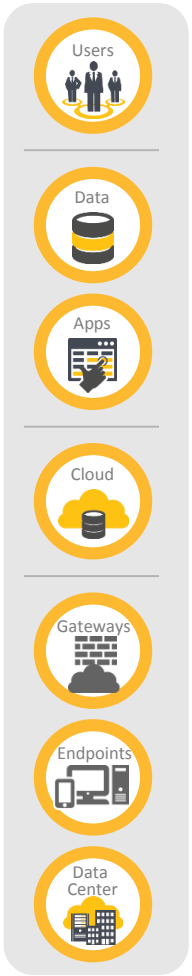
SYMANTEC DATA CENTER SECURITY

SYMANTEC UNIFIED SECURITY STRATEGY



Cyber Security Services

Monitoring, Incident Response, Simulation, Adversary Threat Intelligence

Threat Protection

ENDPOINTS | DATA CENTER | GATEWAYS

- Advanced Threat Protection Across All Control Points
- Built-In Forensics and Remediation Within Each Control Point
- Integrated Protection of Server Workloads: On-Premise, Virtual, and Cloud
- Cloud-based Management for Endpoints, Datacenter, and Gateways

Information Protection

DATA | IDENTITIES

- Integrated Data and Identity Protection
- Cloud Security Broker for Cloud and Mobile Apps
- User and Behavioral Analytics
- Cloud-based Encryption and Key Management

Unified Security Analytics Platform

- Log and Telemetry Collection
- Integrated Threat and Behavioral Analysis
- Unified Incident Management and Customer Hub
- Inline Integrations for Closed-loop Actionable Intelligence
- Regional and Industry Benchmarking

DATA CENTER SECURITY IS HARD AND IS GETTING HARDER – EVEN IF YOU ARE PREPARED

TRADITIONAL DATA CENTER

- Rogue IT; Point Security Tools; Manual Processes
- Compliance($Non-compliance= 3x $compliance)
- Over 80% of orgs maintain legacy platforms (WIN 2003)

THREAT LANDSCAPE

- Breaches with over 10 million records are up 125% (2015)
- A new zero-day exploits was found every week on average in 2015
- Growing in Scale and Sophistication (ex: Regin, Heartbleed, Turla)

NEXT-GEN DATA CENTER

- Perimeter-centric Security Does Not Work
- Multiple vendors, platforms
- On-prem, hybrid, public/private cloud

HOW AGILE IS YOUR SECURITY?

If there is a new critical vulnerability, how fast can you scan, assess, and secure your systems from exploits?

How long does it take to provision security for newly created workloads?

If a workload is compromised, how fast can you prevent the lateral spread of infection?

How quickly are you able to discover & secure rogue IT?

How are you protecting critical applications running on legacy and unsupported (EOL) platforms?

If there is change to the application or platform, how quickly can you adjust the security settings in response to these developments?

WHAT MAKES A STRONG, AGILE SECURITY STRATEGY FOR THE SDDC?

ANTIMALWARE & THREAT PROTECTION

Designed for performance & resource optimization, not just an endpoint protection client

MOBILE WORKLOADS

Support the migration and co-mingling of workloads with varied trust levels

PERIMETER & NETWORK SECURITY

Visibility and control of internal VM to VM traffic

COMPLIANCE & HARDENING

Automated
asset discovery, configuration and validation

Support & Simplify Security Across Traditional and Next Gen IT with:

Security embedded into the Platform protecting hosts and guests

Application-level security controls and policies for workloads anywhere

Security integrated with DevOps Automation Tools & Processes provides faster provisioning, reduces Rogue IT instances and ensures timely protection.

DATA CENTER SECURITY STRATEGY IS A LIFECYCLE NOT A JOURNEY

ASSESS

- Conduct Asset Auto Discovery
- Assess Server Configuration
- Report Against Mandates and Standards
- Aggregate Risk Scores
- Prioritize Remediation

ORCHESTRATE

- Aggregate, Automate and Orchestrate Security Policy Across Products
- Enable application-level security
- Automate Security Provisioning and Response Across Platforms

PROTECT

- Monitor and Harden Physical, Virtual, and Cloud
- Protect Current and Next-gen Data centers
- Secure Virtual Desktops
- Protect Application and File Stores

What’s new in 6.7

DCS 6.7 SIMPLIFIES ACHITECTURE & MANAGEMENT, AND ADDS PLATFORM SUPPORT DOCKER ENVIRONMENTS

Release Objective
- Simplified architecture for easier deployment
- Improved high availability of web console
- Full support for Docker platform

Customer benefit
- Consistently manage security across physical and virtual environments across on-prem, public and private clouds

Target
- Customers building software defined data centers looking to secure their infrastructure

