COMMVAULT

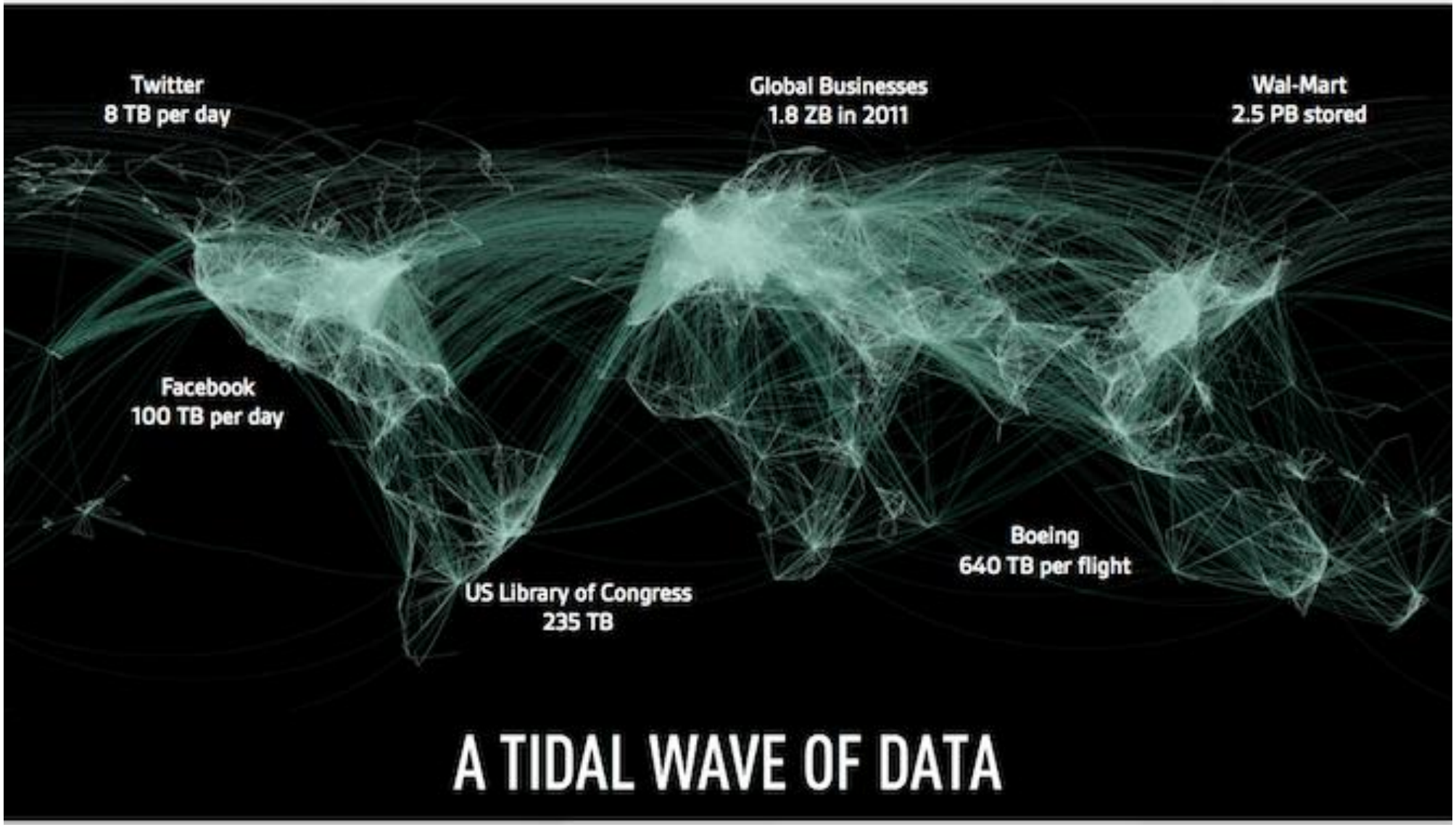
Planning for Data Security
Why Backup and Recovery Should Be On Your List!

David Langley
Sr. Director Systems Engineering – West
dlangley@commvault.com

September 29, 2016

PROTECT | ACCESS | COMPLY | SHARE

What's the most interesting number in the image?



