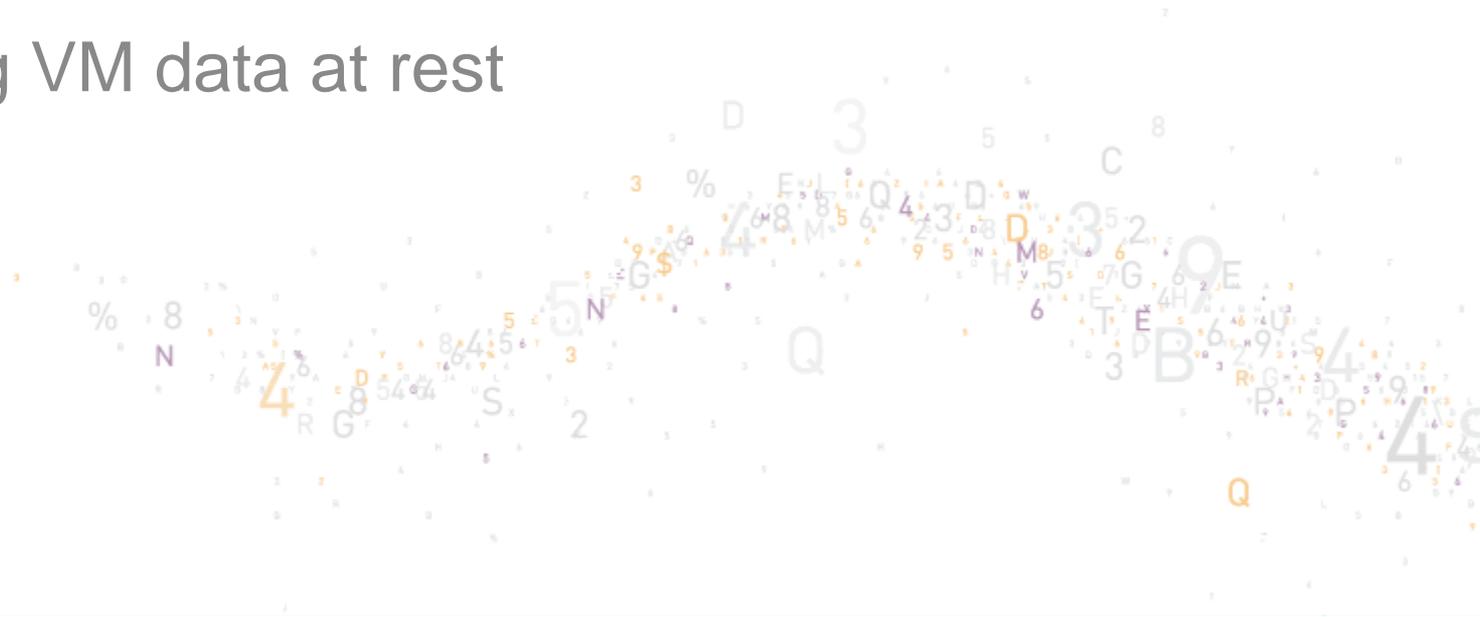




THE  
DATA  
PROTECTION  
COMPANY

# ProtectV

Protecting VM data at rest



**Marko Bobinac**

**PreSales Engineer CEE, Russia & CIS**

**Actinet, June 2013**

# Customer Journey to the Cloud

Security and compliance concerns prevent many of our customers from advancing in their cloud journey.

## Efficiency

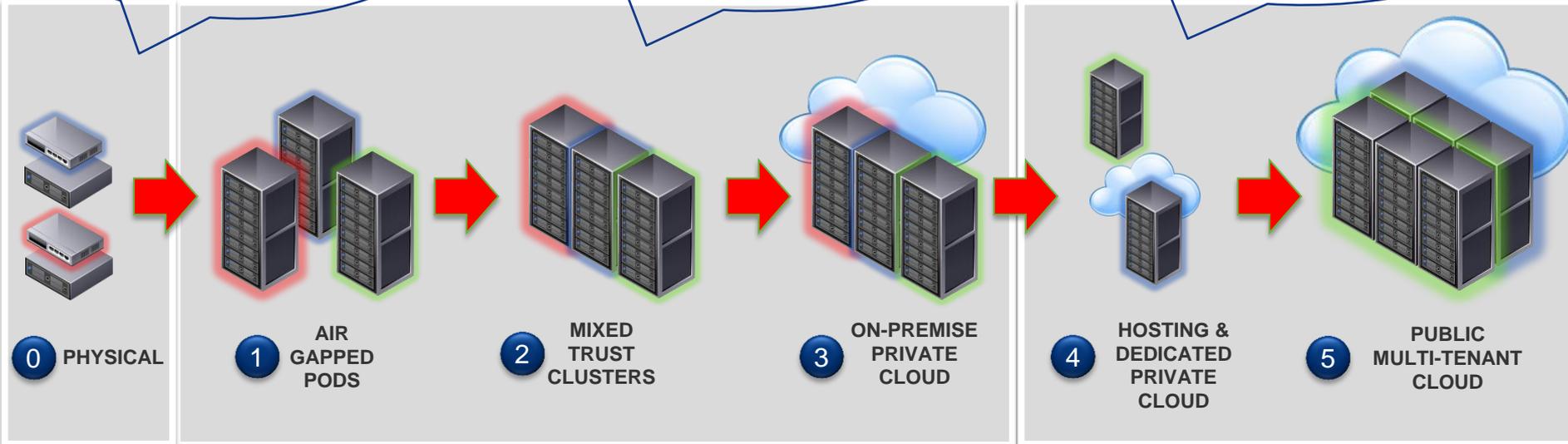
I want to reduce IT costs through server consolidation, but if I can't secure and audit business critical apps using existing processes, I'm not going virtual in the first place, let alone cloud.

## Automation

I want to automate IT to keep developers and other users in-house and under our control – but security isn't agile and misconfigurations put us at risk.

## Availability

Economics tell us that cloud is the only way to get cost effective BCDR...but what is that provider doing with my data? And can another tenant access my data?



# VM Encryption Can Help Clear Obstacles to the Cloud

vCNS partners such as SafeNet provide data encryption solutions to ensure confidentiality across cloud infrastructures.

