



Data Sovereignty and Security in a Software Defined World

Cloud Expo Asia, Singapore

12 October 2016

Patrick J Conte, VP & GM International

HyTrust **workload security** solutions enable
secure private, public and hybrid **cloud**
infrastructure



Reduce
Risk



Guarantee
Availability

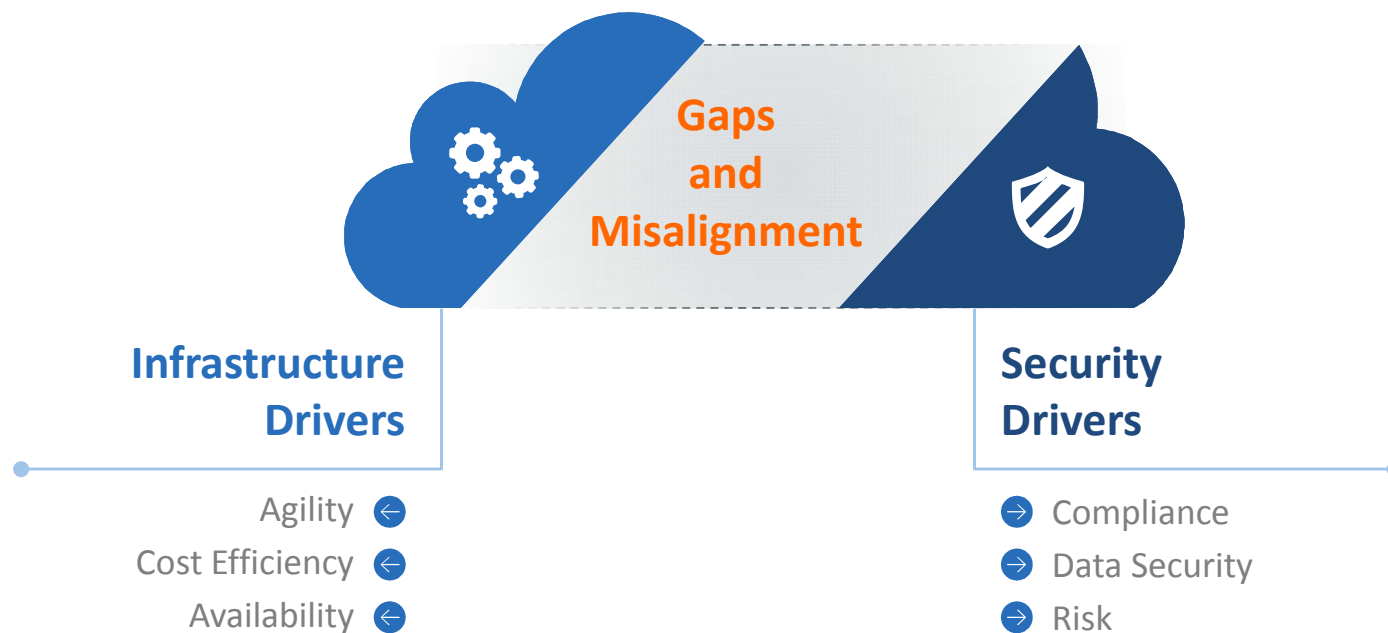


Accelerate
Savings

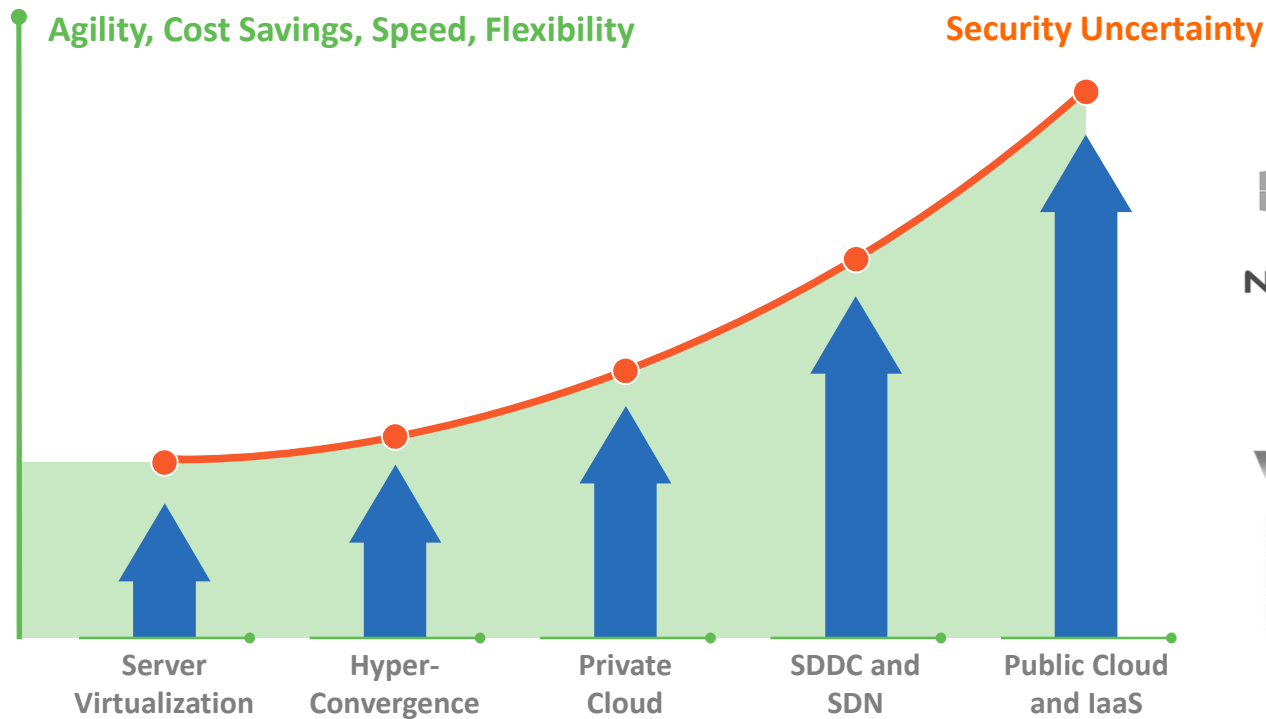


Automate
Compliance

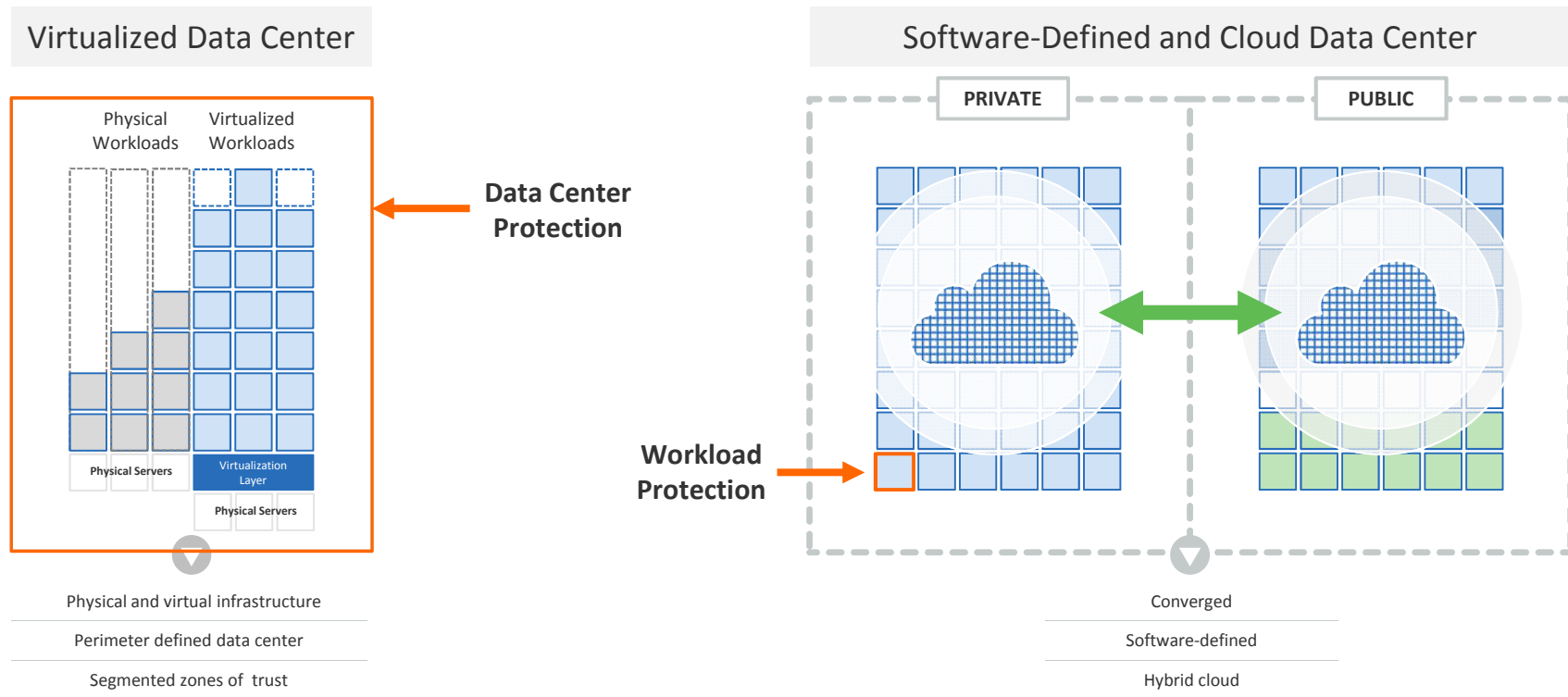
A Key Obstacle to Infrastructure Transformation



