Symantec™

CLOUD SECURITY SUMMIT 2018

Securing the Cloud Generation

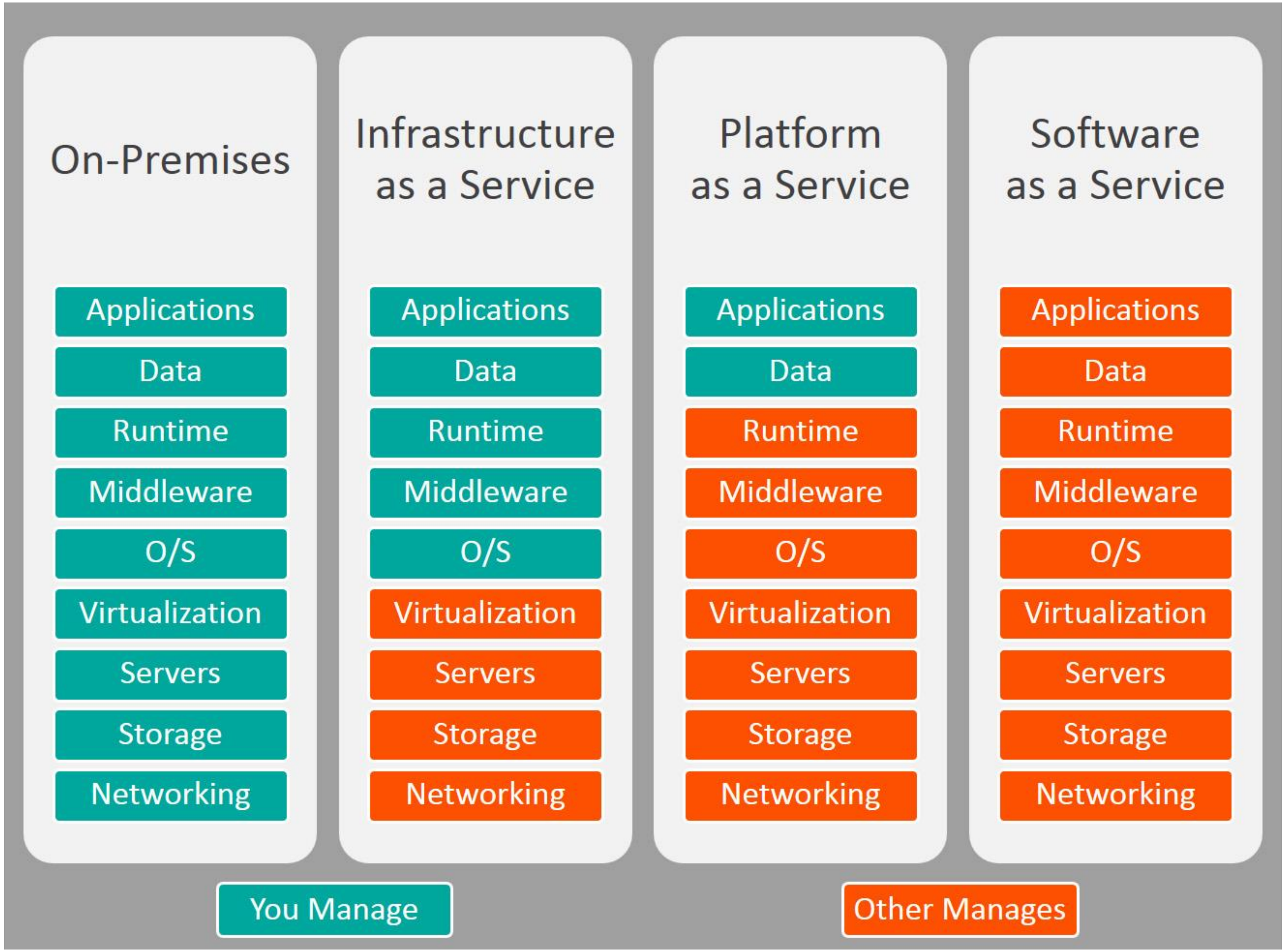
Marco Mazzoleni

Sr. Manager, Systems Engineering @Italy

31 Ottobre, 2018

GitHub
Adobe Creative Cloud
DocuSign
ORACLE
Google Cloud Platform
slack
servicenow
G Suite
rackspace
Azure
salesforce
zendesk
Dropbox
Office 365
amazon web services
LinkedIn

Who is in charge?



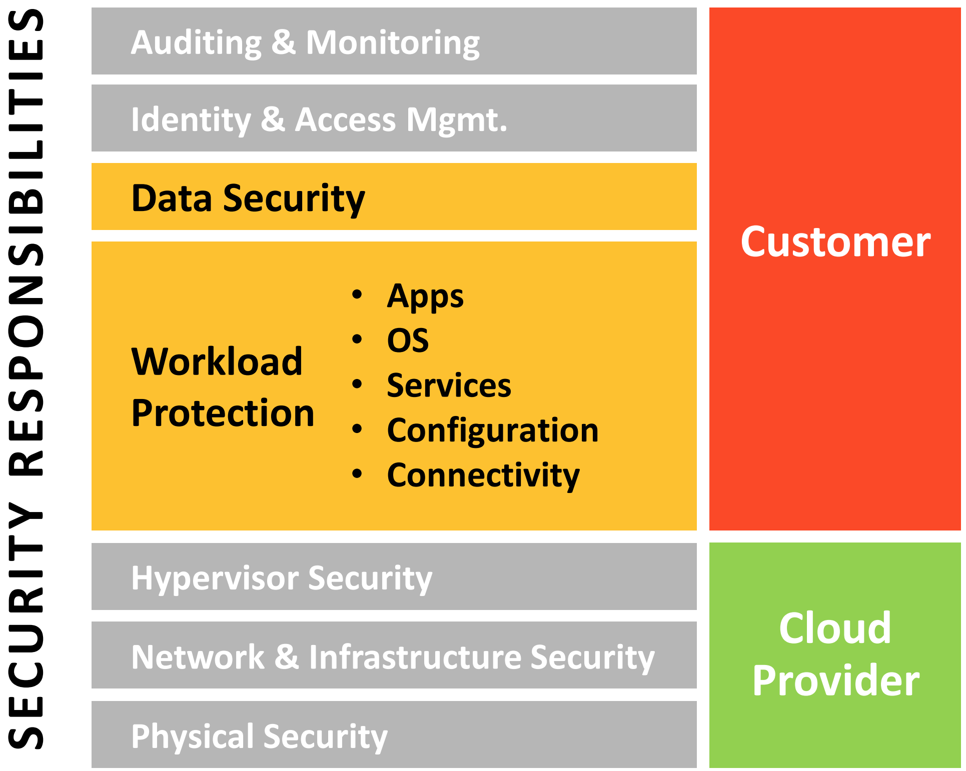
On-Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟩 Applications	🟩 Applications	🟩 Applications	🟧 Applications
🟩 Data	🟩 Data	🟩 Data	🟧 Data
🟩 Runtime	🟩 Runtime	🟧 Runtime	🟧 Runtime
🟩 Middleware	🟩 Middleware	🟧 Middleware	🟧 Middleware
🟩 O/S	🟩 O/S	🟧 O/S	🟧 O/S
🟩 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟩 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟩 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟩 Networking	🟧 Networking	🟧 Networking	🟧 Networking

🟩 You Manage

🟧 Other Manages

Shared Responsibility Models

Customers Are Still Responsible for Security



SECURITY RESPONSIBILITIES

Auditing & Monitoring

Identity & Access Mgmt.

Data Security

Workload Protection

- Apps
- OS
- Services
- Configuration
- Connectivity

Hypervisor Security

Network & Infrastructure Security

Physical Security

Customer

Cloud Provider

Public Cloud “Shared Responsibility” Model

Some Cloud Security Challenges:

- Cloud Storage left open to public access by accident
- Zero-day exploits against cloud workloads and containers
- Malware outbreak via cloud storage
- Attackers insert rogue processes into authorized workloads
- Traditional endpoint protection does not work in cloud environments!