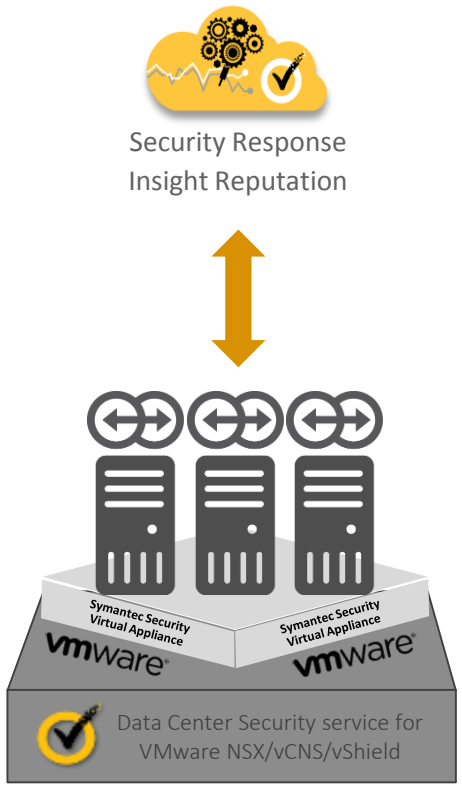
Release Highlights

DCS: Management Console
- Docker platform support

DCS: Server/Monitoring/Server Advanced
- Docker support (Server Advanced & Monitoring)
- Improved high availability
- Simplified architecture

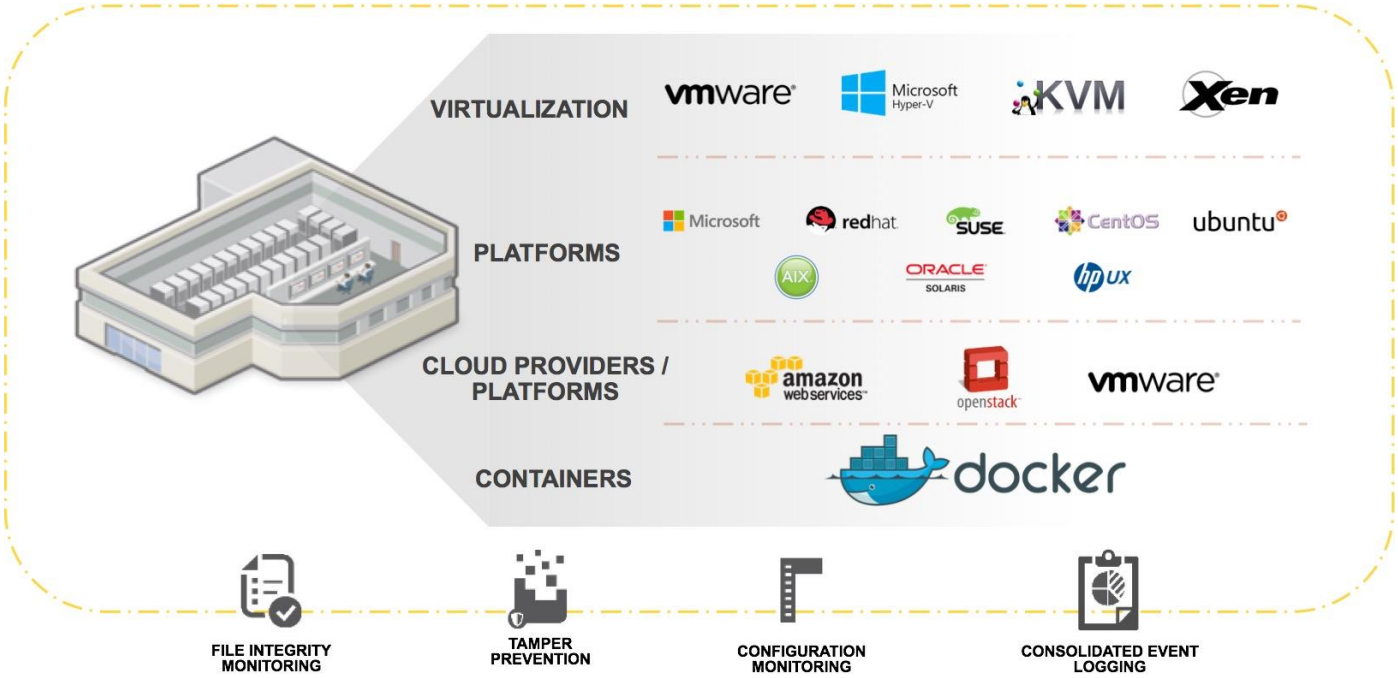
DCS: Server Advanced
- Protection, visibility, and management for Docker containers
- Any DCS Manager can be used for management
- Simplified deployment for easier upgrades

SYMANTEC DATA CENTER SECURITY: SERVER 6.7 – WHAT'S NEW?



