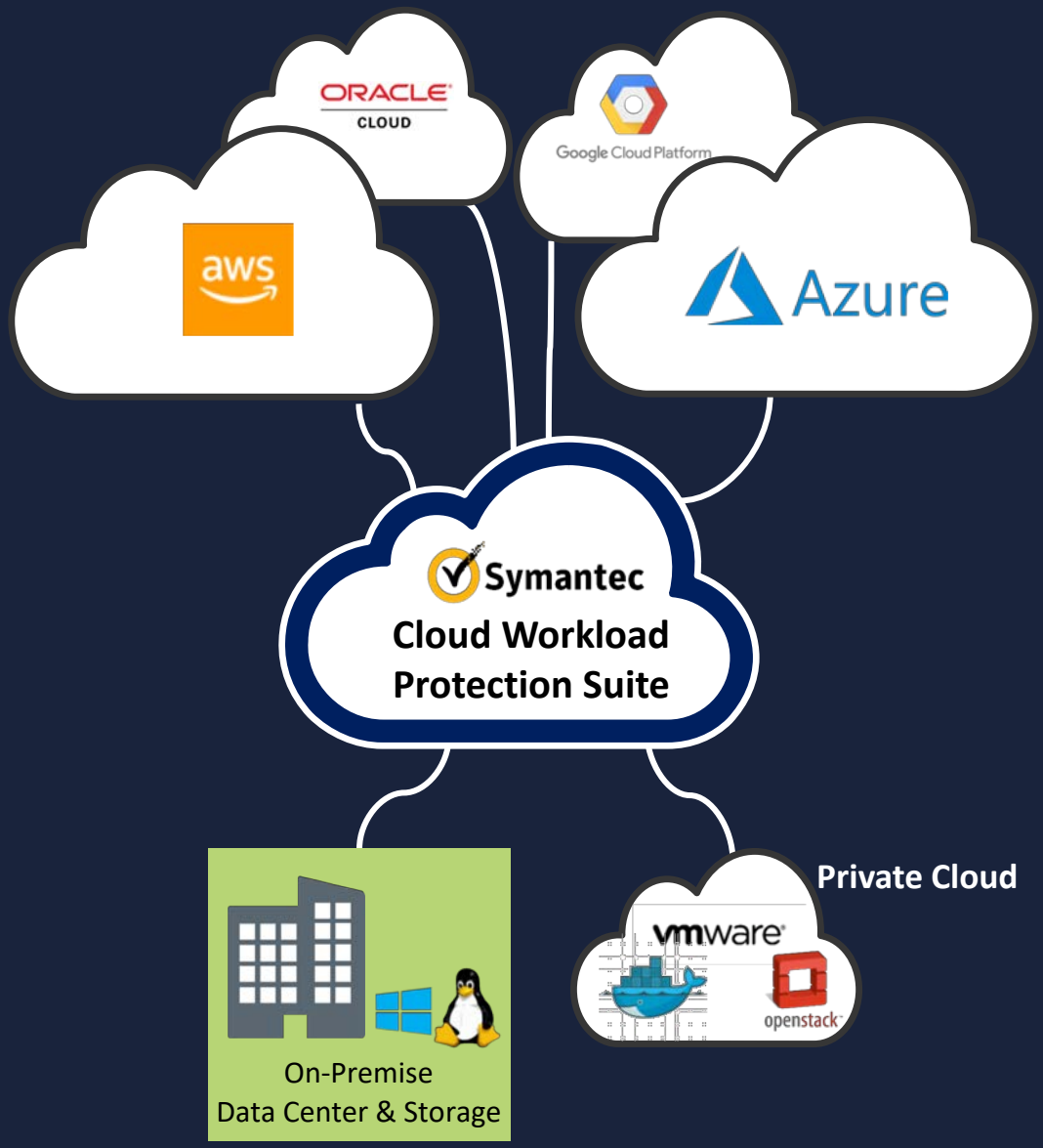
IaaS Security

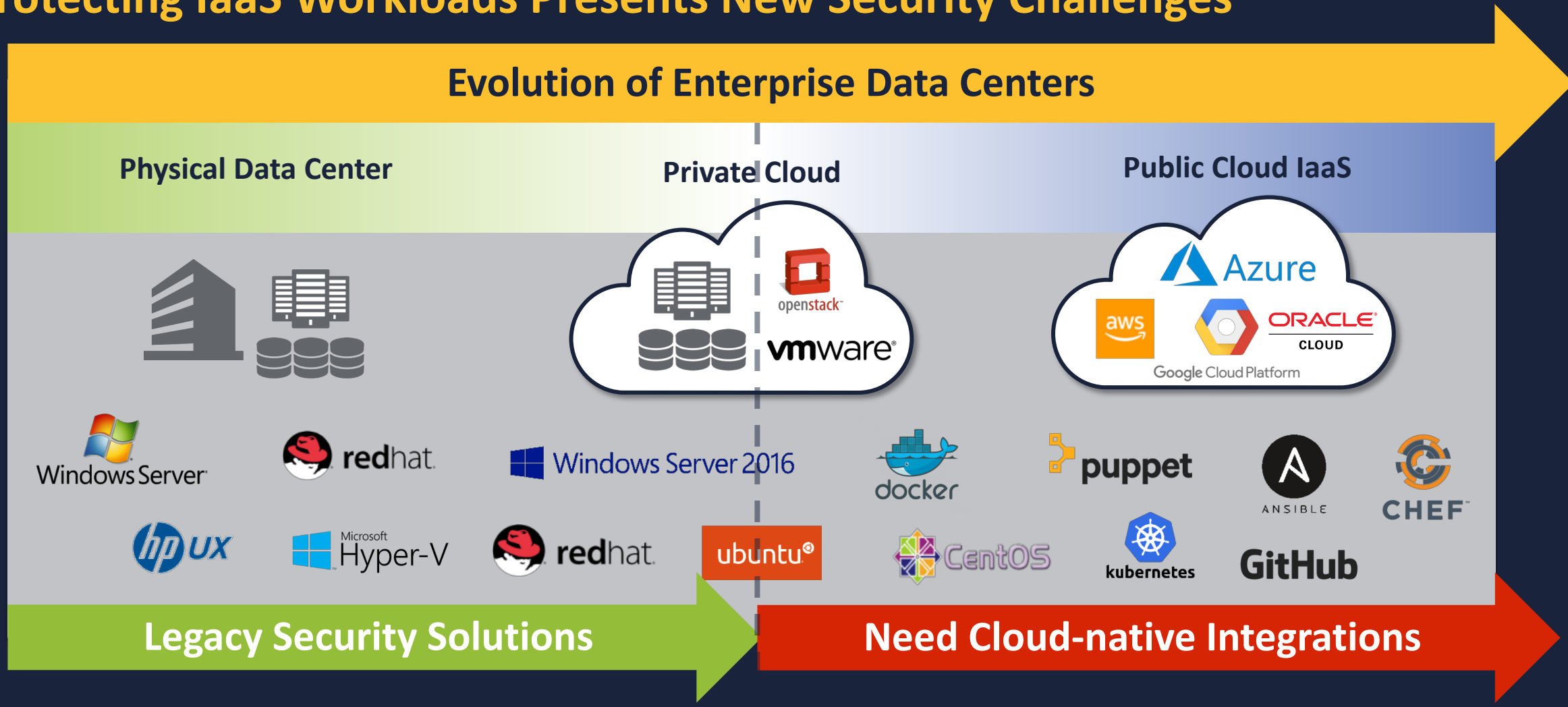
Sheetal Venkatesh,

Product Management

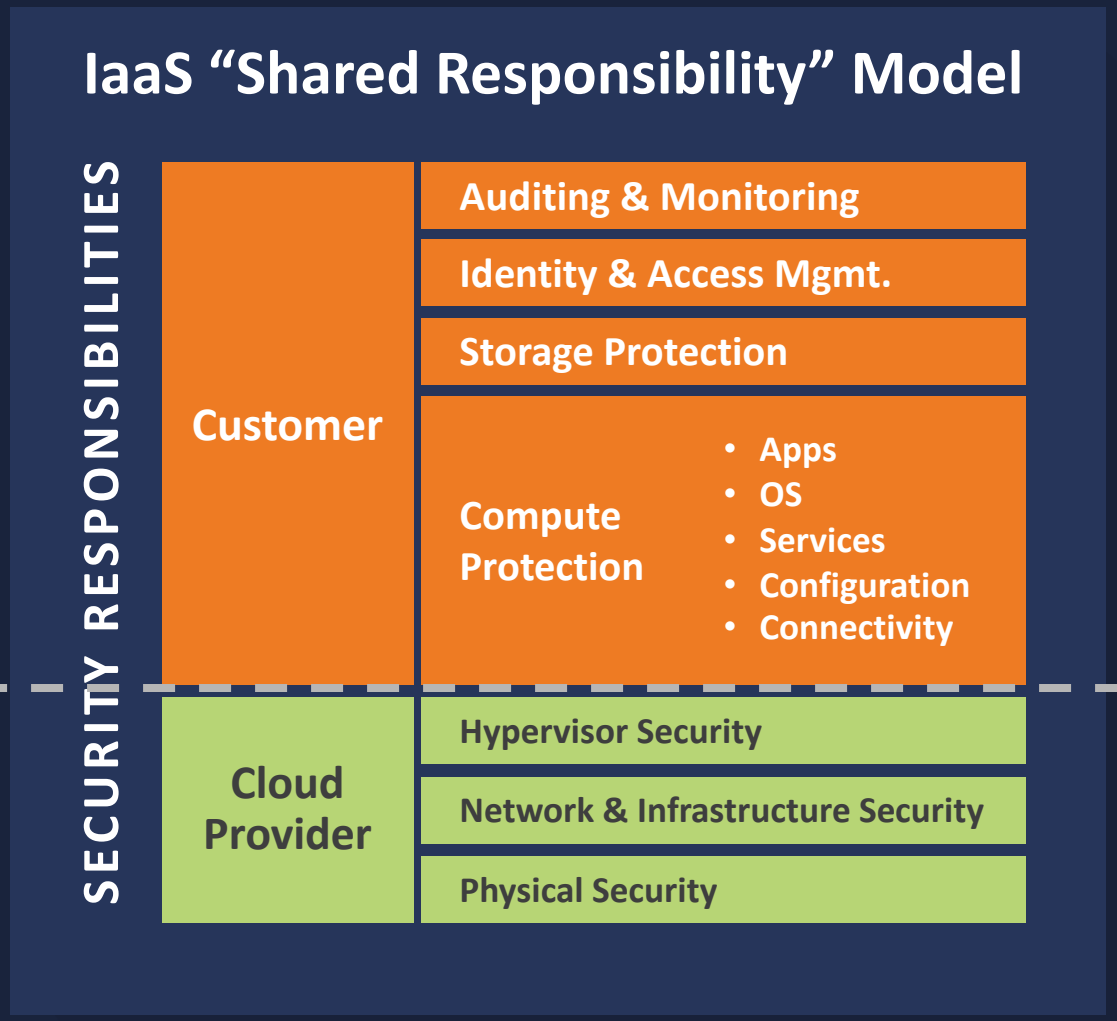


Today's Reality: Cloud and "Hybrid" Data Centers

Protecting IaaS Workloads Presents New Security Challenges



Cloud Changes the Security Model



Enterprises responsible for:

- Security of workloads, apps, data, and accounts
- Everything above the Hypervisor

Critical Issues with Moving Workloads to the Cloud

Security Responsibilities Don't Go Away

Shadow IaaS Compute and Vulnerabilities

- Incomplete workload visibility and security status
- Unprotected and unpatched IaaS compute and containers

Limited Visibility

Ransomware

IaaS Storage Infection and Misconfiguration

- Storage can be used to house and distribute malware
- Risk of data breach and compliance violations

Malware

Data Breaches

Increased Risk Profile and Compliance Violations

- Missing or inadequate security controls increase risk
- Compromised accounts and compliance issues

Non-compliance

Need Protection for Legacy/Hybrid Cloud Workloads and Storage

- Many enterprises are using a Hybrid Cloud approach
- Workloads remaining on-premises still need protection

Legacy Workloads

Attackers Targeting Cloud Vulnerabilities

Unpatched Systems and Misconfigured Storage Lead to Data Breaches

Case Study:
Attack on Compute

Open Source Software Vulnerability

Victim: Large Credit Reporting Agency

Information Targeted: Customer Database

Method of Attack:

- Unpatched Apache Struts vulnerability enabled compromise of corporate web servers
- Attackers gained access to databases with transactional information and PII

Impact: Massive PII Data Breach

- Large fines and loss of credibility
- Loss of data integrity requiring complete restore and rebuild

Case Study:
Attack on Storage

Amazon S3 Data Breach

Victim: Unnamed Military Outfit

Information Targeted: Military Personnel Records

Method of Attack:

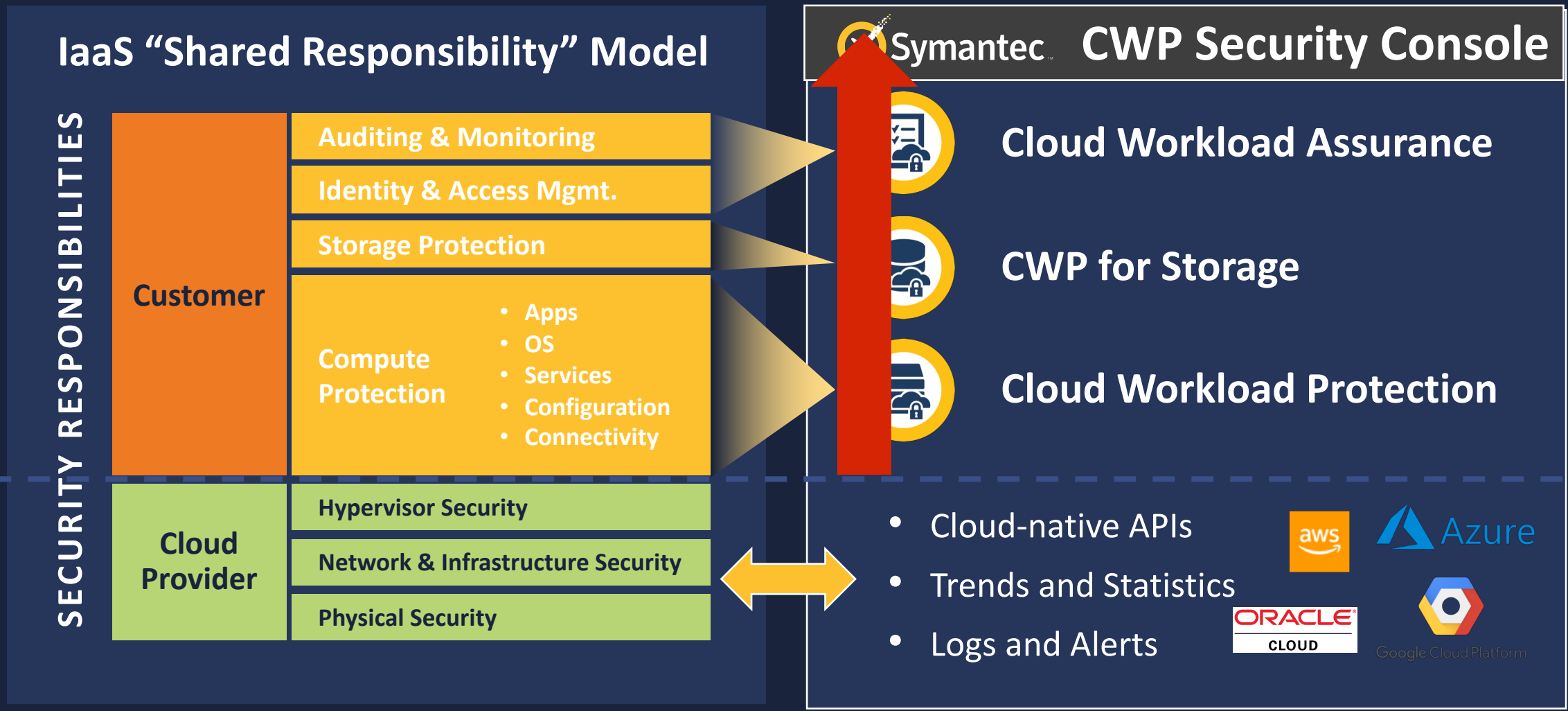
- Applications from military recruits (Word Docs) accepted by front-end containers, then written to Amazon S3 buckets
- Misconfigured Amazon S3 buckets enabled attacker to access recruit applications

