

# 19 tips to prevent *ransomware* attacks for 2018

**Joe Marton**  
Veeam Software  
Senior Systems Engineer, SLED  
[joe.marton@veeam.com](mailto:joe.marton@veeam.com)

**Troy Dunavan**  
Veeam Software  
Senior Systems Engineer, SLED  
[troy.dunavan@veeam.com](mailto:troy.dunavan@veeam.com)

# Who has seen ransomware?

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions
- an automatic, self-installing diskette that anyone can apply in minutes

Important reference numbers: 1234567890

The price of 365 user applications is US\$189. The price of a lease of lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CO. for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-14, Panama ?, Panama.

Press ENTER to continue.

1989 — PC Cyborg (AIDS Trojan)

2012 — Reveton

2014 — Cryptowall

2017 — Ransomware as a Service

# Who has seen ransomware?



**Bristol Airport** ✓

@BristolAirport

Follow



We are currently experiencing technical problems with our flight information screens. Flights are unaffected and details of check-in desks, boarding gates, and arrival/departure times will be made over the public address system. Additional staff are on hand to assist passengers

7:29 PM - 13 Sep 2018

<https://www.infosecurity-magazine.com/news/bristol-airport-hit-by-ransomware>

# What are we talking about?



**Layered defense!**



**There is no one  
single magic bullet!**

# Many tips, many strategies

Select the ones that work best for your organization.

Think of these tips as a mindset rather than a specific architecture.



Bring on the tips!



A hand holding a black pen is signing a document. The document has a 'SIGNATURE' line and some blurred text. A green rounded rectangle with a white border contains the text 'Tip #1'.

## Tip #1

Use special credentials  
for backup storage/backup job

# Tip #1: Use different credentials for backup storage

## Worst practice

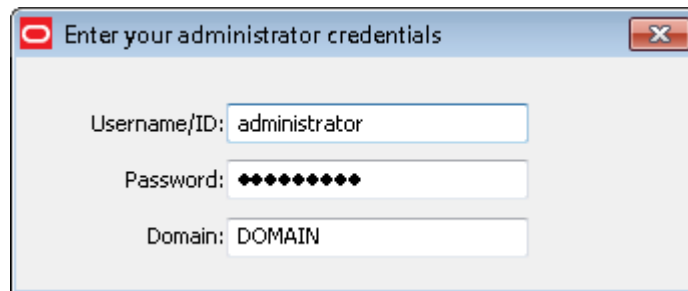
using DOMAIN\Administrator for everything

## Better practice

Use DOMAIN\service-account

## Best practice

Use LOCALHOST\service-account  
(don't join the repo to the domain)







## Tip #2

Give each backup admin  
individual access

# Tip #2: Give each backup admin individual access

Important to track who is doing what!

Mischievous backup admin

Compromised account

Accidents

More on visibility coming up later!



**Tip #3**

Utilize offline storage

# Tip #3: Utilize offline storage

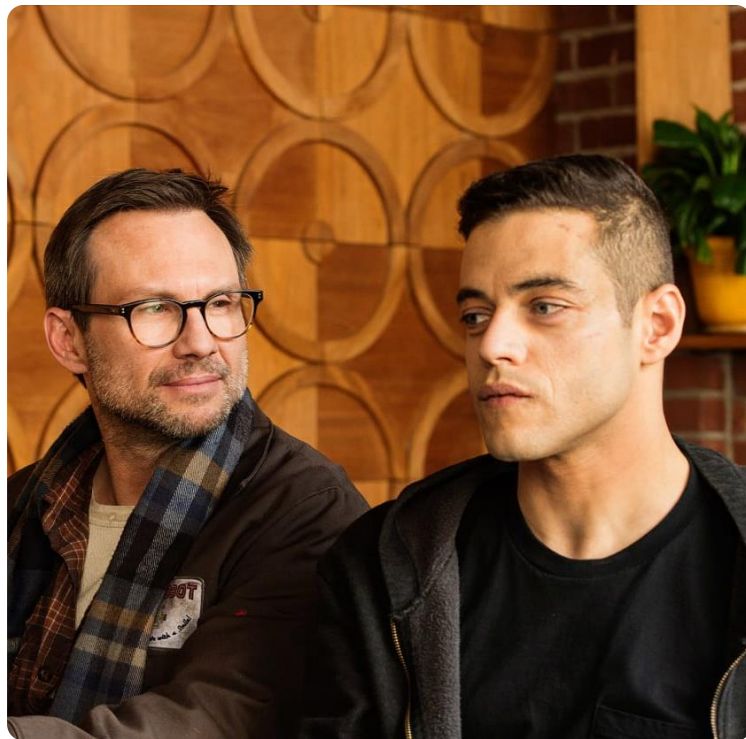
## Why offline?

Ransomware attacks connected shares

Take your media offline when possible

AIR GAP

Don't let Elliott ruin your day!