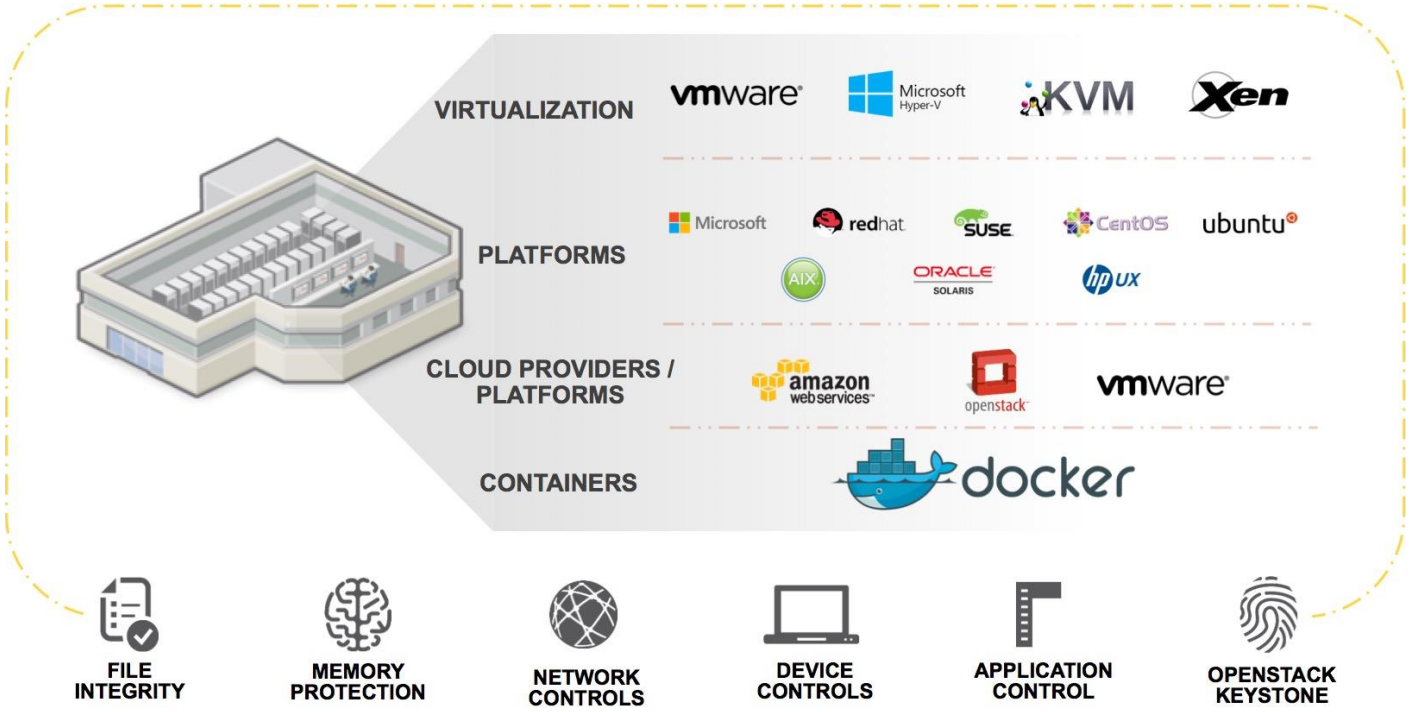
- Added web cosole high availability
- Web console is built into management server
- Extended support for NSX 6.2 with cross Center NSX
- Support for multiple NXS/vCenter

SYMANTEC DATA CENTER SECURITY: MONITORING EDITION 6.7- WHAT'S NEW?



- Monitor Docker container, their metadata and status, online and offline
- Apply Unix real-time security & policy to Docker host
- Integrated security & compliance into container management
- Expanded platform support

SYMANTEC DATA CENTER SECURITY: SERVER ADVANCED 6.7 – WHAT'S NEW?



- Harden and protect Docker containers
- Added web cosole high availability
- Web console is built into management server
- Expanded platform support

SYMANTEC DATA CENTER SECURITY PROTECTS DOCKER!