Rapid Data Center Technology Evolution



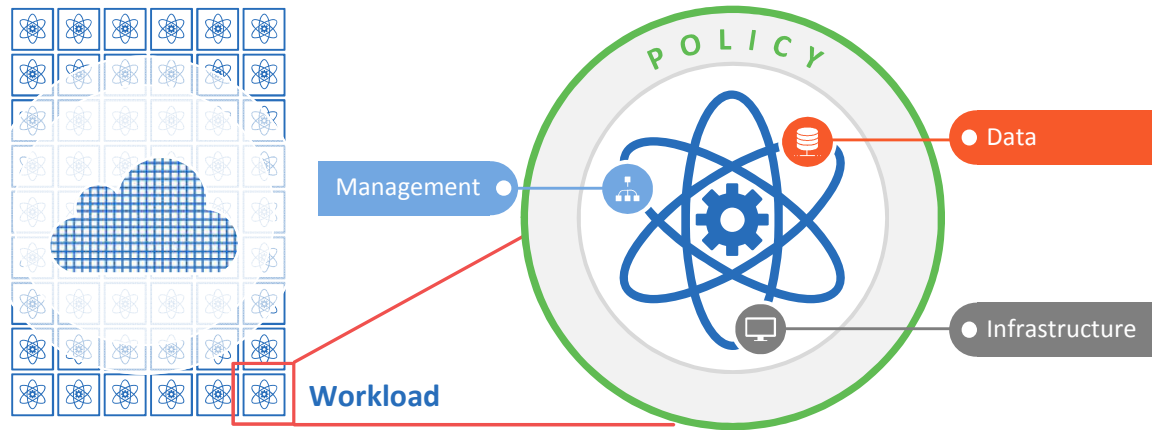
Software-Defined and Cloud Data Center Migration



THE WORKLOAD:

The New Atomic Unit of IT

COMPUTE | NETWORK | STORAGE



Key Elements:

Data



- Key Management
- Encryption
- Admin rights

Management



- Role-based access control
- Secondary Approval
- Multi-factor authentication

Infrastructure



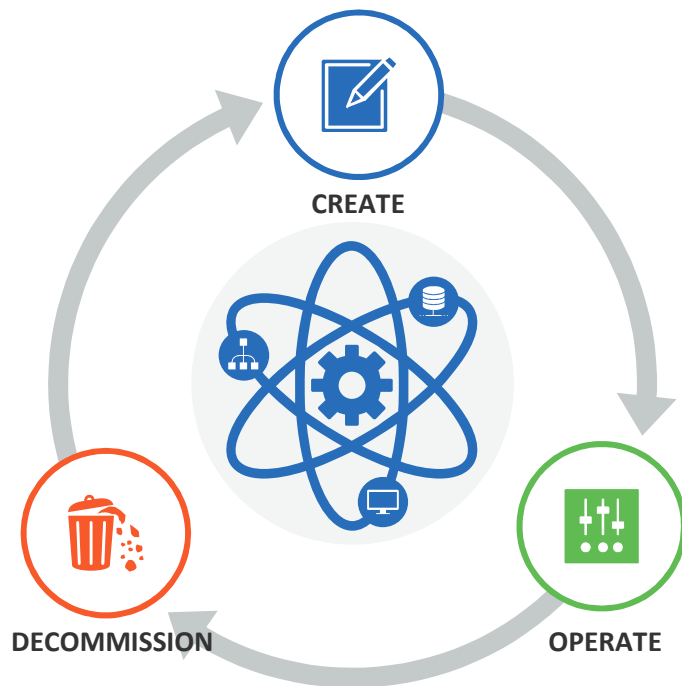
- Boundary-based policy
- Tag policy
- Hypervisor hardening

Policy



- Automation for workload policy
- Any cloud abstraction
- Workload and asset tagging

