datacentrix showcase 2017

the reality of singularity

McAfee™

Together is power.

datacentrix showcase 2017
the reality of singularity

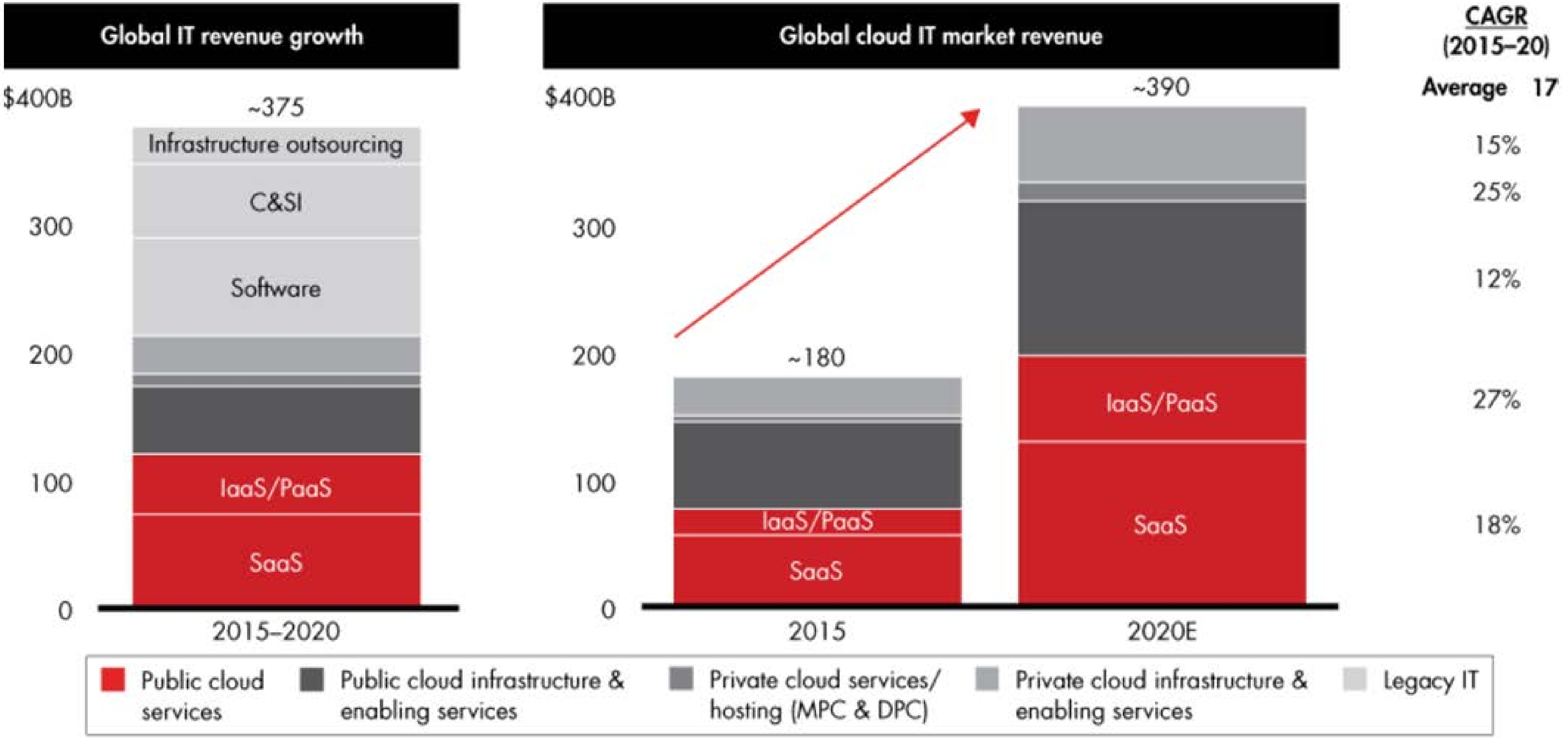
State of Cloud Adoption

Cloud usage is over 90%, are you ready?

