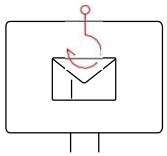
#RANSOMWARE Are you protected?

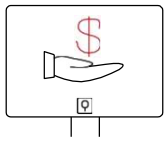
Create a resilient backup infrastructure

VERITAS™

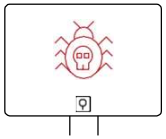
The truth in information.



Jerry in HR clicks on a resume attached to a job application email.



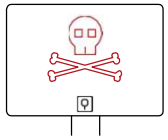
His computer suddenly locks up and a message appears demanding money for its release.



Alarmed, Jerry calls Pete in IT, who checks and confirms Jerry's machine has fallen victim to a ransomware attack.

To pay or not to pay:

How easily could your business be held to ransom?



Pete quickly discovers that the damage is worse than he'd feared: The company's main file server has been infected, and his anti-virus software can't fix it.

The company's critical data has been compromised and it's faced with a major dilemma...

The Growing Threat

91% of cyberattacks begin with a spear-phishing email commonly used for ransom

Ransomware infections by country[5]

Every 2 minutes

Beginning of 2016

Every 40 seconds

End of 2016

Every 14 seconds

End of 2019

Every 11 seconds

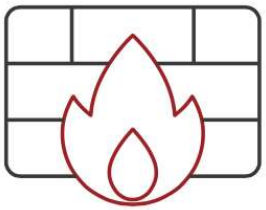
In 2021

Russia

Canada

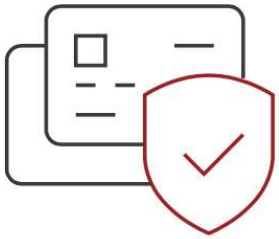
Other Countries

The Best Ways to defend against Ransomware



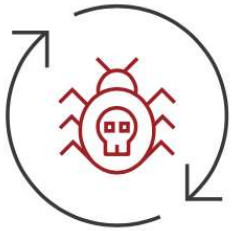
Firewall
& Network
Segregation

Email
& Spam
Filters

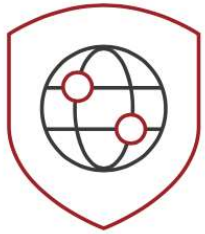


User Security
Awareness
Training Programs

Endpoint Scanning
(Anti-virus or
Anti-malware)

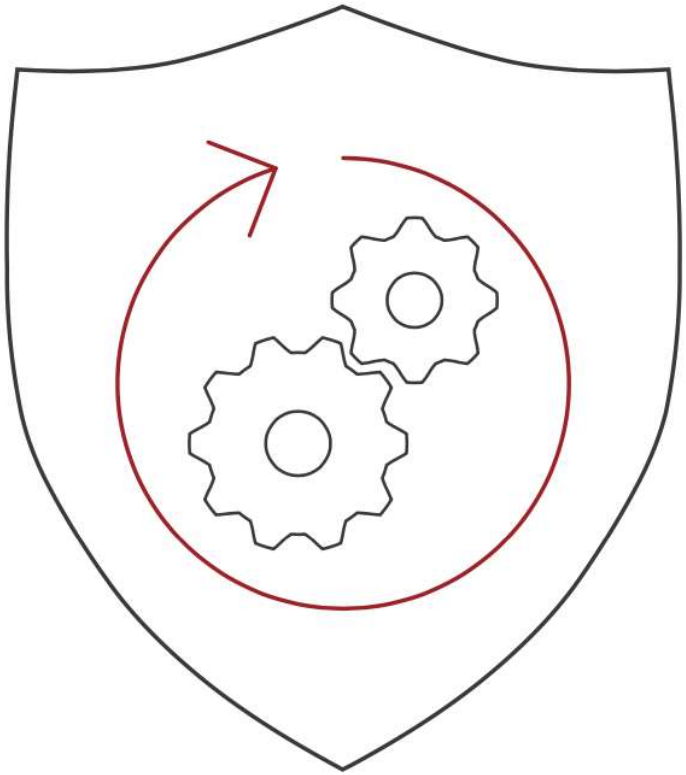


Malware
Detection
& Isolation



Security
Vulnerability
Patching

Optimize your backup strategy



- AIR Gap Backups
- Multiple Copies
- Restrict use of backup credentials
- Evaluate your RPO
- Smart Steps
  - Harden Backup Server
  - Update the backup software
  - Backup regularly
  - Test Restore