Operationalizing the Workload Life Cycle



CREATE

- Group policy
- MFA and RBAC
- Encryption policy
- Workload Tags



OPERATE

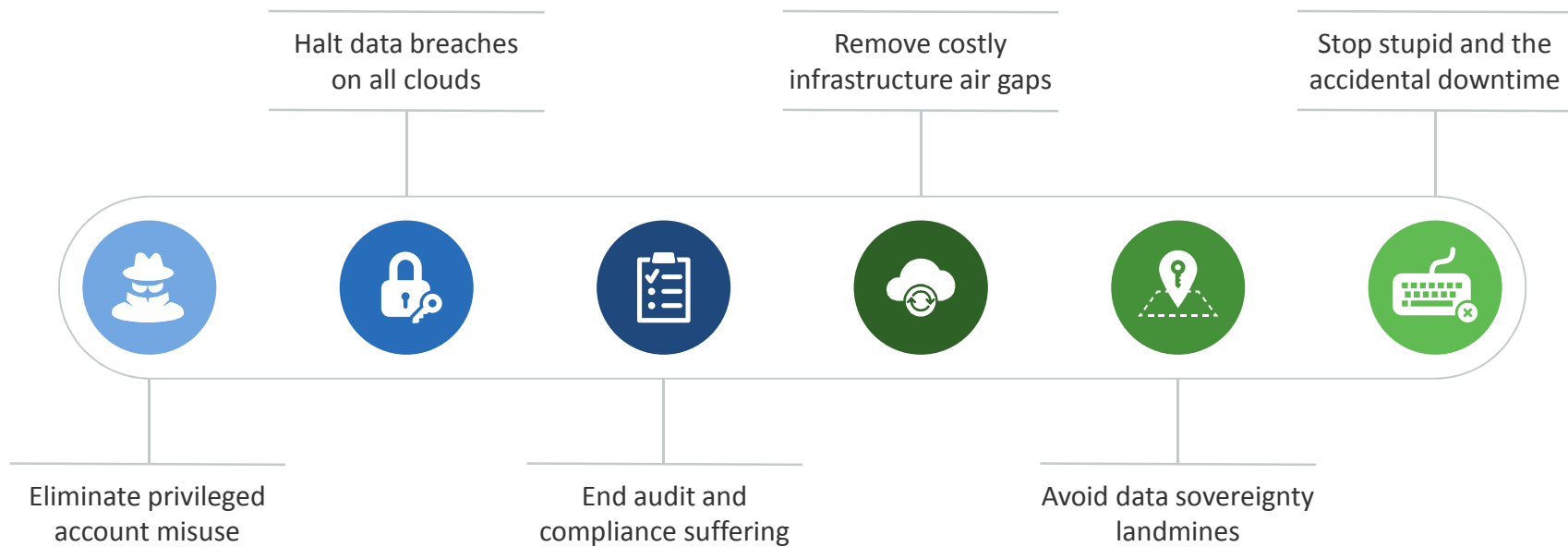
- Auditing
- Visibility
- Logging
- Availability