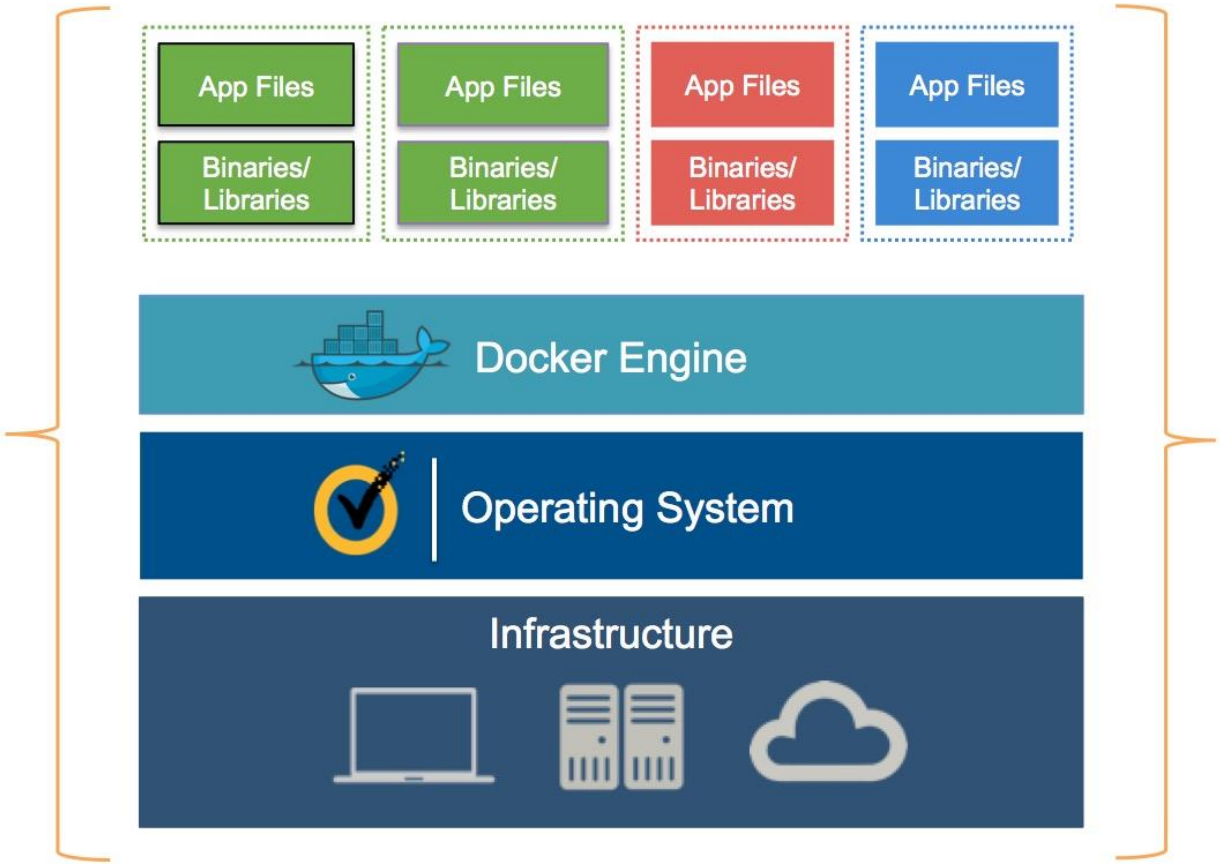
Data Center Security: Server Advanced

Visibility | **Compliance** | **Hardening** | **Management**

SYMANTEC DATA CENTER SECURITY PROTECTS DOCKER!