# Tip #3: Utilize offline storage

Media type	Characteristic
Tape	Completely offline when not being written to or read from
Replicated VMs	Powered off and, in most situations, can be a different authentication framework (ex: vSphere and Hyper-V hosts are on a different domain)
Primary storage snapshots	Can be used as recovery techniques and usually have a different authentication framework
Veeam® Cloud Connect backups	It's not connected directly to the backup infrastructure and uses a different authentication mechanism along with different API
Rotating hard drives (rotating media)	Offline when not being written to or read from (similar to tape)

# Tip #3a: Insider protection

Technology that permits Veeam Cloud Connect backups to keep backup data safe from a number of potentially dangerous situations:



**Insider attacks**



**Accidental deletion**



**Malicious deletion**



**Disgruntled employees**



**Ransomware**

# Insider protection use case

## Protection from catastrophic loss of backup data

### Veeam Availability Suite™



On-premises installation and backup data



### Cloud repository



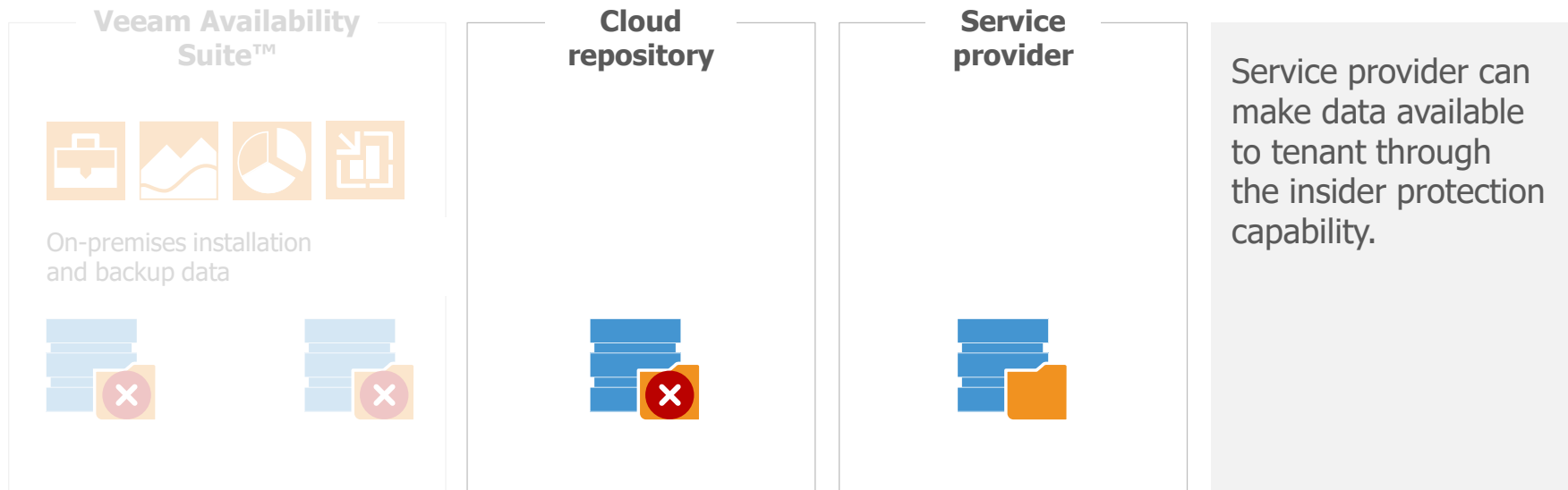
In the unfortunate situations where:

- All backups are deleted or removed from the end user's on-premises infrastructure
- All backups are deleted or removed from Veeam Cloud Connect Backup repositories

The Veeam Cloud Connect Backup service provider can make backup data available again outside of the customer's control.