VERITAS NETBACKUP APPLIANCE

Create a resilient backup infrastructure

VERITAS™

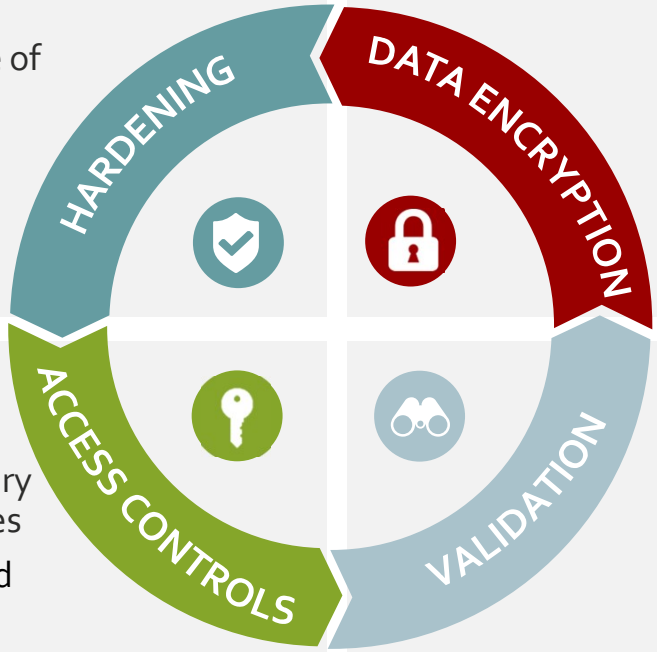
The truth in information.

Veritas NetBackup Appliance Layered Security

Combines multiple mitigating security controls to protect resources and data

Developed from Inception for Security

- Hardening based on National Institute of Standards and Technology (NIST)
- Built in IDS/IPS
- Security Technical Implementation Guides (STIGs) for RHEL.



Encrypted MSDP

- Simple Deployment
- Transparent to End-users
- Compliance made easy
- AES 128-bit or AES 256-bit
- FIPS 140-2 standard

User Authentication

- NetBackup services do not use ordinary user accounts to access backup images
- Only assigned users can configure and manage the NetBackup Appliance
- Prevents unauthorized access to the backup data on the NetBackup Appliance

Tested for Vulnerabilities

- Each element of the NetBackup Appliance is tested
- Regular scanning with industry-recognized vulnerability scanners
- Every new version is verified for vulnerabilities before release

Security Features in NetBackup and Appliances

NetBackup Appliance Security Features

DISA STIG	FIPS 140-2	RBAC	IPv6	Firewall	SDCS
Security Technical Implementation Guides	Federal Information Processing Standard	Role Based Access Control	IPv6 Support	Control incoming and outgoing network traffic	Symantec Data Center Security
System Hardening	**Cryptographic-Based Security**	**Access Control**	**Communications Protocol**	**Network Security**	**IDS/IPS**