## Efficiency

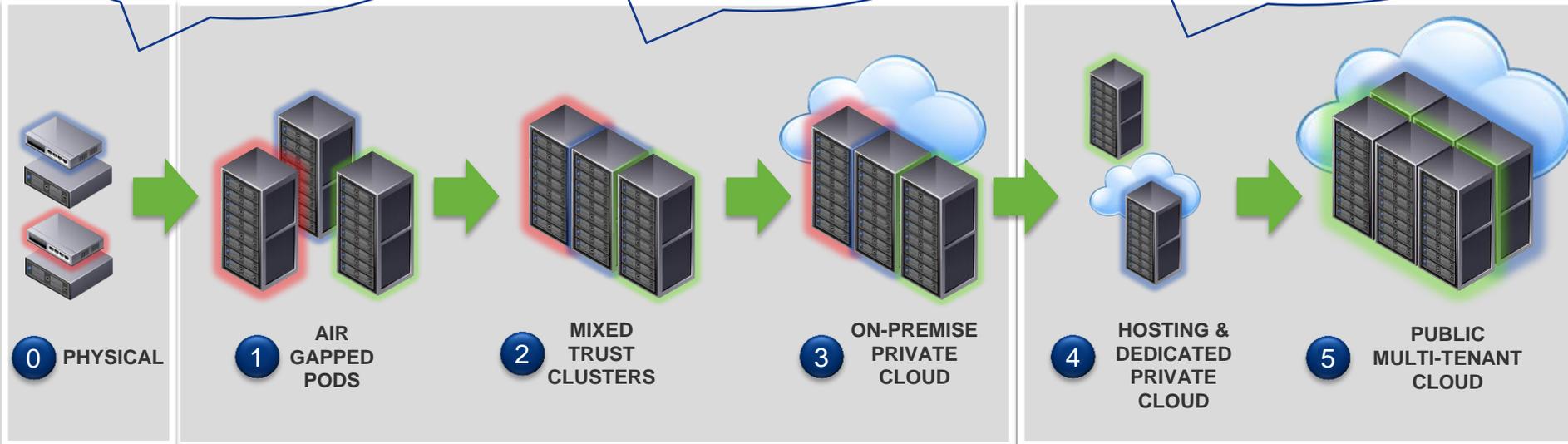
I'm ready to virtualize because I know that VMs with sensitive data will always remain encrypted at rest, regardless of the backend storage device.

## Automation

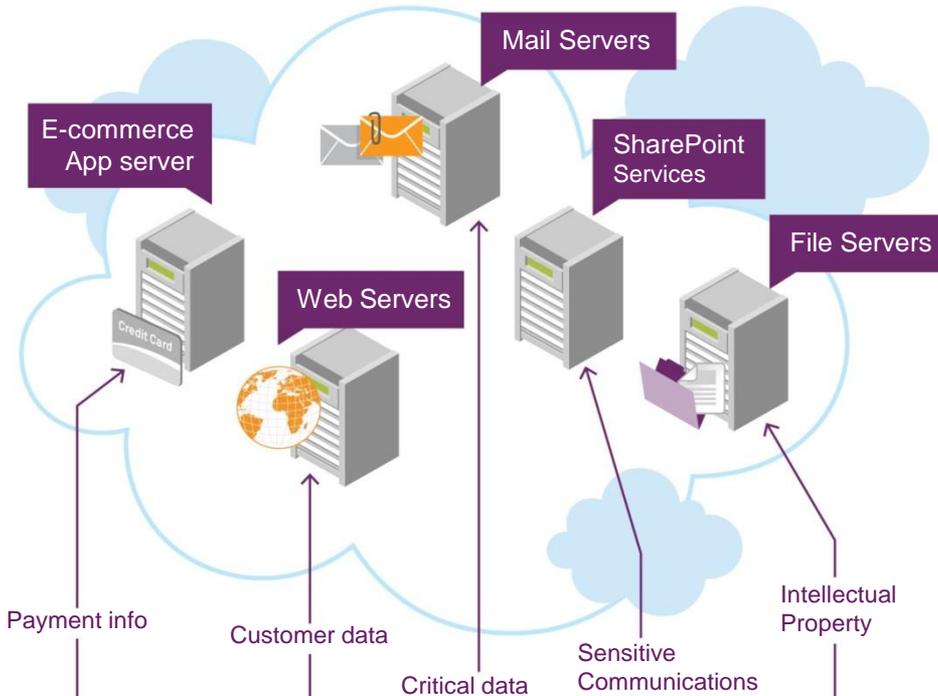
My encryption policies are tied to VMs and other logical constructs so that when they move within my data center or to other clouds, they are automatically protected.

## Availability

I can get cost-effective services from a 3<sup>rd</sup> party provider – such as capacity on demand and disaster recovery – without worrying about unauthorized access to my data.



# Cloud Risks



- Do I have control of my data?
- Who is accessing my data?
- Where is my data?
- Is InfoSec going to stop me from moving to the cloud?

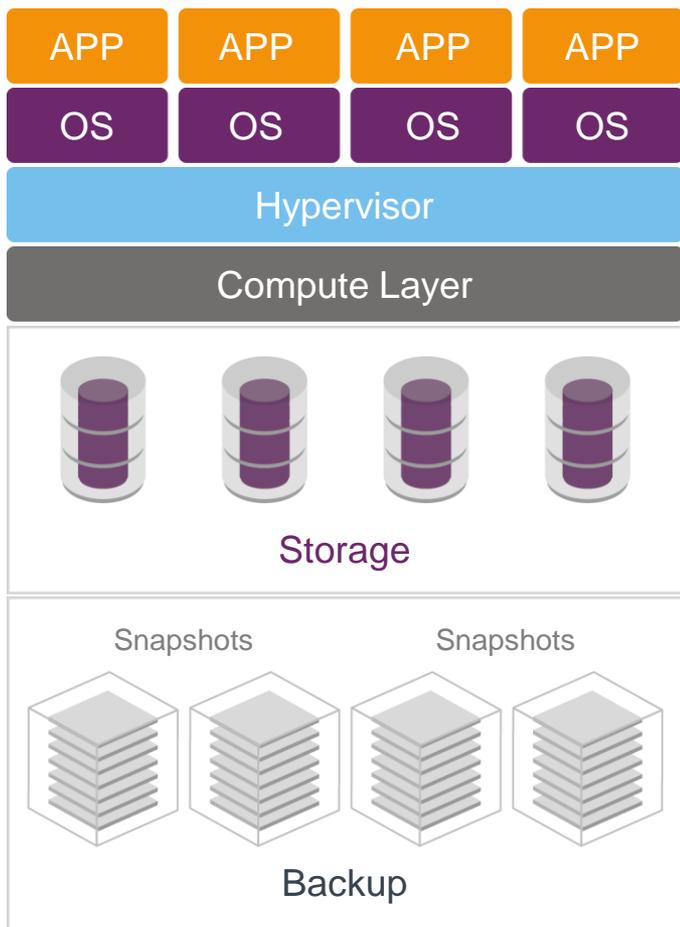
4A!6W6Z015 \*158R7 T68Y87 2P{66! 46Z64A!6 64Z55546E65D\$66A55S4096 9 Q1 5 \*158R7 T68Y87 2P{66! 46Z64A!6  
66A55 879U54164 099P7A65S2679G6+6Q1W\$66A55 546D6+6Q1W5F\*158R75T6PY 7879U54164\099P7A65S2679G6+6Q1W\$66A55  
65Y43 F4 654G312TY6GFAS643234655X 6G5465Y4 U21B35D6F45 \$87D161W 134F4 654G312TY6GFAS643234655X46G5465Y43  
5F4D34R6U46%U65A44S3 5Z24X11Y5H66 84R6 9F4D36F W44H36VF4RR6 58+4S3546%Q65A44S35Z24X11Y5H66T84R65F4D3  
32DF19 2 \*03988!93048LSK93M{ %W 654 5S4 939{8933+809 9 2 \*03988!93048LSK93M{ %WJ6565S4U32DF1  
9P7A6LG5Z51 C96X65V33N34B6655U54164\099P7A65S26D35F\6G4H56J4TJK334\ LX6Z51 C96X65V33N34B6655U54164\099P7A6



THE  
DATA  
PROTECTION  
COMPANY

# Virtualization Risks

## How secure is my data in a virtualized world?



VMs are easy to copy (and steal).