Impact: PII Data Breach

- Exposure of highly sensitive personnel records
- Malware remediation required

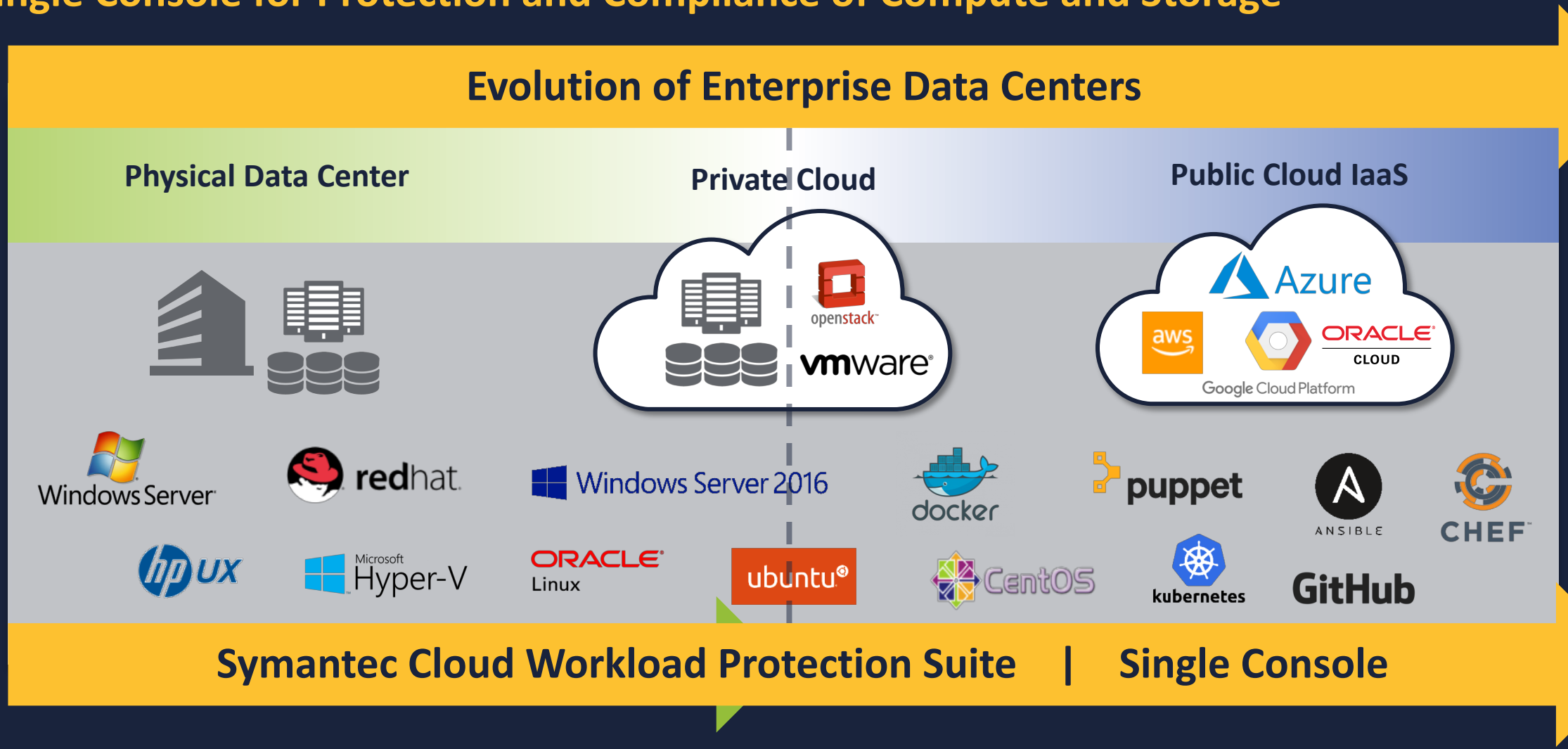
Symantec Cloud Workload Protection Suite

