CATALOGIC

Protect & Recover your NetApp Filers from Ransomware Attacks

Webinar, 7/21/2021

Aaron McCune
Solutions Architect
amccune@catalogicsoftware.com

@AaronMcCune20

William Bush
Field CTO Europe
wbush@catalogicsoftware.com

@VirtualVizion

About us

Leading Provider of Data Protection and Data Management Solutions

Quick Facts

World class support organization: 95% Customer satisfaction

20+ year history protecting data for the world’s largest organizations

Transparent pricing and great value

End-to-end support 24/7 commitment

1000+ global customers

Associated Bank

Disney+

Department of Labor · United States of America

Independence Blue Cross

FOOD LION

CONAIR

U.S.ARMY

Credit Acceptance *We change lives!*

MCKESSON

CATALOGIC

Smart Data Protection and Security Solutions

Smart Choice in Data Protection

DPX

An efficient and flexible all-purpose data protection solution supporting disk, tape, and cloud

vprotect

Data protection for open virtualization platforms such as RHV/oVirt, Nutanix Acropolis, Citrix XenServer, Oracle VM and KVM, among others

Smart Home for Cloud Data Protection

cloudcasa

Data protection as a service for cloud native workloads: Kubernetes and Cloud Databases

Zero Infrastructure at Cloud Scale

NetApp Tools

CryptoSpike

Ransomware detection and recovery

RestoreManager

File index, search, and restore

DataAnalyzer

File data analysis

NetApp: Ransomware Detection and Protection

CryptoSpike

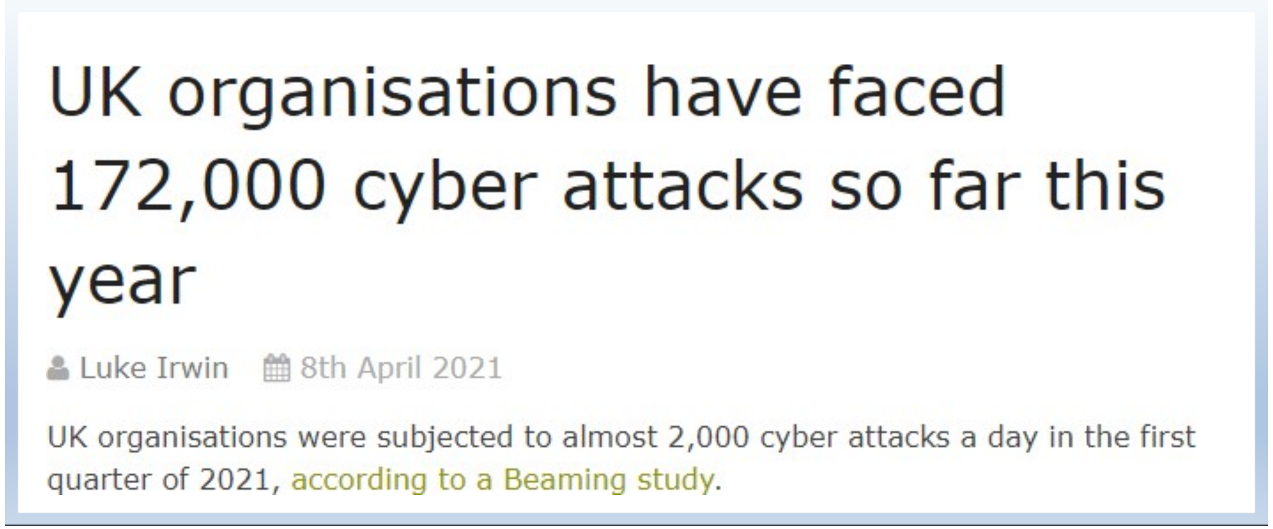
01 Real-time detection of ransomware on NetApp file systems

02 Stops spread of infection with automatic user blocking

03 One-button restore of affected files from NetApp snapshots

04 Access transparency: file access auditing (who touched what files)

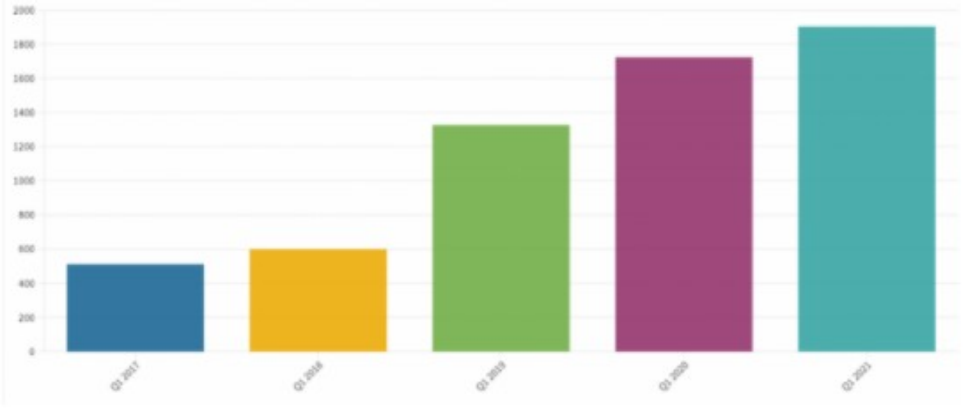
NetApp: Ransomware Detection and Protection