VMs are easy to move.



VMs introduce a new class of privileged users and administrators—server, storage, backup, and application—all operating independently.



VMs have multiple instances, snapshots and backups of data.



And what about your Disaster Recovery site?



THE  
DATA  
PROTECTION  
COMPANY

# Closing Virtual Datacenter Security Gaps



Comprehensive encryption of VMs and storage

Solves critical challenges of **security**,  
**governance** and **control** of data in a virtual  
infrastructure or cloud

Certified by VMware

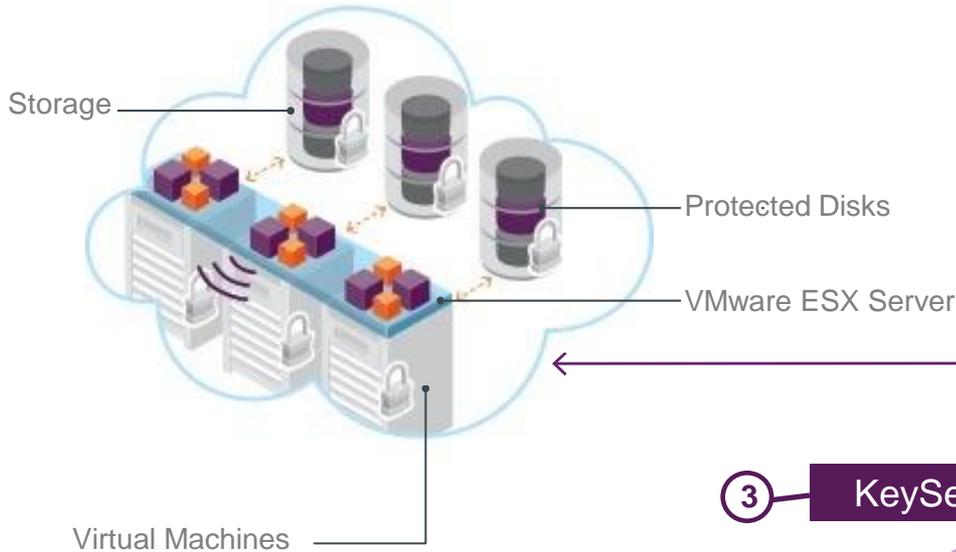


THE  
DATA  
PROTECTION  
COMPANY

# Anatomy of Securing a Virtual Datacenter

## 1 ProtectV Client

ProtectV Client is installed on your VMs.

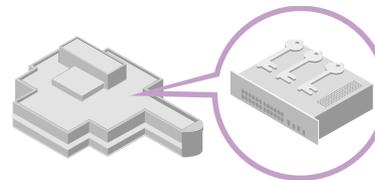


## 2 ProtectV Manager

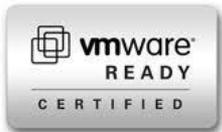
ProtectV Manager is a virtual machine that runs as a VM in a VMware environment.



## 3 KeySecure



KeySecure is a hardware-based high-assurance enterprise key management solution.



THE  
DATA  
PROTECTION  
COMPANY

# ProtectV Components

## ProtectV Manager – Control/Scale Out/Integrate

- Policy creation/management /enforcement
- VM authorization
- Key cache
- Log aggregation
- Reliable delivery
- Migration/encryption
- Security process scale out

## ProtectV Client – Protected VMs

- Preboot environment
- System partition encryption
- Volume /data partition encryption
- Application transparent encryption
- Linux and Windows support

## KeySecure – Management/ Audit

- Hardened appliance
- FIPS 140-2 L3
- Key lifecycle management
- Audit



THE  
DATA  
PROTECTION  
COMPANY

# SafeNet ProtectV on Instances

## ProtectV Protection

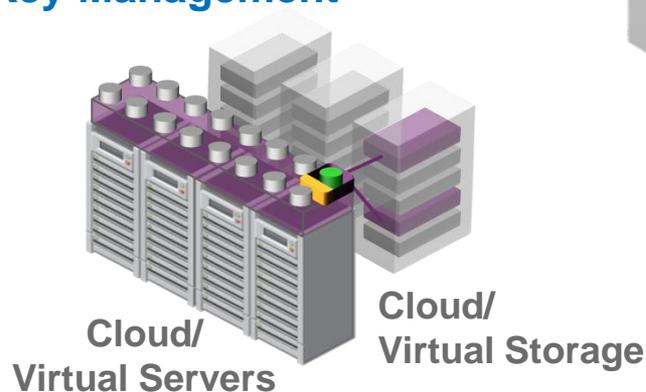
- OS does not boot without authentication
- Entire instance encrypted, protecting OS
- Attached volumes encrypted
- Supports thin provisioning critical to cloud
- Encrypt all data written to disk
- Central Key Management for strong control
- Resists brute-force attacks on keys
- Supports protected snapshots