Data Center Security: Server Advanced

Visibility | **Compliance** | **Hardening** | **Management**

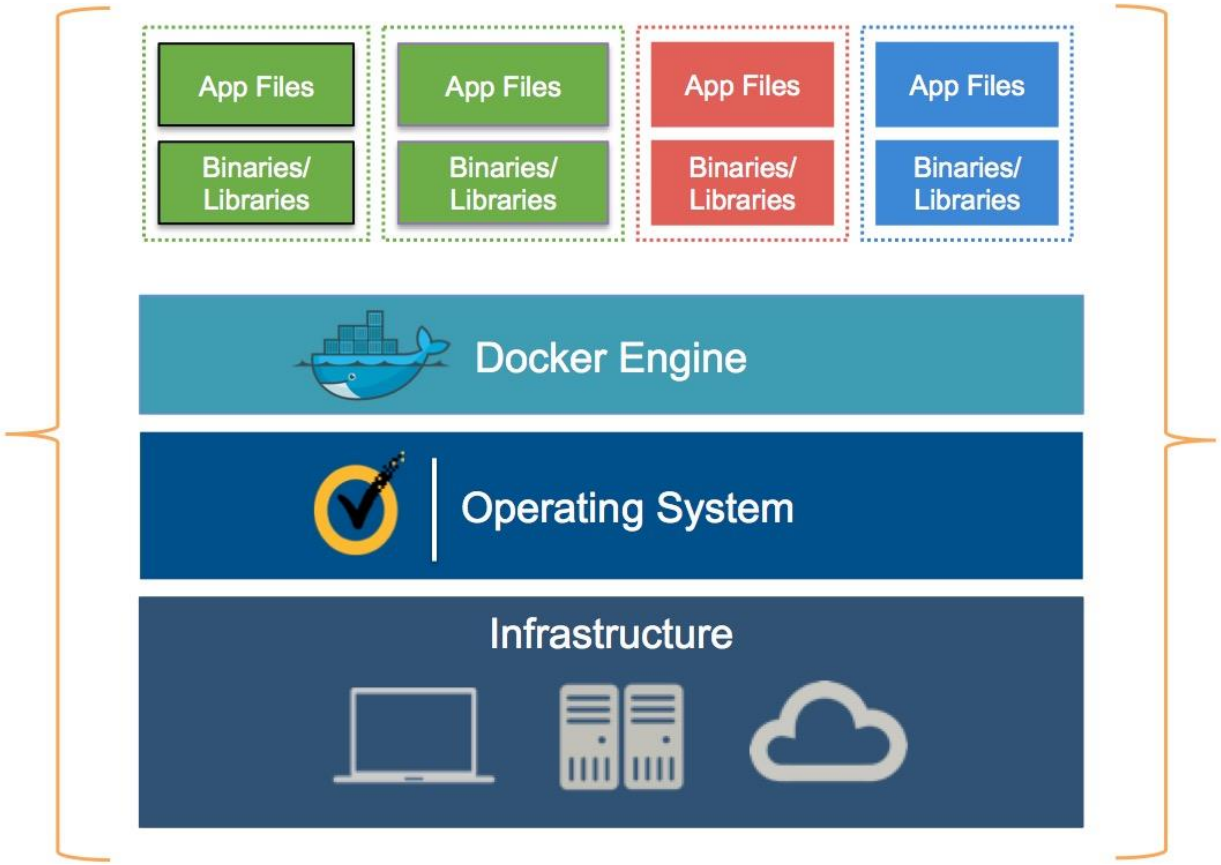


- Single pane of glass view into:
  - Entire Docker deployment
  - Metadata
  - Power status
  - Container workloads both offline and online

SYMANTEC DATA CENTER SECURITY PROTECTS DOCKER!

Data Center Security: Server Advanced

Visibility | **Compliance** | **Hardening** | **Management**

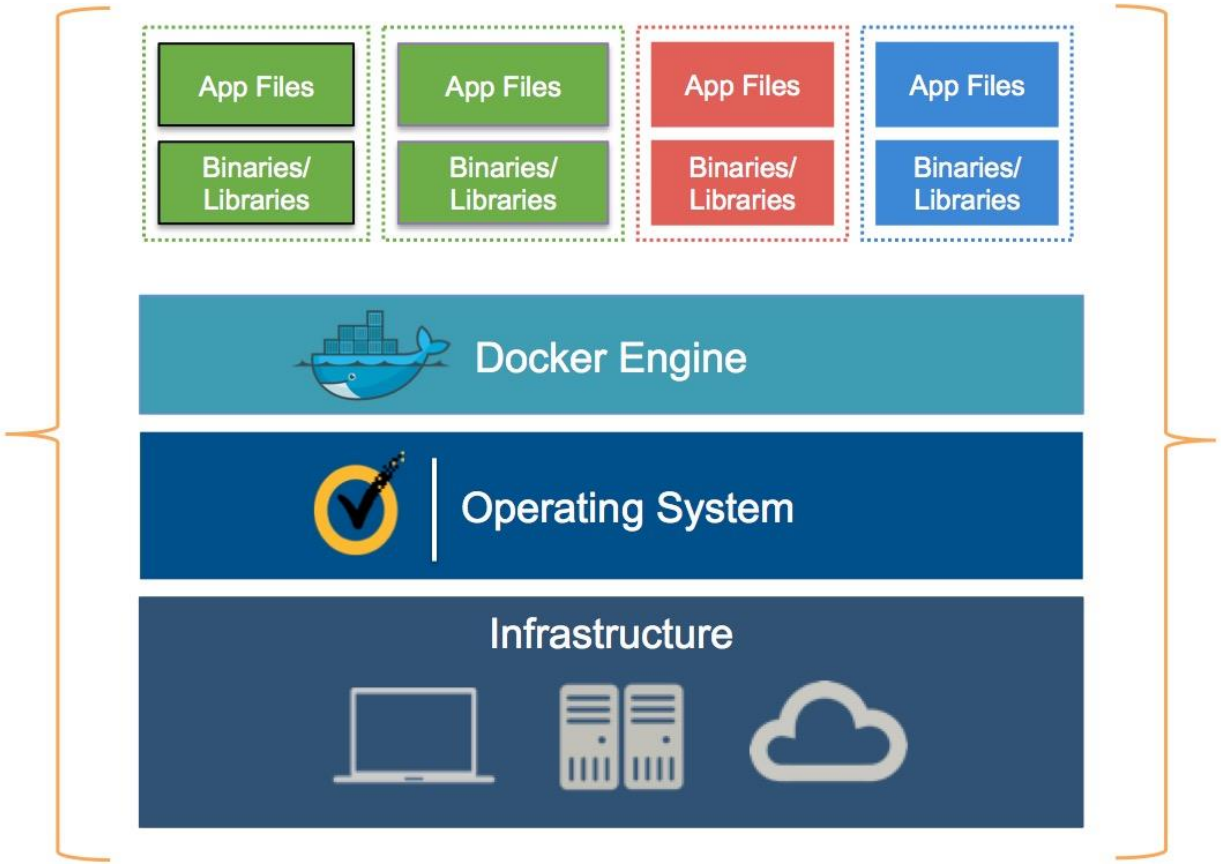


- Unix real-time security & policy to Docker host
- Continuous monitoring of host and all containers
- Real-time file monitoring
- Helps ensure monitoring of files & services in CIS Docker benchmark
- Monitors containers downloaded from Docker hub for auditing
- Enforce user rights compliance on Docker host

SYMANTEC DATA CENTER SECURITY PROTECTS DOCKER!