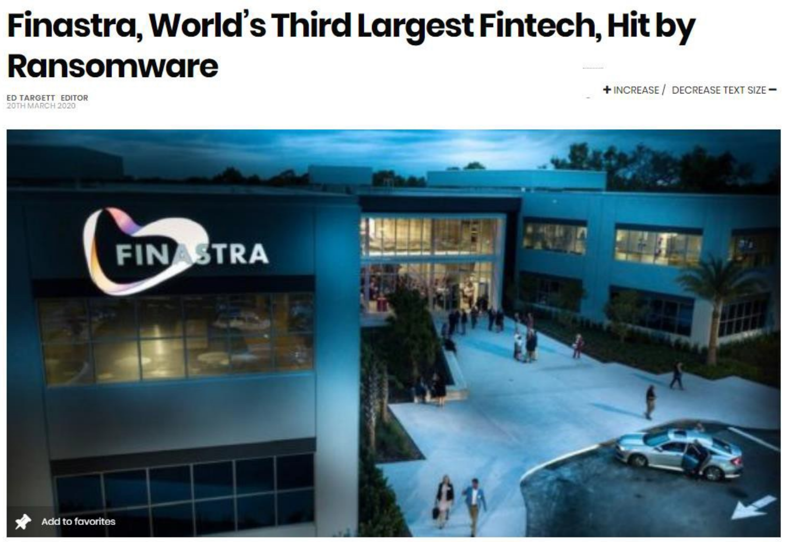
UK organisations have faced 172,000 cyber attacks so far this year

Luke Irwin 8th April 2021

UK organisations were subjected to almost 2,000 cyber attacks a day in the first quarter of 2021, according to a Beaming study.



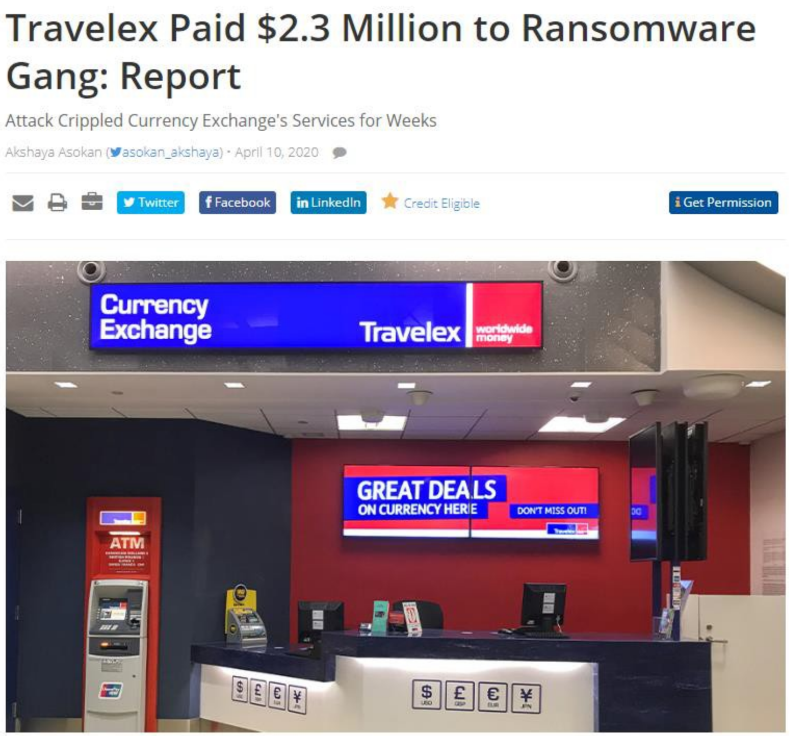
The average daily number of cyber attacks has skyrocketed in the past three years.