### Encrypted Instance

- AES 256

### • Pre-Launch Authentication

### • Policy + Key Management

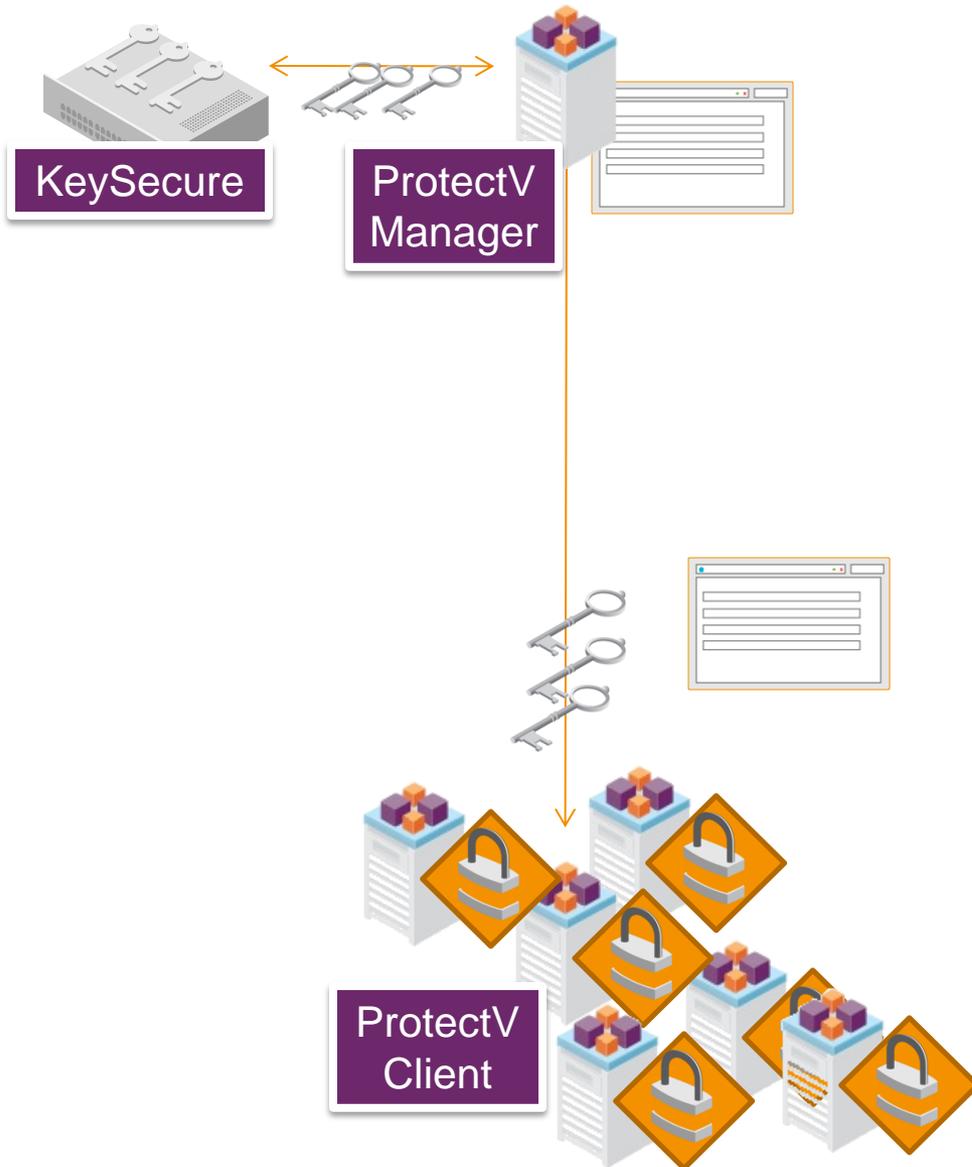


### • Protected Volumes



THE  
DATA  
PROTECTION  
COMPANY

# ProtectV: How It Works



Select machines with sensitive data **1**

Centrally set and apply security policies **2**

Tell client machines to encrypt data with the right key **3**

Authenticate before VM is launched **4**

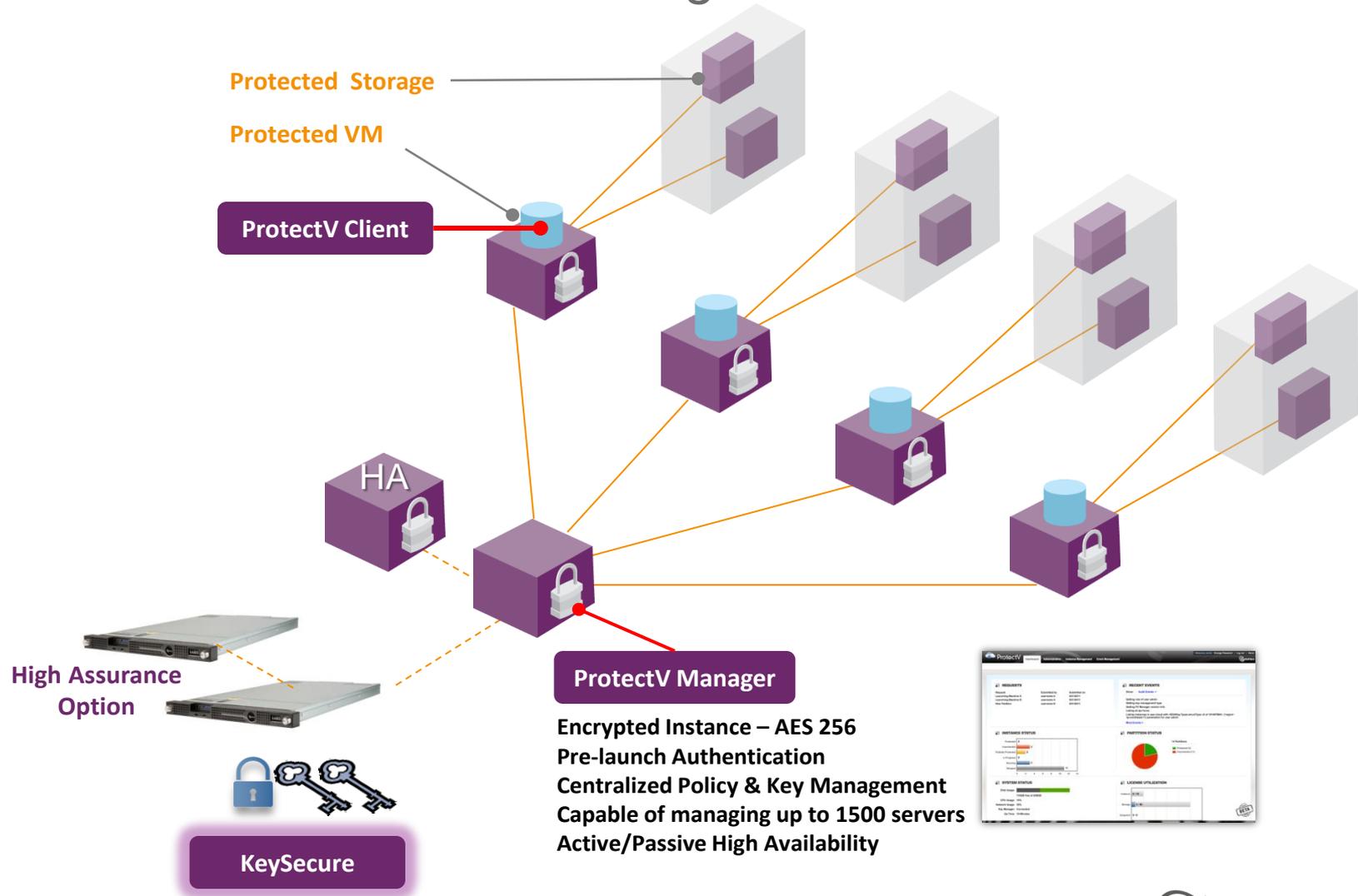
Clients get the *encrypt* command and key— and start encrypting the data! **5**



