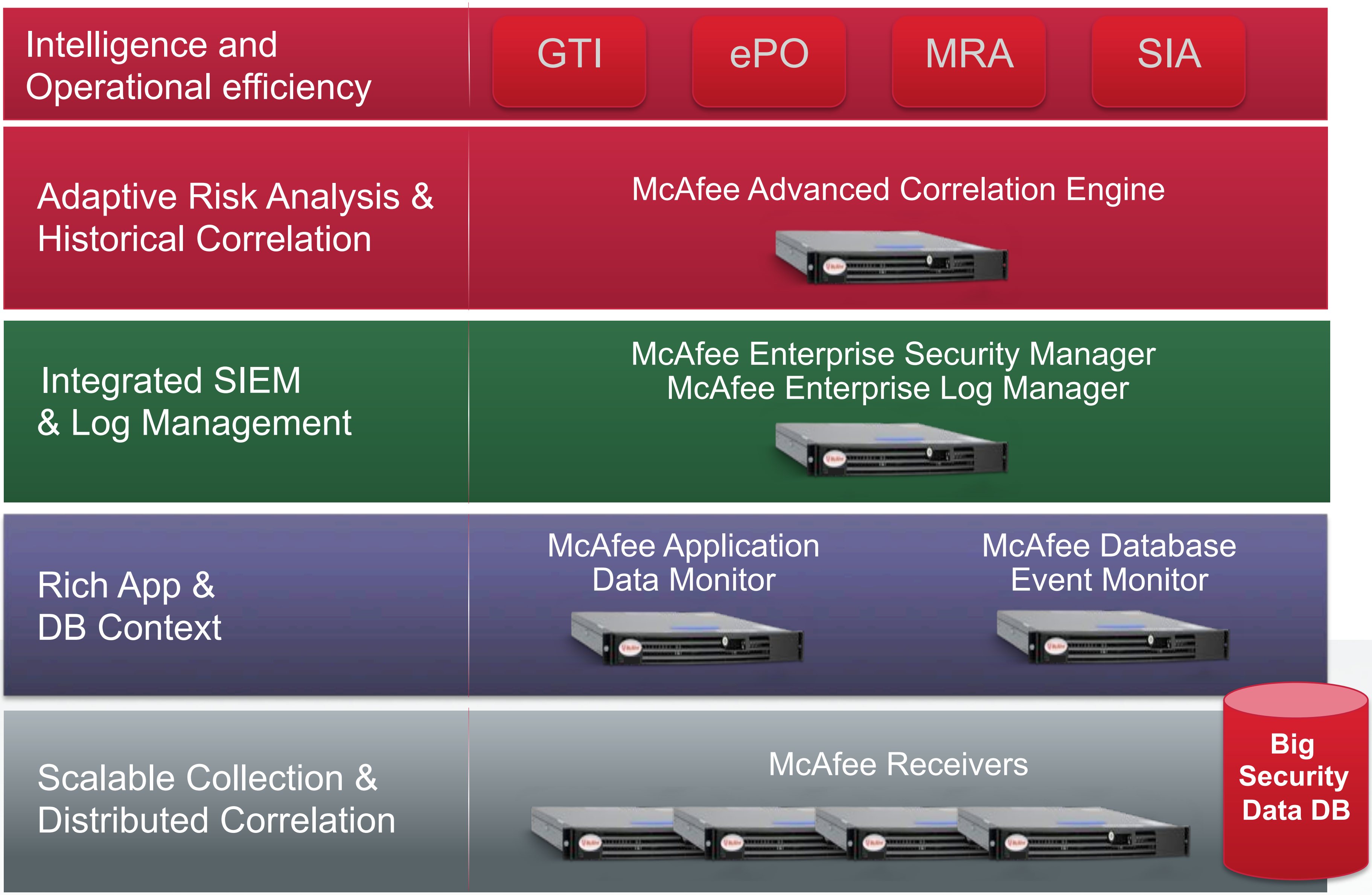
McAfeeDB

- Real-time, complex analysis
- Indexing purpose-built for SIEM
- Massive context feeds with enrichment
- Historical retrieval and analytics
- Integrated log and event management
- No DBA required

