ARMOR™

BETWEEN YOU AND THE THREAT

Uncloud Your Judgment

Real Tips for Securing Your Data & Workloads in the Public Cloud

RUSS MURRELL VICE PRESIDENT, PRODUCT MANAGEMENT

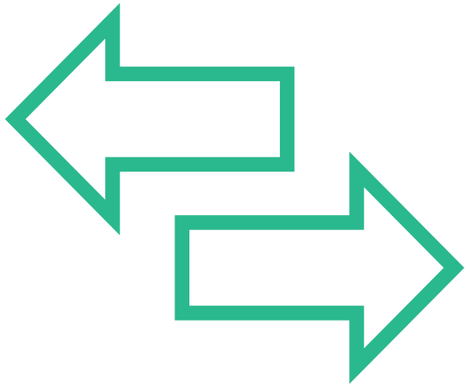
SARAH ECK DIRECTOR, PRODUCT MARKETING

The Leader in Active Cyber Defense

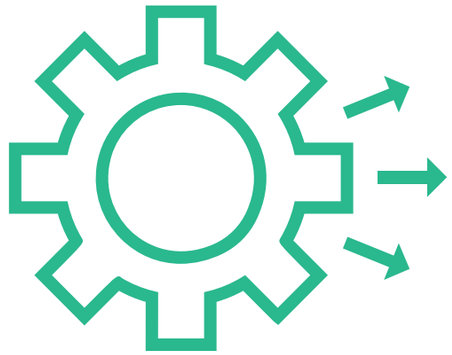
MAY 26, 2016

Why the Public Cloud

Price



Flexibility



Workload Strategies

But some workloads just aren't a good fit for public cloud.
This is why more and more organizations are leveraging multiple clouds.