Cloud-native, Single Console Security and Compliance for IaaS



Symantec Cloud Workload Protection Suite

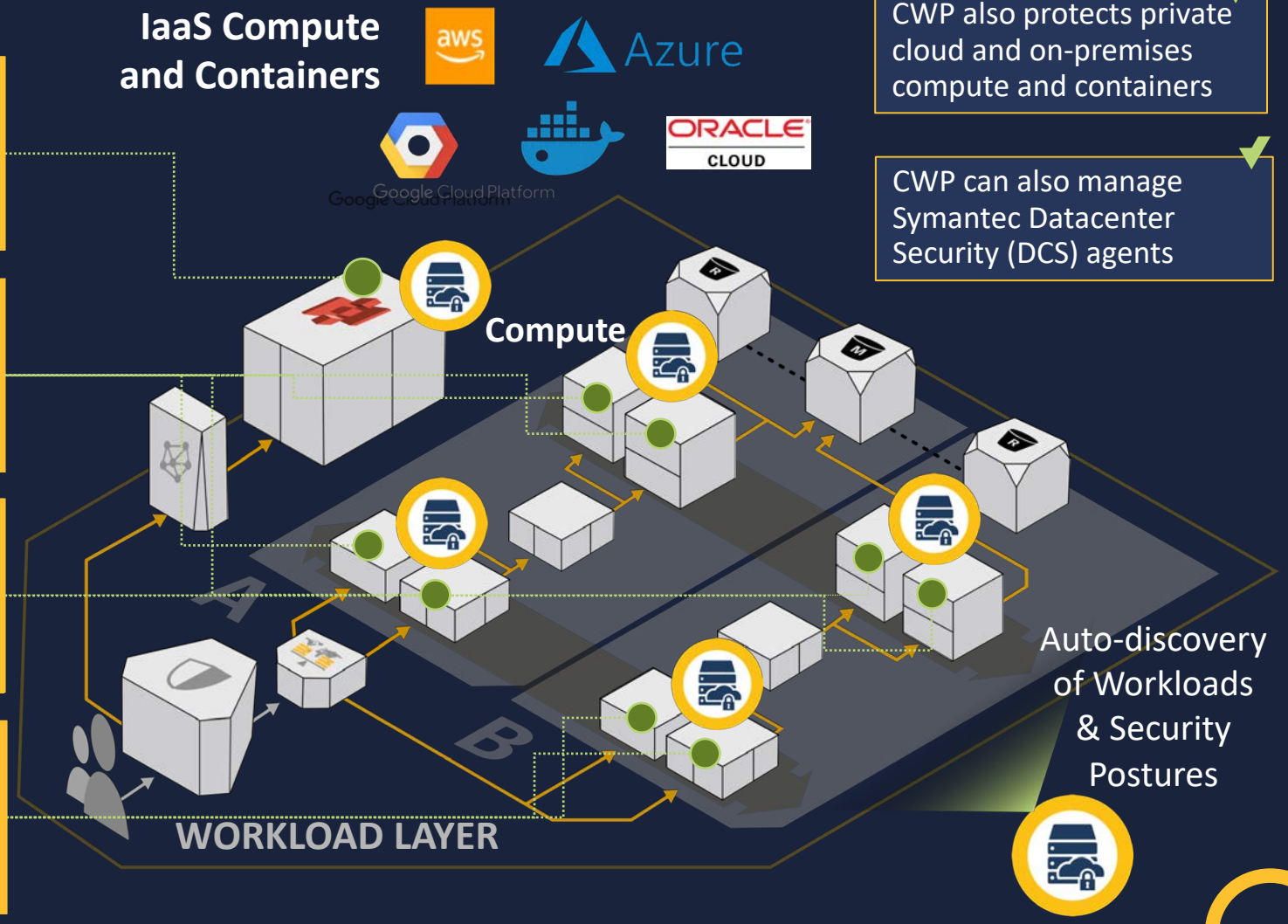
Single Console for Protection and Compliance of Compute and Storage