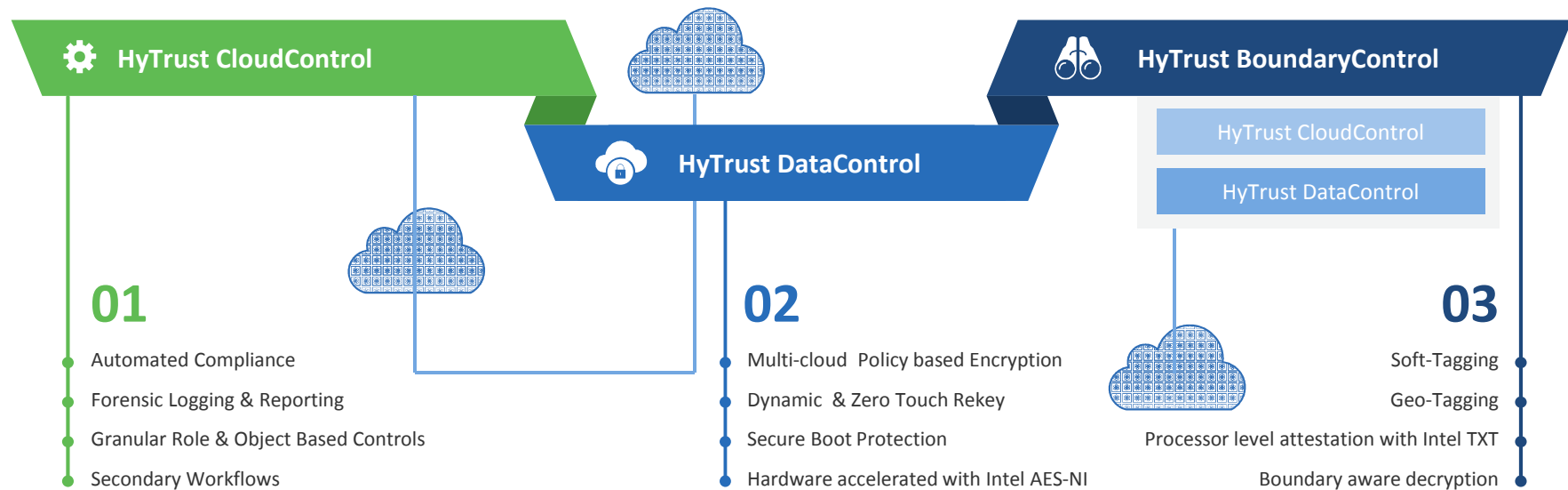
DECOMMISSION

- Data destruction
- Key management
- Workload logs
- SLA's

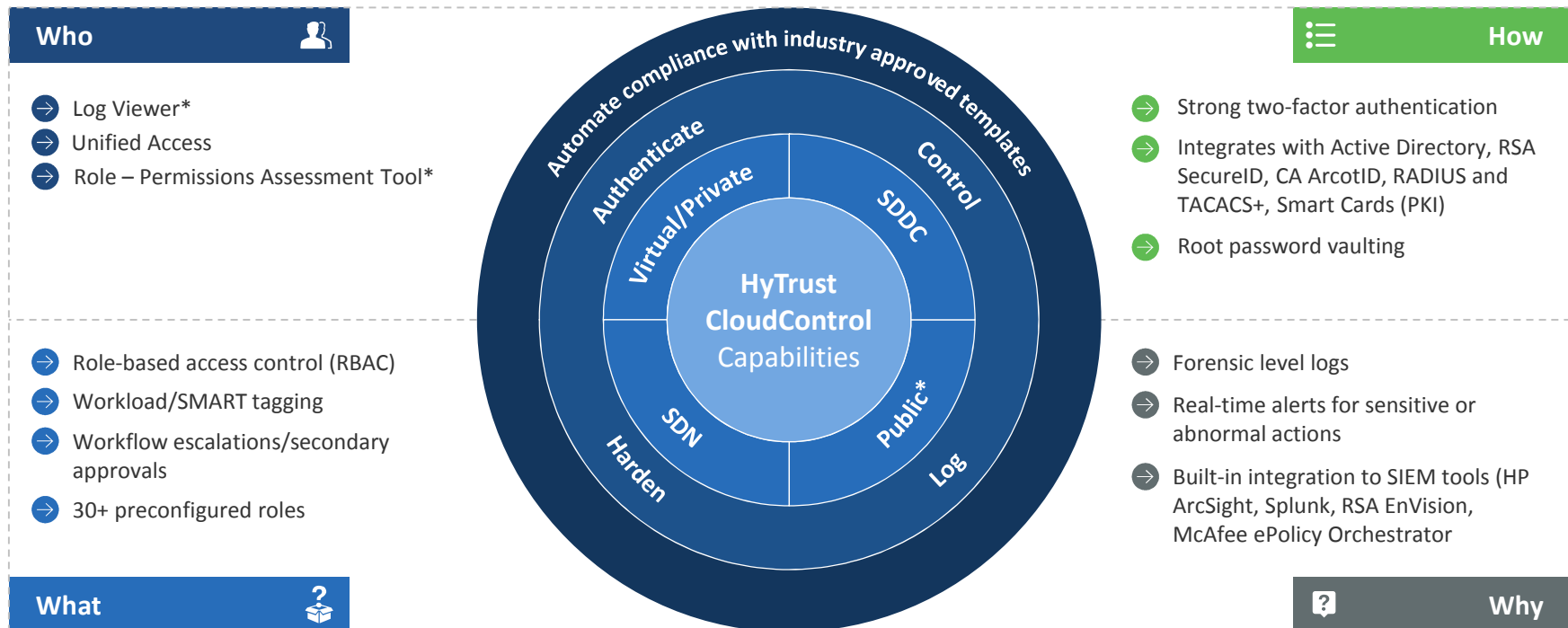
Workload Security Use Cases Solved by HyTrust