Ransomware | Immutability

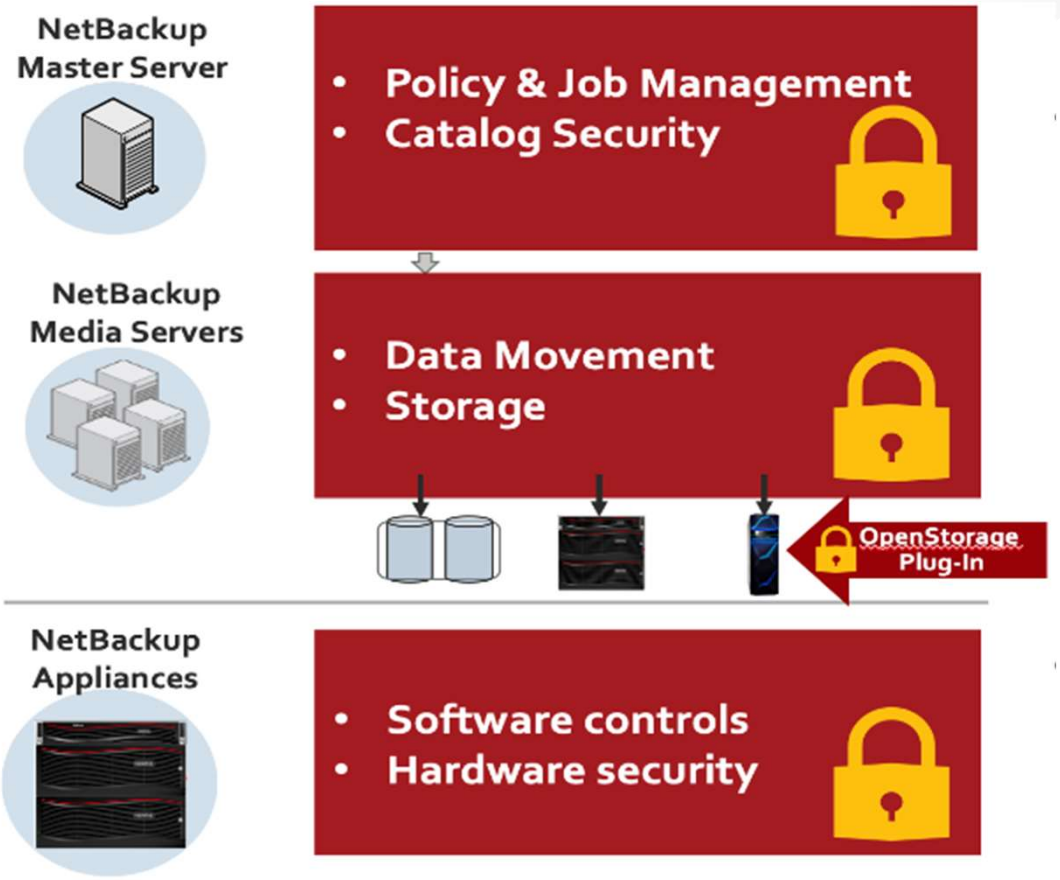
Immutability:
Data cannot be modified, destroyed, or removed by anyone

Consideration for the Data Protection Layer:

- Immutability delivered at every level
- Integrated & Awareness throughout
- Minimize infrastructure requirements

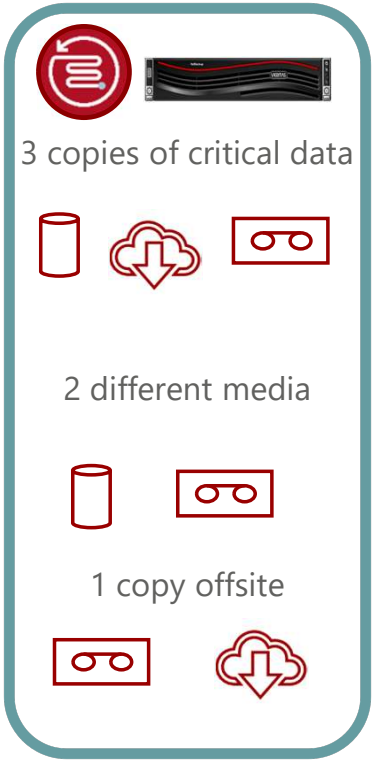
BENEFITS OF A VERITAS SOLUTION

- Protects backups from end to end
- Truly integrated out of the box solution
- Does not require doubling infrastructure
- Not a consulting science project