Finastra, World's Third Largest Fintech, Hit by Ransomware

ED TARGETT EDITOR
20TH MARCH 2020

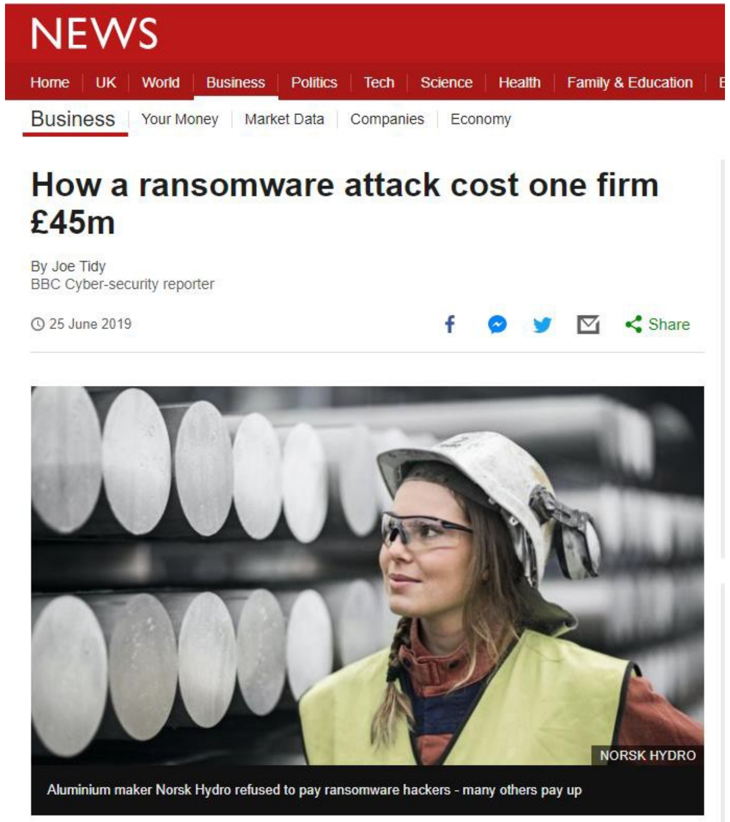
+ INCREASE / DECREASE TEXT SIZE −



Travelex Paid $2.3 Million to Ransomware Gang: Report

Attack Crippled Currency Exchange's Services for Weeks

Akshaya Asokan (asokan_akshaya) • April 10, 2020



How a ransomware attack cost one firm £45m

By Joe Tidy
BBC Cyber-security reporter

25 June 2019

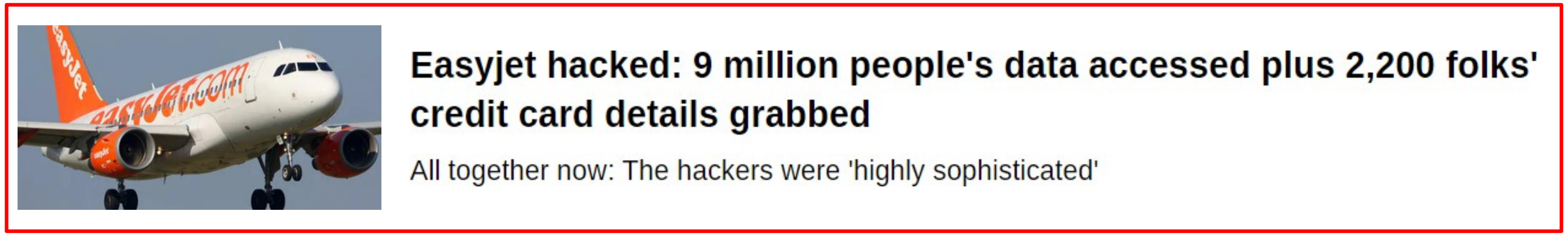
Aluminium maker Norsk Hydro refused to pay ransomware hackers - many others pay up

Ransomware – A growing 'industry'

*Experts predict there will be a ransomware attack every 11 seconds in 2021

*https://safeatlast.co/blog/ransomware-statistics/#gref

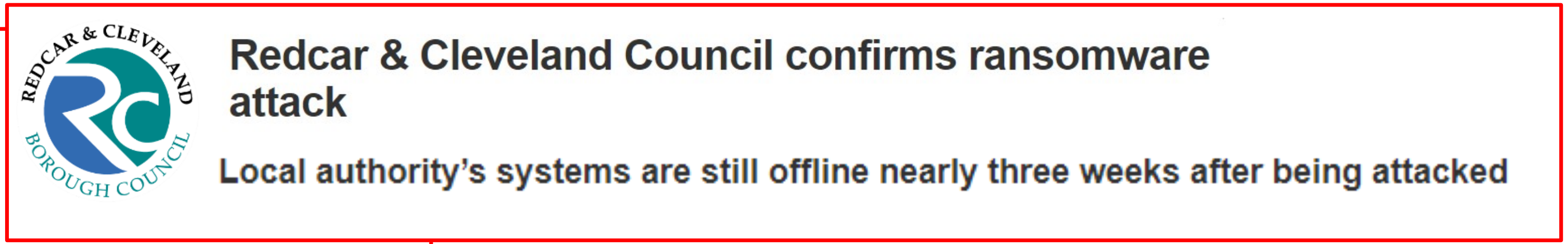
Do you think these companies didn’t have Endpoint/Edge Protection?



Easyjet hacked: 9 million people's data accessed plus 2,200 folks' credit card details grabbed

All together now: The hackers were 'highly sophisticated'

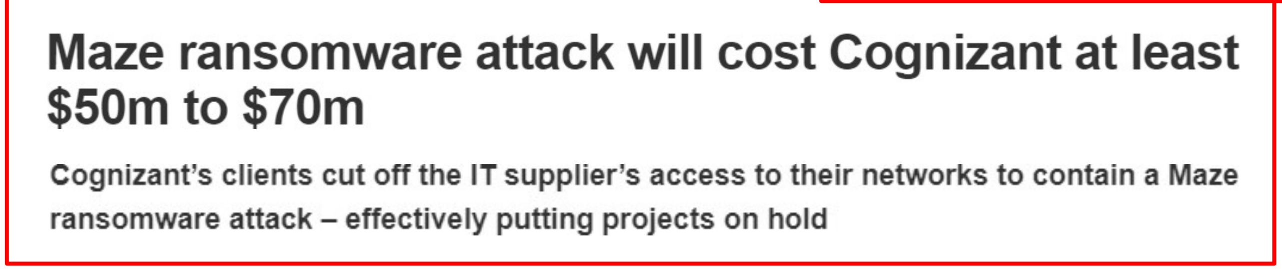
If you think safety is expensive… try an accident!