# Insider protection use case

## Service provider can retrieve backup data







## Tip #4

Leverage different file systems / protocols for backup storage

# Tip #4: Leverage different file systems/protocols for backup storage

**Example:** Linux repositories, Deduplication appliances



Dell EMC



**Dell EMC DataDomain**  
Using DDBoost



Hewlett Packard  
Enterprise



**HPE StoreOnce**  
Using Catalyst



EXAGRID



**ExaGrid**  
Using native  
Veeam data mover



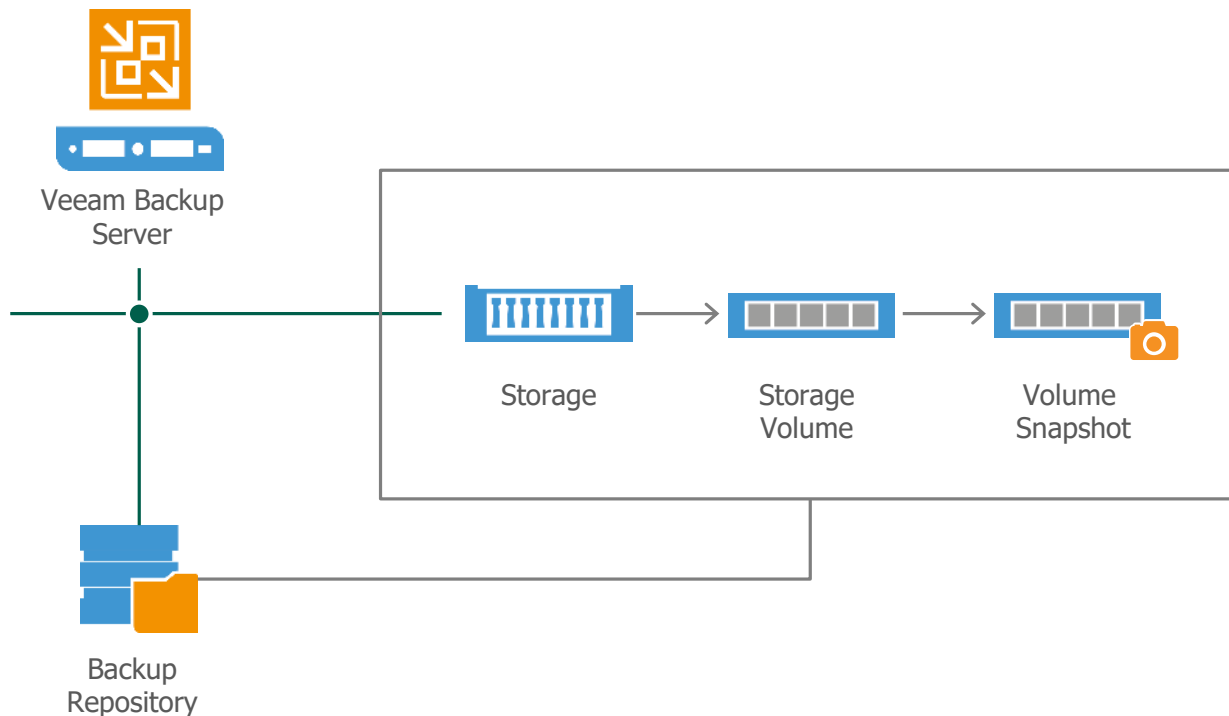
**Linux server  
with JBOD**