Why you need a Security Layer

- **Security Owership**: subscriber is in charge of its own security

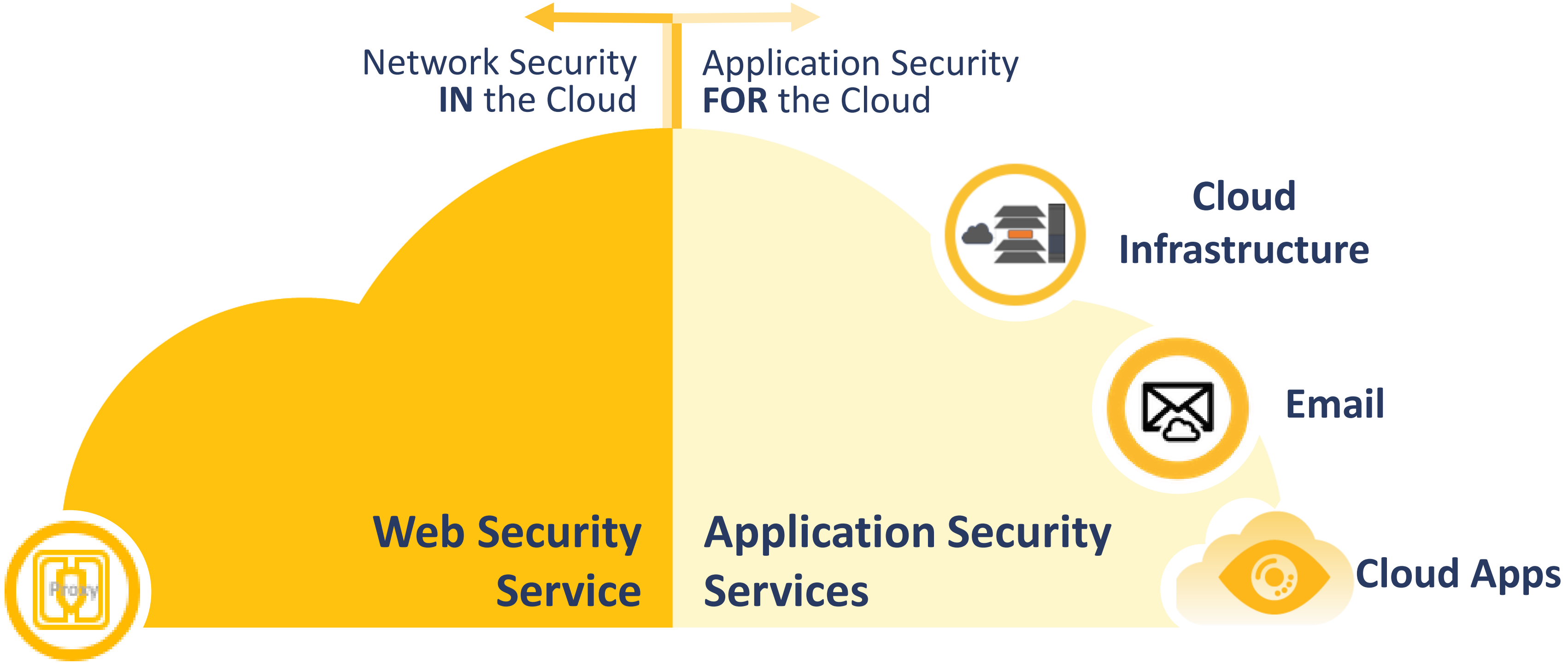
- **Information Protection**: subscriber is in charge of information use/consumption access etc

- **User Behaviour**: subscriber is in charge of endusers/administrators behavior

- **Incident Handling**: subscriber is in charge of incident management, notification and remediation

Symantec Cloud Security

Secure your cloud transformation



Network Security
IN the Cloud

Application Security
FOR the Cloud

Web Security Service

Application Security Services

Cloud Infrastructure

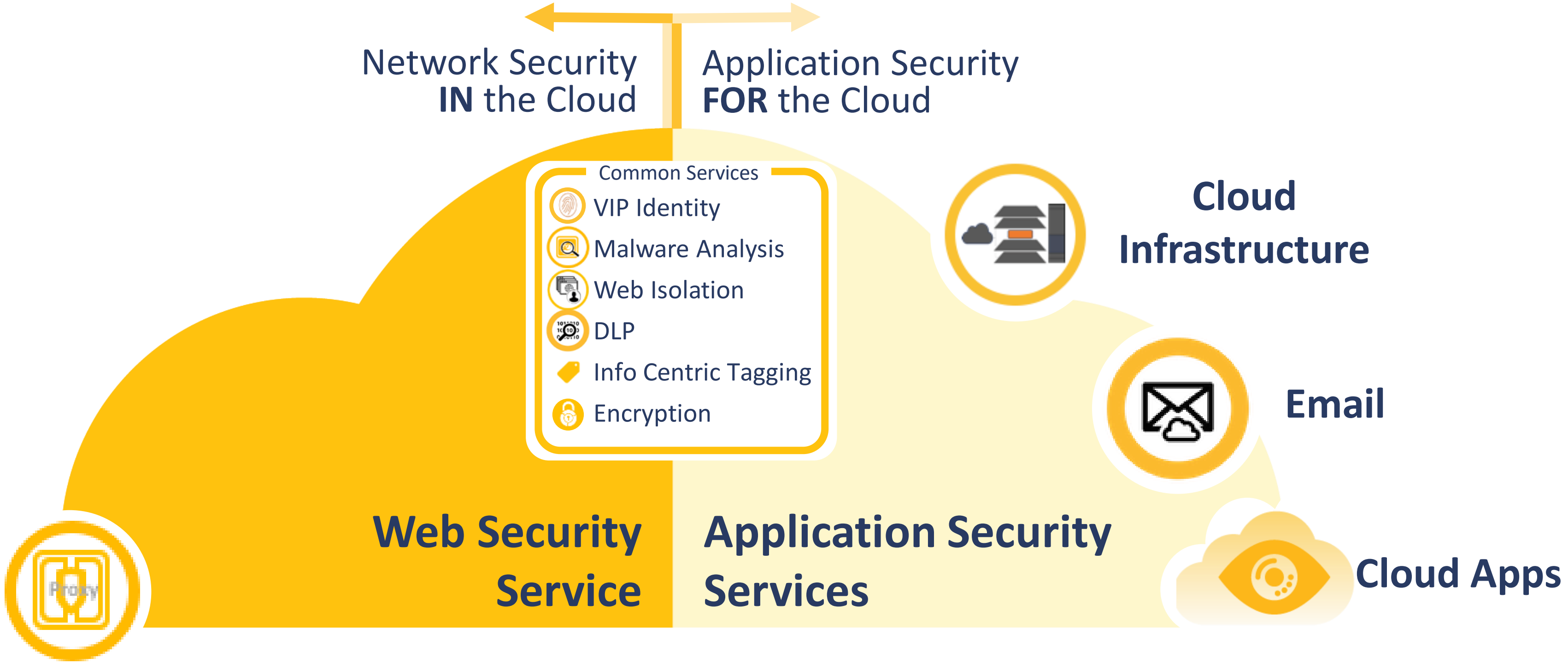
Email

Cloud Apps

- Secure remote sites and users with full network security stack IN the cloud
- Reduce MPLS backhaul costs and accelerate cloud application performance
- Migrate applications, email, and infrastructure to public cloud with confidence