McAfee™

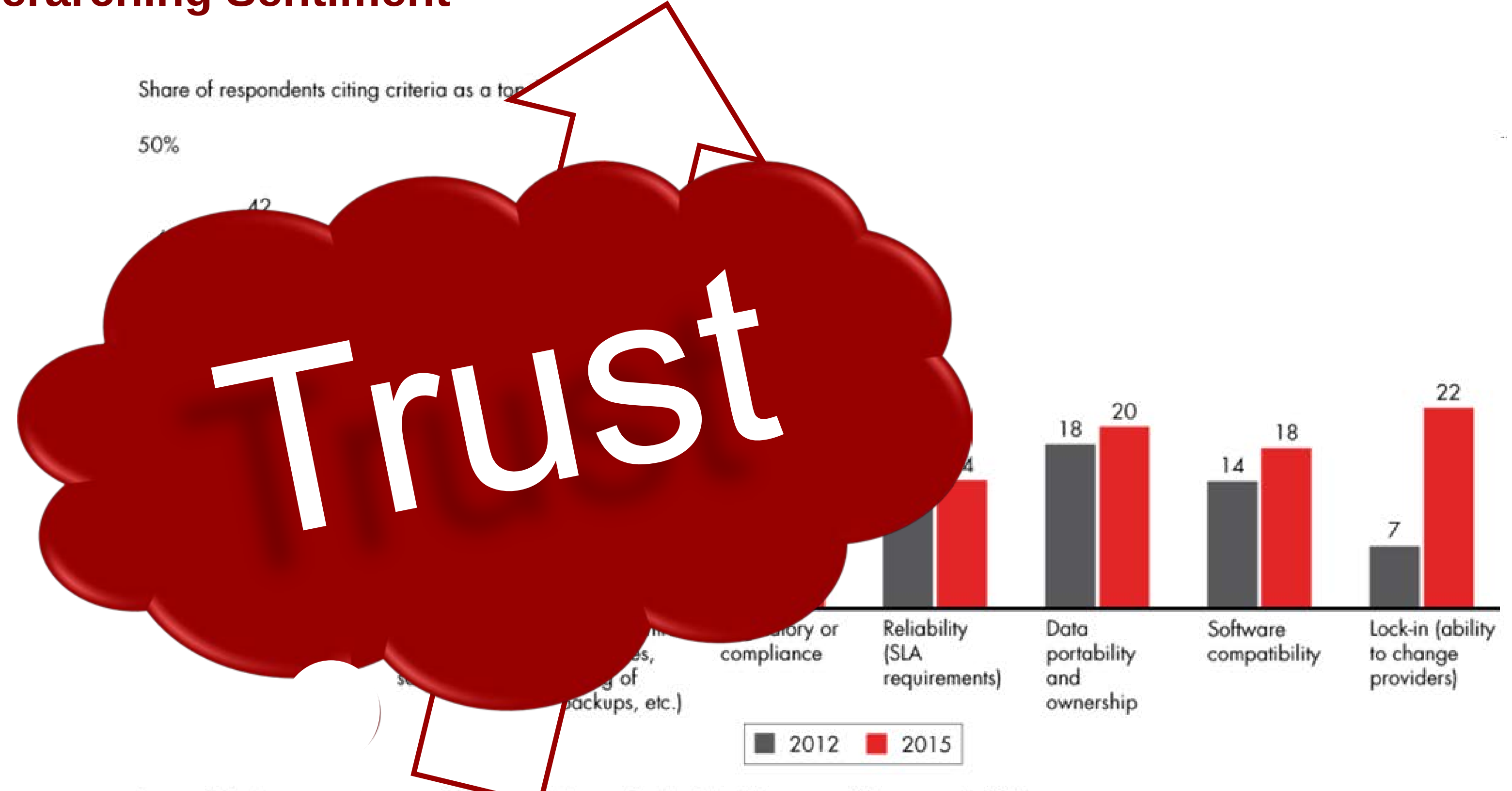
State of Cloud Adoption

Cloud hardware, software and services are capturing 60% of IT market growth, mostly in the public cloud space



Trust & Concerns

Overarching Sentiment



Sources: Bain clou... ...uring survey, 2015 (n=...); Morgan Stanley AlphaWise survey of IT managers (n=304)

Security Research Findings

93%

Of organisations utilize cloud services in some form….but

40%

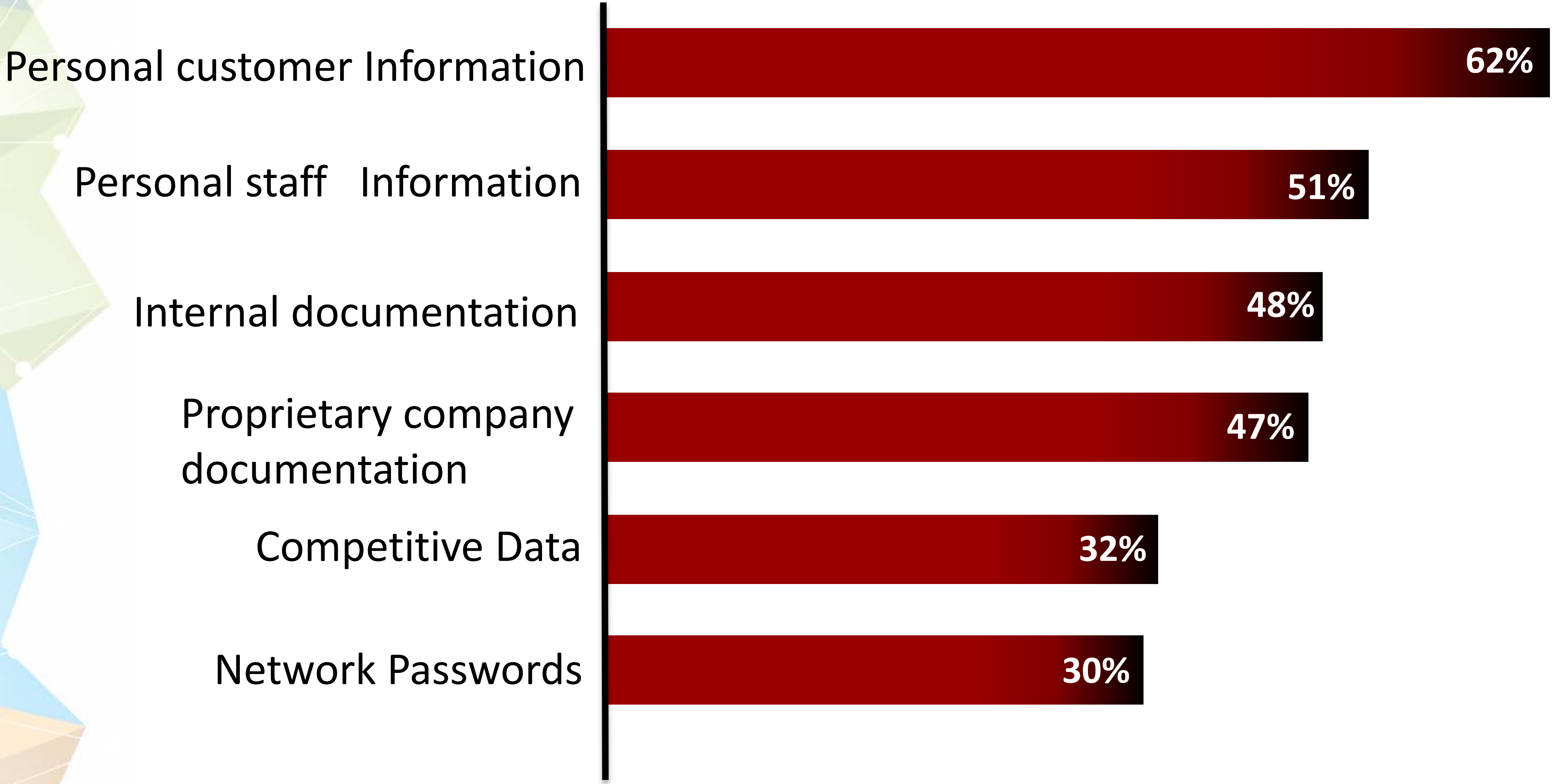
Public cloud services procured outside of IT.