THE  
DATA  
PROTECTION  
COMPANY

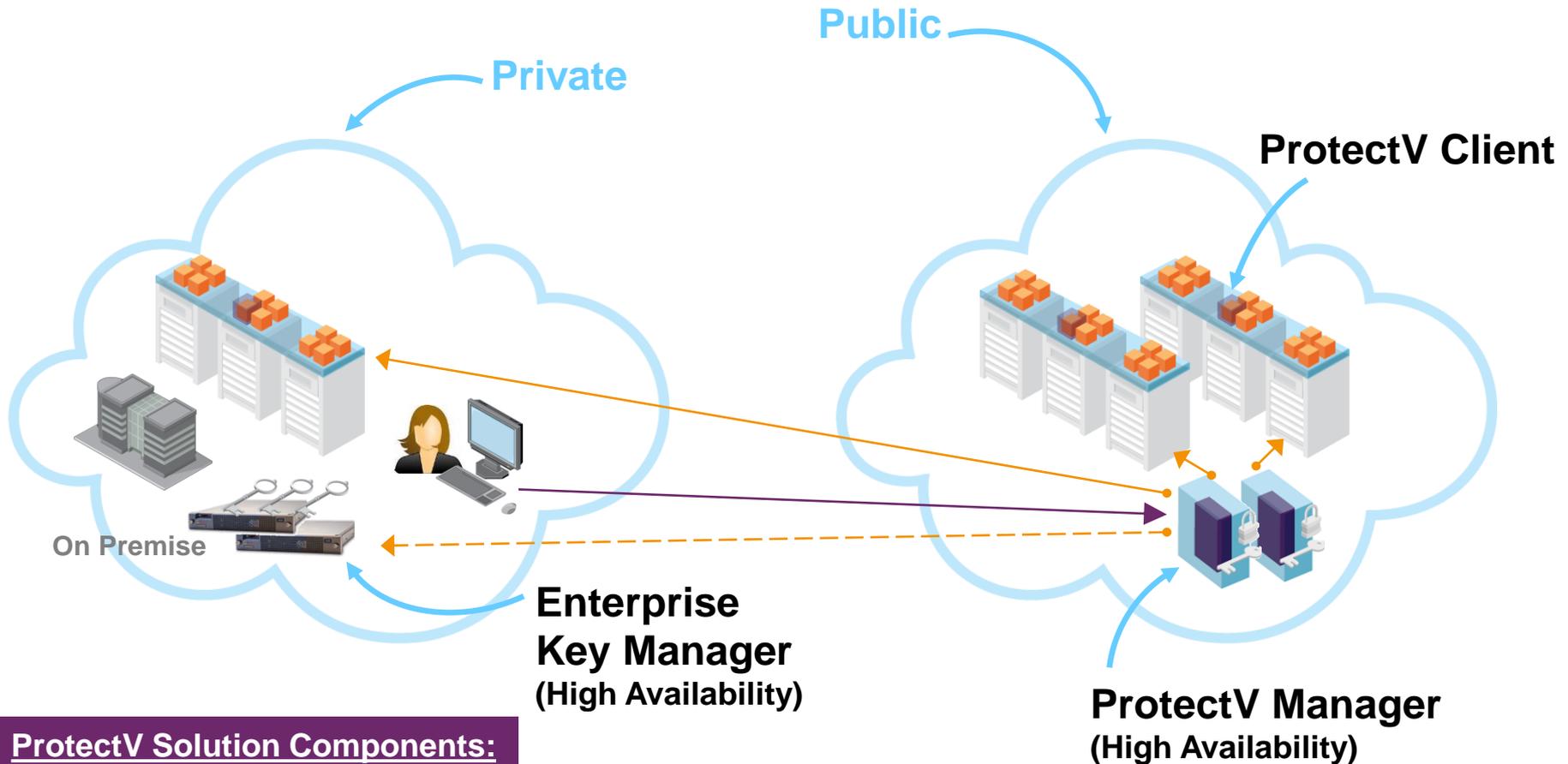
# ProtectV and Scaling in Large Environments

## *ProtectV and ProtectV Manager*



THE  
DATA  
PROTECTION  
COMPANY

# ProtectV Deployment Scenario

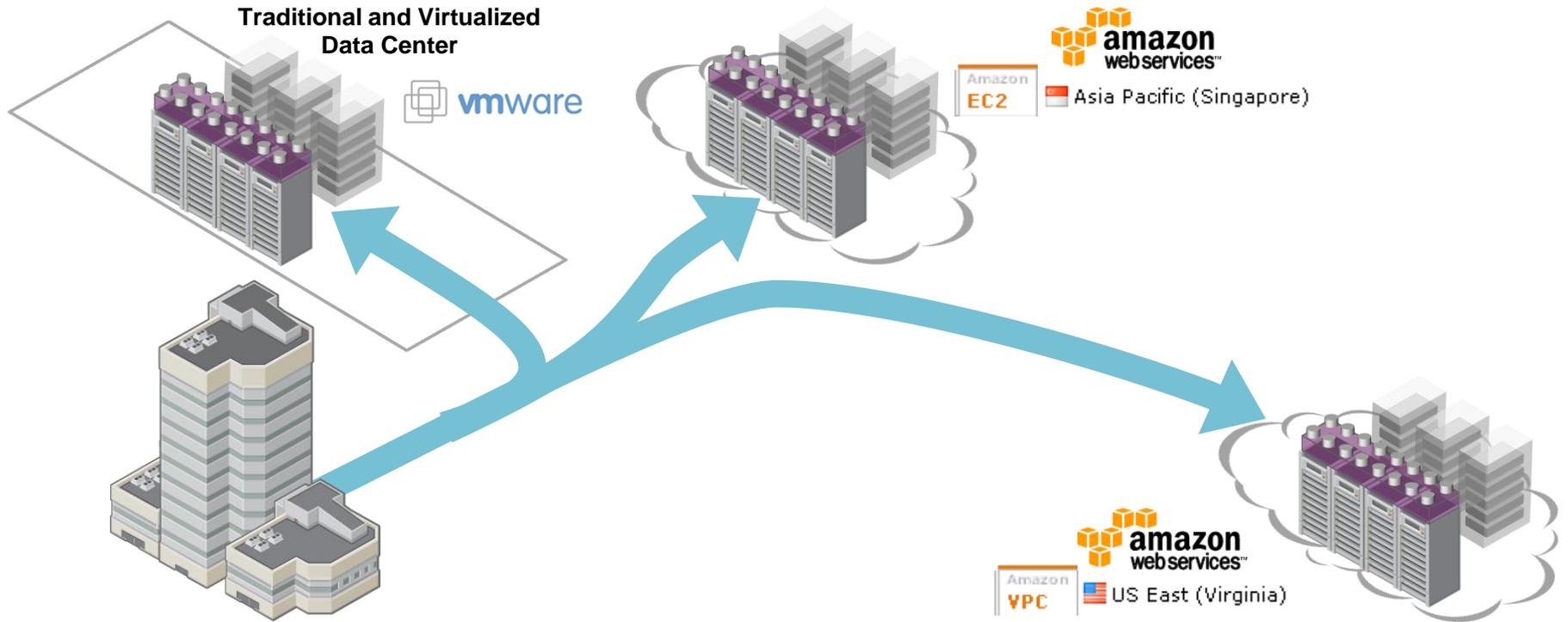


## ProtectV Solution Components:

- ProtectV Client
- ProtectV Manager
- Enterprise Key Manager

# ProtectV

*Elasticity, agility, and large scale architecture*



## Design Factors

- Integration to cloud management platforms
- Scalability to large scales, across cloud zones as well as cloud providers
- Key management to preserve elasticity and true data portability across cloud