Symantec Cloud Security

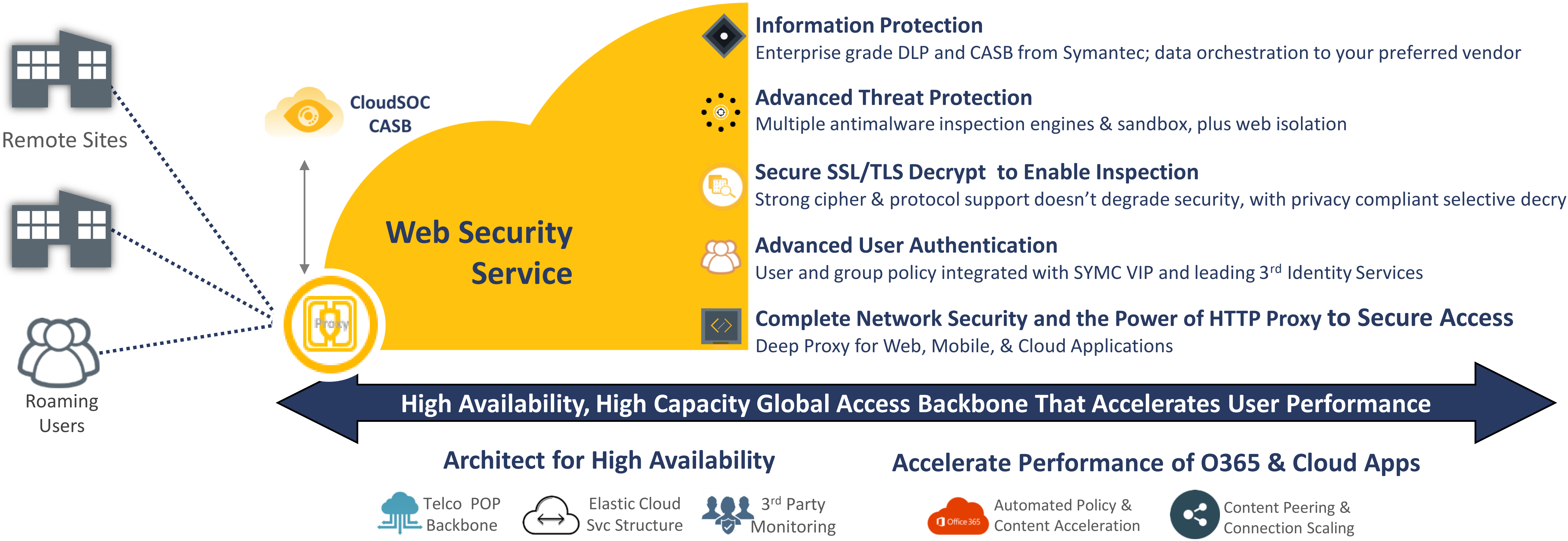
Secure your cloud transformation



- Re-architect Access Networks with a Full Network Security Stack IN the Cloud
- Migrate applications, email, and infrastructure to public cloud with confidence
- Extend enterprise grade threat and information protection to the cloud
- Unify security management across cloud, IaaS, on-prem infrastructure

Cloud Generation Network Security

A Full Network Security Stack IN the Cloud



Information Protection
Enterprise grade DLP and CASB from Symantec; data orchestration to your preferred vendor

Advanced Threat Protection
Multiple antimalware inspection engines & sandbox, plus web isolation

Secure SSL/TLS Decrypt to Enable Inspection
Strong cipher & protocol support doesn't degrade security, with privacy compliant selective decrypt

Advanced User Authentication
User and group policy integrated with SYMC VIP and leading 3rd Identity Services

Complete Network Security and the Power of HTTP Proxy to Secure Access
Deep Proxy for Web, Mobile, & Cloud Applications

High Availability, High Capacity Global Access Backbone That Accelerates User Performance

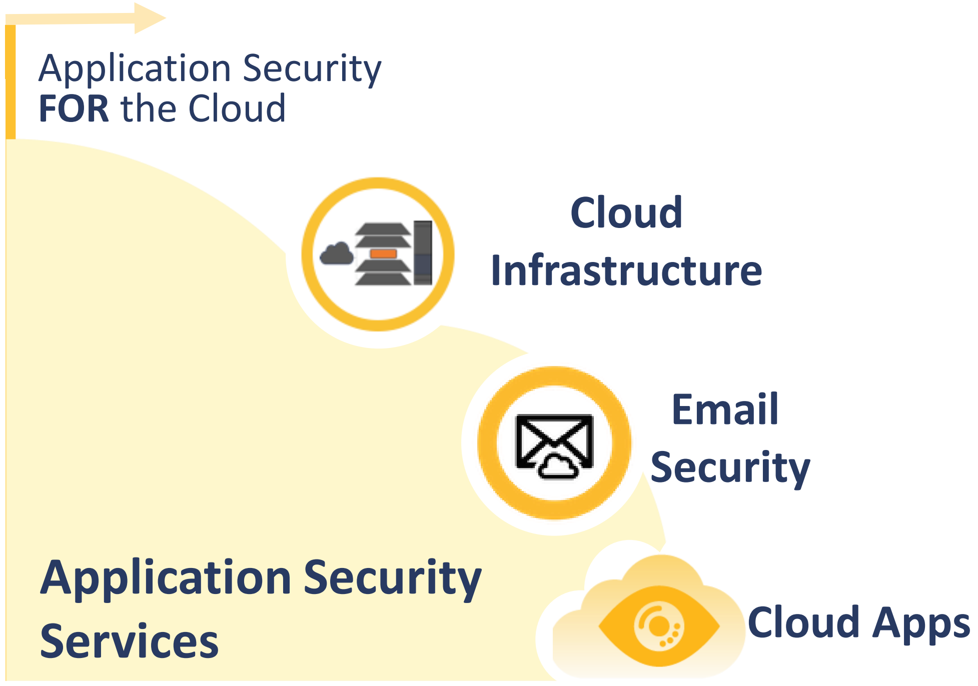
Architect for High Availability

- Telco POP Backbone
- Elastic Cloud Svc Structure
- 3rd Party Monitoring

Accelerate Performance of O365 & Cloud Apps

- Automated Policy & Content Acceleration
- Content Peering & Connection Scaling

Securing Use of Cloud Apps & Services



Application Security
FOR the Cloud

Cloud Infrastructure

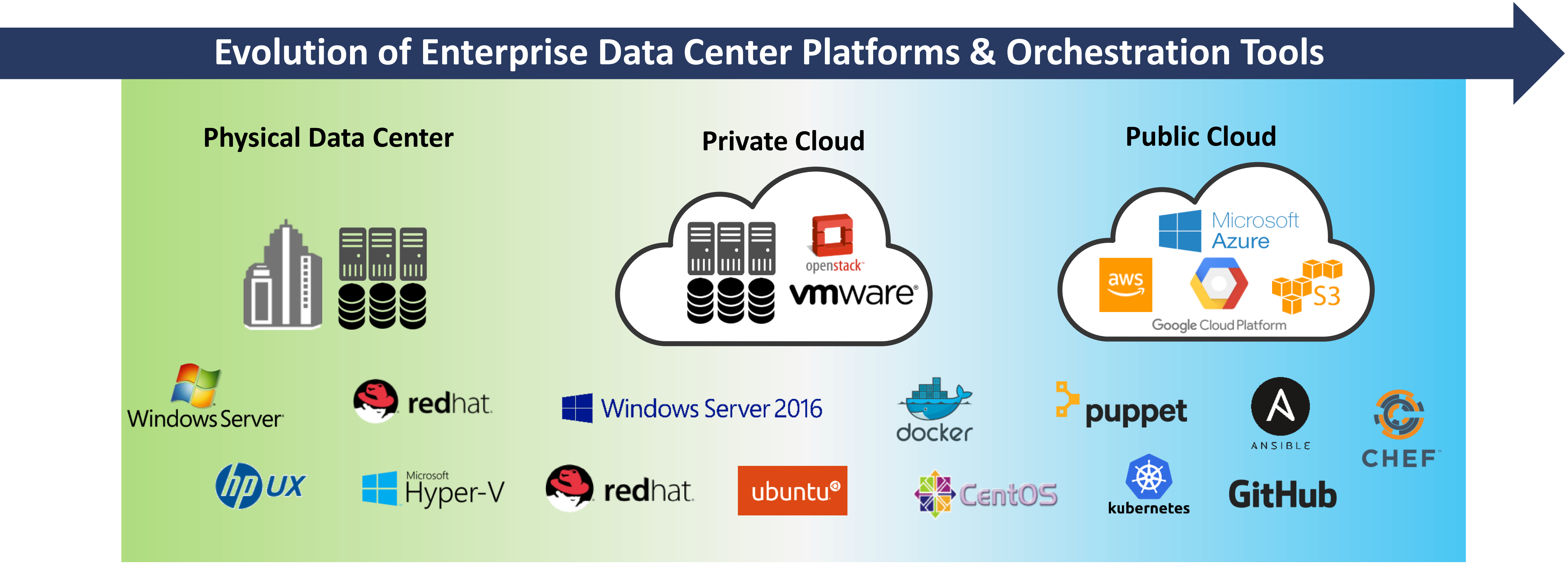
Email Security

Cloud Apps

Application Security Services

Where are you on your journey to the cloud?

Symantec.