Data Center Security: Server Advanced

Visibility | **Compliance** | **Hardening** | **Management**

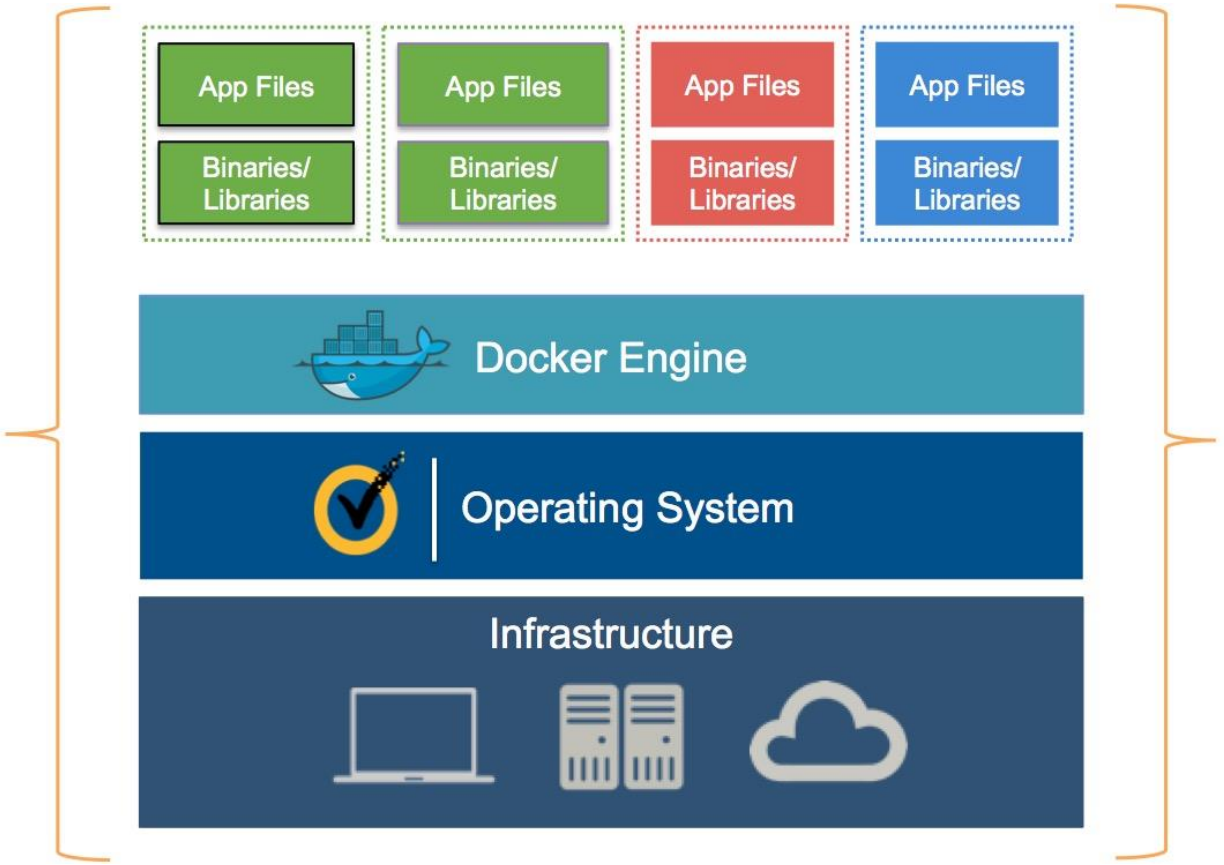


- Agentless security for each container
- Apply hardening policy without impacting:
  - Docker performance
  - Container performance
- Container verification to protect OS
- Protects against container escape
- Host based firewall restricts access to network

SYMANTEC DATA CENTER SECURITY PROTECTS DOCKER!

Data Center Security: Server Advanced

Visibility | **Compliance** | **Hardening** | **Management**



Access via RESTful API's

- Easy integration into Symantec Data Center Security: Server Advanced with existing DevOps workflow
- Security delivered at run time
- Security built into container during provisioning

INTRODUCING SYMANTEC DATA CENTER SECURITY

Symantec

INTRODUCING SYMANTEC DATA CENTER SECURITY

ASSESS

Control Compliance Suite

Trusted by 10/10 Top US banks

ORCHESTRATE

Operations Director

1st to market with Software Defined Security for any platform

PROTECT

DCS: Server / Server Advanced

Undefeated at Black Hat 7 years running

Market leader in Gartner MQ for Endpoint Protection

CONTROL COMPLIANCE SUITE DELIVERS CONTINUOUS ASSESSMENTS AND RISK-PRIORITIZED REMEDIATION

- Automate Security & Compliance Assessments
- Align IT Operations and Security
- Continuous Assessments for Cyber Security