Redcar & Cleveland Council confirms ransomware attack

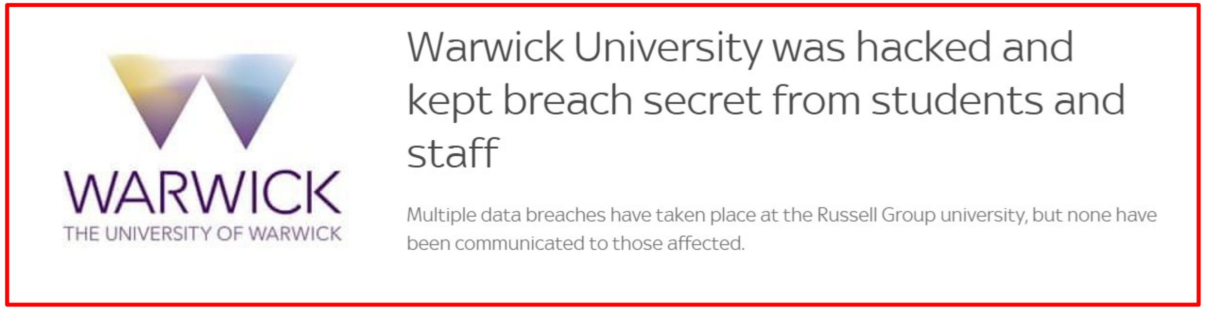
Local authority’s systems are still offline nearly three weeks after being attacked

Cognizant



Maze ransomware attack will cost Cognizant at least $50m to $70m

Cognizant’s clients cut off the IT supplier’s access to their networks to contain a Maze ransomware attack – effectively putting projects on hold



WARWICK
THE UNIVERSITY OF WARWICK

Warwick University was hacked and kept breach secret from students and staff

Multiple data breaches have taken place at the Russell Group university, but none have been communicated to those affected.

Protect your company’s data. Don’t be another news headline.

User & Data Access Transparency

- CryptoSpike monitors and logs all user file access (reads, writes, opens, etc.) for an additional level of security auditing
- Identify who was infected, who accessed which files, made changes to files, deleted files, etc

How CryptoSpike Blocks Ransomware

Blocklist

- Blocks known ransomware signatures and file types.
- Updated automatically.
- Filters can also be added manually.

Passlist

- Blocks all files EXCEPT allowed file list.
- Good security but limits types of files.
- Effective when applied at a granular level (e.g. an accounting folder allows only Excel files).

Learner Module

- Monitors user behavior on file system to detect day-one threats.
- Detects unusual behavior (e.g. too many files changed in a period of time) and cuts off user access.

User Blocking and File Recovery

User blocking

- Ransomware is correlated to the infected user
- User is blocked via calls to NetApp FPolicy server
  (blocked = set to read-only file access)