Evolution of Enterprise Data Center Platforms & Orchestration Tools

Physical Data Center

Private Cloud

Public Cloud

Traditional / IT Ops Managed

Modern / DevOps Managed

Symantec Cloud Workload Protection

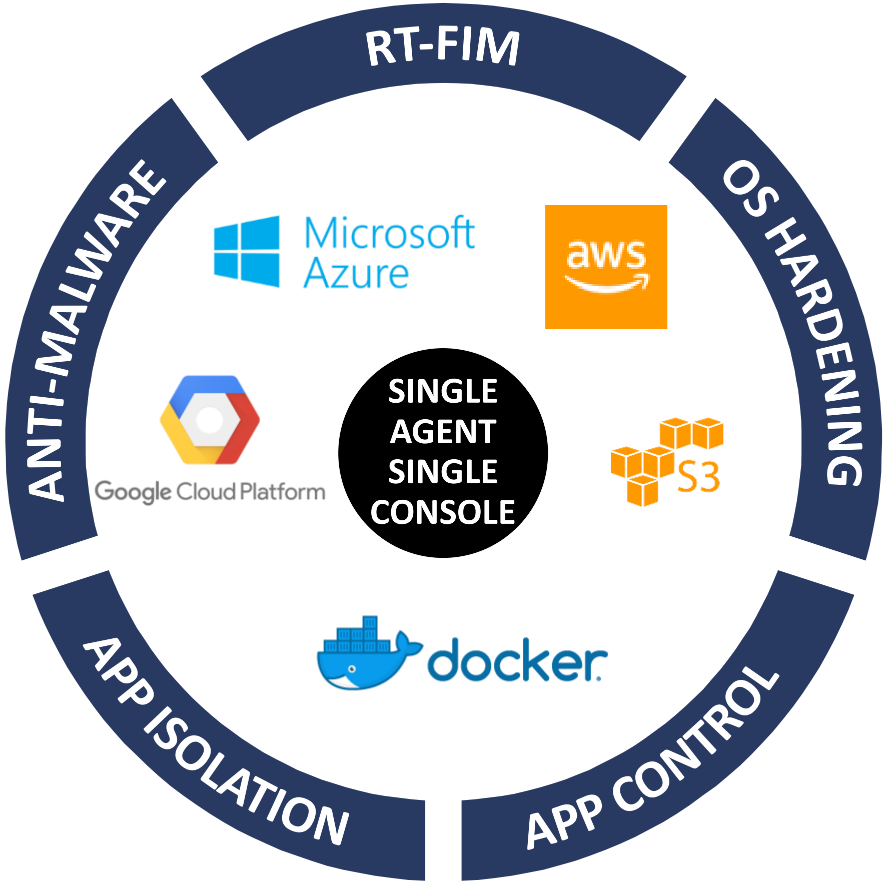
Anti-malware

For Compute:

- Multilayered cloud-native anti-malware scanning
- Prevents malware from infecting compute instances and servers

For Storage:

- Automatic and scheduled anti-malware scanning for AWS S3 buckets
- Prevents spread of malware between cloud-based applications and users



Compute Hardening

- Real-time file integrity monitoring (RT-FIM) prevents unauthorized system changes
- OS hardening stops zero-day threats
- Unique application isolation blocks exploits targeting known and unknown vulnerabilities
- Protection and monitoring for Docker containers

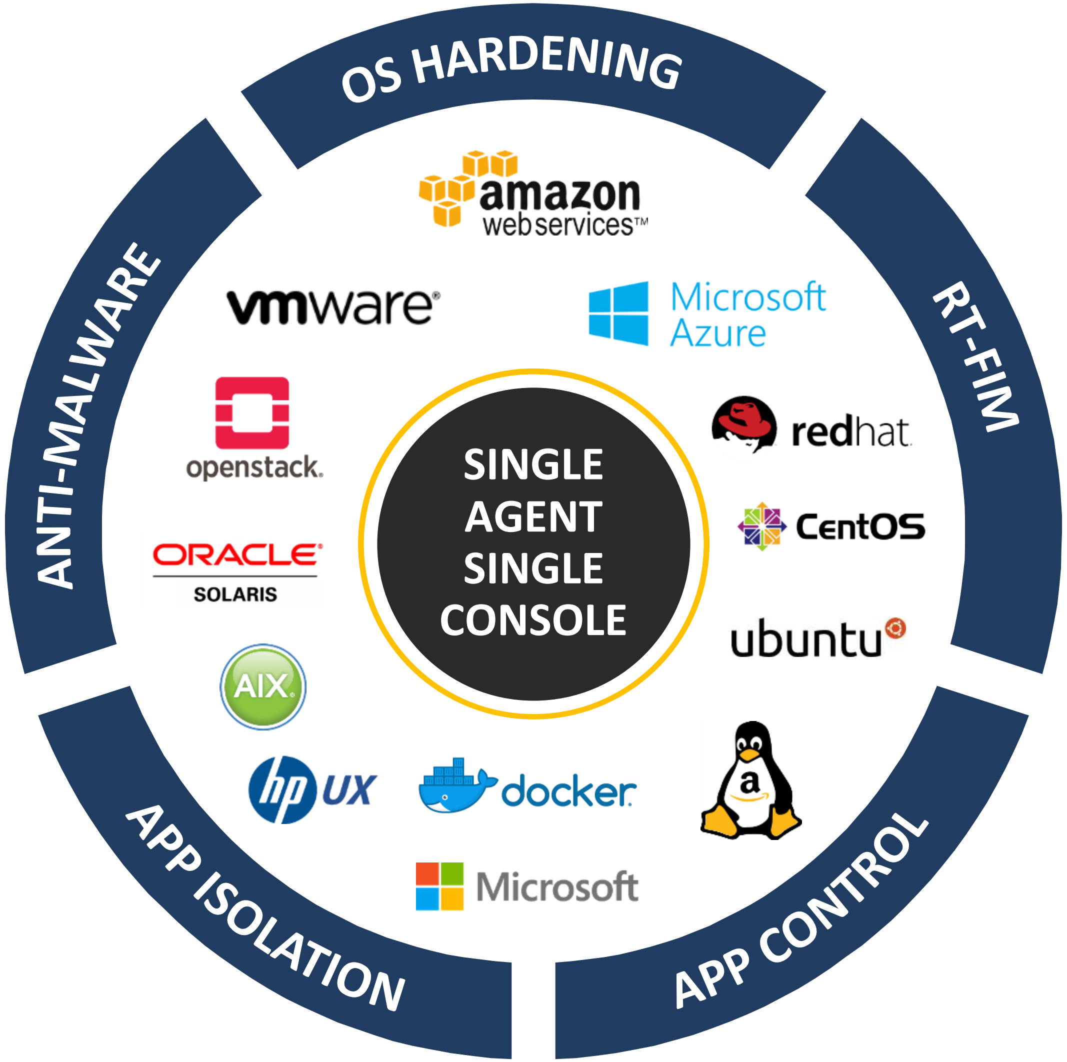
Use Case: Maintain current visibility of cloud and on-prem environments

- **Integration with all cloud, and on premise environments**.
- Security that protects your data as your business grows.
- **Single portal for all cloud security needs**.
- 24/7 monitoring and visibility, alerting for new and existing threats:
  - Threat map provides view of all cloud environments.
- Reports on exposed-to-public storage devices on AWS.
- Advanced Persistent Threat (APT) monitoring:
  - Malware that exists in your network for months, ‘phoning home’.
  - Once discovered, responding with an accurate view of your instances is critical.

Solution: Visibility with Single Agent Single Console

SINGLE AGENT

- Architecture that builds multiple "technology blades" in the same agent
- Reduces complexity and improve operational efficiency for customers



SINGLE CONSOLE

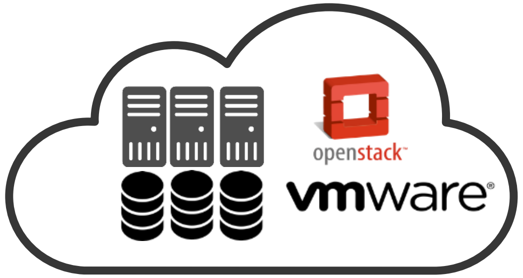
- Both On-Prem and Public Cloud workloads can be managed from the same Cloud console
- Unified policies secure both traditional and cloud workloads

Use Case: Ensure proactive, real time security everywhere

- **Automate protection** for new, and existing instances in the cloud.
  - New instances, and applications need to be protected from day one.
  - Policies that activate instantly.
- **Live alerts** for exposed storage, and data.
  - Insufficient access management can lead to a misconfiguration in your storage with public rights.
- The intelligence I have must be real time, and deploy **everywhere**.