Fast

# Scalable and Intelligent Architecture

McAfee
An Intel Company



Intelligence and Operational efficiency

GTI

ePO

MRA

SIA

Adaptive Risk Analysis & Historical Correlation

McAfee Advanced Correlation Engine

Integrated SIEM & Log Management

McAfee Enterprise Security Manager
McAfee Enterprise Log Manager

Rich App & DB Context

McAfee Application Data Monitor

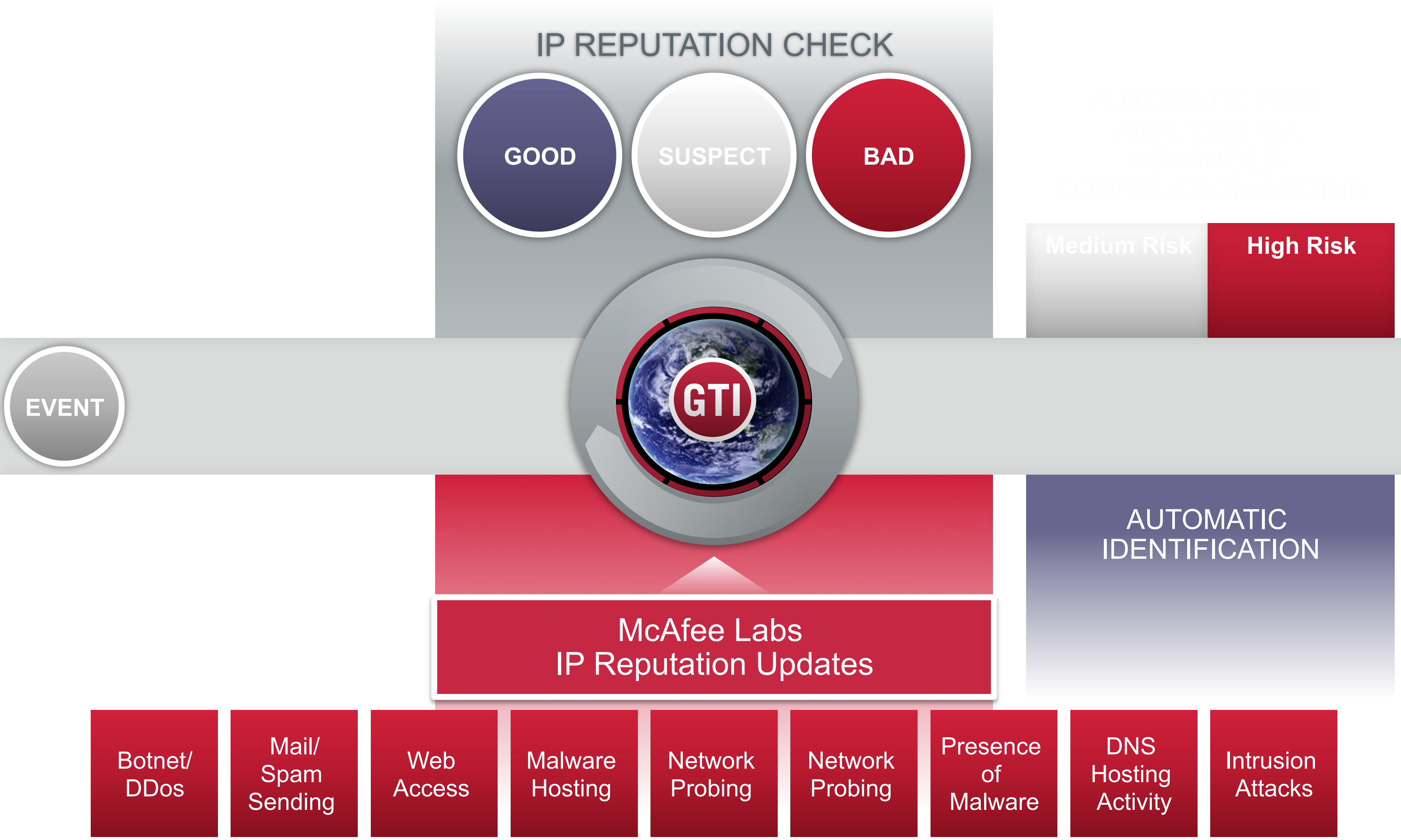
McAfee Database Event Monitor

Scalable Collection & Distributed Correlation

McAfee Receivers

Big Security Data DB

# Global Threat Intelligence and SIEM



IP REPUTATION CHECK

GOOD

SUSPECT

BAD

GTI

EVENT

AUTOMATIC RISK
ANALYSIS VIA
ADVANCED
CORRELATION ENGINE

Medium Risk

High Risk

AUTOMATIC
IDENTIFICATION

McAfee Labs
IP Reputation Updates

Botnet/
DDos

Mail/
Spam
Sending

Web
Access

Malware
Hosting

Network
Probing

Network
Probing

Presence
of
Malware

DNS
Hosting
Activity

Intrusion
Attacks

# GTI with SIEM Delivers Even Greater Value

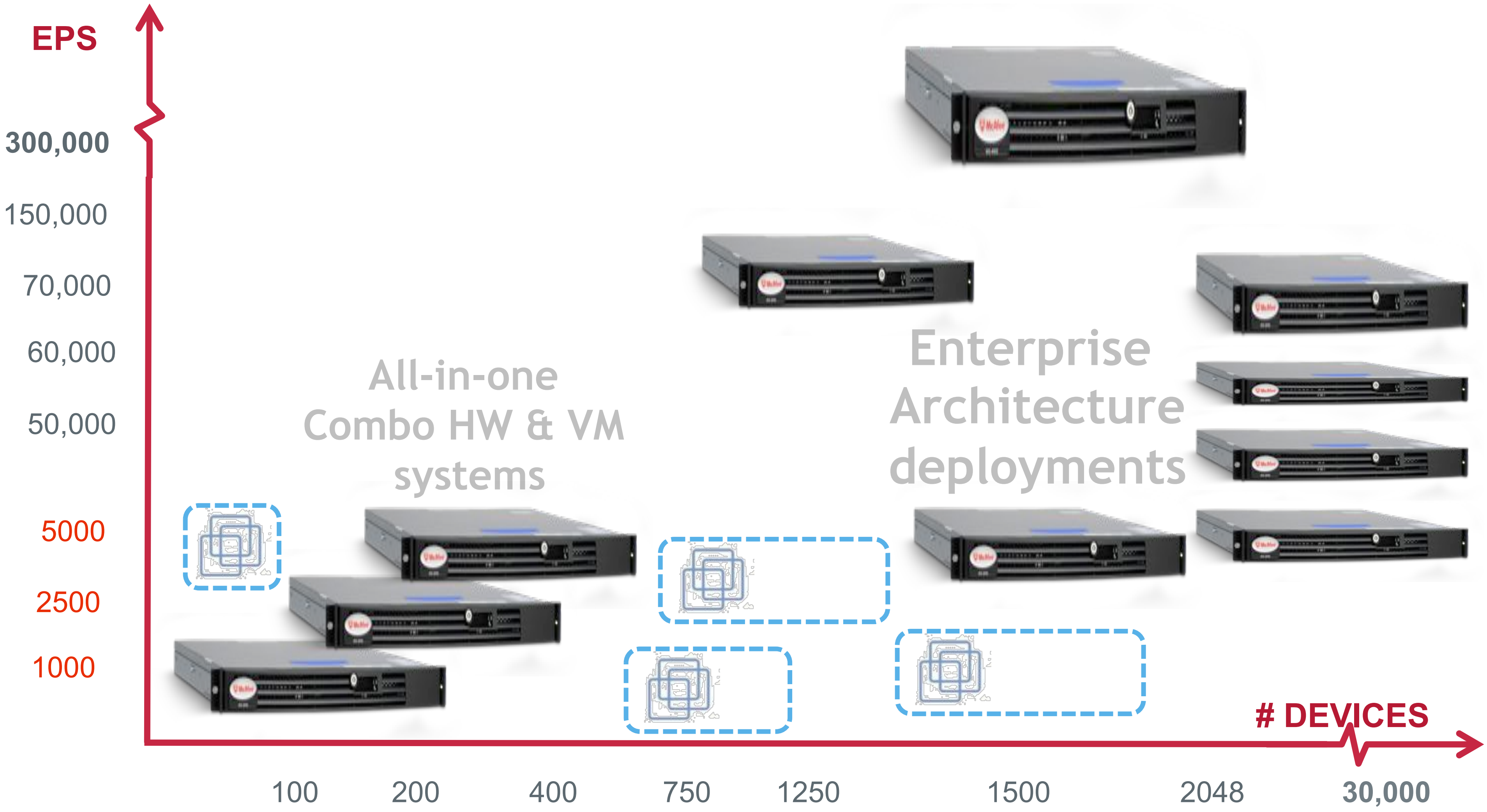
McAfee
An Intel Company

## Sorting Through a Sea of Events…

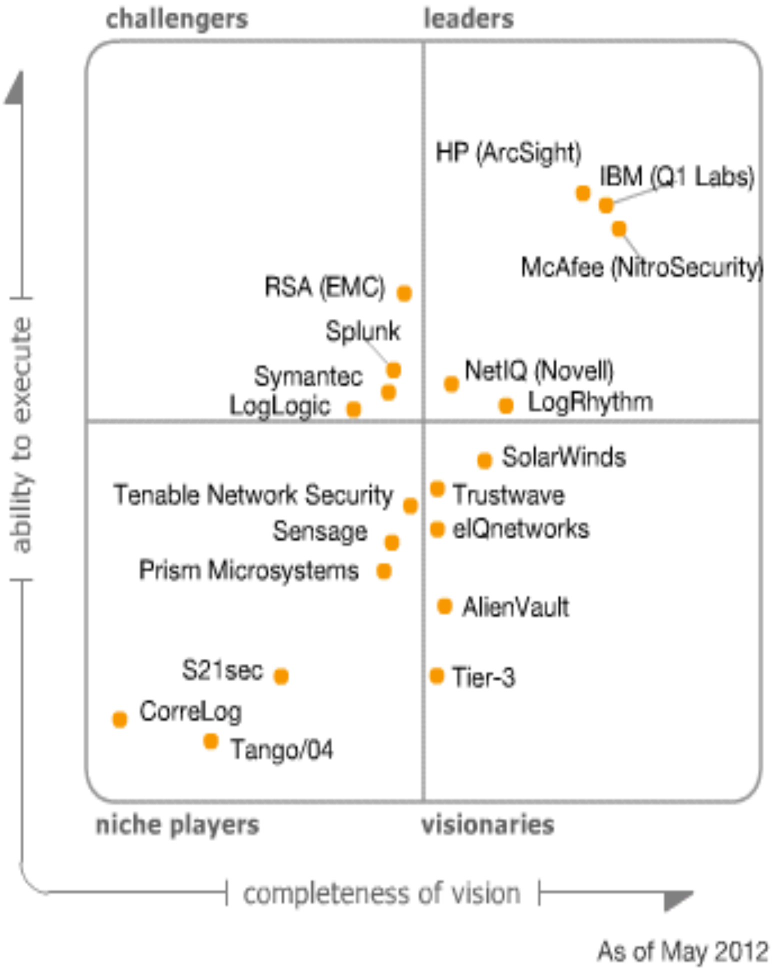
| | | |
|---|---|---|