THE  
DATA  
PROTECTION  
COMPANY

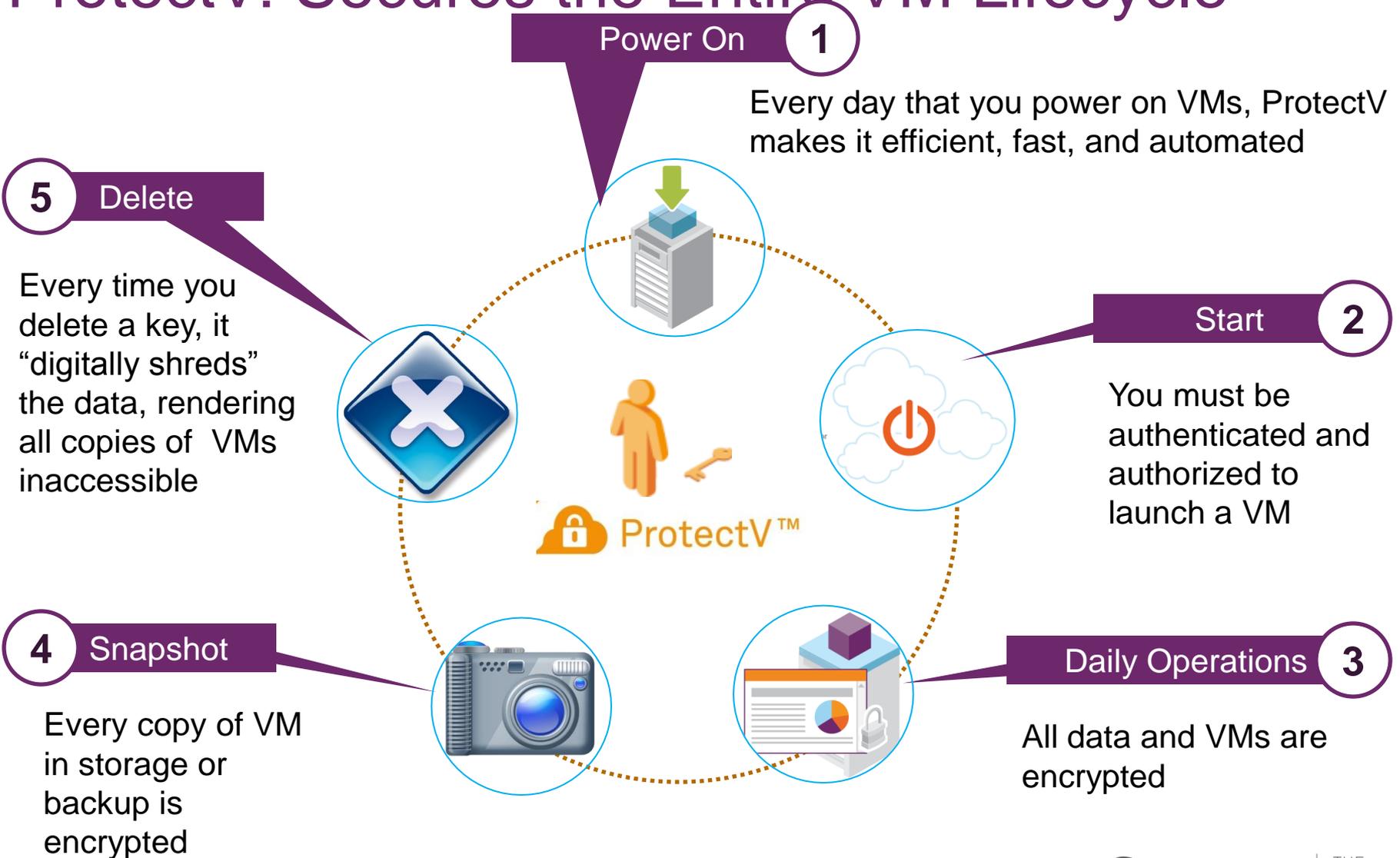
# ProtectV: Environments, Impact, Products

- ProtectV currently supports the following environments:
  - Amazon Web Services EC2
  - Amazon Web Services VPC
  - VMware vCenter 4 or 5
- ProtectV impacts performance by 10% - 15% in standard AWS EC2 scenarios
- Complementary products to ProtectV:
  - KeySecure (k150 and k460)
  - DataSecure (i150 and i450)



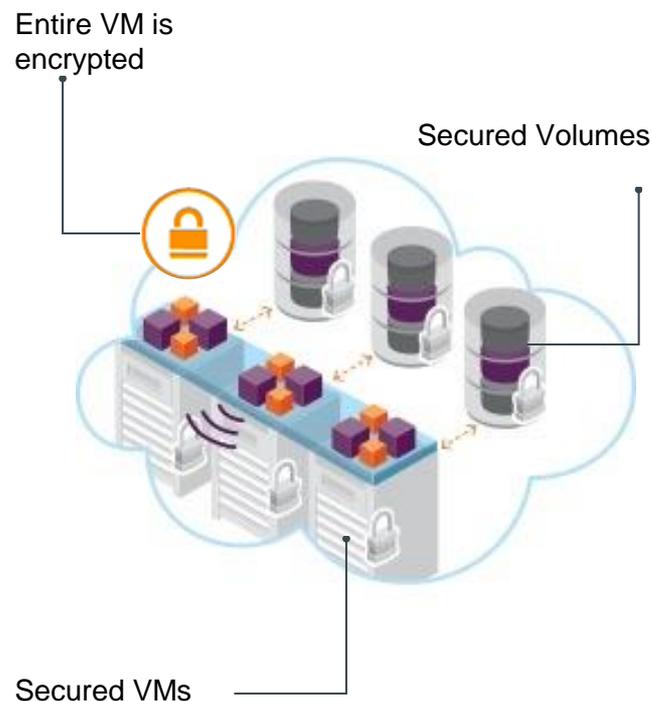
THE  
DATA  
PROTECTION  
COMPANY

# ProtectV: Secures the Entire VM Lifecycle



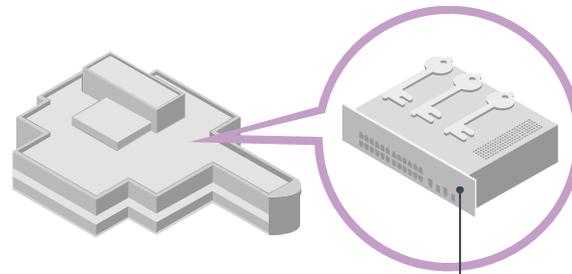
# ProtectV Delivers Complete VM Encryption

- Encryption of entire VM
- Encryption of system/OS partition
- Encryption of data partition
- Encryption of associated snapshots and backups (DR sites etc.)