49 %

Businesses delaying further cloud deployment due to the cybersecurity skills gap….so

Visibility of Cloud Services is Key

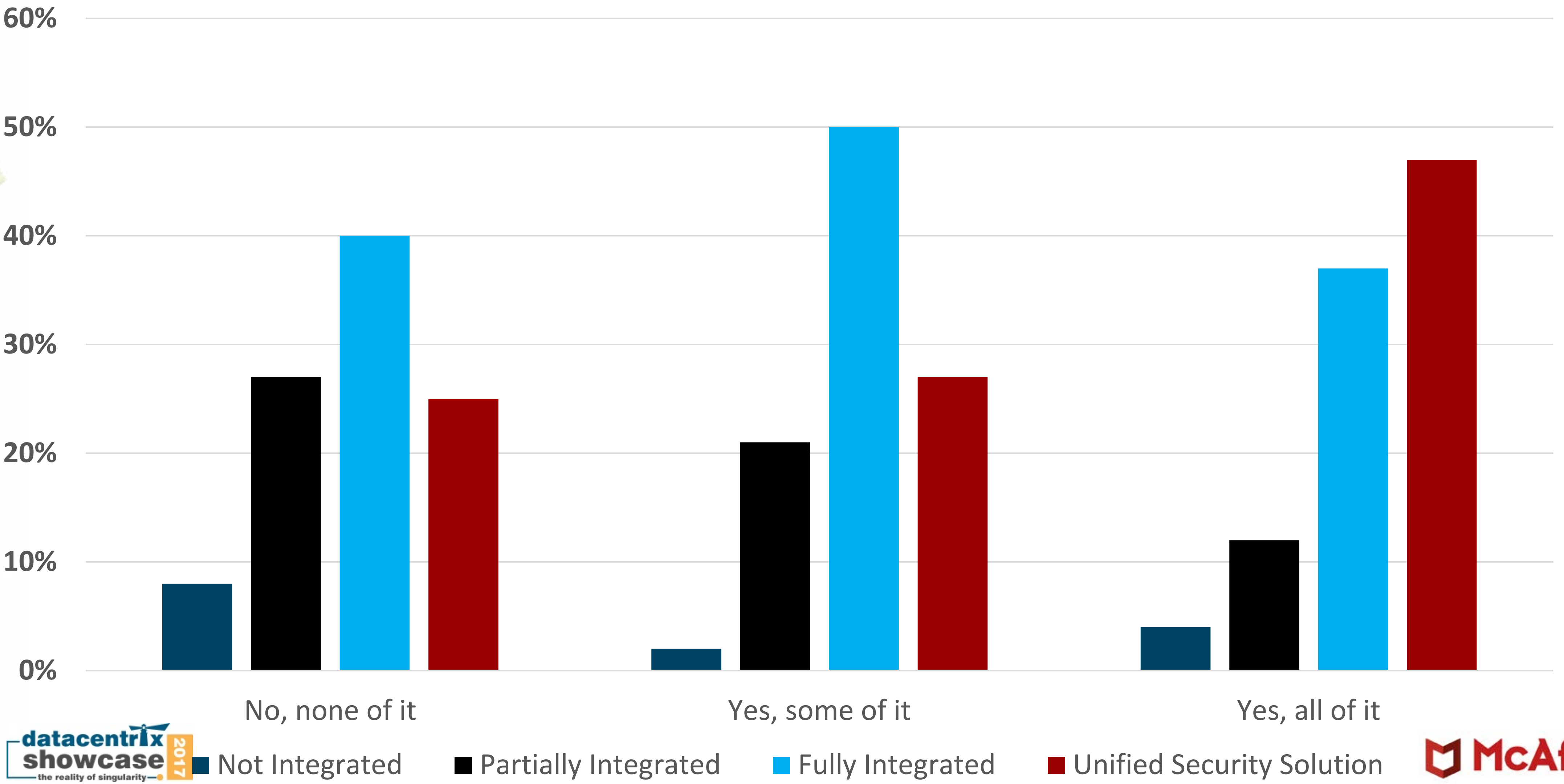
Sensitive Data & the Cloud



Integrated security better at securing sensitive data

Integrated Security & Sensitive Data

Does your organization's public cloud service store your organization's sensitive data? (split by level of integration of security solutions)



Key Requirements for Cloud

What makes the CxO sleep better at night?

Visibility and Data Control

Strategy Agnostic

Efficiencies

Multi-Environment Policy

Orchestrated Management

CAPEX / OPEX Expenditures

How McAfee helps Customers

TO the Cloud

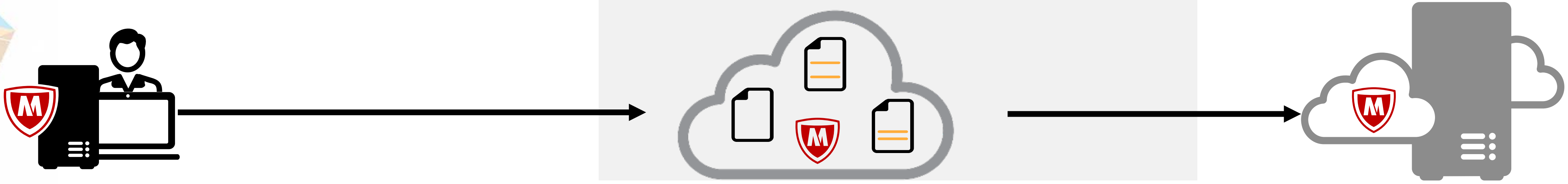
- **Web Gateway and Web Gateway Cloud Service**
  protect users as they browse
- **DLP** monitors for and/or impedes data leakage to the Cloud
- **DLP** provides visibility and control for data uploaded to the Cloud (Box)
- **CASB** monitors application activity and protects data as it moves to SaaS Apps