HyTrust Workload Security Platform

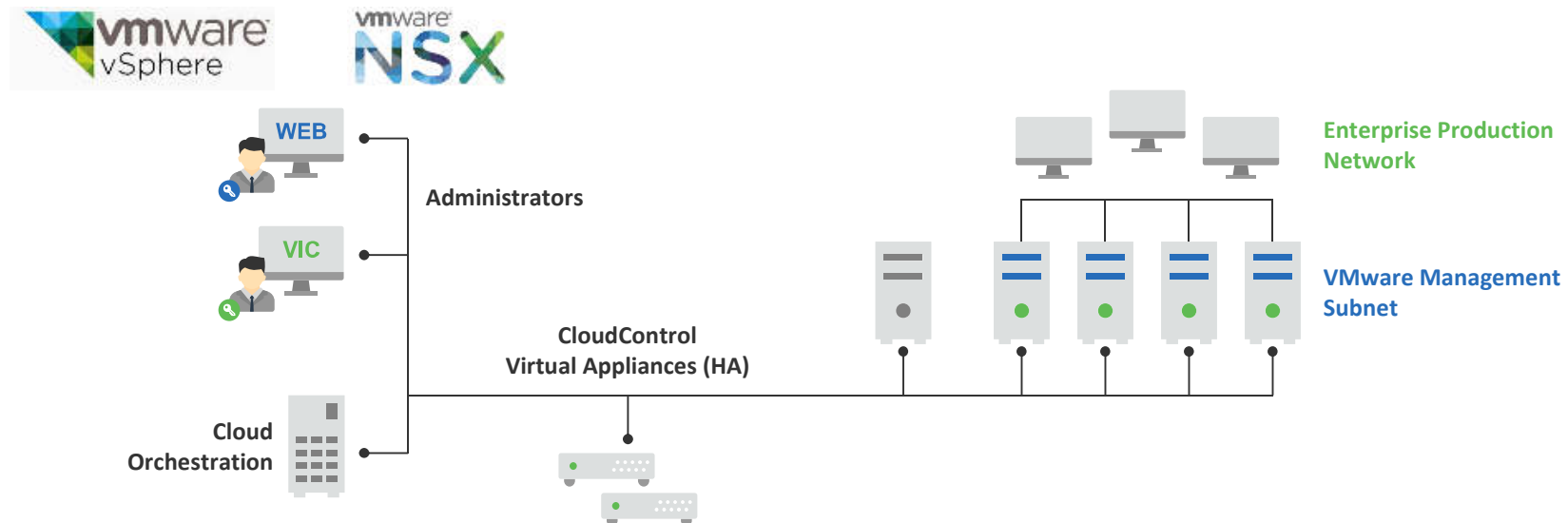


HyTrust CloudControl – Security & Compliance in Private Clouds



*Coming in future releases

Where does HyTrust CloudControl fit?



- Deployed as virtual machines or dedicated server
- Positioned between virtual infrastructure/management and administrator stations
- Applies controls and monitors activity with NO change to the administrators experience
- Not in-line with production data – NO impact on application availability or latency

HyTrust DataControl halts Data Breaches on All Clouds



HTDC protects data everywhere

- **On-premises and cloud ready** – across all major cloud providers
- **Hyper-Convergence ready** – built into Nutanix, Simplivity, others
- **Storage ready** – including SSD technology



HTDC provides easy management

- Scalable, zero downtime re-key management and encryption
- Single interface regardless of where the workload runs
- Pre-integrated to KMIP client/server for easy extensibility



Key Control – the key manager that ensures enforcement of policy via key management