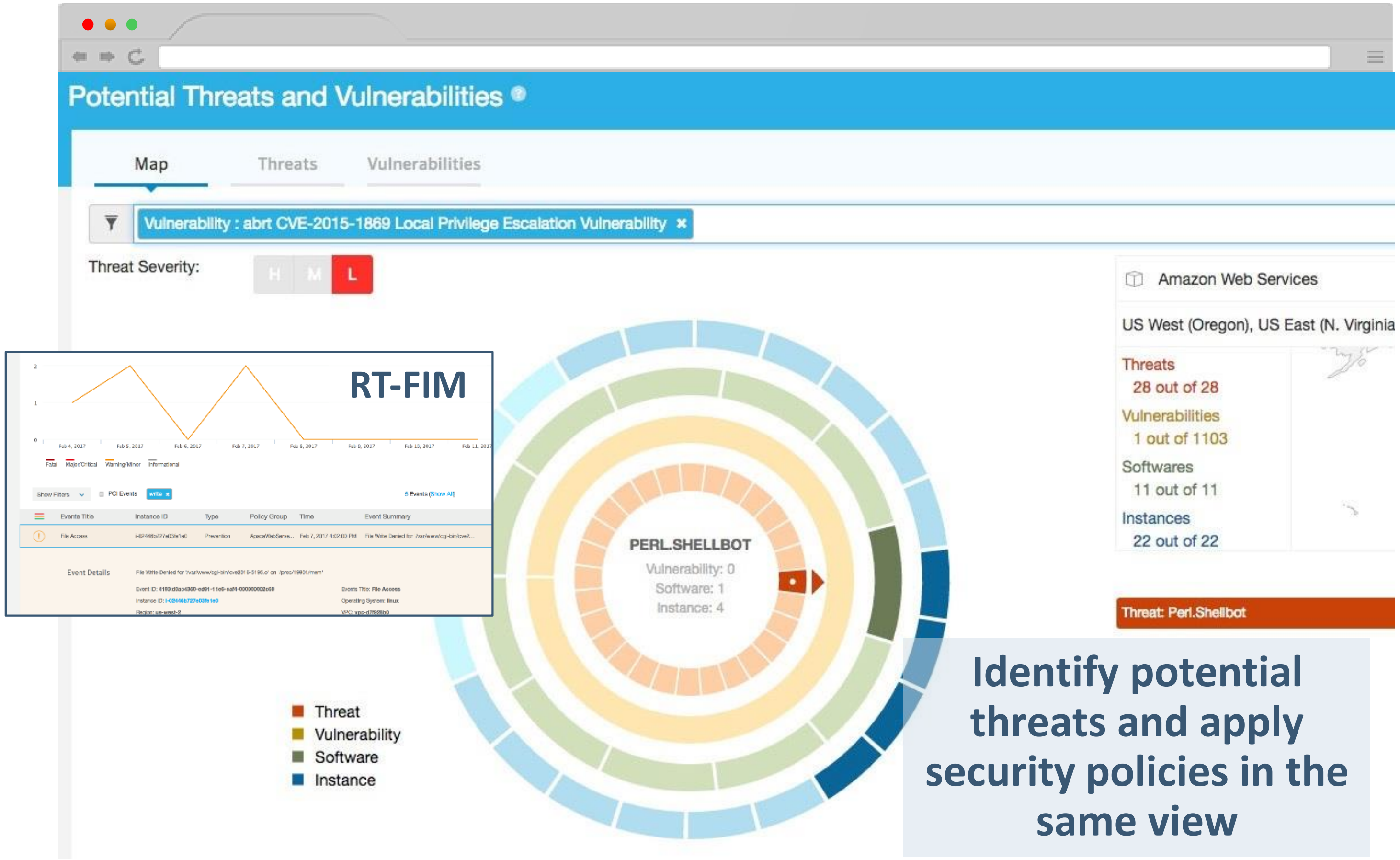
Public Cloud

Private Cloud



Solution: Automated policy-based controls

- Unique **application isolation** blocks exploits targeting known and unknown vulnerabilities
- **OS hardening** stops zero-day threats
- **Real-time file integrity monitoring** (RT-FIM) prevents unauthorized changes
- Real-time user activity and **application process monitoring** identifies suspicious behaviors
- **Automated deployment** at launch



Potential Threats and Vulnerabilities

Vulnerability : abrt CVE-2015-1869 Local Privilege Escalation Vulnerability

Threat Severity: H M L

Amazon Web Services

US West (Oregon), US East (N. Virginia

Threats: 28 out of 28

Vulnerabilities: 1 out of 1103

Softwares: 11 out of 11

Instances: 22 out of 22

Threat: Perl.Shellbot

PERL.SHELLBOT

Vulnerability: 0

Software: 1

Instance: 4

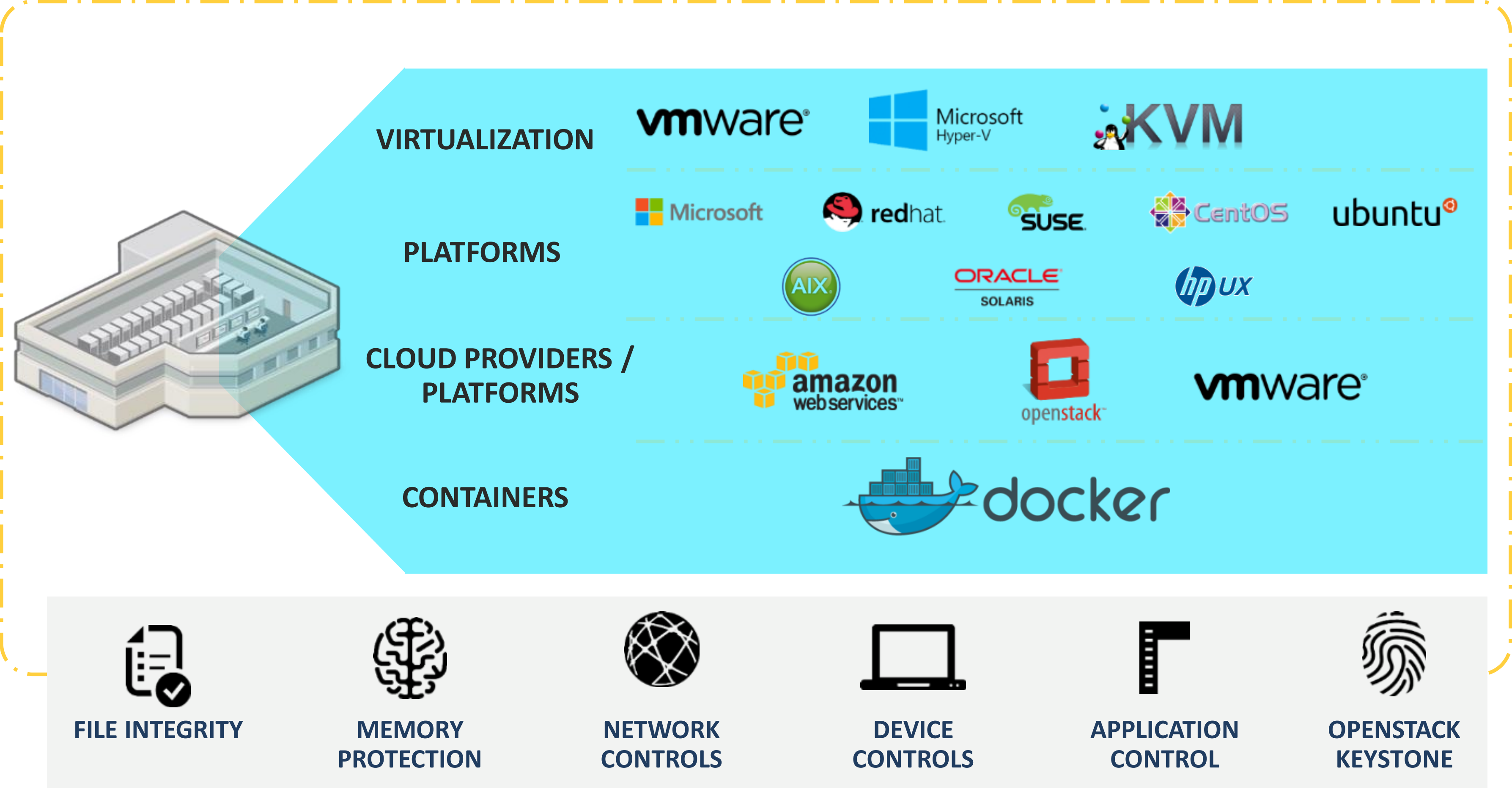
Identify potential threats and apply security policies in the same view

Use Case: Ensure security intelligence is tailored to specific cloud configurations

- **Prioritize security** based on risk.
- **Dynamic view** of risk posture.
- **Versioning** of instance and operating system type.
- Manage exploits with “just the right” response to ensure business continuity, without loosing application functionality.
- Common Vulnerabilities and Exposures (CVE) are published daily.
  - You don’t need to know about all of them. Just the ones that affect your environment.