Evolving Customer Challenges

1

High Cost of Proprietary based infrastructure

2

New recovery mandates

Always on Always Available

3

Traditional backup increasingly unable to meet today's demands

Massive data volume, meeting SLA's

4

Get more value from your data investments

Accessing data across multiple data silos with moving it

5

Access & collaboration

Limited end user access to production / historical data

6

Regulatory and Compliance Risk

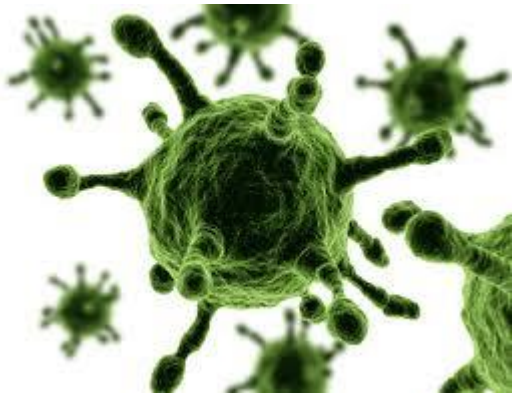
Properly manage data from inception for compliance and regulatory needs

Turning an Insurance Policy into Proactive Threat Reduction – Three Use Cases

1. Reduce the impact of Ransomware

Ransomware

Definition: A type of malicious software designed to block access to a computer system until a sum of money is paid



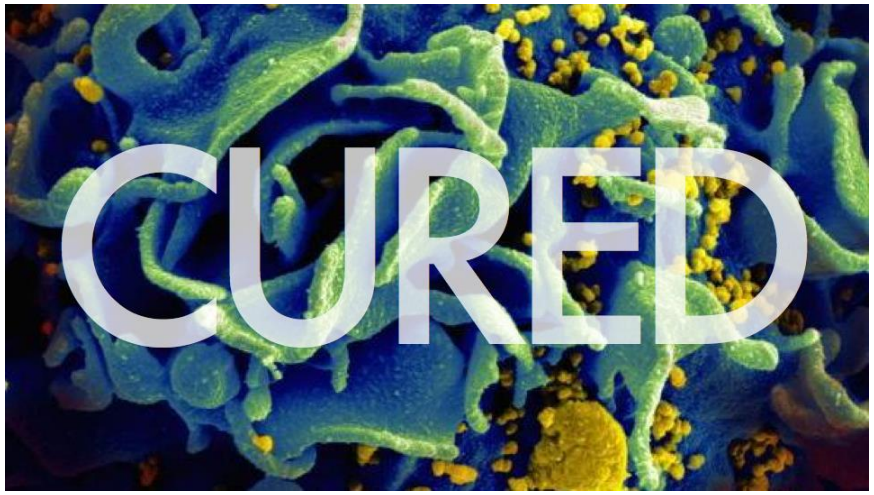
- Usually encrypts files.
- Hops from one disk subsystem to another easily.
- Rapidly evolving
  - Now attacking backup systems specifically
- Impacts the credibility of the affected organization
- In the first three months of 2016, the known amount paid by victims was $209,000,000. Conservative estimates put the total 2016 amount over $1,000,000,000.*