IN the Cloud

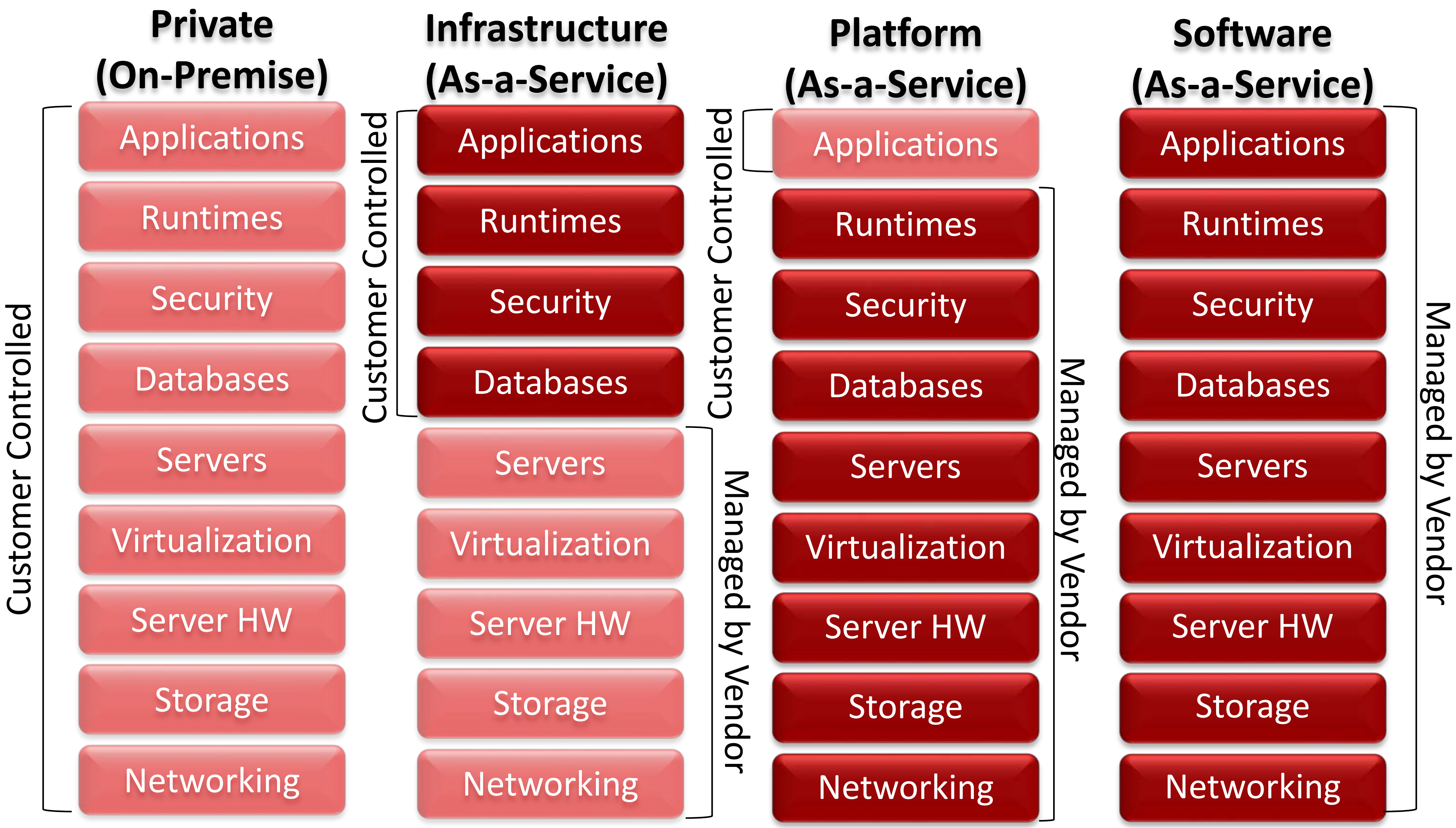
- **Cloud Workload Discovery** provide discovery, visibility, assessment and control
- **Server protection suites** protect workload environments
- **MOVE and/or Application Control** both leverage **TIE, Policy Auditor**
- **vNSP** protects east/west traffic in the Cloud or SDDC

FROM the Cloud

- **Cloud ePO**
- **Web Gateway Cloud Service**
- **Cloud Threat Detection**



Understanding Cloud Computing Stack



Private (On-Premise)

Customer Controlled

- Applications
- Runtimes
- Security
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

Infrastructure (As-a-Service)

Customer Controlled

- Applications
- Runtimes
- Security
- Databases

Managed by Vendor

- Servers
- Virtualization
- Server HW
- Storage
- Networking

Platform (As-a-Service)

Customer Controlled

- Applications

Managed by Vendor

- Runtimes
- Security
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

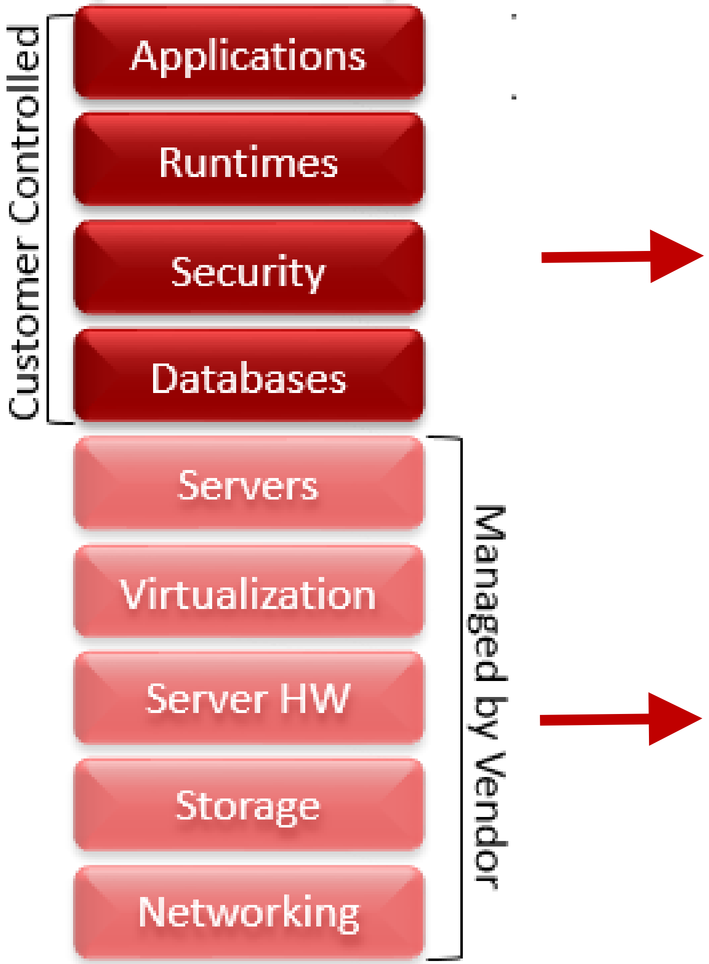
Software (As-a-Service)