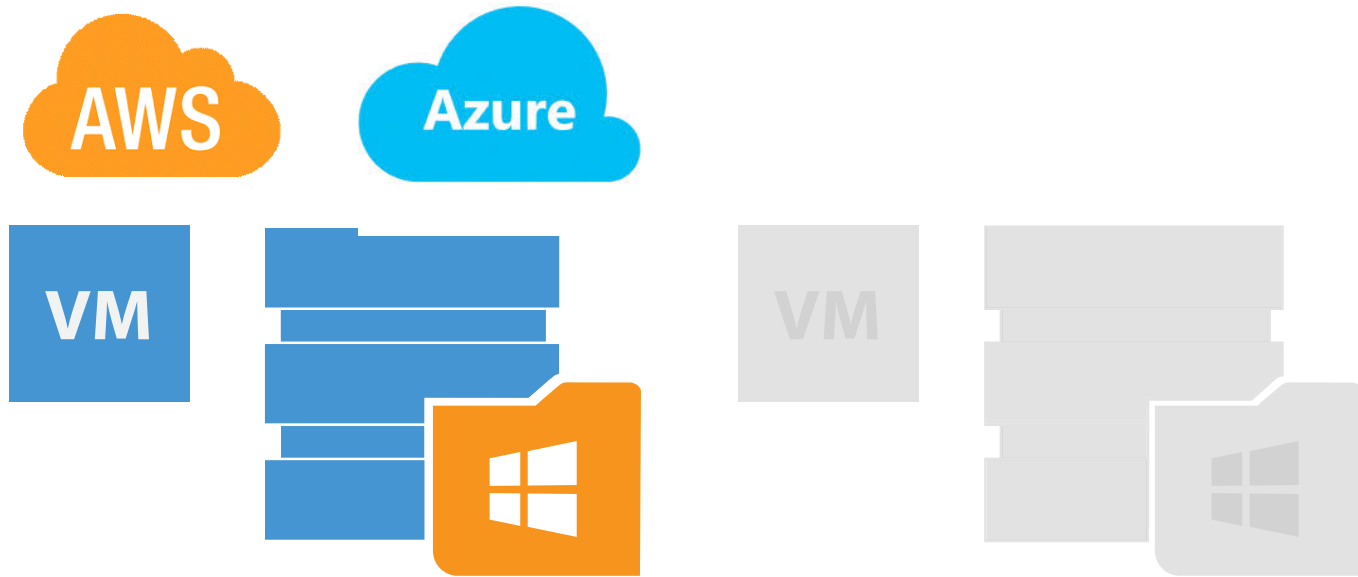
## Tip #5

Backup storage with native  
snapshot capabilities

# Tip #5: Take storage snapshots on backup storage if possible



# Tip #5a: Have a snapshot of a cloud instance in AWS or Azure





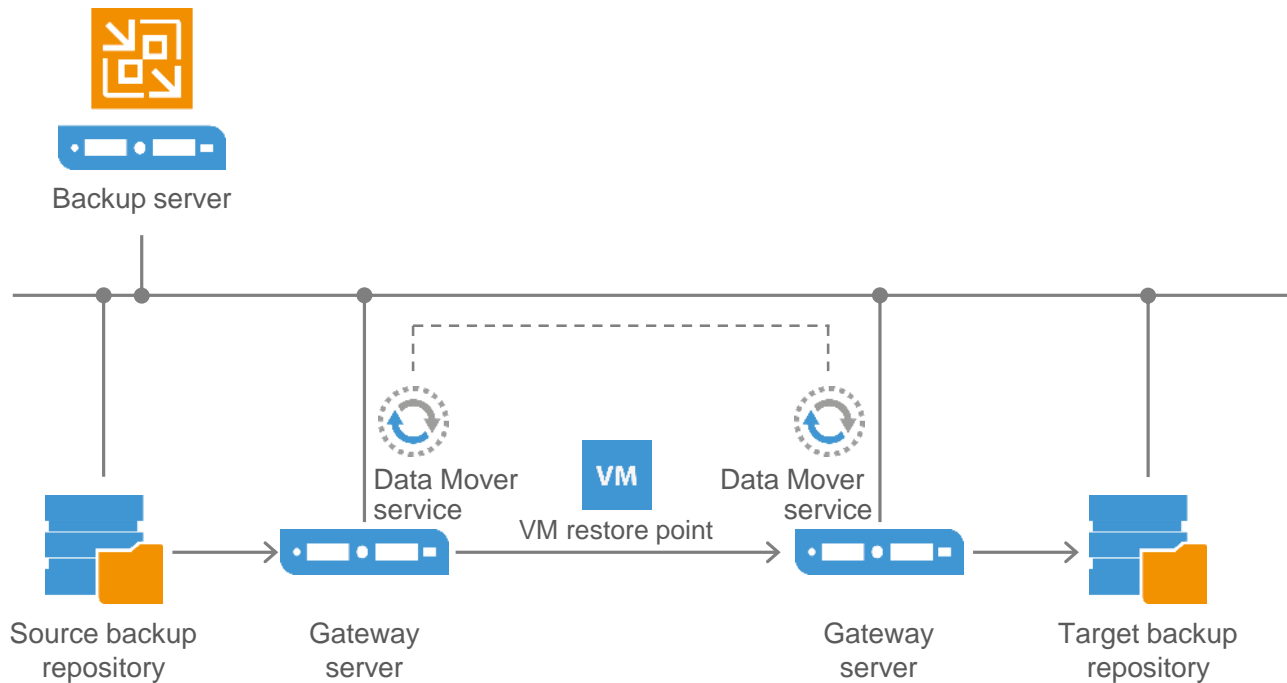
**Tip #6**

Let the Backup Copy Job  
do the work for you

# Tip #6: Let the Backup Copy Job do the work for you

The Backup Copy Job can be a valuable mechanism in a ransomware situation because there are different restore points in use with the Backup Copy Job.