# ProtectV Delivers Ownership & Control of Your Data

- Pre-launch user authorization to access a VM
- Separation of duties between storage, VI and security administrators
- Hardware-based FIPS 140-2 level 3 certified Enterprise Key Manager



On-Premise EKM

Pre-Launch Authentication



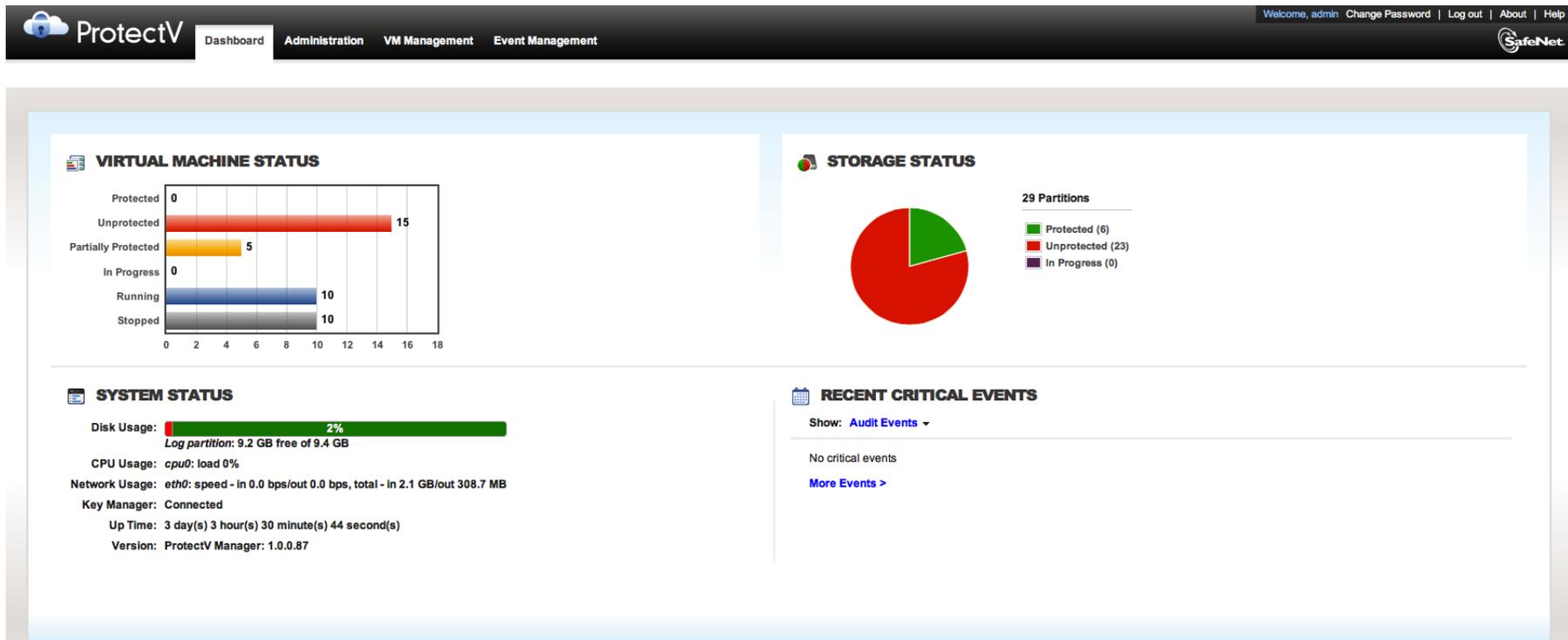
Secured VMs



THE  
DATA  
PROTECTION  
COMPANY

# Visibility & Proof of Data Governance

- Unified management - at-a-glance dashboard view and central audit point
- On-premise key management audit for encryption keys



# Role-Based Separation of Duties

The screenshot displays the 'Users' management page in the ProtectV Administration console. The 'admin' role is selected, showing its permissions and assigned VM groups.

**User "linuxadmin" Role Scope**

User Role	Role Description	Role Scope (Assigned VM Groups)
<input checked="" type="radio"/> admin	Built-in Administrator Role	Default Role, Linux Servers
<input type="radio"/> observer	Built-in Observer Role.	
<input type="radio"/> security-admin	Built-in Security Administrator Role.	
<input type="radio"/> vm-admin	Built-in VM Administrator Role.	

Showing 1 to 4 of 4 entries

**Role "admin" Permissions**

- Dashboard:
- Administration: 
  - Users: 
    - View Users:
    - Add User:
    - Delete User:
    - Change Password:
    - Change Default Role:
    - Assign VM Group:
  - Roles: 
    - View Roles:
    - Add Role:
    - Clone Role:
    - Delete Role:
    - Change Role Description:
    - Update Role Permissions:
  - System Settings: 
    - View Cloud Credential:
    - Modify Cloud Credentials:
    - View Networking:
    - Modify DNS:
    - View Key Manager Settings:
    - Modify Key Manager Settings:

**Assigned VM Groups**

- Linux Servers (4)
  - aws\$us-east-1@i-436db225
  - aws\$us-east-1@i-4f508f29
  - aws\$us-east-1@i-3970af5f
  - aws\$us-east-1@i-b52af5d3



THE  
DATA  
PROTECTION  
COMPANY

# ProtectV Manager – VM Management Tab

## Manage Virtual Machines

Select your Cloud to begin.

VM Group Take Action ? ↓

Clouds

- VMware vSphere
  - Training
  - VM Group (2)
    - all-machines (19)
    - test1 (1)

Show 25 entries

Name	System Status	Public IP	Virtual Machine FQDN
<input type="checkbox"/> Nint01	stopped		vsphere\$protectv@50020af8-a9cd-8af2-1394-c447b5b23a28
<input type="checkbox"/> Ni-Win2008	stopped		vsphere\$protectv@50022f40-415f-d709-3e16-032bb819e0d9
<input type="checkbox"/> For Nadav-Linux	stopped	10.9.18.9	vsphere\$protectv@50024b49-f7d3-ccf3-aa12-03a895ed330e
<input type="checkbox"/> Nint-CentOS	stopped		vsphere\$protectv@50028f0b-1967-1df2-c43e-51948e79207f
<input type="checkbox"/> For Nadav	stopped	10.9.18.8	vsphere\$protectv@5002d405-3c0e-6859-4671-2cca9ee3e5bc
<input type="checkbox"/> PVM1.1.1	running	10.9.18.50	vsphere\$protectv@50070b9a-915d-6a08-495a-d4719f8fe028
<input type="checkbox"/> Windows 2008 - 20120717150801	stopped		vsphere\$protectv@50070d5a-4572-ce5a-54e6-4c95194bd708
<input type="checkbox"/> PVM1.1-2	stopped		vsphere\$protectv@50073360-faac-9fda-ce7e-1d016c3b3515
<input type="checkbox"/> Windows 2008 R2 - Member Server 1	stopped		vsphere\$protectv@500739e0-d2a1-7753-b6cd-7e55e0aae4dd
<input checked="" type="checkbox"/> PVC2008-1.1.1	running	10.9.18.55	vsphere\$protectv@500743a1-02dd-89ec-c8d2-5f287a56120e
Partition Name	Protection Status	Size	Encrypted Bytes
<input checked="" type="checkbox"/> C: (System)	Unencrypted	39.9 GB	0.0 bytes
<input type="checkbox"/> PVM#1	stopped		vsphere\$protectv@50075644-6186-2907-fdd6-67be3bce796d
<input type="checkbox"/> PVM-1.1	stopped		vsphere\$protectv@50075dc2-abe1-5987-72a0-ce50b1576169
<input type="checkbox"/> Team-1 PVM95	stopped		vsphere\$protectv@500785f1-f50b-2fe-b101-62e2a5261125
<input type="checkbox"/> Windows 2008 R2 - Member Server 2	stopped	10.9.21.3	vsphere\$protectv@50078ade-99c8-2ca2-b99f-888c20f48c7d
<input type="checkbox"/> CentOS 5.6 PVC	stopped		vsphere\$protectv@5007a895-13c0-05cc-f9a4-d6b70cc1501
<input type="checkbox"/> Windows 2008 R2 - AD	stopped	10.9.21.1	vsphere\$protectv@5007b74d-d289-4f6d-1b0c-d9f1371aef2
<input type="checkbox"/> Windows 7	stopped		vsphere\$protectv@5007bab0-ef42-1d65-a9a7-ebec7bf7d793
<input type="checkbox"/> PVM#2	stopped		vsphere\$protectv@5007d4a0-752a-4b80-9ba4-017bb1a4e4be
<input type="checkbox"/> Win2008R2 PVC	stopped	10.9.40.4	vsphere\$protectv@5007de0a-d5c4-368d-de6a-97bb9473360c