Managed by Vendor

- Applications
- Runtimes
- Security
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

Where our Solutions Fit - IaaS

Infrastructure (As-a-Service)



Solutions

- MOVE AV/Server Security Suites
- Database Security
- Data Protection Suites
- Virtual NSP
- ESM for AWS

- Encryption
- Web Security
- Network Security
- Data Center Connectors
- Intel Security Controller

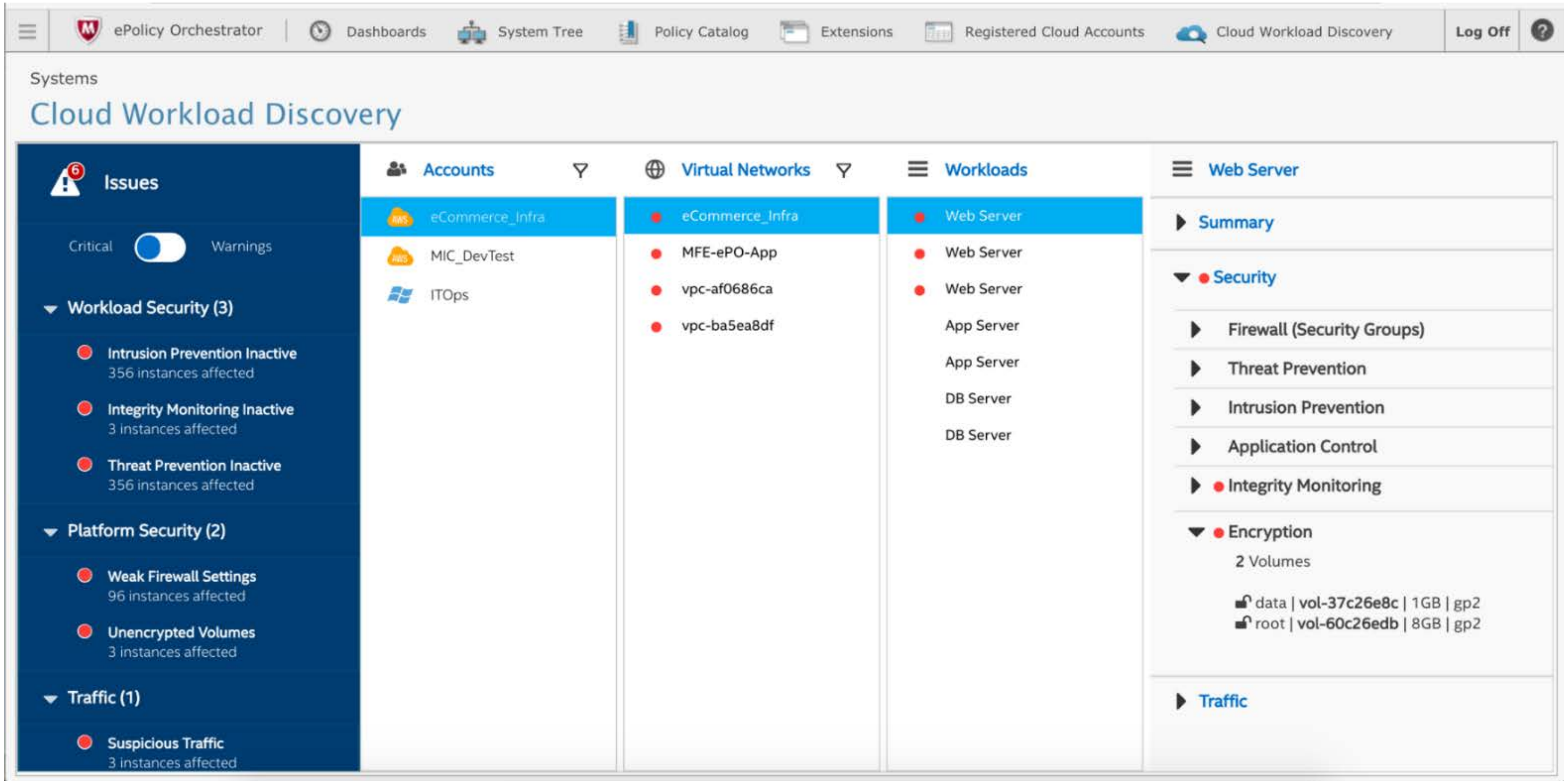
- Encryption

What Enterprises care about

- Uptime
- Server Performance
- Visibility
- Application Security
- Shadow IT
- Protect Sensitive Data
- Security Breaches

- Protect Sensitive Data

How many workloads are there? How safe are they?



Systems

Cloud Workload Discovery

Issues 6

Critical / Warnings

- Workload Security (3)
  - Intrusion Prevention Inactive – 356 instances affected
  - Integrity Monitoring Inactive – 3 instances affected
  - Threat Prevention Inactive – 356 instances affected
- Platform Security (2)
  - Weak Firewall Settings – 96 instances affected
  - Unencrypted Volumes – 3 instances affected
- Traffic (1)
  - Suspicious Traffic – 3 instances affected