# Tip #6: Let the Backup Copy Job do the work for you



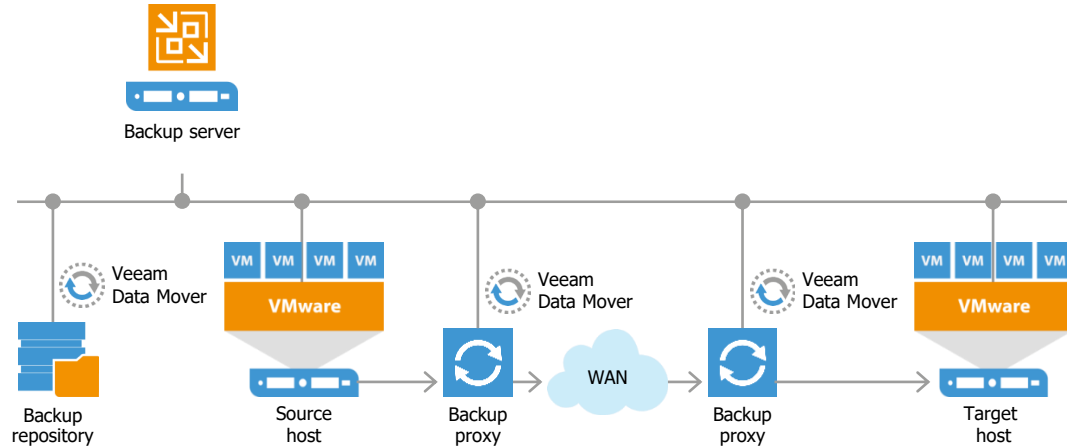




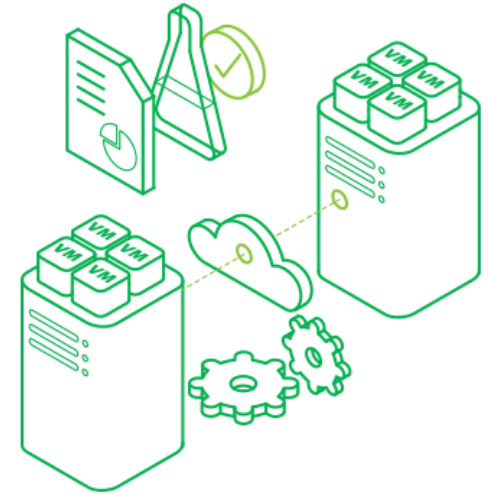
**Tip #7**

DR isn't just for natural  
disasters

# Tip #7: DR isn't just for natural disasters



Replication



Orchestration

A large warehouse filled with stacks of paper and documents. The stacks are arranged in rows, and the background shows a long aisle with windows and structural columns. The overall scene is dimly lit, emphasizing the vast quantity of paper.

## Tip #8

Document your  
recovery plan

# Tip #8: Document your recovery plan

## Report Overview

---

### Plan Test Execution Result

Execution Result	✓ Completed - Success
Total Duration	00:07:04
Plan Start State	Disabled
Plan End State	Passed

### Plan Test Schedule

Schedule Name	Manual run
Schedule Start Time	Manual run
Schedule Duration (RTO)	Manual run
Enforce RTO	No
Virtual Lab	VEEAM-VAO\VLAB1

### Plan Properties

Plan Name	Tier1-Exchange
Plan Description	Failover Plan for Exchange Servers
Plan Contact Name	John Doe
Plan Contact Email	<a href="mailto:administrator@vmce.lab">administrator@vmce.lab</a>
Plan Contact Tel:	

## Plan Test Execution

---

### Plan Overview

Status	✓ Completed - Success
Run/Scheduled By	VMCE\siteadmin
Recovery Point Objective (RPO)	Use the latest Restore Point
Recovery Time Objective (RTO)	4 Hours
Start Time	9:13:43 PM
Start State	Disabled
End Time	9:20:47 PM
End State	Passed
Total Duration	00:07:04

### Plan Summary

Result	Plan Groups	Start Time	Duration
✓ Success	<a href="#">Pre-Failover Steps</a>	9:13:43 PM	00:00:00
✓ Success	<a href="#">Mission Critical VMs - Exchange Servers</a>	9:13:43 PM	00:07:04
✓ Success	<a href="#">Post-Failover Steps</a>	9:20:47 PM	00:00:00

# Tip #8a: If you have a DR plan...

But do you have a plan of response for ransomware...

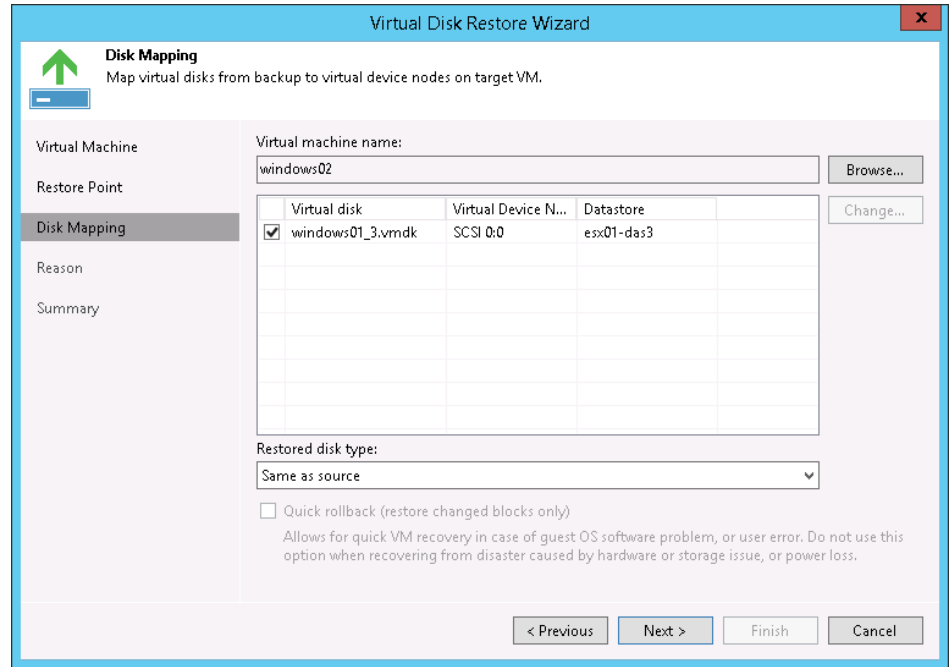
## Tip #9

Restore the minimum

# Tip #9: Restore the minimum

Of the 57 ways to restore, it makes sense to take the best restore option in a ransomware situation:

- Data volume
- Files only
- Application items, etc.





**Tip #10**

Veeam Backup *for*  
*Microsoft Office 365* data





# But it is SaaS....

Right, but do you know where the data is stored and how?