HOW A LARGE HEALTHCARE ORGANIZATION ACHIEVED COMPLIANCE WITH SYMANTEC CONTROL COMPLIANCE SUITE

Use Case : The organization needs to adhere to broad range of security and privacy-related regulations

Problem

Manual security checks

Multiple systems and platforms

Need to aggregate results of evidence data

Response

Implement:

- CCS Standards Manager
- Assessment Manager
- Risk Manager
- Vendor Risk Manager

Action

Address need to collect, process, and report on technical evidence data

Address need to assess current procedural controls

Address HIPAA Omnibus rules and PCI-DSS v3 requirements

Result

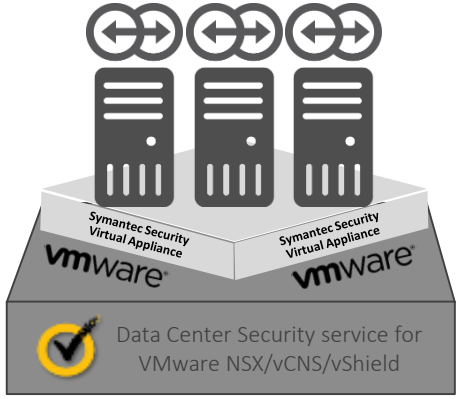
Automated process and consolidation of evidence data

Adhere to security and privacy related regulations

Symantec Advantage:

Automation Comprehensive Solution Aggregation

AGENTLESS HOST AND GUEST THREAT PROTECTION FOR VIRTUAL ASSETS WITH DATA CENTER SECURITY: SERVER



Fully integrated with VMware (NSX/vCNS/vShield)	→	Lower OPEX Manage complexity Reduce boot storms
Auto deployment of Hypervisor-based security virtual appliance (SVA)	→	Always-on security for hosts and virtual guests
Security Orchestration and integration with DCS: Server Advanced and third-party security tools	→	Agile security provisioning and threat response for hosts & virtual guests

SYMANTEC DATA CENTER SECURITY DELIVERS AGILE, AGENTLESS THREAT PROTECTION

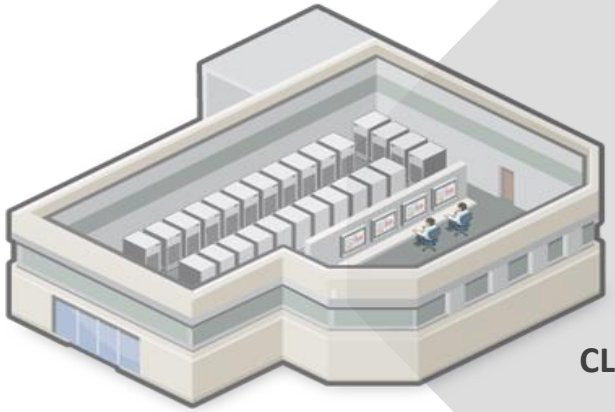
Use Case : New business application deployment

Problem	Response	Action	Result
IT asset provisioning takes minutes but security provisioning takes days Security is the bottleneck for scaling out the new services	IT service request Capture security and compliance attributes during IT service requests Security requests for new IT assets sent to security admin Operations Director automatically creates task for security admin	Viruses are detected, blocked, and logged Rapid 7 Nexpose (via Operations Director integration) runs vulnerability scans & risk assessment Operations Director recommends antimalware, NIPs, firewall (via Palo Alto integration), and hardening	Security is deployed quicker; mitigating rogue and unsecure IT assets Increased business responsiveness Server is protected throughout its lifecycle

Symantec Advantage:

Automated Always On Agent-less

SECURE CRITICAL INFRASTRUCTURE WITH DCS: SERVER ADVANCED (CSP)



VIRTUALIZATION

vmware · Microsoft Hyper-V · KVM · Xen

PLATFORMS

Microsoft · redhat · SUSE · CentOS · ubuntu · AIX · ORACLE SOLARIS · hp UX

CLOUD PROVIDERS / PLATFORMS

amazon web services · openstack · vmware

CONTAINERS

docker

FILE INTEGRITY

MEMORY PROTECTION

NETWORK CONTROLS

DEVICE CONTROLS

APPLICATION CONTROL

OPENSTACK KEYSTONE

- SIMPLICITY – Consistently manage security across physical, virtual, public, and private clouds
- VISIBILITY – Centralized security, monitoring, and hardening across platforms and applications
- AGILITY – Align security and IT Ops with automated and orchestrated security down to the application layer

CRITICAL CUSTOMER PORTAL AUTOMATICALLY PROTECTED AGAINST ZERO-DAY EXPLOIT

Use Case : Mission critical web server must be secure and highly available

Problem	Response	Action	Result
Multiple applications and subcomponents, each with their own vulnerabilities Each component must be secure and compliant without downtime	Symantec Data Center Security: Server Advanced has Out-of-the-box sandboxes to secure each tier of the infrastructure	Attacker attempts to install malicious file through an IIS zero-day exploit Attack is blocked as IIS is not allow to install software or modify the OS	Customer portal maintains security and availability despite zero day vulnerability on whitelisted application