Each needs their own hardening policy

Solution: Tailored polices to harden servers



VIRTUALIZATION

PLATFORMS

CLOUD PROVIDERS / PLATFORMS

CONTAINERS

FILE INTEGRITY

MEMORY PROTECTION

NETWORK CONTROLS

DEVICE CONTROLS

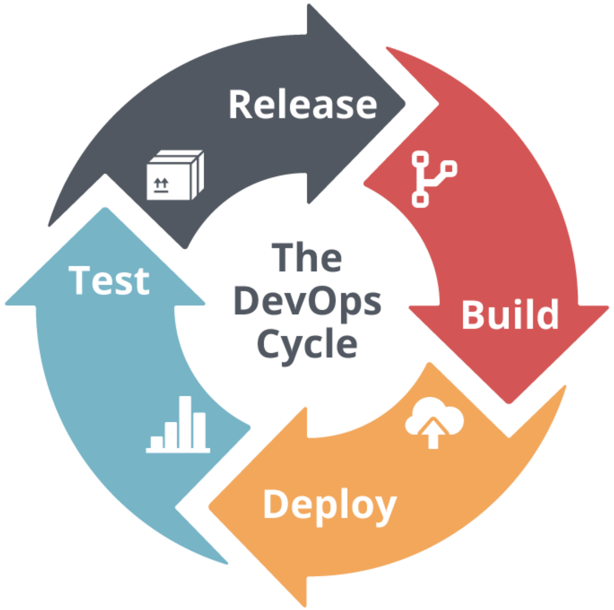
APPLICATION CONTROL

OPENSTACK KEYSTONE

- **SIMPLICITY** – Consistently manage security across physical, virtual, public, and private clouds
- **Hardening** – Centralized security, monitoring, and hardening across all these platforms and applications
- **Tailored security** – Align security and IT with security down to the application layer

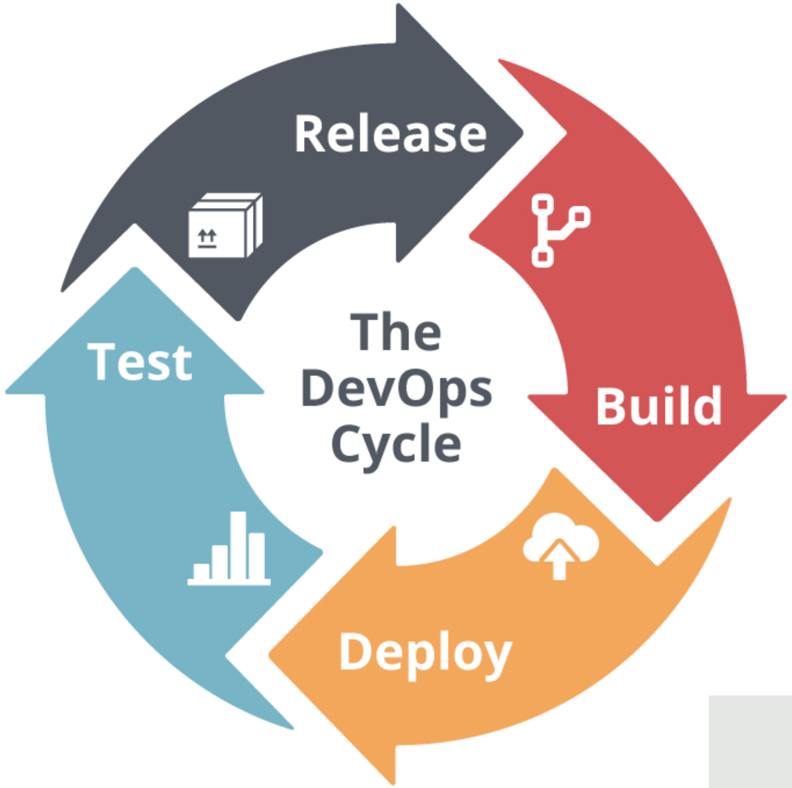
Use Case: Automate deployment and integration with cloud service providers

- **Agile and fast setup** wizards to each major cloud provider.
- **Open API** for DevOps to Integrate Security into Infrastructure as Code.
- Open API for Incident Response integration.
- Support for **full Dev/Ops life cycle**.
  - Using Puppet, Chef, and Anisble software for automation.
- **Immutable workloads** support.



Solution: Cloud Workload Protection is cloud native

Symantec.



CWP Integrates with DevOps Build & Deploy Cycles

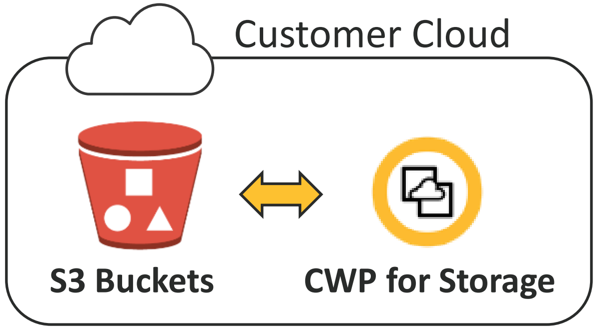
- Puppet/Chef/Ansible Integrated Agent Deployment
- Deployment Scripts Available on GitHub
- Azure Virtual Machine Extensions
- Workloads are immutable

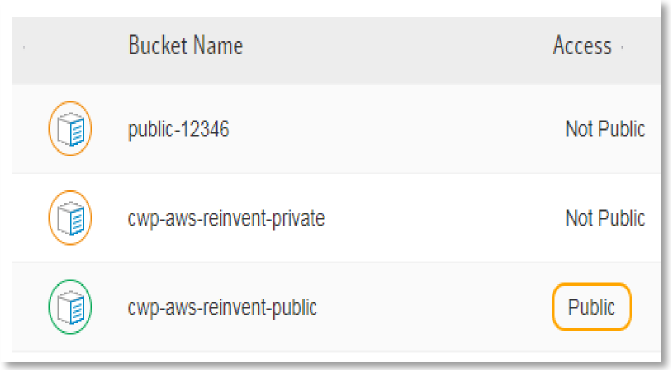
Also enables DevOps orchestration tools:

CHEF GitHub puppet ANSIBLE Microsoft Azure

Cloud Workload Protection for Storage

Automatic & Scheduled Anti-malware Scanning for AWS S3 Buckets





Bucket Name	Access
public-12346	Not Public
cwp-aws-reinvent-private	Not Public
cwp-aws-reinvent-public	Public

Elastic, Scalable Storage Protection

Threat scanning infrastructure scales elastically for cost optimization

Enables secure adoption of containers and serverless compute

Customer Data Never Leaves Their Cloud

Ensures privacy of sensitive data during assessment

Anti-malware scanning occurs entirely inside of the customers cloud

Alerts to Prevent Public S3 Exposures

Helps to protect against data breaches by discovering and alerting when S3 buckets are misconfigured or exposed to the public internet

DLP Policy Enforcement!

IaaS/PaaS – Posture Assessment

Inadequate Visibility

Do I have visibility into my cloud resources and who is using them?

Misconfigurations

Are my cloud services configured properly?