The Multi-Cloud Landscape

74%

Managing On-premise Private Clouds Mixed with Hosted Private Clouds

50%

Maintaining On-Premise Private Clouds with Public Clouds

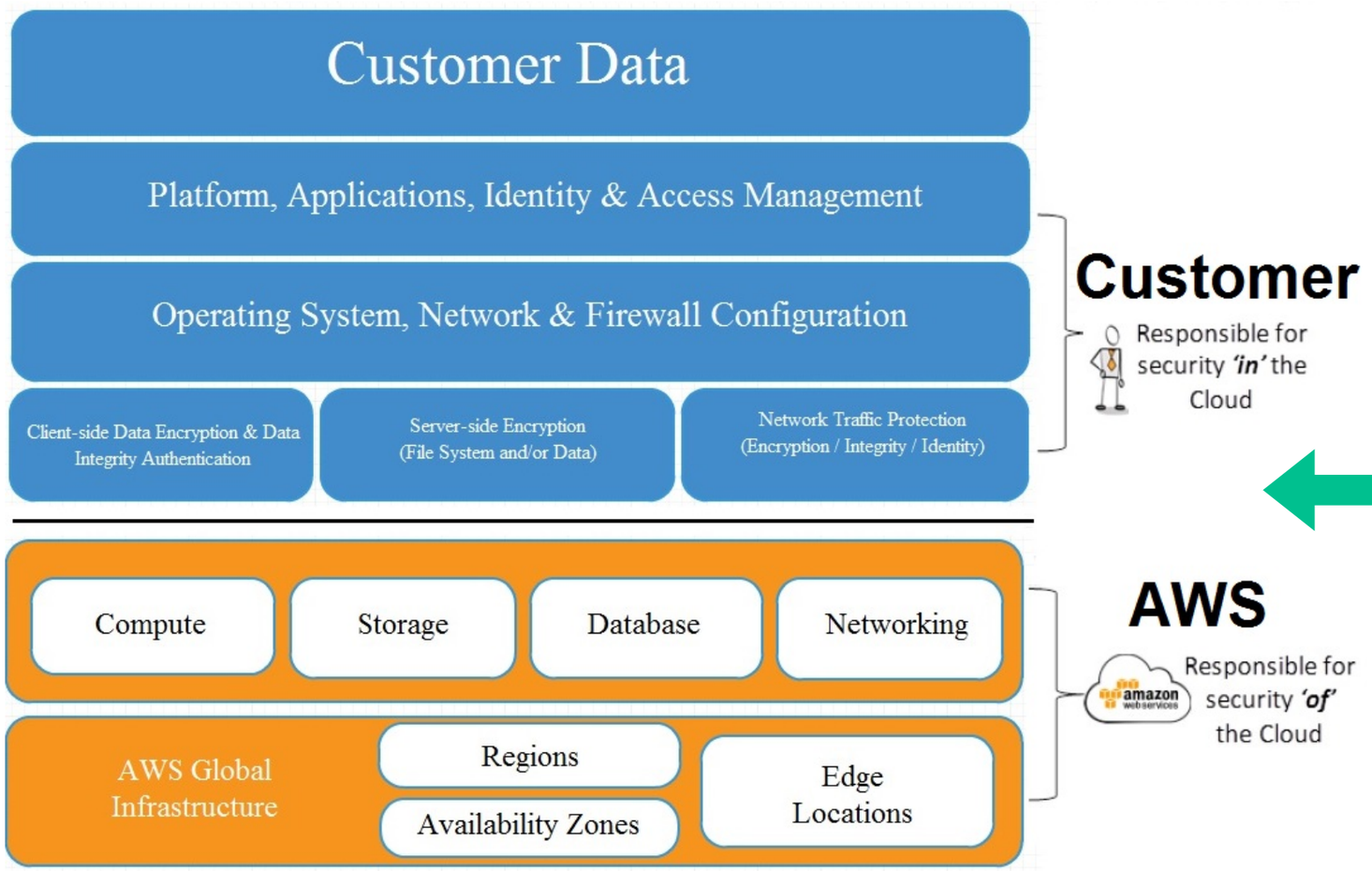
33%

Managing Hosted Private Clouds with Third-Party Public Cloud Services

Source: 451 Research Report: Hosting and Cloud Study 2016: The Digital Revolution, Powered by Cloud

What does security look like in the public cloud?

Public Cloud, Your Responsibility



Customer is responsible for the items that are:

1. Hardest
2. Most expensive
3. Most relevant to compliance

It's More than Tools

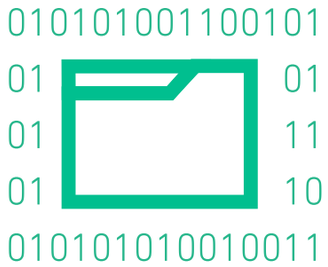
Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft

Source: Gartner Report: Forecast: Public Cloud Services, Worldwide, 2013-2019, 3Q15 Update

ARMOR

Security from the Inside Out

The recent evolution in data security thinking is helping organizations improve the management of their security from the inside out.



Classify the data, then protect

Build a host-level strategy

Establish a protected enclave

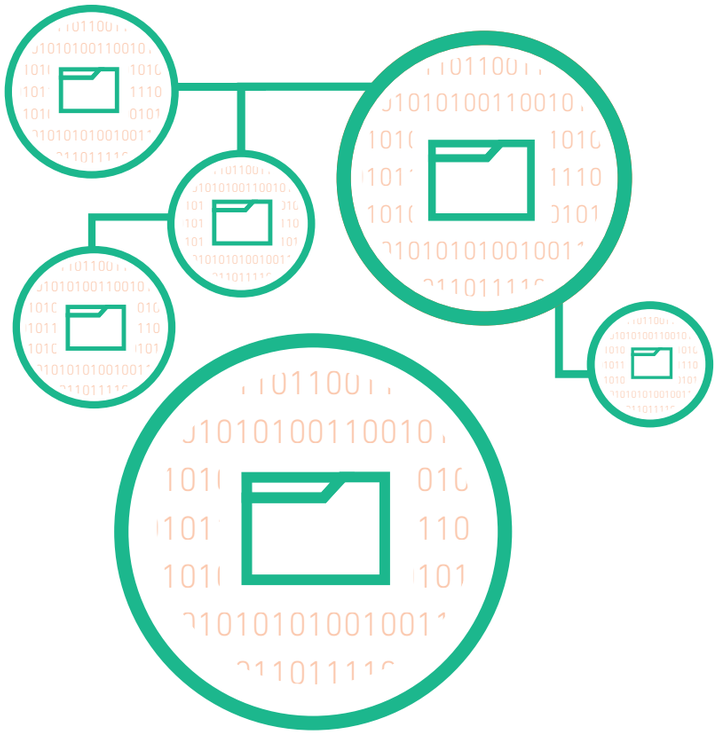
Encrypt data at different levels

It's time we transform big data problems into a small data solution

How do I approach securing my workloads?