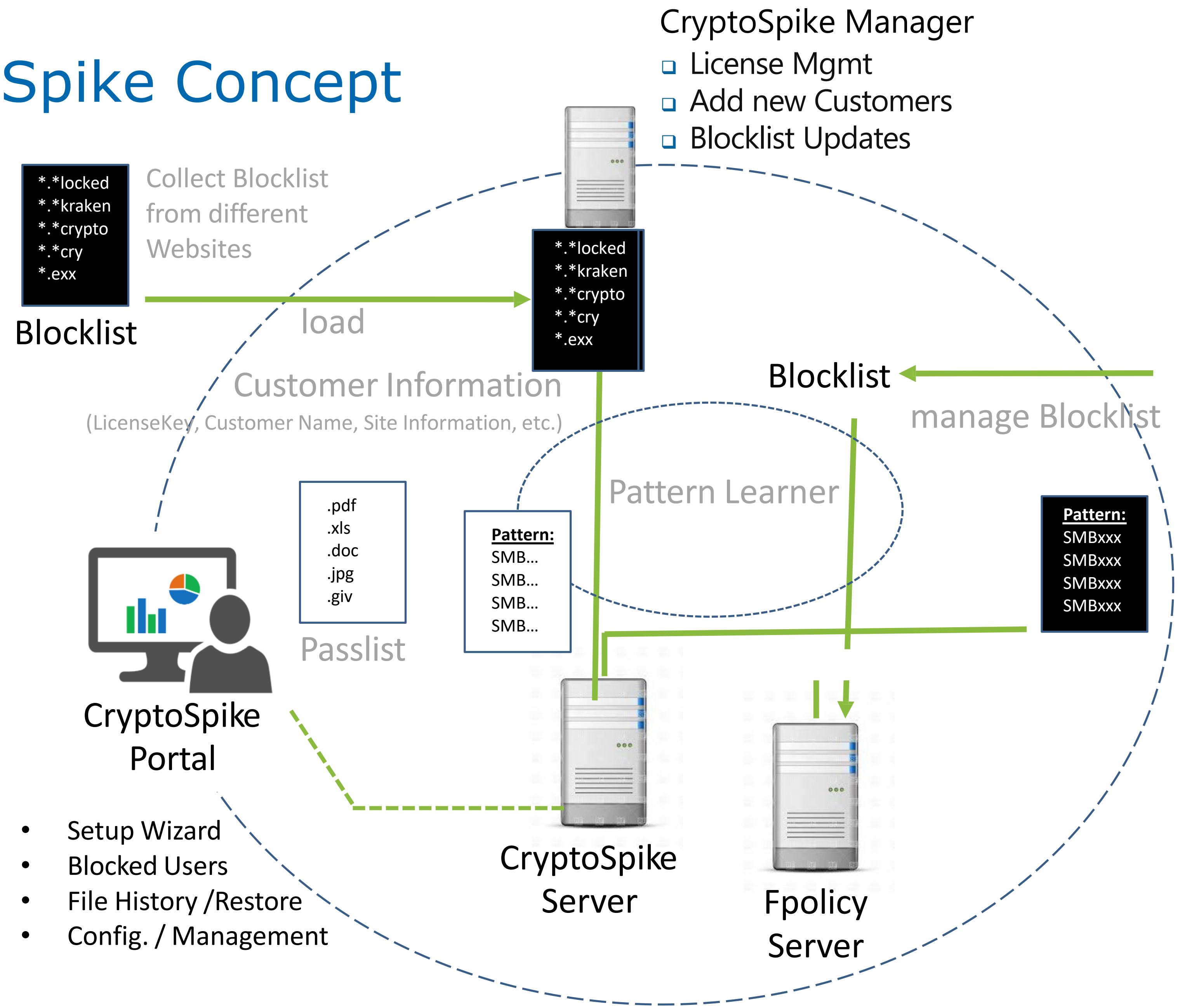
Targeted File Recovery

- CryptoSpike identifies the infected files
- Push-button recovery of only the infected files using NetApp snapshots
- No need to roll-back an entire volume or folder

User Remediation

- The infected user is identified
- This allows IT security team to pull the infected device from the network and apply remediation measures

CryptoSpike Concept



CryptoSpike Manager

- ❑ License Mgmt
- ❑ Add new Customers
- ❑ Blocklist Updates

*.*locked
*.*kraken
*.*crypto
*.*cry
*.exx

Blocklist

Collect Blocklist from different Websites

load

*.*locked
*.*kraken
*.*crypto
*.*cry
*.exx

Customer Information

(LicenseKey, Customer Name, Site Information, etc.)

Blocklist

manage Blocklist

Pattern Learner

.pdf
.xls
.doc
.jpg
.giv

Passlist

Pattern:
SMB…
SMB…
SMB…
SMB…

Pattern:
SMBxxx
SMBxxx
SMBxxx
SMBxxx

CryptoSpike Portal

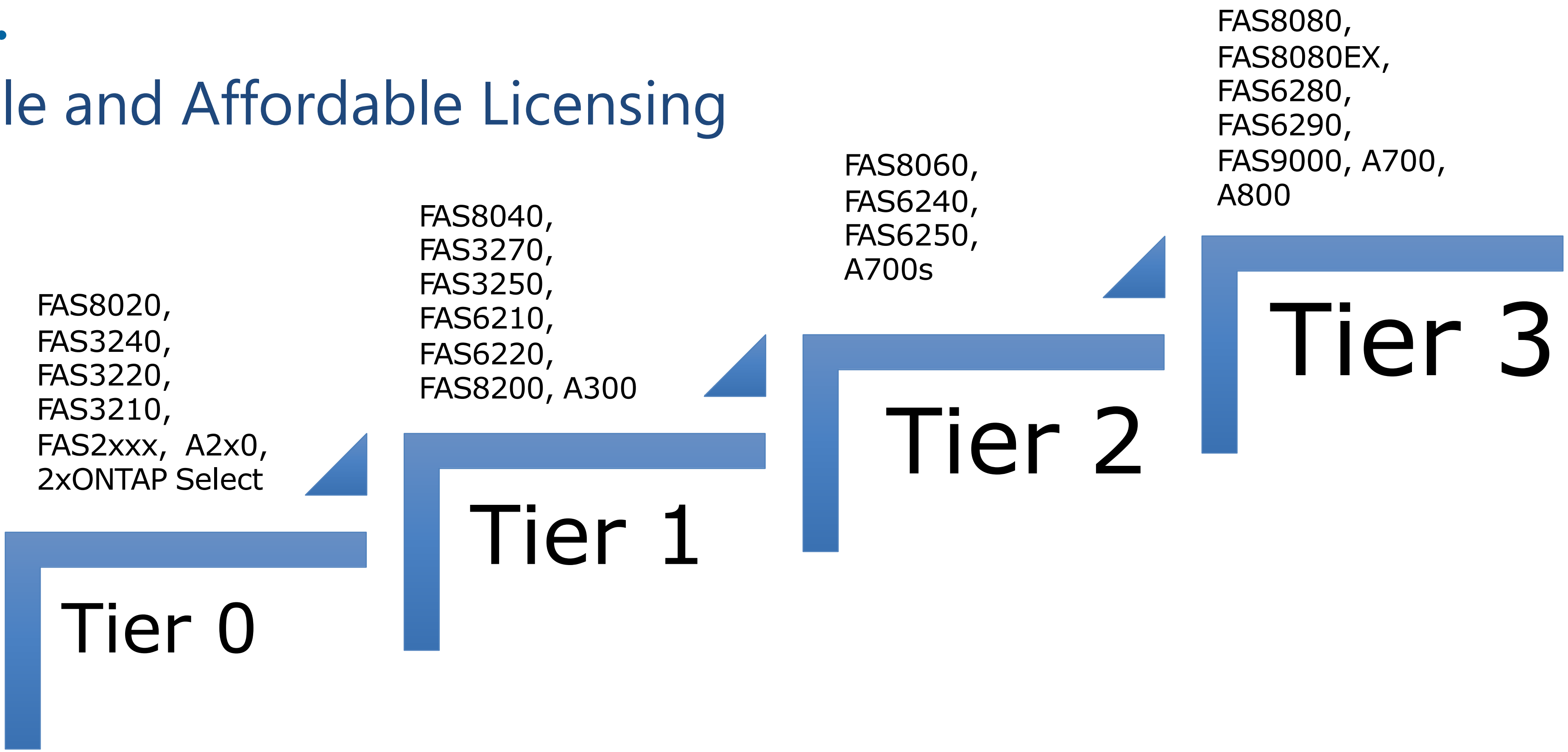
- Setup Wizard
- Blocked Users
- File History /Restore
- Config. / Management