Accounts

- eCommerce_Infra
- MIC_DevTest
- ITOps

Virtual Networks

- eCommerce_Infra
- MFE-ePO-App
- vpc-af0686ca
- vpc-ba5ea8df

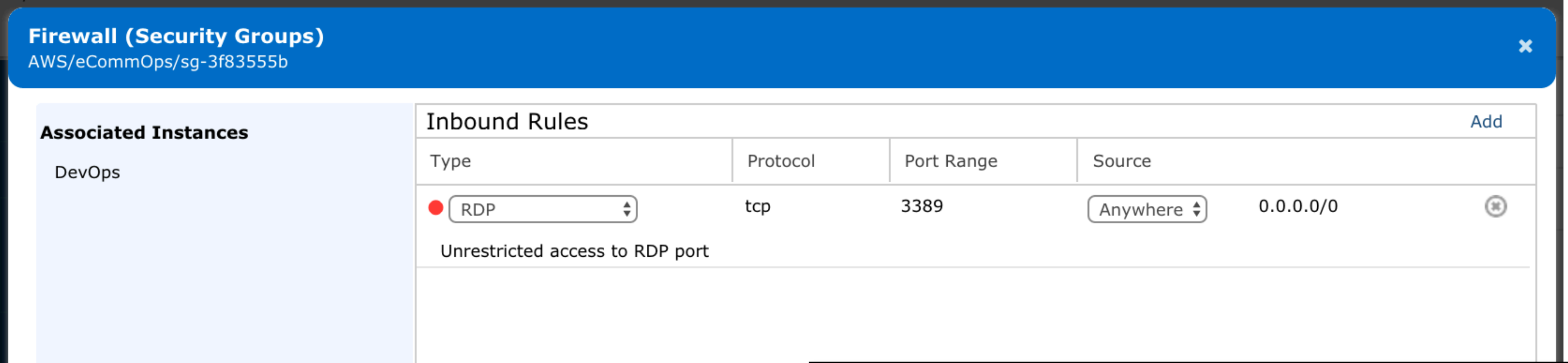
Workloads

- Web Server
- Web Server
- Web Server
- App Server
- App Server
- DB Server
- DB Server

Web Server

- Summary
- Security
  - Firewall (Security Groups)
  - Threat Prevention
  - Intrusion Prevention
  - Application Control
  - Integrity Monitoring
  - Encryption
    - 2 Volumes
    - data | vol-37c26e8c | 1GB | gp2
    - root | vol-60c26edb | 8GB | gp2
- Traffic

Customer Value: Instant visibility into security posture



Firewall (Security Groups)
AWS/eCommOps/sg-3f83555b

Associated Instances

DevOps

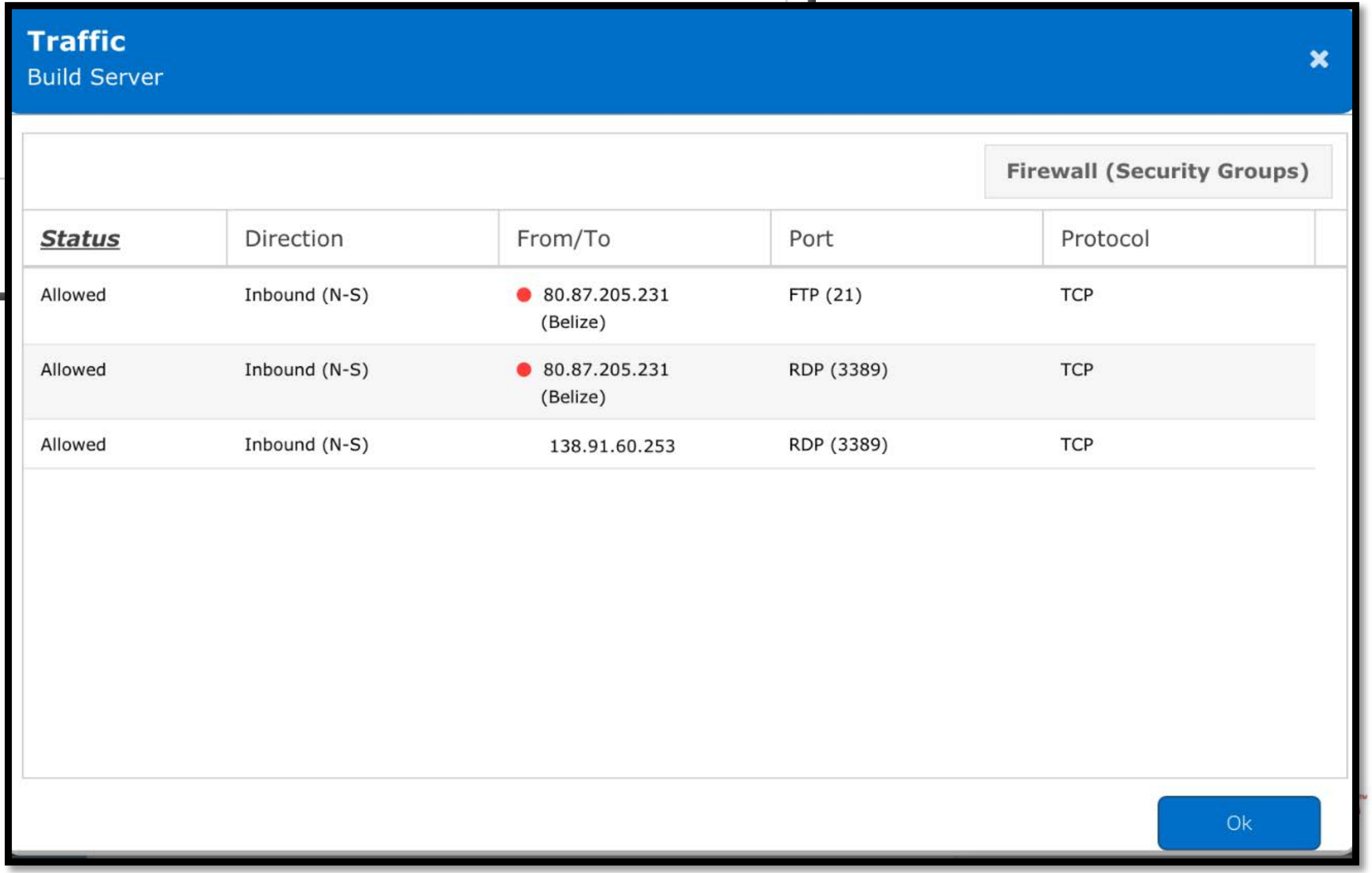
Inbound Rules — Add

Type	Protocol	Port Range	Source	
● RDP	tcp	3389	Anywhere	0.0.0.0/0

Unrestricted access to RDP port

Customer Value:

Visibility into whether best practices are being followed



Traffic
Build Server

Status	Direction	From/To	Port	Protocol
Allowed	Inbound (N-S)	● 80.87.205.231 (Belize)	FTP (21)	TCP
Allowed	Inbound (N-S)	● 80.87.205.231 (Belize)	RDP (3389)	TCP
Allowed	Inbound (N-S)	138.91.60.253	RDP (3389)	TCP

Customer Value:

Insight into whether any workloads are compromised

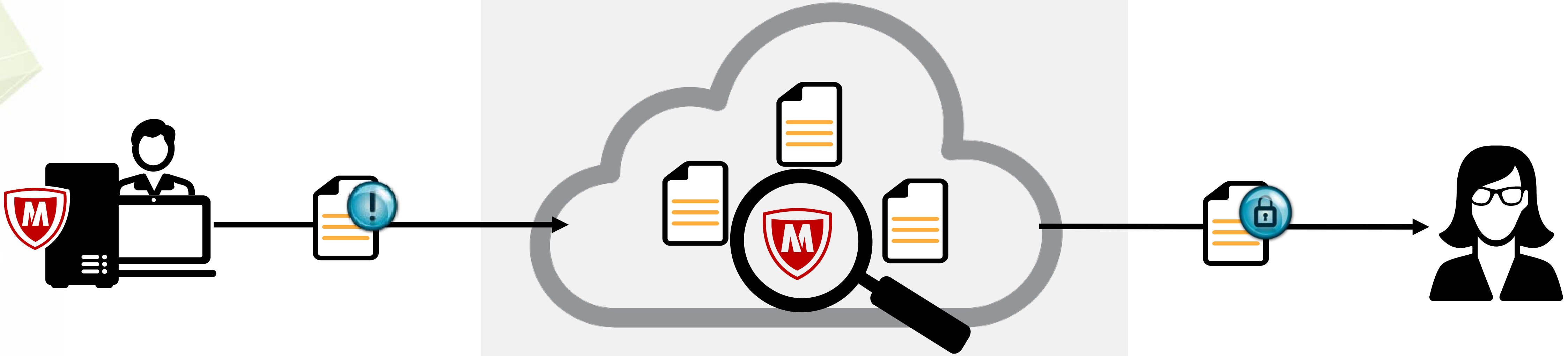
Protecting Data In the Cloud

New Cloud Discovery Feature

Uploading

In the Cloud

Downloading



Scan/block sensitive files being uploaded

Remediation; change sharing permission; apply encryption

Protect/Secure sensitive file downloaded to endpoint

McAfee vNSP for Cloud | Security for Public/Private Cloud

Built for the Cloud

- Inline IPS/IDS
- Security Group
- AutoScale
- CloudTrail/VPC logs

Built in Security

- Delivered with CloudFormation Template
- Ansible/Chef/Puppet

Load Balanced

- Automatic client based load balancer
- Integrated with AutoScale

Virtual Overlay Network

- Micro-segmentation across heterogeneous cloud
- App Fencing

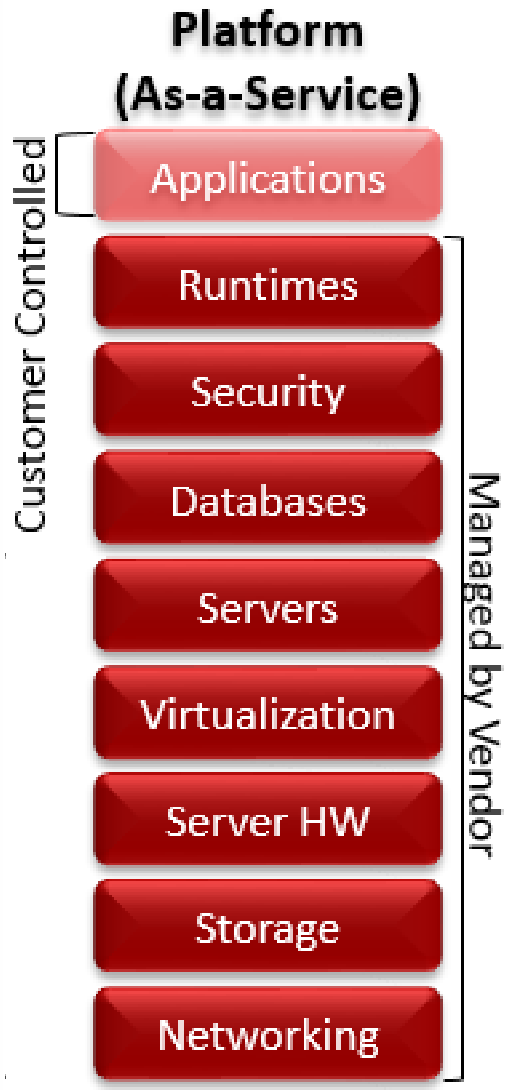
Low OpEx/CapEX

- Ready for Orchestration
- Live Update of Sensors & Agents
- Flexible License

Single Console

- Single NSM to manage appliance, OpenStack, VMware & AWS
- Manage from AWS or On-Premises
- Monitor user access across cloud

Where our Solutions Fit - PaaS


Platform (As-a-Service)