Solution: Cloud Workload Protection (CWP)

Securing IaaS and Hybrid Cloud Compute and Container Workloads

Discover and remediate malware using industry-leading SEP anti-malware technologies	ANTI-MALWARE
Lock down system configuration files and isolate processes to protect against zero-day attacks	RT-FIM OS HARDENING
Allow only authorized applications into production and block advanced threats to reduce attack surface	APP CONTROL APP ISOLATION APP FIREWALL
Identify attacks targeting container infrastructure, even at the kernel level, and block them before they can propagate	CONTAINER PROTECTION



CWP also protects private cloud and on-premises compute and containers

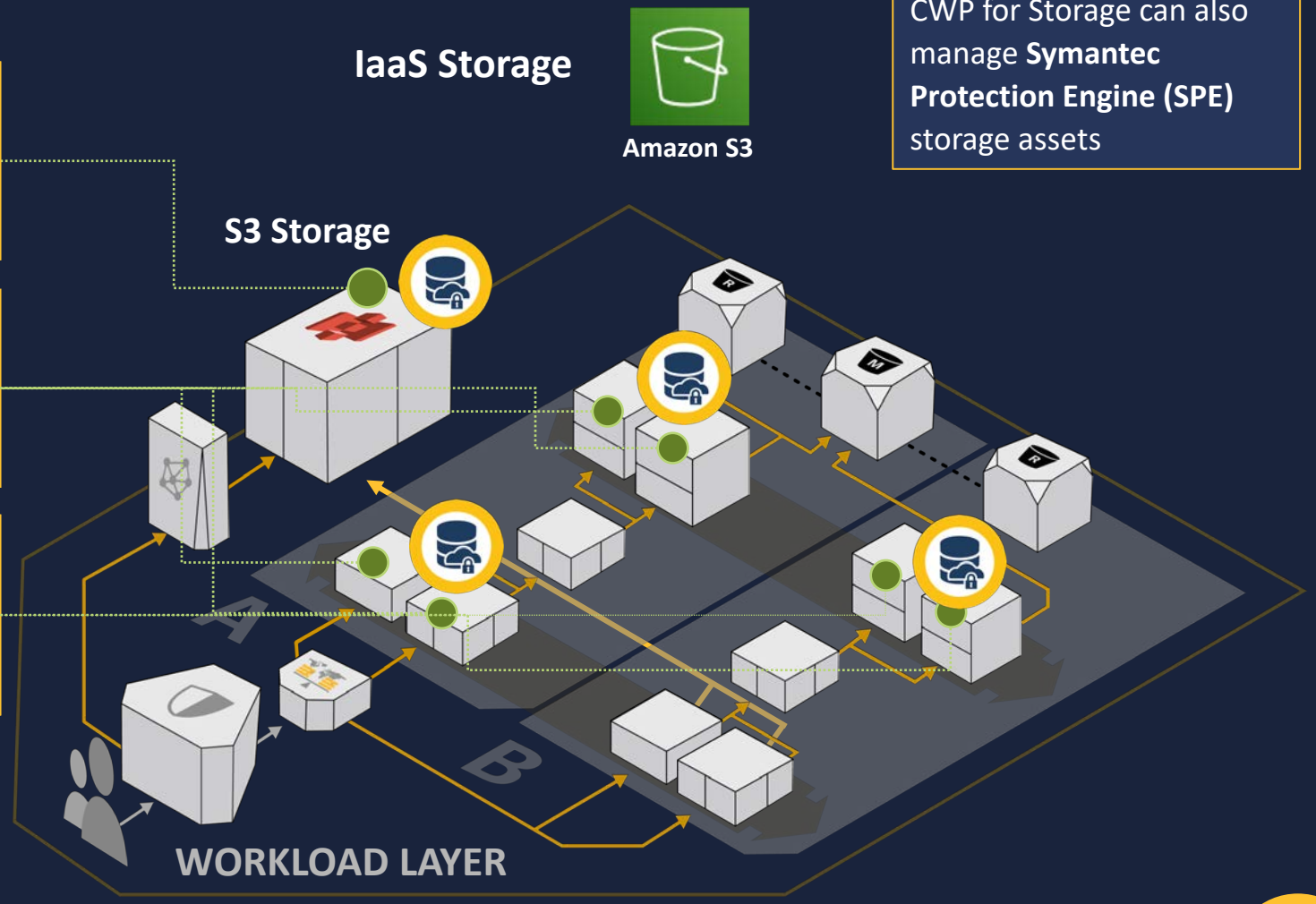
CWP can also manage Symantec Datacenter Security (DCS) agents