Showing 1 to 19 of 19 entries

First Previous 1 Next Last

Name	Value
Partition Name	C: (System)
Volume Name	PhysicalDrive0
System Name	Volume{ee608d74-7e75-11e1-acfb-806e8f6e8963}
Partition ID	2178c928-0953-4fc3-bf67-da1f4c0c517d
File System Type	NTFS
System Volume	True
Protection Status	Unencrypted
Key Name	
Encrypted Bytes	0.0 bytes
Cipher	
Time Left	0

# ProtectV Manager – Instance Tab - Boot

ProtectV Dashboard Administration **VM Management** Event Management Welcome, admin Change Password | Log out | About | Help 

**Manage Virtual Machines** VM Group Take Action

Select your Cloud to begin.

CLOUDS

- VMware vSphere
  - Training
    - VM Group (2)
      - all-machines (19)
        - test1 (1)

Show  entries Search:

<input type="checkbox"/>	Name	System Status	Public IP	Virtual Machine FQDN
<input type="checkbox"/>	Nirit01	stopped		vsphere\$protectv@50020af8-a9cd-8af2-1394-c447b5b23a28
<input type="checkbox"/>	Ni-Win2008	stopped		vsphere\$protectv@50022f40-415f-0709-3e16-032bb619ef09
<input type="checkbox"/>	For Nadav-Linux	stopped	10.9.18.9	vsphere\$protectv@50024b49-f7d3-ccf3-aa12-03a895ed330e
<input type="checkbox"/>	Nirit-CentOS	stopped		vsphere\$protectv@50028f0b-1967-1df2-c43e-51949e79207f
<input type="checkbox"/>	For Nadav	stopped	10.9.18.8	vsphere\$protectv@5002d405-3c0e-6859-4671-2cca9ee3e5bc
<input type="checkbox"/>	PVM1.1.1	running	10.9.18.50	vsphere\$protectv@50070b9a-915d-8a08-495a-d47198fe028
<input type="checkbox"/>	Windows 2008 - 20120717150801	stopped		vsphere\$protectv@50070d5a-4572-ce5a-54e6-4c95194bd708
<input type="checkbox"/>	PVM1.1-2	stopped		vsphere\$protectv@50073360-faac-9fda-ce7e-1d016c3b3515
<input type="checkbox"/>	Windows 2008 R2 - Member Server 1	stopped		vsphere\$protectv@500739e0-d2a1-7753-b6cd-7e55e0aae4dd
<input checked="" type="checkbox"/>	PVC2008-1.1.1	running		vsphere\$protectv@500743a1-02dd-89ec-c8d2-5f287a56120e

<input type="checkbox"/>	Partition Name	Protection Status	Size	Encrypted Bytes
<input type="checkbox"/>	PVM#1	stopped		vsphere\$protectv@50075644-6186-2907-fdd6-67be3bc796d
<input type="checkbox"/>	PVM-1.1	stopped		vsphere\$protectv@50075dc2-abe1-5987-72a0-ce50b1576169
<input type="checkbox"/>	Team-1 PVM95	stopped		vsphere\$protectv@500785f1-f50b-2ffe-b101-62e2a5261125
<input type="checkbox"/>	Windows 2008 R2 - Member Server 2	stopped	10.9.21.3	vsphere\$protectv@50078ade-99c8-2ca2-b99f-888c20f48c7d
<input type="checkbox"/>	CentOS 5.6 PVC	stopped		vsphere\$protectv@5007a895-13c0-05cc-f9a4-d6b7f0cc1501
<input type="checkbox"/>	Windows 2008 R2 - AD	stopped	10.9.21.1	vsphere\$protectv@5007b74d-d289-4f6d-1b0c-d9f1371aee72
<input type="checkbox"/>	Windows 7	stopped		vsphere\$protectv@5007bab0-ef42-1d65-a9a7-ebec7bf7d793
<input type="checkbox"/>	PVM#2	stopped		vsphere\$protectv@5007d4a0-752a-4b80-9ba4-017bb1a4ecbe
<input type="checkbox"/>	Win2008R2 PVC	stopped	10.9.40.4	vsphere\$protectv@5007de0a-d5c4-368d-de6a-97bb9473360c

Showing 1 to 19 of 19 entries First Previous 1 Next Last

Name	Value
Operating System	
System Status	running
Unattended Reboot	Enabled
Public DNS	
Public IP	
Virtual Machine FQDN	vsphere\$protectv@500743a1-
Tags	Name = PVC2008-1.1.1

Set IP Address

- Start Virtual Machine
- Boot to OS**
- Edit Unattended Reboot
- Query Clone Readiness
- Encrypt Partition
- Decrypt Partition
- Enable Partition Access
- Recover Volume
- Find Shared Keys



# Virtual Machine and Storage Protection—*SafeNet ProtectV*

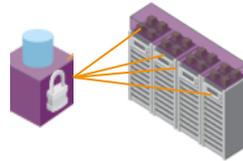
With **SafeNet ProtectV**, customers can protect regulated data on VMs and storage volumes on both **private and public clouds**

- Data isolation in multi-tenant environments
- Separation of Duties
- Pre-Launch Authentication

- Large scale deployments
- Centralized management dashboard—single audit point for real time monitoring and auditing

- On-premise, hardware-based, high assurance root of trust (FIPS 140-2 L3)
- Unified keys across data centers, private and public clouds

## ProtectV Client



## ProtectV Manager



## KeySecure



## Why *SafeNet ProtectV*?

- **Physical and Logical Data Encryption** – Your data and your snapshots are fully encrypted from co-mingling, cross-wiring and super user privileges; your cloud provider can only turn over cipher text if called upon by any jurisdictional authority
- **Ownership and Control of Keys** – You have complete control of your keys and ownership over their lifecycle, even when you choose to host clear text in the cloud
- **Data Isolation** – Run your systems as if it was your own private data center, even in co-mingled or multi-tenant environments
- **Compliance with Lawful Orders** – Isolate data and create separation of duties for role-based, granular access control



FIPS 140-2 L3 validation in process



THE  
DATA  
PROTECTION  
COMPANY



THE  
DATA  
PROTECTION  
COMPANY

[marko.bobinac@safenet-inc.com](mailto:marko.bobinac@safenet-inc.com)

Thank you