- Fixed local disk systems
- SMB3 shares
- Proxy / repository architecture is not the same as Veeam Backup & Replication™
  - Main thing to note is that workgroups are not supported
- Many of the requirements stem from having to "run" the supported Microsoft Exchange database type

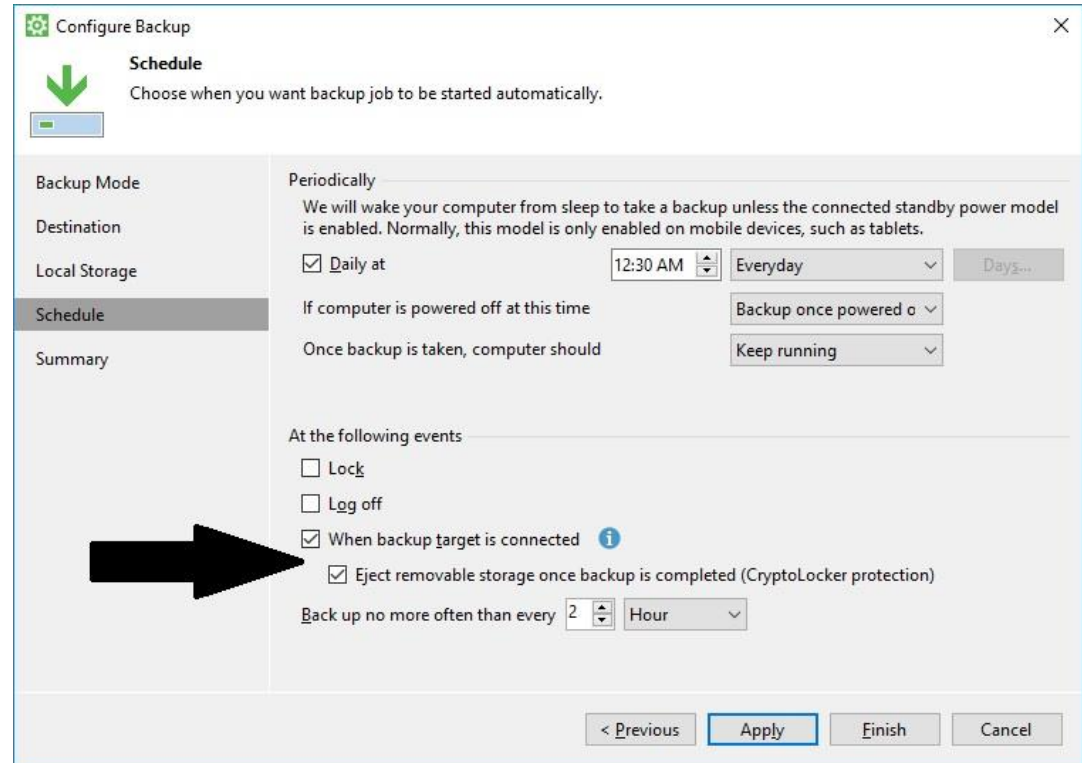


**Tip #11**

Agents

# Windows agents with USBs

Nice option to eject media once the backup is complete.



# For connected agents – Options!

For Windows and Linux agents, you can have backups sent to any of the following targets:

NAS resource

Fixed local disk

Veeam Backup & Replication repository

Veeam Cloud Connect repository

## Tip #12

vPower® & the cloud

# Leverage these as special beds

Data Labs and public cloud restores are a great way to restore to see if an issue would re-propagate if restored.

**Direct Restore**  
*to Microsoft Azure /  
AWS EC2*

**Data Lab**  
from replicas

**Data Lab**  
from backups

**Data Lab from**  
storage snapshots

A large-scale construction project is shown, with numerous workers in blue shirts and hats working on the wooden framework of a building's roof. The workers are positioned across the entire structure, which is under construction. The background is a clear, bright sky. The image is overlaid with a semi-transparent dark grey layer, and a white rounded rectangle is centered over the middle of the image, containing text.

## Tip #13

Veeam patch  
management



# Updates...

It's a lot of work, but it needs to happen. For the backup infrastructure, you could make the case that this is more important than anything. Consider aggressive patch management for:

Software for the backup infrastructure	Hardware
Veeam backup server	Server hardware, firmware
Veeam backup proxies, software repos	Hypervisor hardware
Windows Operating Systems	<b>Backup repositories</b>
Linux Operating Systems	

# Follow @VeeamKB

**veeam KB**

**Tweets** 579   **Following** 2,612   **Followers** 3,001   **Likes** 2   [Follow](#)

**Veeam Knowledge Base**  
@VeeamKB  
This is the account for the Veeam Knowledge Base (KB). Curated mostly by @BenMilligan  
Global  
veeam.com/kb  
Joined July 2013

**Tweets**   **Tweets & replies**

**Veeam Knowledge Base** @VeeamKB · Mar 23  
[Veeam Availability Console] Updating Veeam Availability Console Azure Appliance -

**VEEAM**  
Veeam Knowledge Base

**KB2461: Updating Veeam Availability Console Azure Appliance**  
The article describes how to update the Azure appliance running Veeam Availability Console.  
veeam.com

**New to Twitter?**  
Sign up now to get your own personalized timeline!  
[Sign up](#)

**You may also like** · Refresh

- Veeam User Group** @VeeamUG
- Veeam® Software** @veeam
- VeeamVanguard** @VeeamVanguard
- Anton Gostev** @qostev

A person is standing in the ocean, with only their head and one hand raised above the water. The hand is open, palm facing forward, in a gesture of seeking help. The sky is filled with heavy, grey clouds, and the water is dark and choppy. The entire scene is framed by a white rounded rectangle.