Solution: Symantec CWP for Storage

Securing IaaS Cloud Storage

Discover and remediate malware and threats in IaaS storage before they can spread to apps and users	**ANTI-MALWARE**
Alert when storage buckets are misconfigured or exposed to the public internet to prevent data leakage	**PUBLIC ACCESS ALERTS**
Apply DLP policy to discover and tag sensitive information in IaaS storage to align with compliance mandates	**DLP INTEGRATION**

CWP for Storage with DLP extends on-premises DLP policy to Amazon S3 buckets

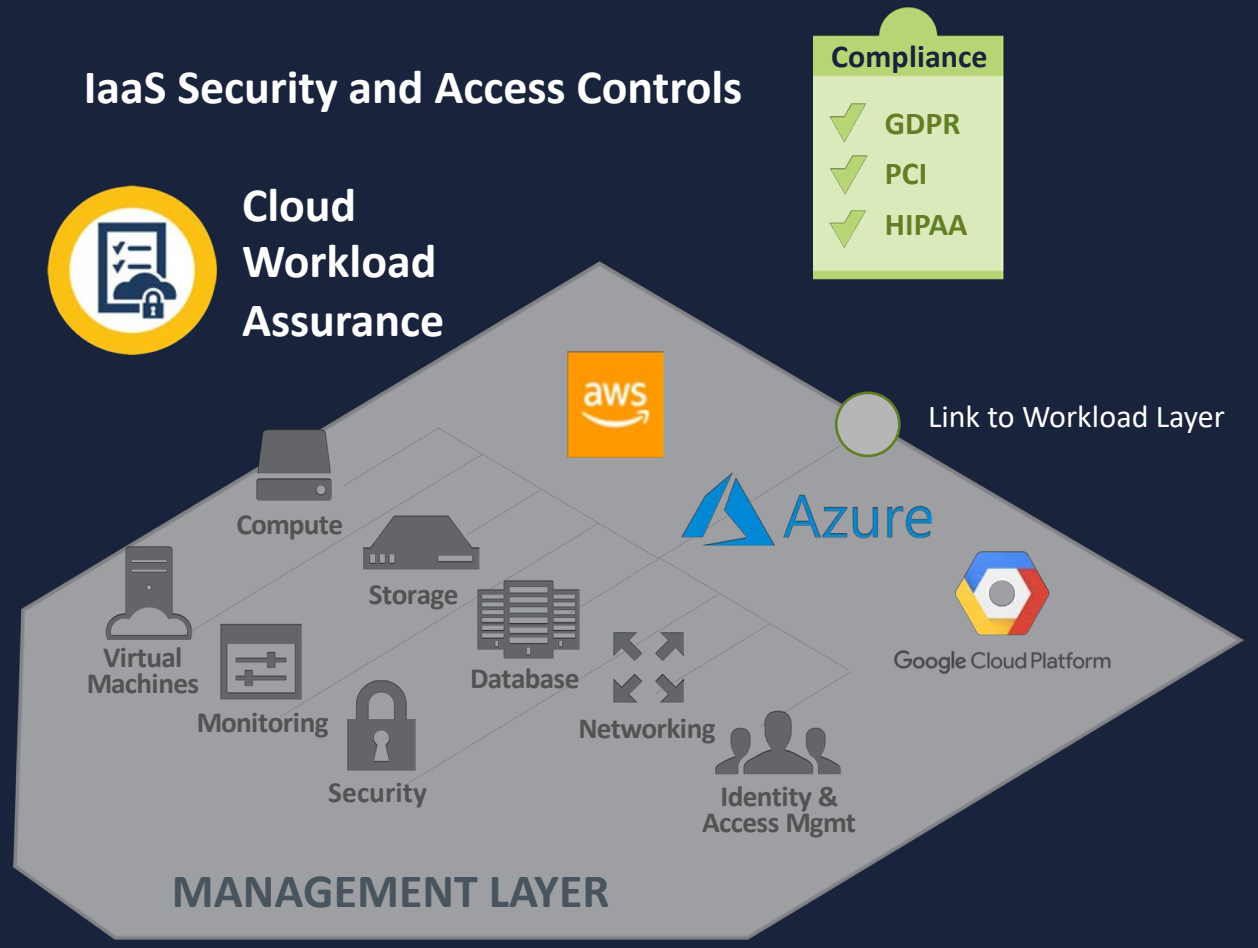


CWP for Storage can also manage **Symantec Protection Engine (SPE)** storage assets

Solution: Cloud Workload Assurance (CWA)

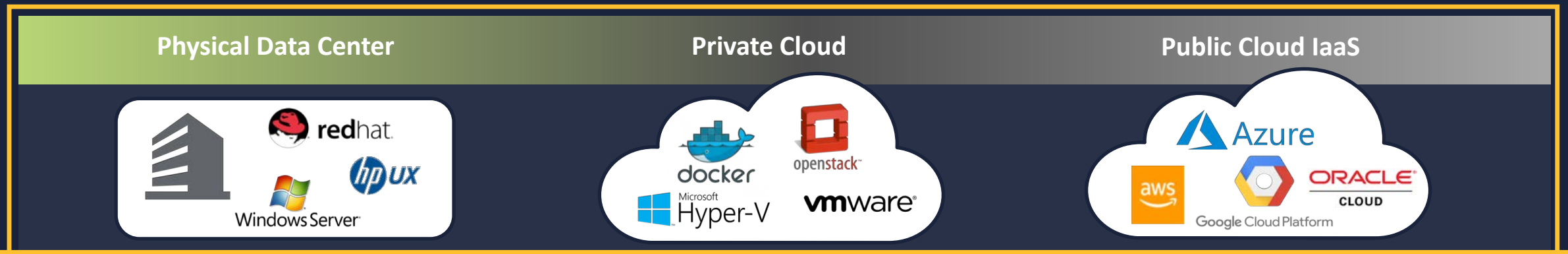
Manage risk and compliance for multi-cloud environments

Discover all cloud resources and view their security postures in a centralized console	**RESOURCE DISCOVERY**
Monitor security settings and infrastructure changes and alert on policy violations	**CONFIGURATION MONITORING**
Benchmark security policies and settings against industry best practices and regulations	**COMPLIANCE ASSESSMENT**
Quickly remediate misconfigurations and apply security policies to improve security posture and maintain compliance	**AUTO-REMEDIATION**



Symantec Cloud Workload Protection Suite

Products and Protections



Symantec Cloud Workload Protection Suite | Single Console

Products	**CWP Anti-Malware***	**Cloud Workload Protection (Security for IaaS and Hybrid Cloud Compute and Containers)**					**CWP For Storage**	**Cloud Workload Assurance**
Protections	**ANTI-MALWARE FOR COMPUTE** Discover and eradicate malware targeting compute instances	**REAL-TIME FILE INTEGRITY MONITORING** Prevent unauthorized changes to infrastructure and app files	**OPERATING SYSTEM HARDENING** Protect from OS vulnerabilities without patching	**APPLICATION CONTROL** Allow only authorized applications into production	**APPLICATION ISOLATION** Protect applications from exploits against known/unknown vulnerabilities	**APPLICATION LEVEL FIREWALL** Reduce attack surface and block advanced threats	**ANTI-MALWARE AND DLP FOR IAAS STORAGE** Remediate malware from IaaS storage buckets and apply DLP policy	**IAAS CONTROL PLANE SECURITY** Mange risk and compliance for multi-cloud infrastructure services

* CWP Anti-Malware is an anti-malware-only product SKU for customers who do not require compute hardening capabilities

Symantec™

Thank You