What is Data Classification?

Simply put, data classification is the tagging of data with meaningful description, so an organization knows what level of protect it requires based on its data classification policy.



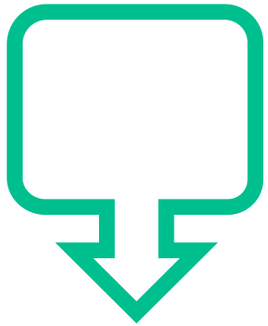
- Not all data are equal in the eyes of the threat actors
- Only about 30% of all data has significant value to criminals
- It is important to classify data to ensure the most valuable data is given priority protection

3 Levels of Data Classification

SEVERE — HIGH	ELEVATED — MODERATE	LOW — MINIMUM
High-Risk and/or High-Availability Production Workloads	**QA, Testing, Staging or Production Workloads**	**Public Information**
DATA & PERFORMANCE NEEDS • "Tier 0" applications • Applications/data with PII that require high-level access • Data and application security • Requires compliance with industry (PCI) or regulatory (HIPAA) mandates • Intellectual property • High-availability architecture • Low-latency performance requirements	**DATA & PERFORMANCE NEEDS** • Non-production data • No personally identifiable information (PII) or company IP • Risk-based level of security performance and availability • Early-stage development	**DATA & PERFORMANCE NEEDS** • Data that's already publicly available • Non-sensitive files

Focus on the Instance

Guest OS



Application

Access Control

Live Poll

Armor | Anywhere

Managed security for any cloud. Anywhere

1

Extends Armor's proven threat intelligence and cyber security solutions to protect workloads.

Adds security to any environment.

2

Improves security posture and allows companies to focus on their primary business.

Reduces the complexity of DIY.

3

Designed for sensitive workloads.

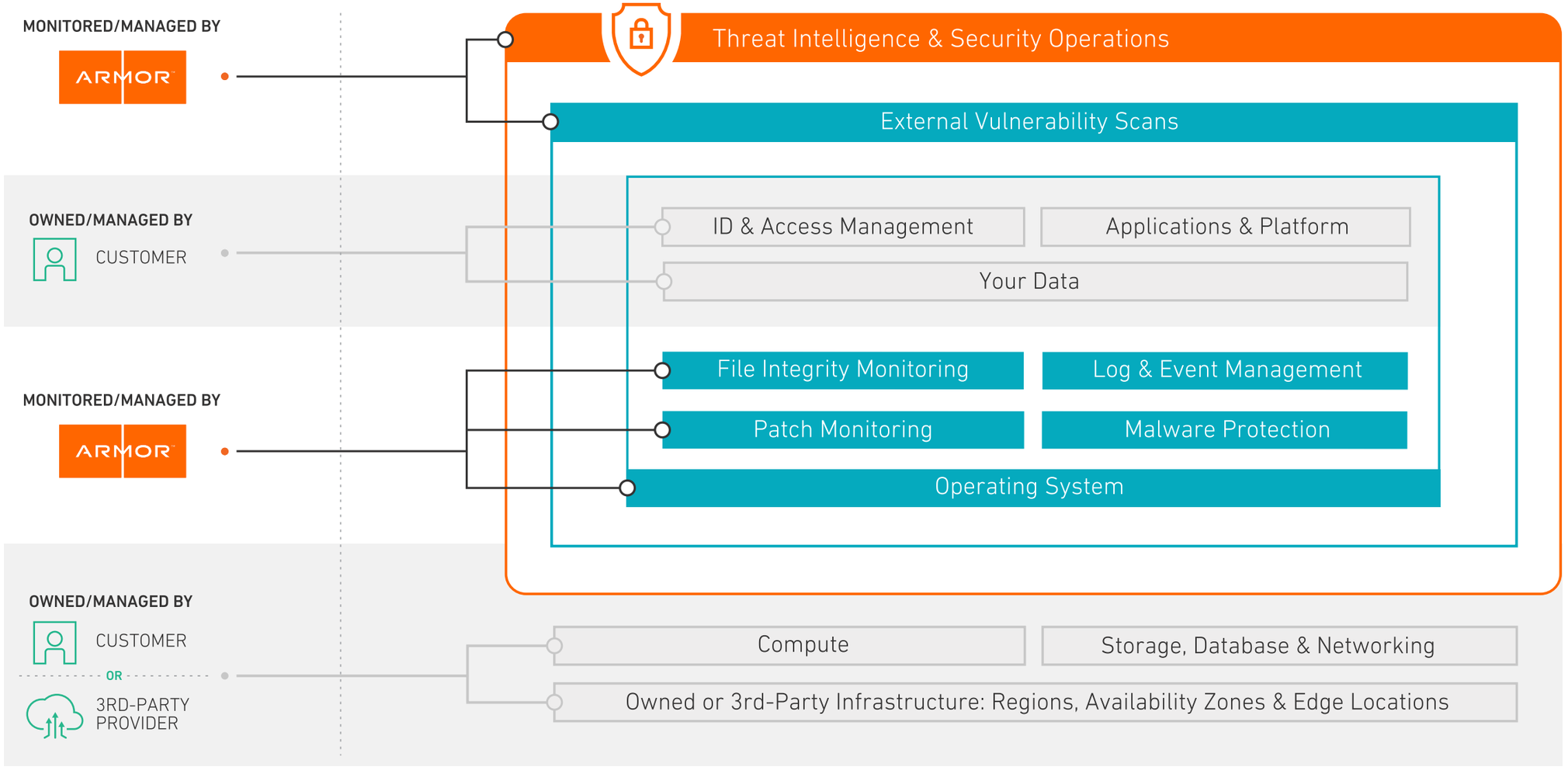
Secures private information, company IP, and PII.