Policy Agent – ties policy to workload and executes encryption and decryption



Policy Engine – ensure appropriate controls with context



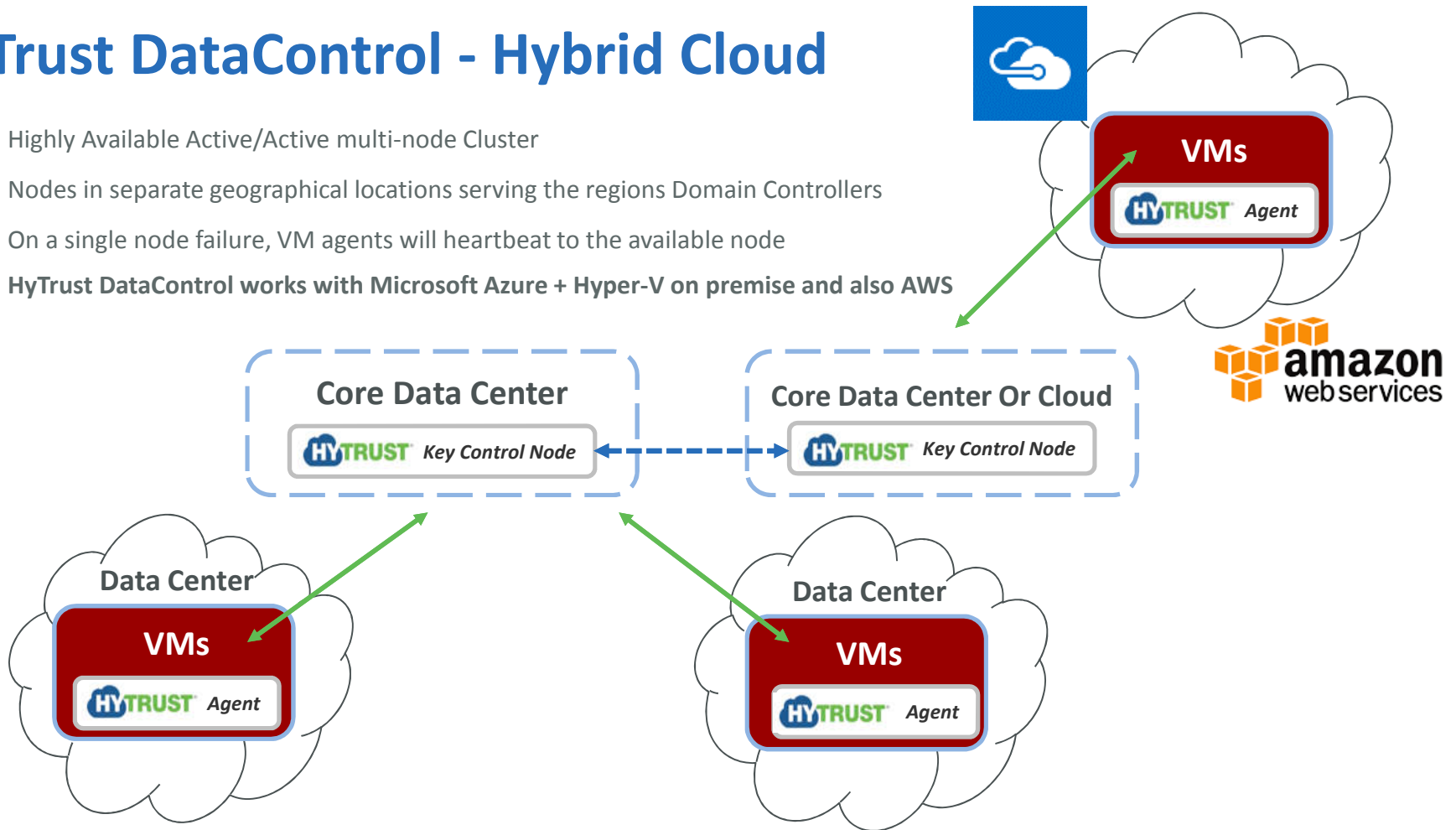
HTDC provides deep protection

- Workload protection from boot to data with complete stack protection
- Portable policy travels with workload to ensure always on protection
- Connects with HyTrust BoundaryControl and HyTrust CloudControl for automated and workflow oriented security
- **Hardware accelerated encryption via integration with Intel AES-NI**



HyTrust DataControl - Hybrid Cloud

- Highly Available Active/Active multi-node Cluster
- Nodes in separate geographical locations serving the regions Domain Controllers
- On a single node failure, VM agents will heartbeat to the available node
- HyTrust DataControl works with Microsoft Azure + Hyper-V on premise and also AWS

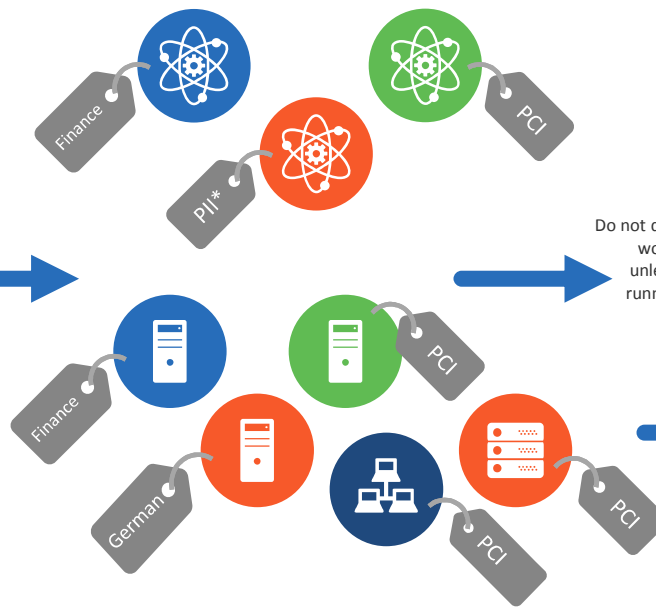


HyTrust Boundary Controls - Avoid Data Sovereignty Landmines

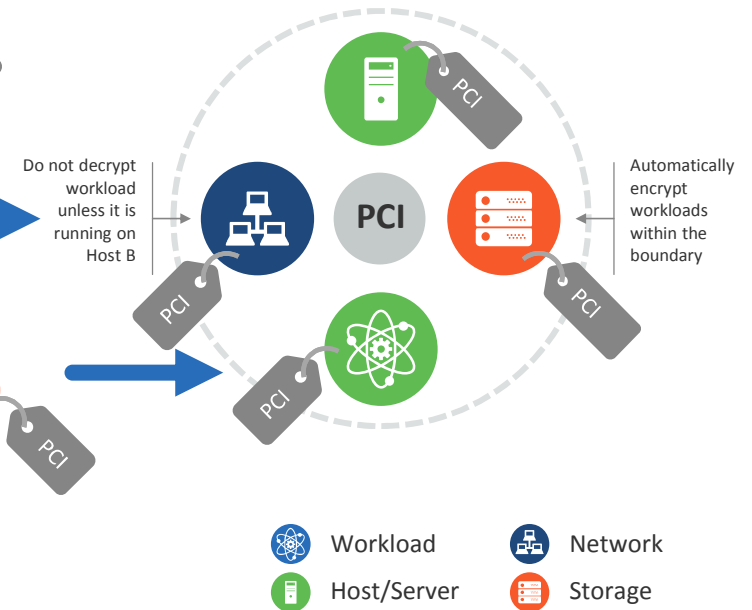
Define and create a logical boundary by geography, regulatory standard, department, etc.