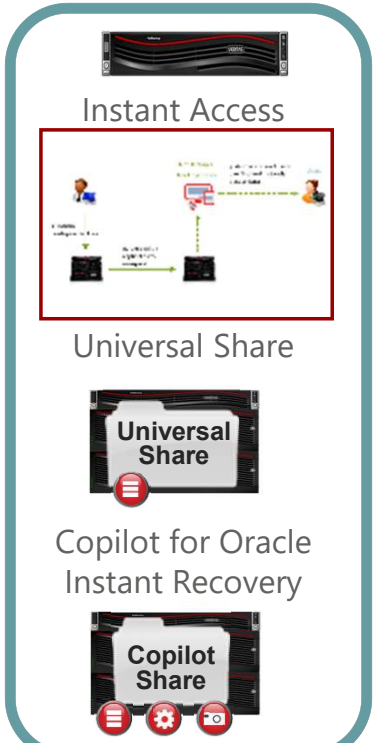


Ransomware Resiliency | Current state

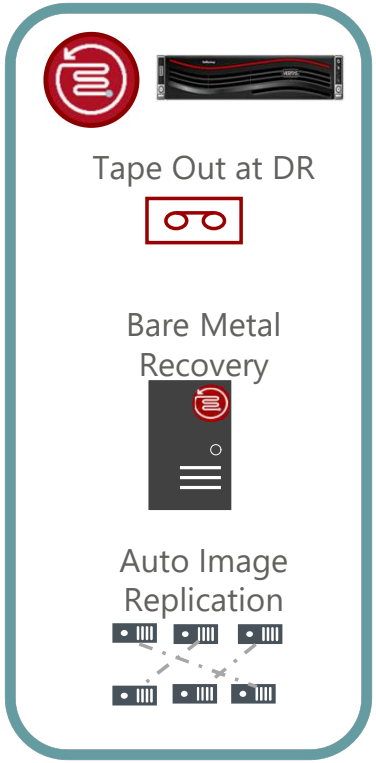
3-2-1 RULE



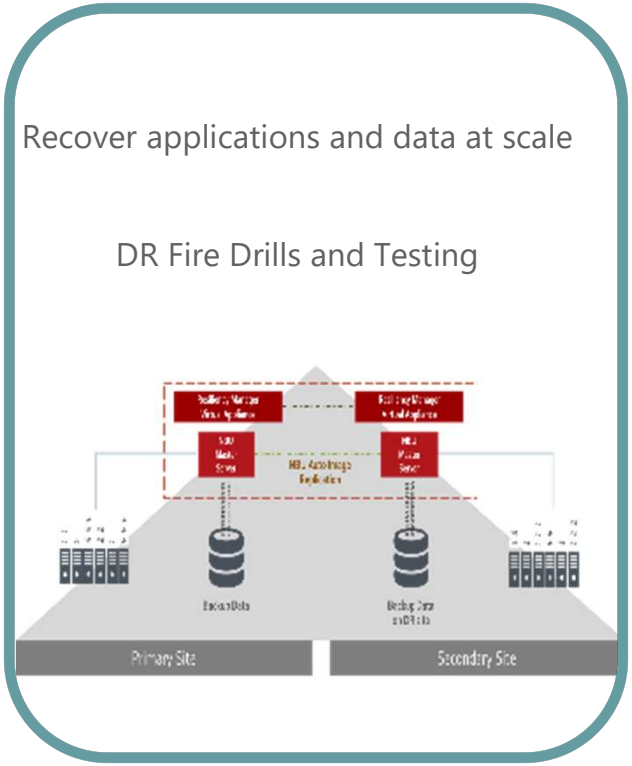
Faster Recovery



Single server Recovery



Recover at Scale



Reference – Ransomware Protection Whitepaper

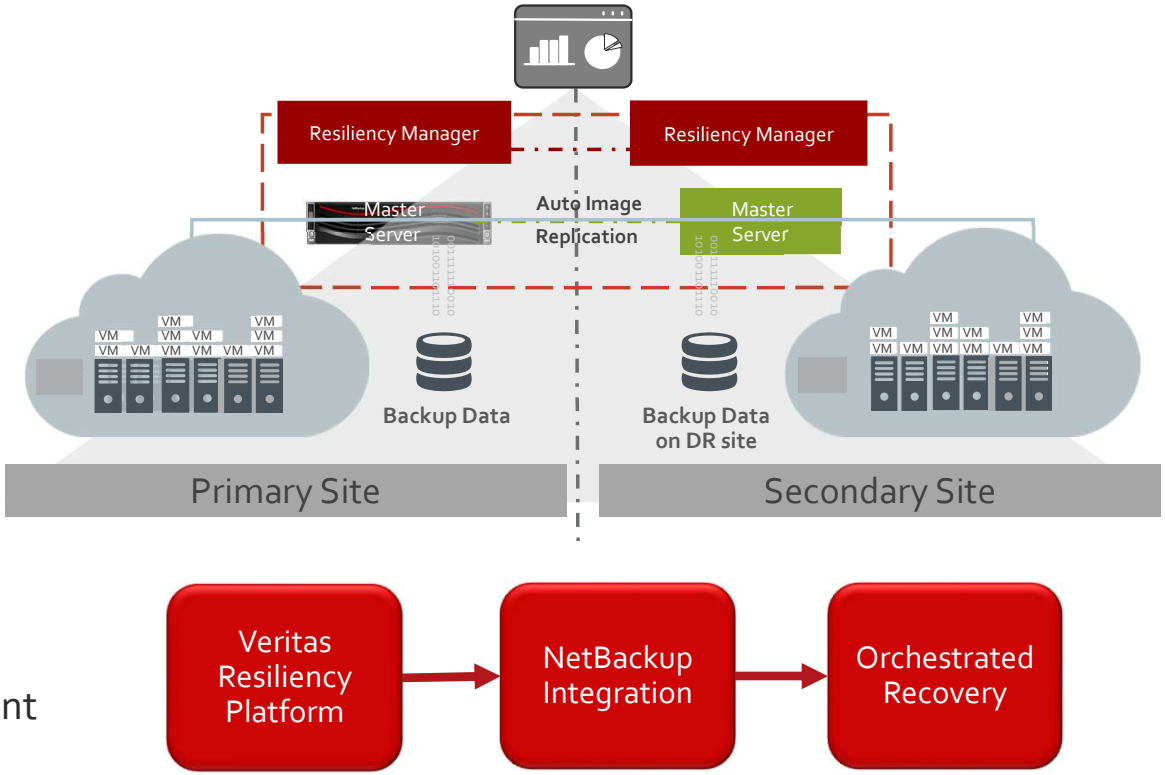
Recover At Scale

Challenge

- "How can I recover large number of virtual machines quickly in case of a mass ransomware attack?"
- "I struggle to migrate applications"
- "I need to test DR regularly to remain compliant "

Solution: NetBackup + Resiliency Platform

- ✓ Recover VM's in the cloud using NetBackup
- ✓ Automated bulk Failover & Failback, Rehearsal in cloud with NetBackup
- ✓ Meet different Service Level Objectives for different workloads