Compliance

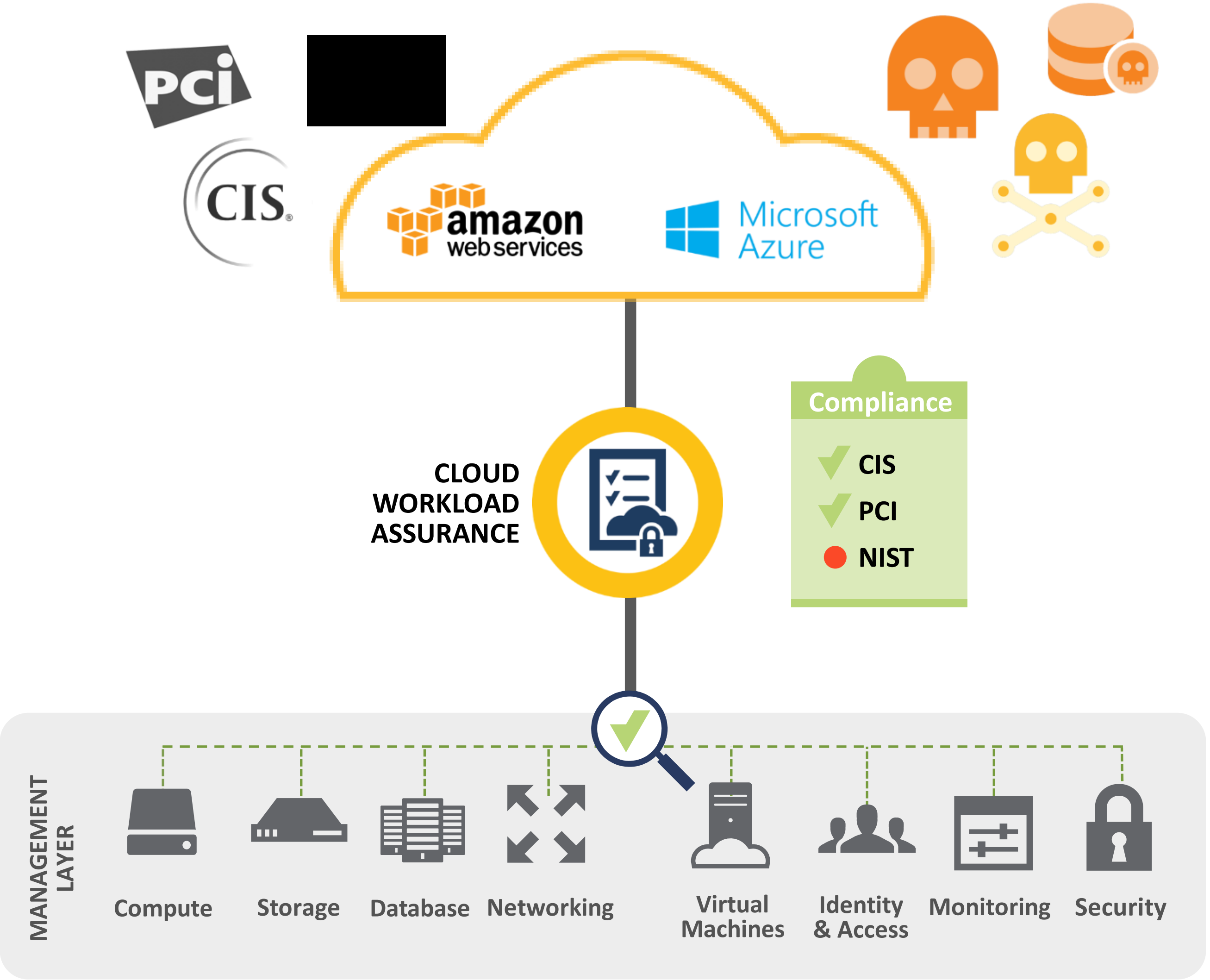
How do I assess my cloud environment for compliance auditing and reporting?

Remediation

I need help to quickly fix misconfigurations in my cloud services.

Cloud Workload Assurance

Symantec.



[redacted]

CLOUD WORKLOAD ASSURANCE

Compliance

- ✓ CIS
- ✓ PCI
- ● NIST

MANAGEMENT LAYER

Compute | Storage | Database | Networking | Virtual Machines | Identity & Access | Monitoring | Security

Cloud Security Posture Management

Visibility

Discover New and Existing Cloud Resources Across AWS & Azure

Monitoring & Remediation

Identify and Fix Misconfigurations with Guided Remediation and Alerts

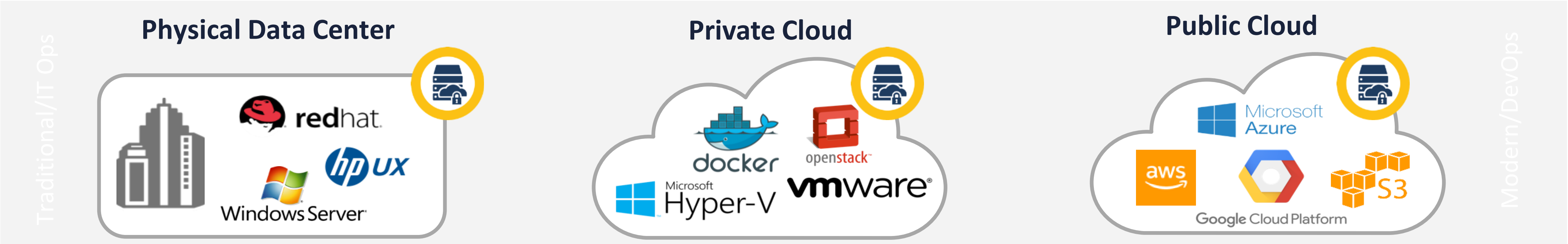
Compliance Assurance

Assess and Report Compliance Posture Against Regs & Benchmarks such as CIS, PCI, HIPAA

Multilayered Protection for IaaS and PaaS

Flexible “Cloud-native”, Single Console Security

HYBRID CLOUD ENVIRONMENT


Physical Data Center

Private Cloud

Public Cloud

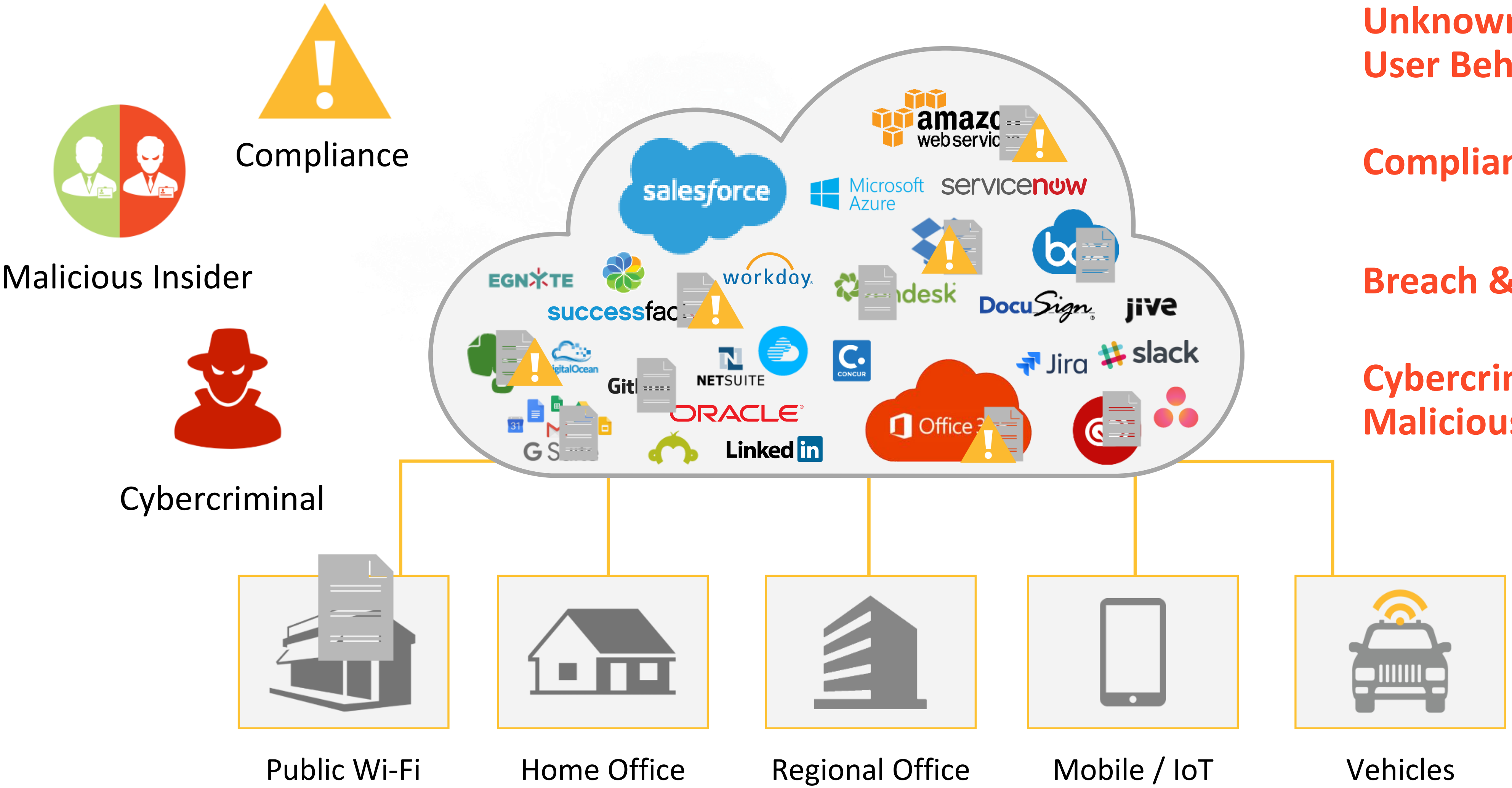
Symantec Cloud Workload Protection Suite | Single Console