Assign tags to key assets



Define policies and automate security control enforcement for your defined boundary



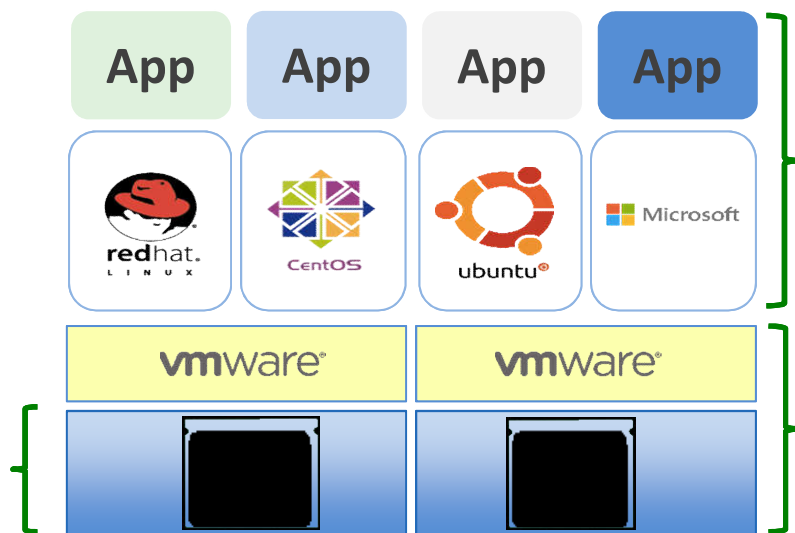
Automatically provision, configure, and enforce security controls for all things inside your defined logical boundaries – Intel TXT provides Hardware Root-of-Trust

Intel TXT + HyTrust + VMware on IBM Cloud: Regulatory Compliance Automation and Data Sovereignty Controls



Xeon hardware with:

- Crypto Acceleration (AES-NI)
- Hardware Root-of-Trust (TXT)
- Geo-location stored in TPM



SOFTLAYER[®]
an IBM Company



VM and Data Encryption with:

- Fully automatic key management
- Zero-downtime encryption/rekey
- HW-speed crypto (using Intel AES-NI)
- Flexible Key Server Placement (On or Off-Prem)



Policy-based controls with:

- Secure Governance of V-Admins
- V-Infrastructure hardening
- Compliance logging and full audit
- Physical host trust-attestation
- Geo and logical boundary enforcement (using Intel TXT)

HyTrust Workload Security Allows You To...

	Accelerate Savings 	Automate Compliance 	Reduce Risk 	Guarantee Availability 
	Financial Services Provider Remove Air Gaps	University Hospital Operationalize NSX	Financial Services Provider Mitigate Data Breaches	Payments Tech Company Operational Control
Challenge	→ Six networks – air gapped for security and compliance needs → Infrastructure needed \$30M for HW and SW to meet security needs	→ Implementing VMware NSX for micro-segments in SDDC → Maintain admin lines of control between networking and security teams	→ Large number of VMs with admin teams located globally → Ensure an admin can't copy and load VM in home country	→ Virtual infrastructure supporting card transactions → vAdmins inadvertently and often shutting down VMs
Solution	Achieve secure, provable multi-tenancy with reduced spend	Ensure separation of operator duties and monitoring access through RBAC	Implement data sovereignty controls to restrict VMs to operate within a specific country	Require secondary approval before users can perform disruptive VM operations
ROI	33% CAPEX infrastructure savings, reduced OPEX costs	Reduced infrastructure cost and overhead required to achieve compliance	Mitigated breach loss and recovery costs due to exposed data and misuse	Reduced downtime, improved availability, prevented loss of millions in revenue

HyTrust – A Leader in Workload Security

HyTrust Workload Security solutions mitigates the security and operational risks that organizations face when pursuing cloud and virtualization data center transformation.

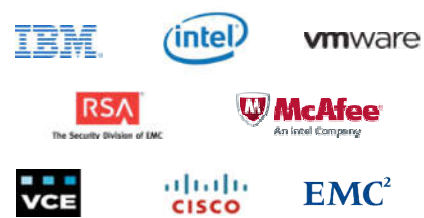
Over 750,000 Virtual Workloads are protected by HyTrust

- ✓ Founded in 2007
- ✓ Extensive virtualization and cloud security expertise
- ✓ 12 granted and pending patents
- ✓ Acquired HighCloud Security in 2013

CUSTOMERS



TECHNOLOGY PARTNERS



STRATEGIC & FINANCIAL INVESTORS



Takeaways

1. Bridging the gap between the advantages of Cloud (including Private Cloud or SDDC) and the requirements of Security and Compliance takes real innovation – but it can be done
2. Securing the Private Cloud requires real access controls, authorization workflows, forensics and workload hardening techniques
3. You can encrypt everything – with leading edge key management and hardware accelerated encryption there are no reasons not to do it
4. Your encryption needs to live with the workload for its entire life – no matter what cloud it travels to
5. Hardware “root-of-trust” based geo-fencing is the strongest Data Sovereignty solution you can implement



Thank You

Come see us!

We are at the Intel Stand - M2