Customer Controlled

Applications

Runtimes

Security

Databases

Servers

Virtualization

Server HW

Storage

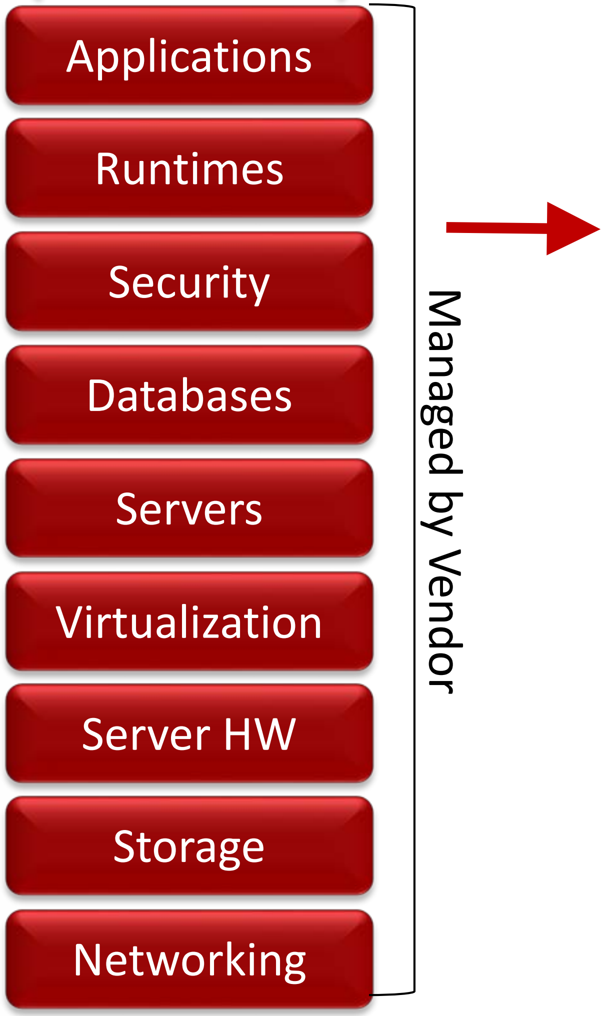
Networking

Managed by Vendor

- Delivered by the provider as a black box.
- Consumer develops applications on top of the platform.
- Provider delivers the hardware, OS and software.
- Consumer focuses on developing code, not management.

Where our Solutions Fit - SaaS

Software (As-a-Service)



Solutions

- Web Gateway SaaS
- ePO Cloud
- Cloud Sandboxing

What customers care about

- Lower cost of entry
- Reduced time to benefit
- Pay as you go
- Shift responsibility for upgrades, uptime and infrastructure
- Lower learning curve and higher adoption rates
- Integration and scalability

McAfee Cloud Visibility – Community Edition

Available to McAfee DLP, Encryption or Web Protection customers

It is a **free** service that provides centralized dashboard view into cloud applications being used.

- Identify cloud applications in use and associated risks
- Monitor sensitive data flowing between users and cloud applications
- Track endpoint health around threats, data leakage and theft

Identify cloud applications:

- **Discover 5000+ cloud services** used across your organization
- **Analyze risk categories for cloud application usage** using common risk database for web and data protection
- Understand, evaluate, and assess the complex technical services of your cloud applications

Addresses the key customer problem of Shadow IT regarding cloud application usage by providing a freemium service

Monitor sensitive data:

- Monitor where sensitive is data flowing
- Determine which users are accessing sensitive data
- Find sanctioned and unsanctioned applications
- Investigate using single easy-to-use management console

Get 360 degree view of user activity from endpoint-to-cloud and define required policies via McAfee ePolicy Orchestrator

Track endpoint health:

- Inspect whether endpoints are protected against threats
- Review endpoint encryption status, which is key to secure data in case of endpoint theft
- Check whether endpoint data loss prevention is configured

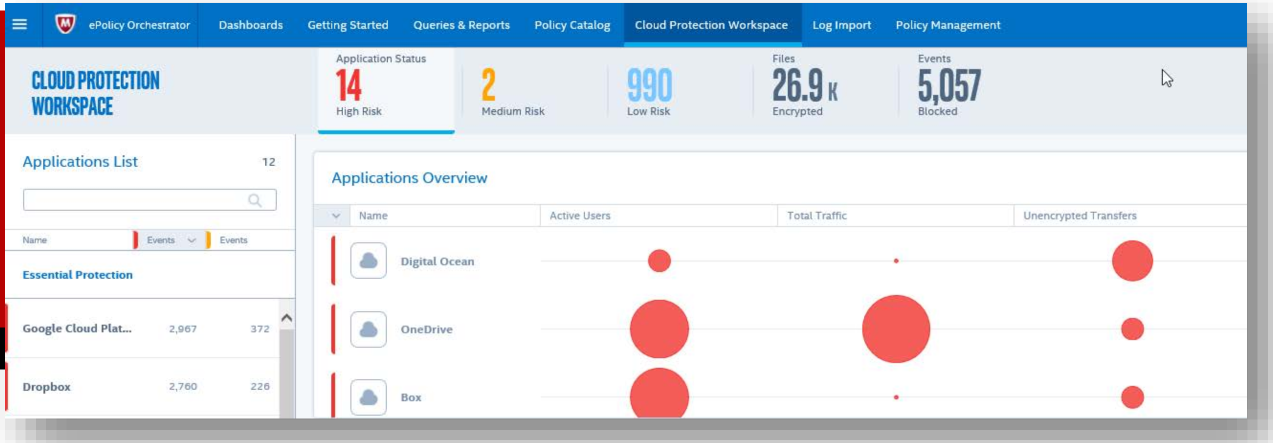
Leverage endpoint health check reports to create a comprehensive threat defense plan across antimalware, encryption and data loss prevention features

Customer Experience

Available to McAfee DLP, Encryption or Web Protection customers

Insightful Dashboards:

1. Cloud Apps Used
2. App Risk Scores
3. Endpoint Health Checks
4. Where is my Sensitive Information?
5. Users sharing sensitive data



CLOUD PROTECTION WORKSPACE

Application Status: 14 High Risk · 2 Medium Risk · 990 Low Risk

Files: 26.9 K Encrypted

Events: 5,057 Blocked

Applications List 12

Name	Events	Events
Essential Protection		
Google Cloud Plat...	2,967	372
Dropbox	2,760	226

Applications Overview

Name	Active Users	Total Traffic	Unencrypted Transfers
Digital Ocean			
OneDrive			
Box			

Customer with	Experience
DLP	Sign-up to activate this with service with an ePO Cloud account and track sensitive data moving between endpoint and cloud applications
Web logs from on-premises McAfee or Blue Coat web gateways	Sign-up to activate this with service with an ePO Cloud account. Upload and analyze web traffic logs into ePO Cloud to track cloud application usage.
McAfee Web Gateway Cloud Service	Traffic data is automatically integrated, and they can immediately track cloud applications once this service is activated in my accounts page

McAfee Key Security Deliverables for Cloud

Visibility and Data Control

Strategy Agnostic

Efficiencies

Multi-Environment Policy

Orchestrated Management

CAPEX / OPEX Expenditures