CryptoSpike Server

Fpolicy Server

DEMO
CryptoSpike

Simple and Affordable Licensing



FAS8020, FAS3240, FAS3220, FAS3210, FAS2xxx, A2x0, 2xONTAP Select

Tier 0

FAS8040, FAS3270, FAS3250, FAS6210, FAS6220, FAS8200, A300

Tier 1

FAS8060, FAS6240, FAS6250, A700s

Tier 2

FAS8080, FAS8080EX, FAS6280, FAS6290, FAS9000, A700, A800

Tier 3

- ✓ Licensing is per-controller node (e.g. dual node HA pair is two licenses)
- ✓ Licensing is tiered by NetApp system size (see tiers at left)
- ✓ No additional charge for number of files, amount of disk capacity, etc.
- ✓ License is subscription-based, priced per month, with minimum one year purchase
- ✓ All nodes in a cluster must be licensed, even if they are not using NAS protocols

Your Last Line of Defense Against Ransomware – Backup and Recovery

Your backup data is secure

- All DPX block and agentless backups are stored as immutable snapshots
- Air-gap security in the form of backup/archive to tape or cloud
- Supports the 3-2-1 rule for backup retention - backups onsite, offsite (via replication), on tape, or in the cloud

DPX

Back up your critical systems more frequently

- Creates incremental app aware backups for physical and virtual environments
- Multiple recovery points so you can spin the clock back to just before the infection happened
- Verification to ensure data can be successfully recovered (block level only)

Fast recovery back to operational status

- Instant recovery of virtual machines, servers, files, or folders
- Recovery from off-site backup in case your on-premise data is inaccessible
- Reporting to show total amount of data protected by day; early warning of significant changes

Next Steps

Get in touch with us! We can then take the following steps:

- Provide pricing
  - All we require for CryptoSpike are your filer models
  - All we required for DPX is the amount of source data (TB) you wish to protect
- Complete a free assessment of your current data protection strategy
- Free PoC trial licence for CryptoSpike and DPX
  - Simple set up
- Purchase CryptoSpike and enhance your data security and visibility across your NetApp estate
- Purchase DPX and enhance your data protection and data recovery capabilities to ensure you can recover under any circumstance including Ransomware Attacks

Thank You!

Speak 1-on-1 with one of our experts:

- Schedule your **demo/technical session**

Contact Us:

- **info@catalogicsoftware.com**

Click below to learn more:

- **NetApp Page**
- **Upcoming Webinars**

Try CryptoSpike for FREE for 60 Days

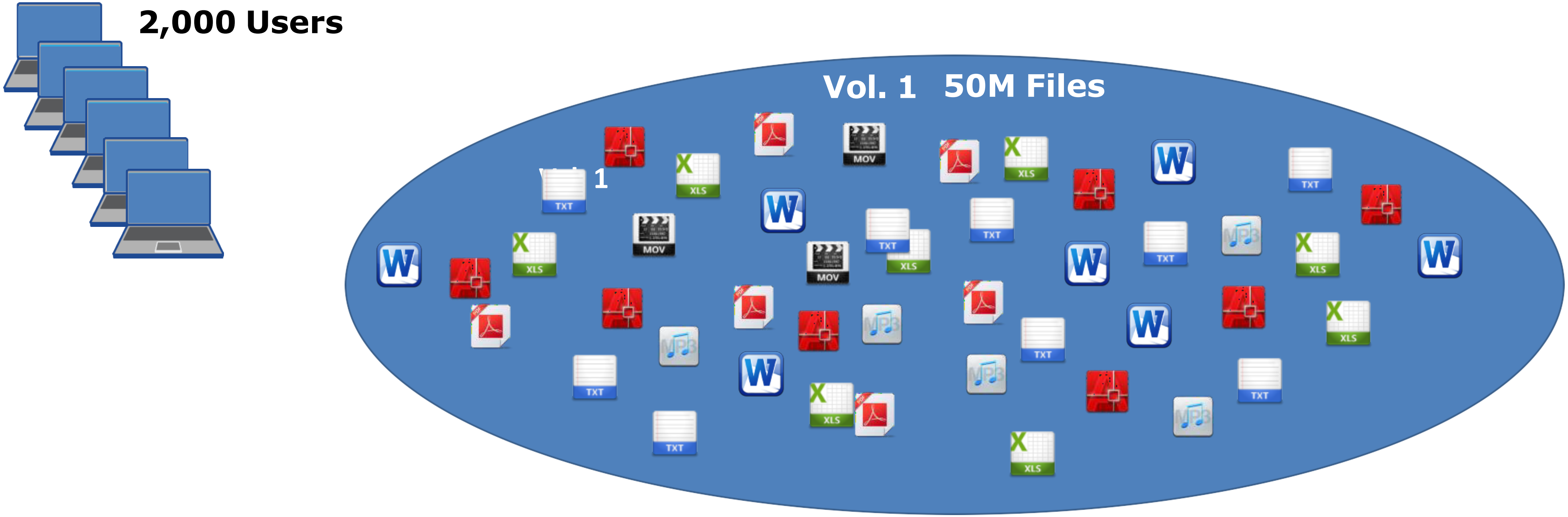
Q&A

Aaron McCune
Solutions Architect

William Bush
Field CTO - Europe

www.catalogicsoftware.com

Operation



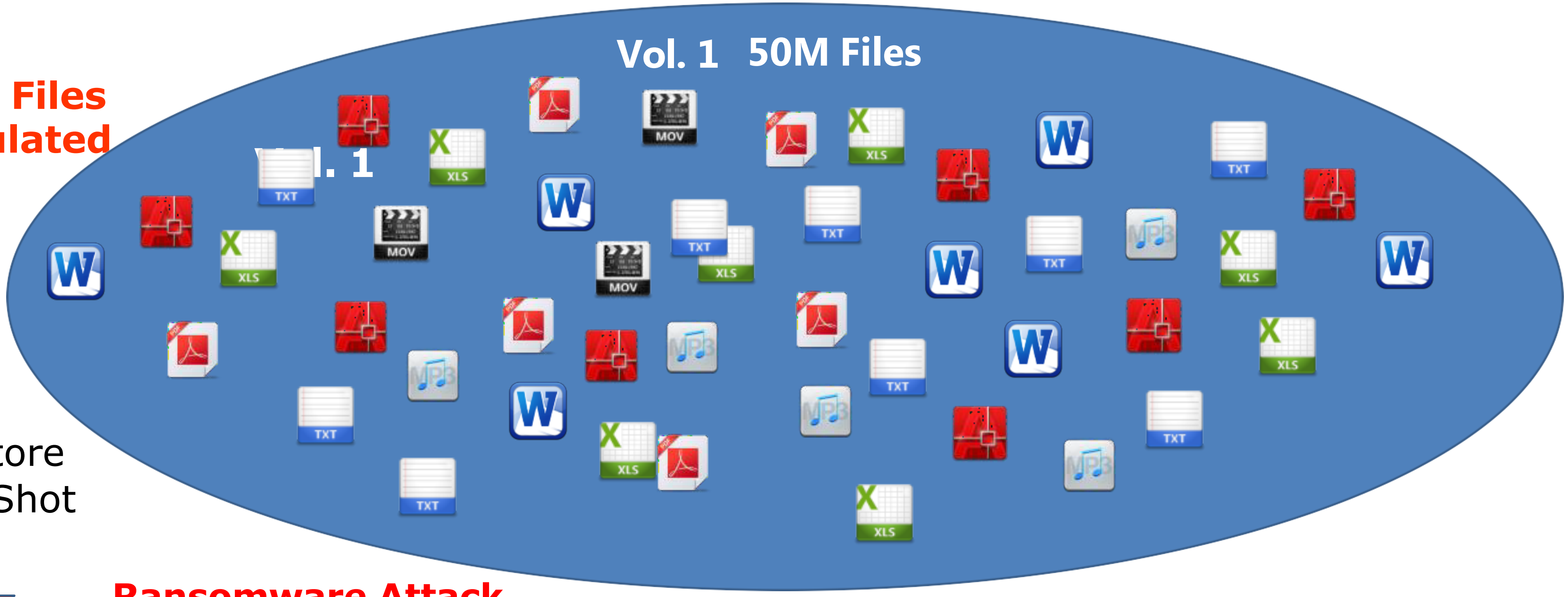
2,000 Users

Vol. 1 50M Files

Ransomware Attack

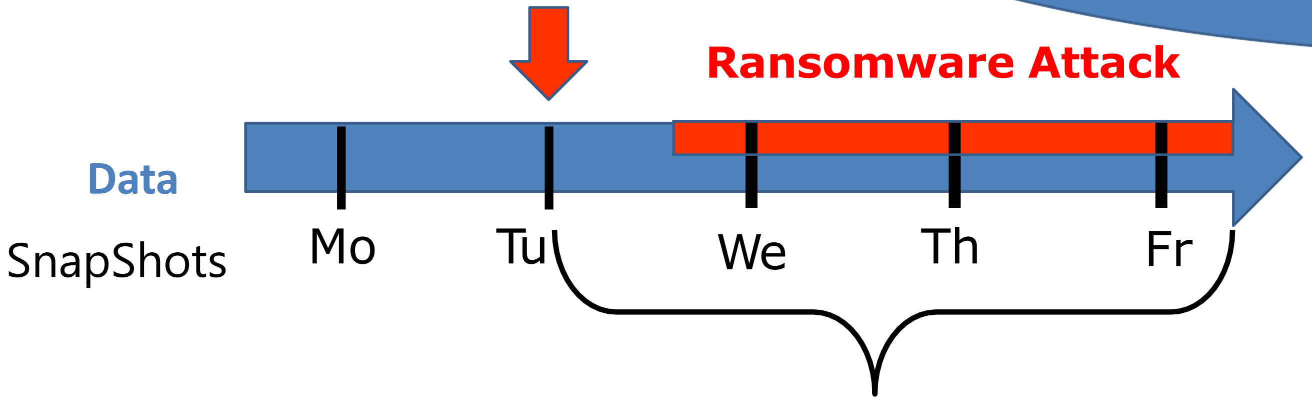
2,000 User

10,000 Files manipulated



Only one option:

Total volume restore
to Tuesday SnapShot



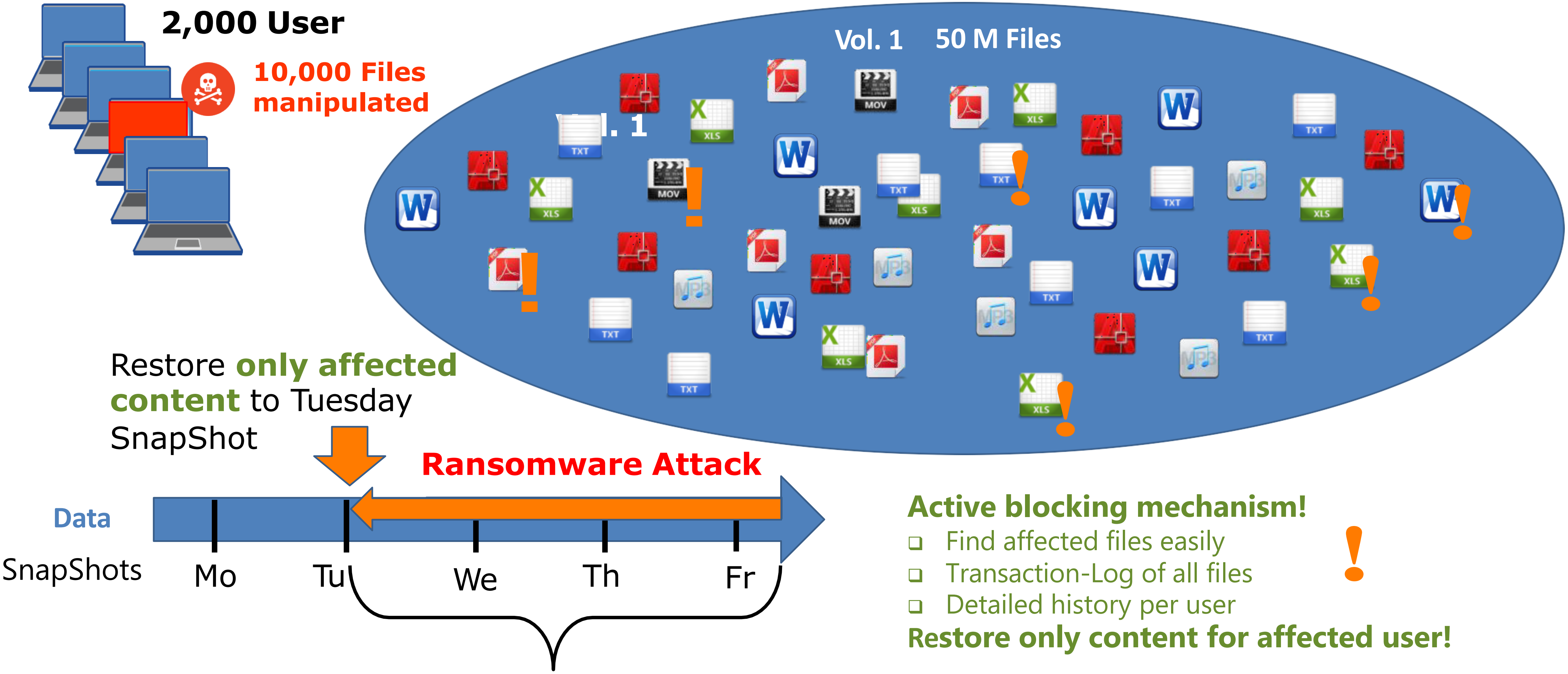
3 days data loss!!!!

Ransomware Attack:

- ❑ File name and file type didn't change!
- ❑ Last access date didn't change!
- ❑ All files look the same!

How can you separate good from bad content?

Solution: CryptoSpike



2,000 User

10,000 Files manipulated

Restore **only affected content** to Tuesday SnapShot

Ransomware Attack

Active blocking mechanism!

- Find affected files easily
- Transaction-Log of all files
- Detailed history per user

Restore only content for affected user!

All other users continue without data loss!