*Herjavec Group study

Ransomware – The defense and the response

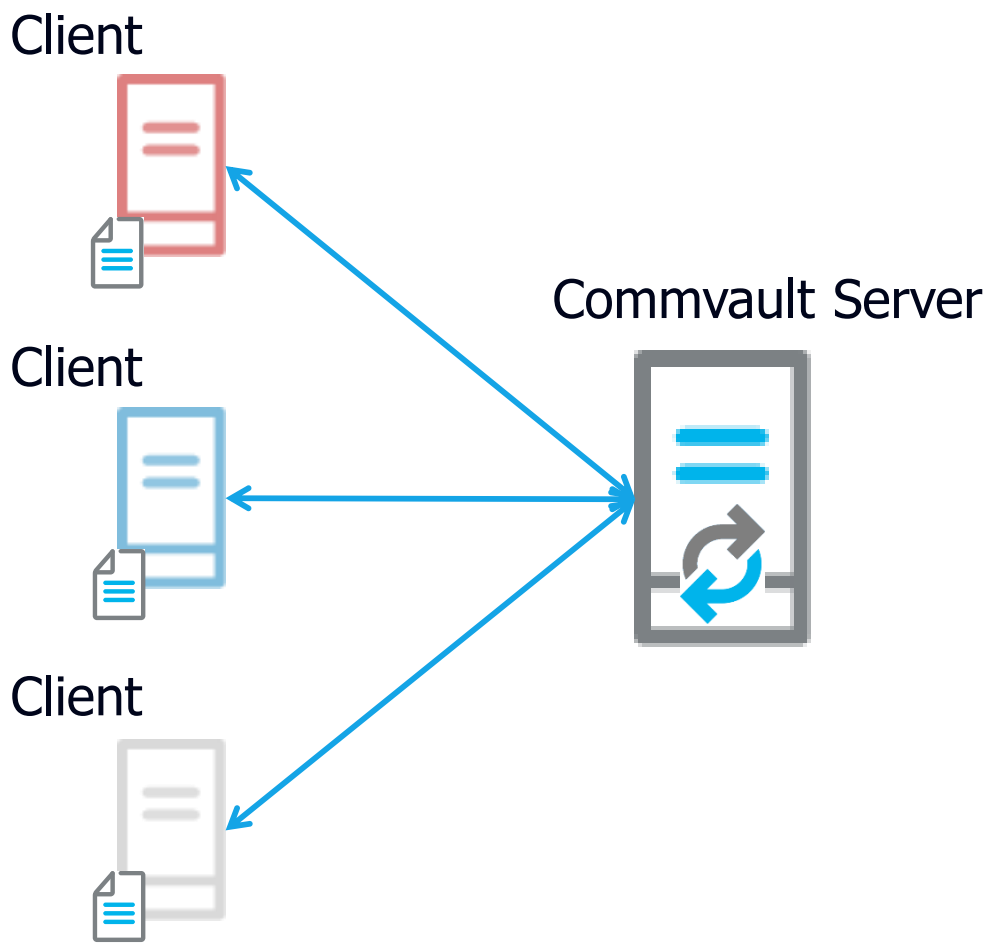
- Early detection
- Automated alerting

- A solid protection strategy on alternate storage like cloud or disk.
- Rapid recovery orchestration



What if Your Data Protection Was Ransomware Aware?

- Small Trojan files hidden install on each backup client
  - File extensions mimic likely Ransomware targets
  - Each time backup runs, BU SW checks to make sure Trojan files have not been modified
  - Alerts you if backup SW detects if file is modified or encrypted



7

Turning an Insurance Policy into Proactive Threat Reduction – Three Use Cases

1. Reduce the impact of Ransomware
2. Securing the edge

The laptop that can cost you your job…

1. 66% of an entity's intellectual property is on the edge, not in the datacenter.[1]
2. The typical lost laptop costs a typical business over $49,000 and 7% of laptops are stolen in their lifetime.[2]
3. When a disgruntled employee leaves, they typically take more than just a box of pens. Getting the laptop back does not mean the data came back with it.
4. If we don't protect the asset, the end users often are with "shadow IT".

1. Gartner study
2. Ponemon "Billion Dollar Lost Laptop Study"

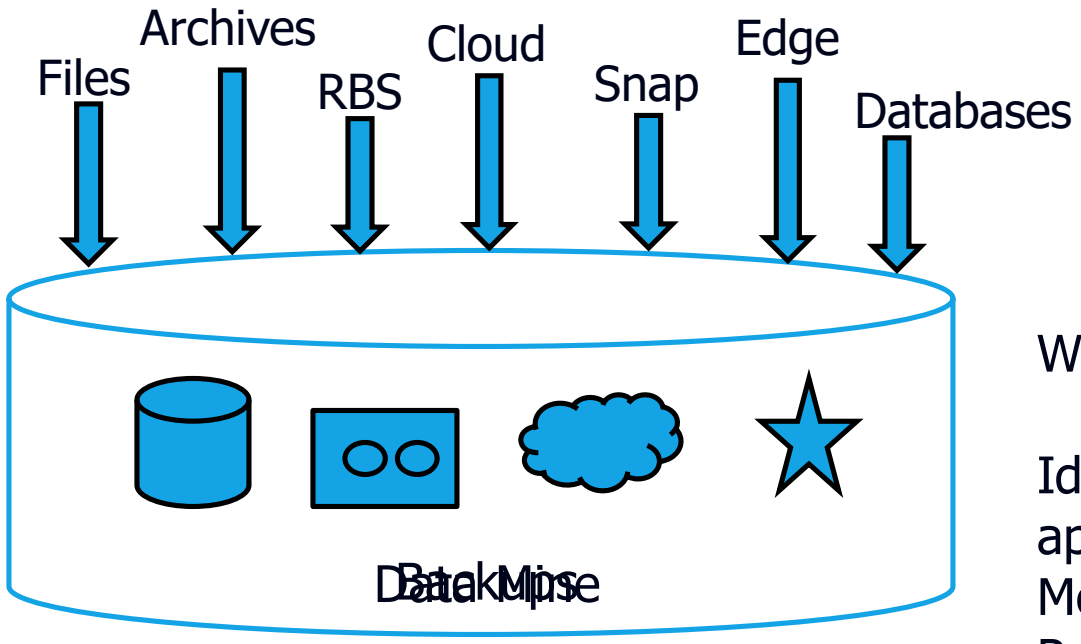
Modern Data Protection to the Rescue

- Provides recoverably
- Provides insight into the past
- Gives users a sense of control
- Centralizes remote data for other purposes
  - Sharing
  - Data Mining
  - Populating new environments

Turning an Insurance Policy into Proactive Threat Reduction – Three Use Cases

1. Reduce the impact of Ransomware
2. Securing the edge
3. Getting to know your data

Reimagine Data Protection into Data Gathering



What to Learn?

Where is my data?
What is it?
Who owns it?
Should I keep it?
Is it in the right place?

What to do about it?

Identify critical IP and Protect appropriately.
Move data to the "right place".
Remove useless / risky data.
Identify weak data classification.

Modern Data Protection

- Provides fast and easy recovery or access to lost or compromised data
- Provides improved understanding into what you have and what you may have lost
- Provides insight into what is happening in your environment

Thank you


COMMVAULT®