DIY versus Security-as-a-Service

SECURITY LAYER	FEATURE/FUNCTIONALITY	IaaS/DIY	Armor Anywhere CORE
Network	Vulnerability Scanning	Customer	Shared
	Encryption in Transit	Customer	Armor
Server / OS	Hardened Operating System	Customer	Armor*
	Customizable Hardening Policies	Customer	Shared*
	OS Patching Monitoring	Customer	Armor
	AV / AM / Adv.Threat Detection	Customer	Armor
	Log Management	Customer	Armor
	File Integrity Monitoring	Customer	Armor
	Customizable FIM Policies	Customer	Armor*
	Customizable Scan Times	Customer	Armor*
	Host Intrusion Detection	Customer	Armor*
Security Operations	Security Monitoring (SIEM)	Customer	Armor
	Threat Intelligence	Customer	Armor
	Incident Management	Customer	Armor

*Available 2H 2016

Shared Responsibility with Armor Anywhere



Inside Armor | Anywhere

Security-as-a-Service

Adds proven security to commodity public cloud infrastructure.

Omnipresent Defense

With OS-level defense and monitoring, designed to protect instances wherever they reside.

Complementary Security

Combination of a tool and managed service.

Detection & Response

Proactive threat intelligence and real-time alerts on public cloud environment

Compliance Ready

Eases your path to PCI and HIPAA compliance

How is Armor Anywhere Impacting Customers?

Implementing a Consistent Security Posture Across Multiple Clouds

PEOPLE MATTER®

SITUATION	Workforce management company with true multi-cloud environment
CUSTOMER NEED	Integrated security across all clouds
WHY ARMOR?	Proven security posture and managed support
SOLUTION & RESULTS	Reduced risk of data loss through increased security on commodity infrastructure

Real-Time Threat Alerts and Real-Time Defense

SITUATION	Start-up providing workplace process management in highly regulated industries
CUSTOMER NEED	Restricted to datacenter location and security and compliance requirements
WHY ARMOR?	Managed security for highly sensitive data
SOLUTION & RESULTS	Active threat intelligence and real-time alerts identified and defeated two attacks from external threat actors

Demo Time

Q&A

Join the Armor Partner Program

Are you a:

- Managed Service Provider
- Reseller Partner
- Technology Alliance Partner
- Referral Partner

Complete the post-event survey and let us know!

If so we want you to join the New Armor Partner Program

- Rich Incentives
- Marketing, Sales and Technical Resources
- Partner Community Portal
- And much more

ARMOR™

BETWEEN YOU AND THE THREAT

Thank You

RUSS MURRELL VICE PRESIDENT, PRODUCT MANAGEMENT

SARAH ECK DIRECTOR, PRODUCT MARKETING

The Leader in Active Cyber Defense

MAY 26, 2016