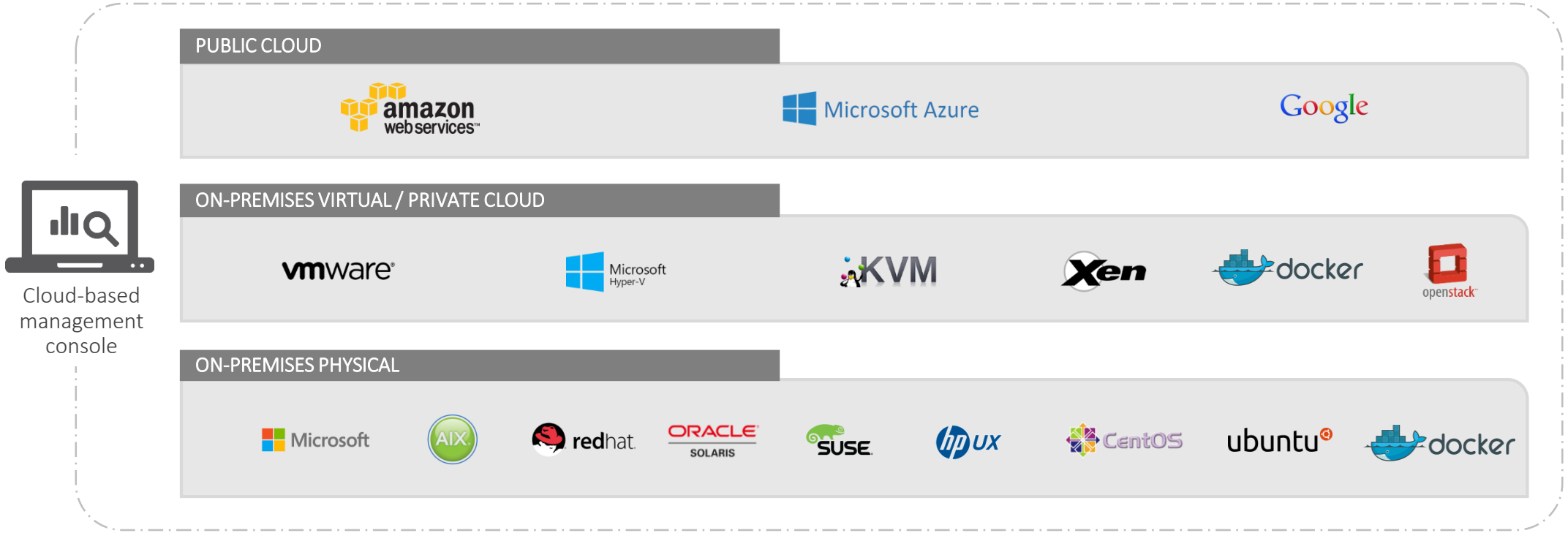
Symantec Advantage:

Application Whitelisting

Out-of-the-box Hardening

MANAGING DATA CENTER SECURITY - ANY FORM, ANYWHERE

Cloud-based management console managing common blades with connectors to platforms



SYSTEM HARDENING

DISCOVERY / ASSESSMENT

VULNERABILITY MANAGEMENT

THREAT PROTECTION

DATA LOSS PROTECTION

KEY MANAGEMENT

SYMANTEC ENABLES DYNAMIC , AGILE, AND ADAPTIVE SECURITY FOR THE DATA CENTER

ASSESS

Asset discovery and automate assessments, aggregate risk scores, prioritize remediation. Demonstrate regulatory & best practice compliance.

ORCHESTRATE

Automate orchestration of policies and settings across security products in response to the changing threat environment and enable business agility.

Combines threat and vulnerability intelligence with workload context to optimize security response.

PROTECT

Enable application-level security, allow workloads with varied trust levels to co-mingle securely, and adapt security settings to changes in threat and IT environment.

Minimize the performance and operational cost to my data center, while enhancing security responsiveness

Q&A

Thank you!

APPENDIX

PLATFORMS SUPPORTED (as of NOVEMBER 2015)

DCS PRODUCT	SUPPORTED PLATFORMS
CONTROL COMPLIANCE SUITE	RHEL, ORCL Linux, Suse, Ubuntu, Solaris, HP-UX, AIX, Windows, VMware ESX
DCS: SERVER	VMware NSX/vCNS/vShield
DCS: MONITORING EDITION	RHEL, ORCL Linux, Suse, Ubuntu, Solaris, HP-UX, AIX, Windows, VMware ESX, VMware NSX, AWS, OpenStack (all modules), Docker
DCS: SERVER ADVANCED	RHEL, ORCL Linux, Suse, Ubuntu, Solaris, HP-UX, AIX, Windows, VMware ESX, VMware NSX, AWS (monitoring only), OpenStack (monitoring for all modules, hardening for OpenStack Keystone), vCNS/vShield, Docker