SYMANTEC PROTECTIONS

CWP for Storage	Cloud Workload Assurance	CWP Anti-Malware	CWP Hardening				
ANTI-MALWARE FOR AWS S3	**CONTROL PLANE SECURITY**	**ANTI-MALWARE FOR COMPUTE**	**REAL-TIME FILE INTEGRITY MONITORING**	**OPERATING SYSTEM HARDENING**	**APPLICATION CONTROL**	**APPLICATION ISOLATION**	**APPLICATION LEVEL FIREWALL**
Discover and eradicate malware from storage buckets	Mange risk and compliance for multi-cloud infrastructure services	Discover and eradicate malware that is targeted at instances	Prevent unauthorized changes to infrastructure and app files	Protect from OS vulnerabilities without patching	Allow only authorized applications into production	Protect application from exploits against known/unknown vulnerabilities	Reduce attack surface; Block advanced threats
For Storage	**For Control Plane**	**For Workloads**	**For Workloads and Containers (Compute)**				

And what about SaaS? Issues in Adoption of Cloud Applications

Symantec



Compliance

Malicious Insider

Cybercriminal

Public Wi-Fi

Home Office

Regional Office

Mobile / IoT

Vehicles

Unknown Risk of User Behavior

Compliance Sensitive Info

Breach & GDPR Concerns

Cybercrime & Malicious Insiders

Symantec CloudSOC™

Symantec

Visibility

Understand & Monitor Risk Exposure Across Public Cloud Apps & Infrastructure

- Shadow IT
- Compliance Sensitive Data
- GDPR Exposure
- Cost Savings

Data Security

Govern Access to Critical Data, Extend Protections Against Breach

- Discover sensitive data
- Implement strong access controls
- Integrate MFA, encryption, & multi-channel DLP
- Leap forward toward GDPR

Threat Protection

Protect Against Threats, Detect, Investigate, and Remediate Incidents

- Protect against malware
- Detect malicious behavior
- Investigate activity – deep forensics across apps
- Respond with revocation, quarantine, & policy

CASB 2.0

CloudSOC makes VIP useful for 2nd factor based on risky actions, not just logins

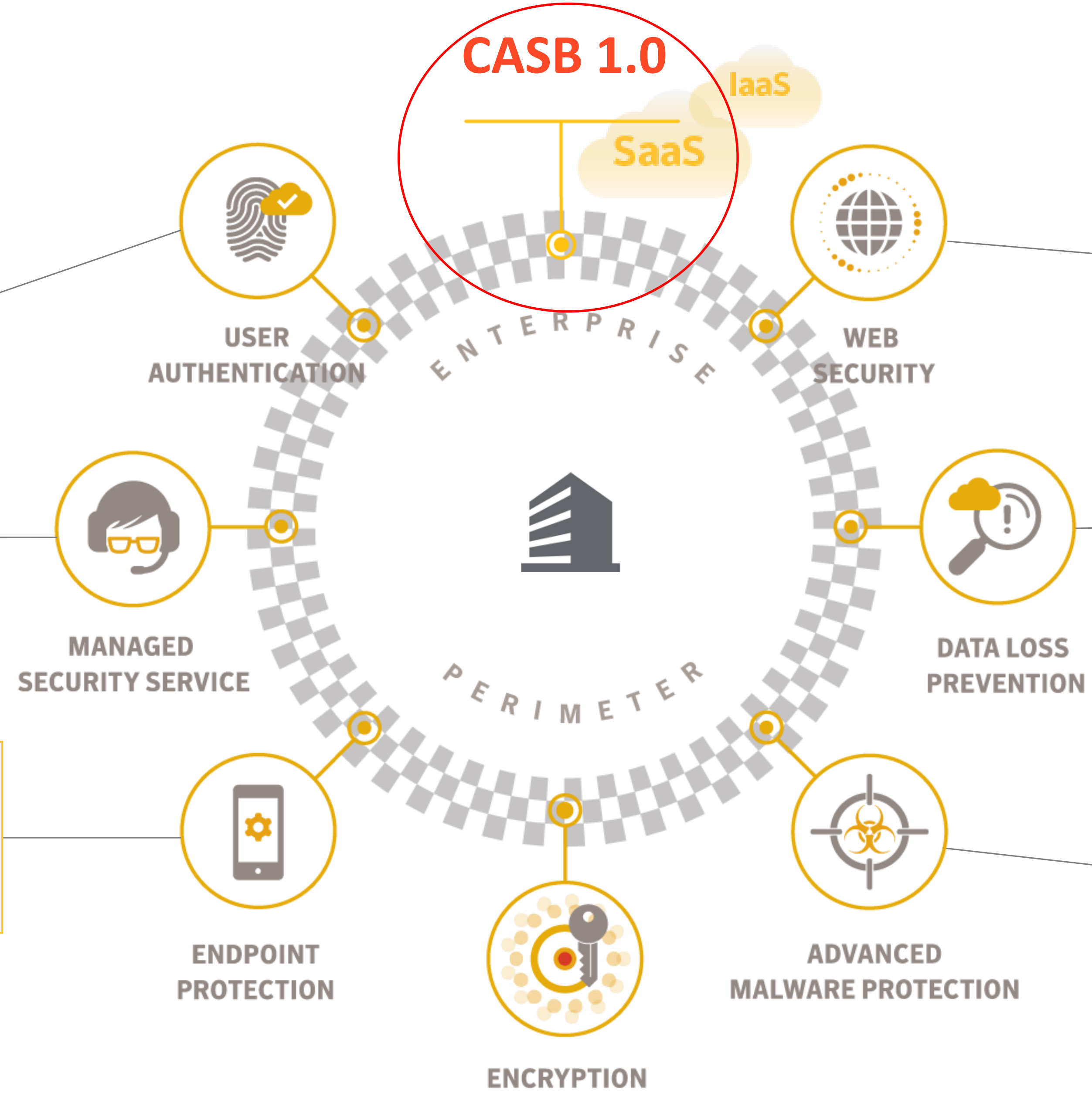
VIP

CloudSOC can expand the IR capability of MSS to Shadow IT & cloud Apps

MSS

CloudSOC can track roaming users as part of Shadow IT analysis

SEP



CloudSOC can make your ProxySG Powerful with 25,000 app controls

ProxySG/WSS

CloudSOC can make your DLP more expansive to all cloud apps

DLP

CloudSOC can apply Symantec's high efficacy malware engines can stop malware in cloud

Malware prevention

CloudSOC enables to ICE the data to help track and revoke it after it leaves cloud?

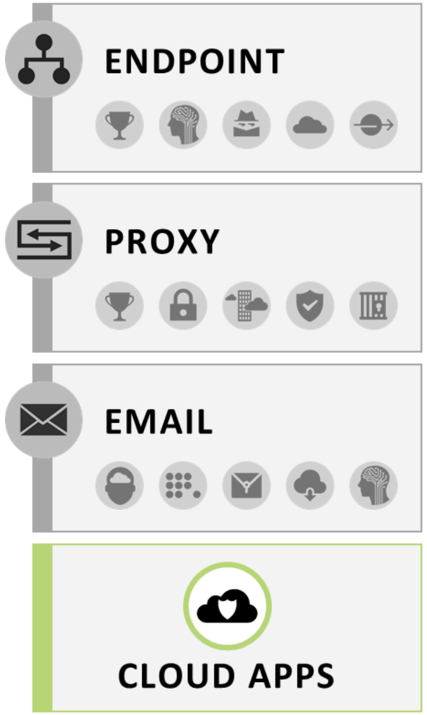
ICE

Defining Cloud Security

Symantec is defining Cloud security by…

- Ensuring **COMPLETE VISIBILITY AND CONTROL** of cloud application and service usage across over 20,000 cloud applications.
- Delivering **ADVANCED CLOUD DATA SECURITY AND THREAT PREVENTION** capabilities across both cloud applications and public cloud infrastructure
- **INNOVATING WORKLOAD PROTECTION** directly into public cloud infrastructures to harden compute platforms and eradicate malware from storage and applications
- Driving **RISK MANAGEMENT OF KEY SERVICES**– configuration assessments, benchmarks against key security frameworks, and access policy enforcement

Symantec safely empowers the transition to cloud applications and infrastructure while ensuring unity with traditional on-premises security needs as a key pillar of our **INTEGRATED CYBER DEFENSE PLATFORM.**



ENDPOINT

PROXY

EMAIL

CLOUD APPS

REQUIREMENTS

- Visibility In Cloud User Behavior
- Control Across all Cloud Applications
- User and User-Action Based Authentication
- Protections Against Malicious Content
- Extends Data Protection to the Cloud

Symantec™

Thank you!