## Tip #14

Prepare for help

# Veeam Tech Support can help!



# What to expect

1

How are customers dealing with ransomware treated from an operations' perspective when they open a case?

2

What steps happen in the SWAT team to help customers get through the situation?

3

What advice would you give someone who is going through this type of situation?

The background features a dark blue grid pattern with a large, semi-transparent blue star in the center. A white rounded rectangle is overlaid on the grid, containing a green box at the top and white text below.

**Tip #15**

Security & network tools

# Resiliency, remediation... But

Prevention and protection should be a strategy as well.

Cisco has a number of solutions:

Cisco Umbrella Roaming, Cisco Advanced Malware Protection (AMP) for Endpoints, Cisco Advanced Malware Protection (AMP) for Email Security, Cisco TrustSec, Firewalls and more

Microsoft Windows Defender

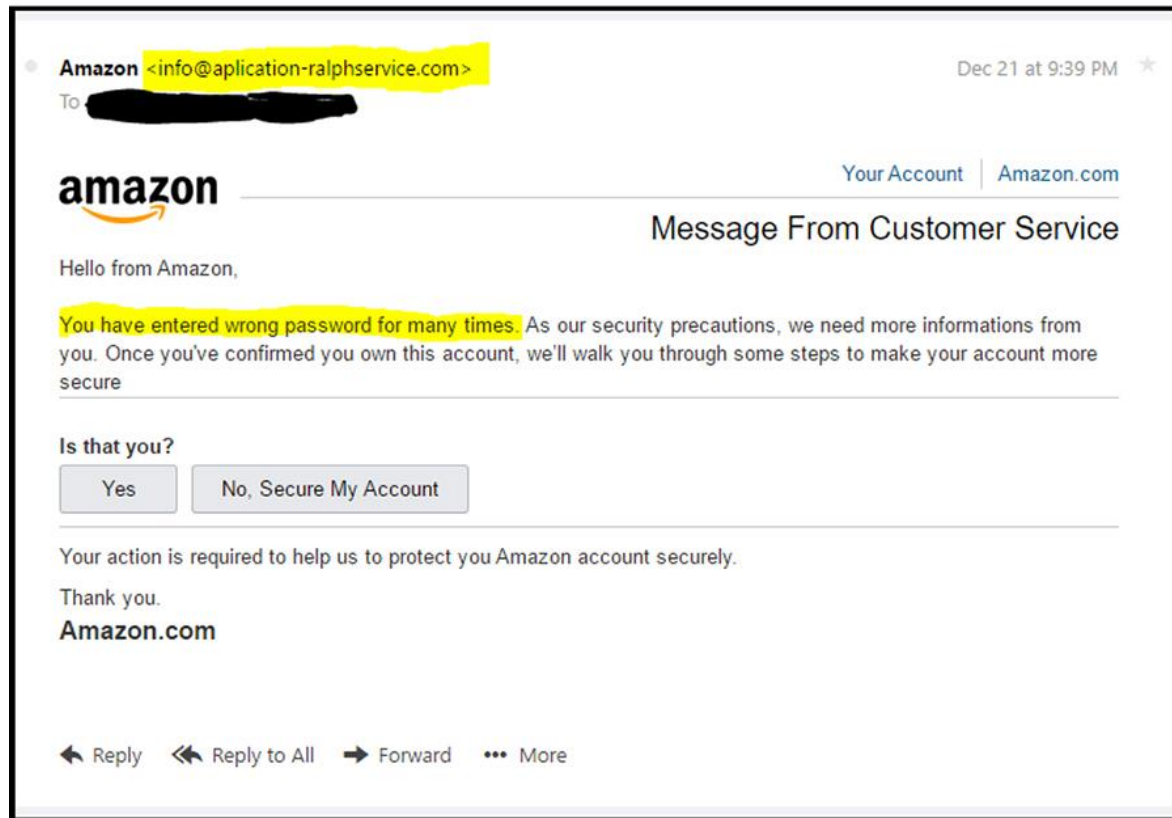


**Tip #16**

Users are your worst  
enemy...



# Tip #16: Users are your worst enemy



A row of security cameras mounted on a brick wall. The cameras are white and black, with black mounting brackets. The wall is made of light-colored bricks. The image is slightly blurred and has a dark overlay.