| | Have I Been Communicating With Bad Actors? | 200M events |
| | Which Communication Was Not Blocked? | 18,000 alerts and logs |
| | What Specific Servers/Endpoints/ Devices Were Breached? | Dozens of endpoints |
| | Which User Accounts Were Compromised? | Handful of users |
| | What Occurred With Those Accounts? | Specific files breached (if any) |
| RESPOND | How Should I Respond? | Optimized response |

# McAfee ESM

## Scalable, Distributed & Purpose-build



# What does Gartner think?



McAfee Enterprise Security Manager is a good choice for organizations that require high-performance analytics under high-event-rate conditions.

Customer references have validated very high scalability and query performance levels for the McAfee Enterprise Security Manager event data store.

# Competition and Differentiation

NitroSecurity competes most often with select best-of-breed vendors, and can win most deals due to NitroView's technical proficiency and scalability

## Most Frequent Competitors

| | |
|---|---|
| ArcSight | ▪ Complex product, heavy services, expensive but best known |
| RSA SECURITY | ▪ Poor standalone product, but can bundle with other services<br>▪ Large existing customer base is turning over |
| Q1 Labs | ▪ Now owned by IBM; adequate product, but doesn't scale easily |

## Occasional

| | |
|---|---|
| LogRhythm | ▪ Mostly log management; poor SIEM; typically in small accounts |
| loglogic | ▪ Log-centric, recently added low-end SIEM; large existing customer base is turning over |

## Non-Factors / Low-End Solutions

netForensics, eIQ networks, TENABLE Network Security, PRISM Secure Networks, TriGeo Network Security, SENSAGE

## Non-Factors / Low-End Solutions

Novell, symantec, ca, NetIQ, QUEST SOFTWARE

## Nitro is Scalable

- Scales easily from SMB to Fortune 500
- Collects all relevant data, not selected sub-sets
- Content-aware & context-aware

## Nitro is Fast

- 100x to 1,000x faster than other solutions
- Single appliance can handle up to 300K EPS
- Only SIEM with real-time insertion & query

## Nitro is Capable

- Comprehensive product offering, covering SIEM, log management, database activity monitor, and application data & protocol monitor

## Nitro is Easy

- Value increases as more information is added through "single pane-of-glass" operation
- Out-of-box full functionality

McAfee®

An Intel Company