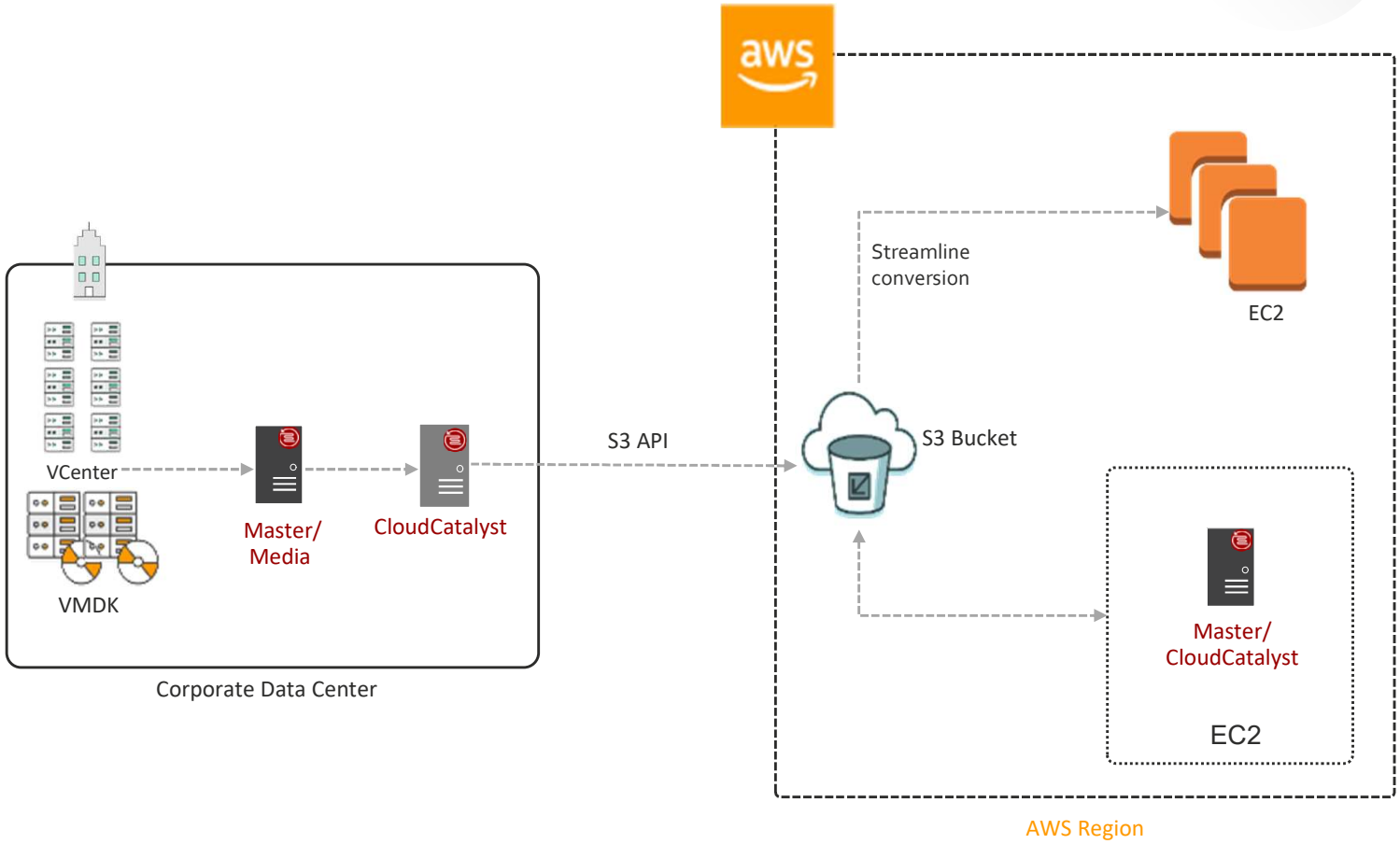
Server Recovery | Virtual server recovery in Cloud

Challenge

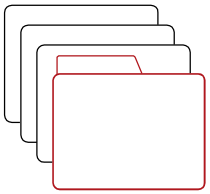
"How do I recover my server into AWS environment in case of a ransomware attack?"

Solution – **NetBackup Cloud Catalyst with AWS**

- Cloud resident Cloud Catalyst recovers on-premises backup data in the cloud
- For VMware backup, Cloud resident Cloud Catalyst can convert it into EC2 instance

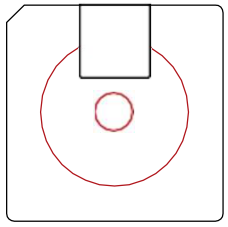


Ransomware Resiliency | Current state



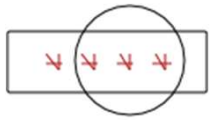
Multiple Copies

Store copies of backup images in different locations to reduce the attacker's ability to gain access.



Air Gap Backups

Create an offline backup copy of your data to keep it out of reach.



Restrict Backup Credentials

To minimize phishing, the most common method of gaining entry, limit—and continually monitor—backup credentials.

Shrink Your RPO

Running backups more often to shrink your Recovery Point Objective (RPO) can reduce potential data loss to hours or even minutes.

Q & A