## Tip #17

Insider threats

# Tip #17: Insider threats



deloitte.wsj.com  
http://vee.am/cATUhw

**THE WALL STREET JOURNAL.** COVERAGE YOU TRUST. INSIGHT YOU NEED.  
\$12 FOR 12 WEEKS  
U.S. EDITION Wednesday, May 11, 2016 As of 5:07 AM EDT  
Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

**CIO Journal.**  
CIO Report | Consumerization | Big Data | Cloud | Talent & Management | Security

CONTENT FROM OUR SPONSOR Please note: The Wall Street Journal News Department was not involved in the creation of the content below.

PREVIOUSLY IN DELOITTE INSIGHTS **Deloitte.** NEXT IN DELOITTE INSIGHTS  
Business-led, Technology-enabled: Insight written and compiled by Deloitte

✉ 📄 in Share 477 🐦 Tweet A A

### Insider Threats: A Bigger Risk Than You Think

*The temptation among employees—especially those in IT—to steal sensitive company data looms surprisingly large, but employers can detect these impulses by tuning in to a wide range of risk indicators.*

The term “insider threats” often refers to individuals who use their knowledge of or access to an organization and its systems to deliberately perpetrate wrongdoing, whether fraud, sabotage, theft, or a violent act. These individuals may be current or former employees, contractors, or employees of third-party service providers.

Insider threats also include individuals who don’t intend to do harm, but whose choices and actions compromise the safety or security of their organizations. For example, new employees who are unaware of their companies’ cybersecurity practices may neglect to properly encrypt email containing sensitive data, leaving those messages vulnerable to certain kinds of



**Tip #18**

Have visibility  
into suspicious behavior















# Tip #18: Have visibility into suspicious behavior

Use monitoring software to automatically detect suspicious VM behavior

**Example:** Predefined alarm “Possible ransomware activity” in Veeam ONE™ — This alarm triggers if there are a lot of writes on disk and high CPU utilization.

- All Alarms
  - VMware
    - vCenter Server
    - Cluster
    - Host
    - Virtual Machine
    - Datastore
    - Any Object
    - vCloud Director vApp
    - vCloud Director Organization
    - vCloud Director Org VDC
    - vCloud Director Provider VDC
    - Resource Pool
  - Hyper-V
    - Host
    - Virtual Machine
    - Cluster
    - CSV
    - Local storage
    - Any Object
  - Backup & Replication
    - Enterprise Manager
    - Backup Server
    - Repository
    - Proxy
    - WAN Accelerator
    - Tape Server
    - Cloud Repository
    - Cloud Gateway
    - Internal

Filters: All  

Type	Name	Source	State	Assignment
	Incompatible version of integration services	Predefined	Enabled	Virtual Infrastructure
	Inconsistency within the failover cluster	Predefined	Enabled	Virtual Infrastructure
	Insufficient disk space	Predefined	Enabled	Virtual Infrastructure
	Invalid IP address detected	Predefined	Enabled	Virtual Infrastructure
	Invalid IP address for cluster resource	Predefined	Enabled	Virtual Infrastructure
	Invalid static MAC address	Predefined	Enabled	Virtual Infrastructure
	Invalid subnet mask detected	Predefined	Enabled	Virtual Infrastructure
	Local volume free space	Predefined	Enabled	Virtual Infrastructure
	Machine remoting system failure	Predefined	Enabled	Virtual Infrastructure
	Missing latest cluster configuration data	Predefined	Enabled	Virtual Infrastructure
	Network communication failure	Predefined	Enabled	Virtual Infrastructure
	No disk space to run this VM	Predefined	Enabled	Virtual Infrastructure
	Not enough memory to start a VM	Predefined	Enabled	Virtual Infrastructure
	Possible ransomware activity	Predefined	Enabled	Virtual Infrastructure

### Alarm details

#### Knowledge

Veeam ONE detected suspicious activity on this VM

#### Cause

This Virtual Machine had high write rate on datastore along with high CPU Usage which can be caused by ransomware activity

#### Resolution

Check if files on VM are encrypted by ransomware. Run up-to-date security software, prevent ransomware propagation, ask for qualified assistance if needed. Backup in a case the files cannot be repaired. If VM was not affected by ransomware, raise the alarm thresholds.

A photograph of a Space Shuttle launch. The shuttle is on the right, ascending vertically with a large plume of white smoke and orange fire at its base. To the left of the shuttle is a tall, white, lattice-structured tower labeled "SPAD". The background is a clear blue sky with some white clouds. The foreground shows the launch complex infrastructure, including various pipes and structures.

## Tip #19

One final thing...

# Tip #19: Master the 3-2-1-0 Rule

Recover from any scenario, **especially ransomware attacks!**

# 3

Different copies  
of data



# 2

Different media



# 1

of which is off-site\*



# 0

No errors after  
backup recoverability  
verification



\* Don't forget your offline copy!



# Thank you

## VEEAM

**Veeam US Headquarters**

20 William Street  
Wellesley, MA 02481

678.353.2140 (Main office)

800.774.5124 (Support)

800.913.1940 (Support)

Join us on:



[www.veeam.com](http://www.veeam.com)