Breach assumed:

Minimizing damage and automating recovery through storage level data monitoring, backup, and data anomaly detection

—

Dave Larimer
Senior Technical Specialist
IBM Systems Storage – Federal Team
dlarimer@us.ibm.com

DAFITC 2025

Department of the Air Force Information Technology & Cyberpower (DAFITC):
A Training and Education Event

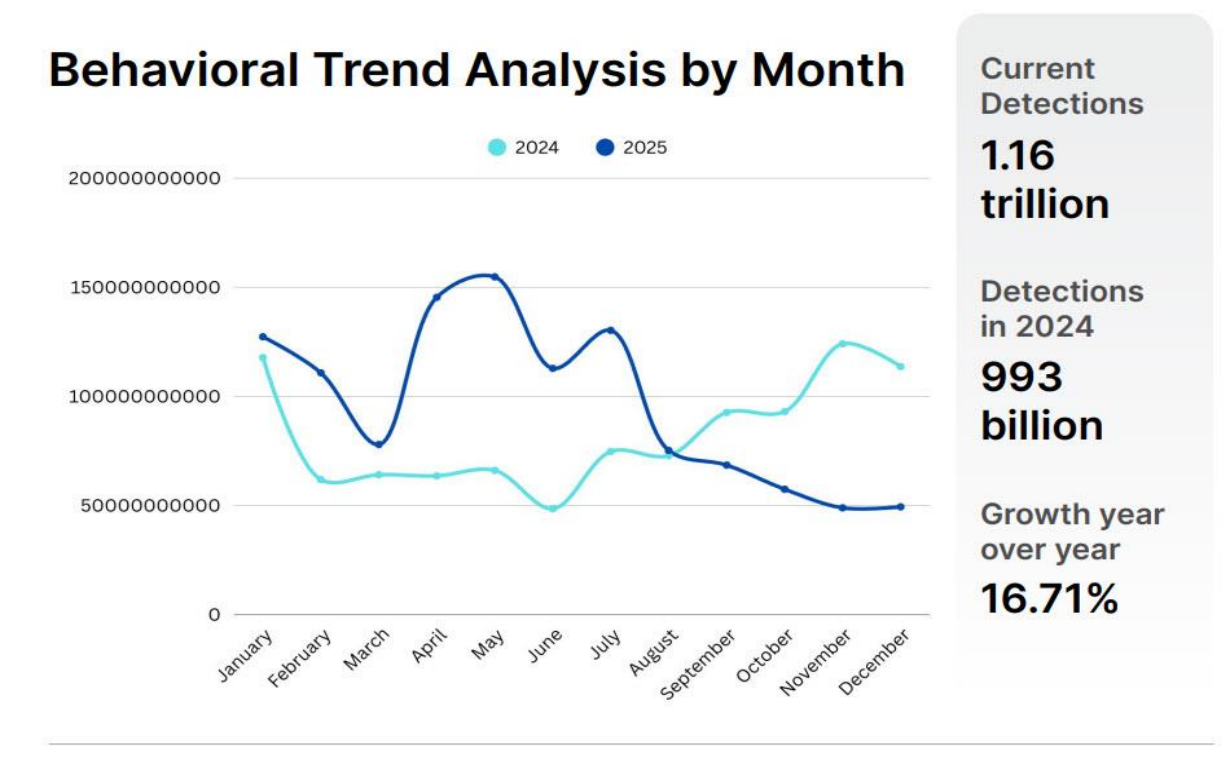
Breach assumed:

WHY?

Fortinet, currently, has reported 1.16 trillion attacks detected in 2025.

This is a 16.71% increase.

Before AI



Something **WILL** get through!

threat-landscape-report-2025.pdf

An attack gets through!

How would you know?

- System
  - Slow
  - Freezing
  - Crashing
- Behavior changes
- New app/icon
- Increased traffic
- Unusual error msg

You know by its EFFECTS

An attack gets through! How will you know?

- System
  - Slow
  - Freezing
  - Crashing
- Behavior changes
- New app/icon
- Increased traffic
- Unusual error msg

An attack gets through! How will you know?

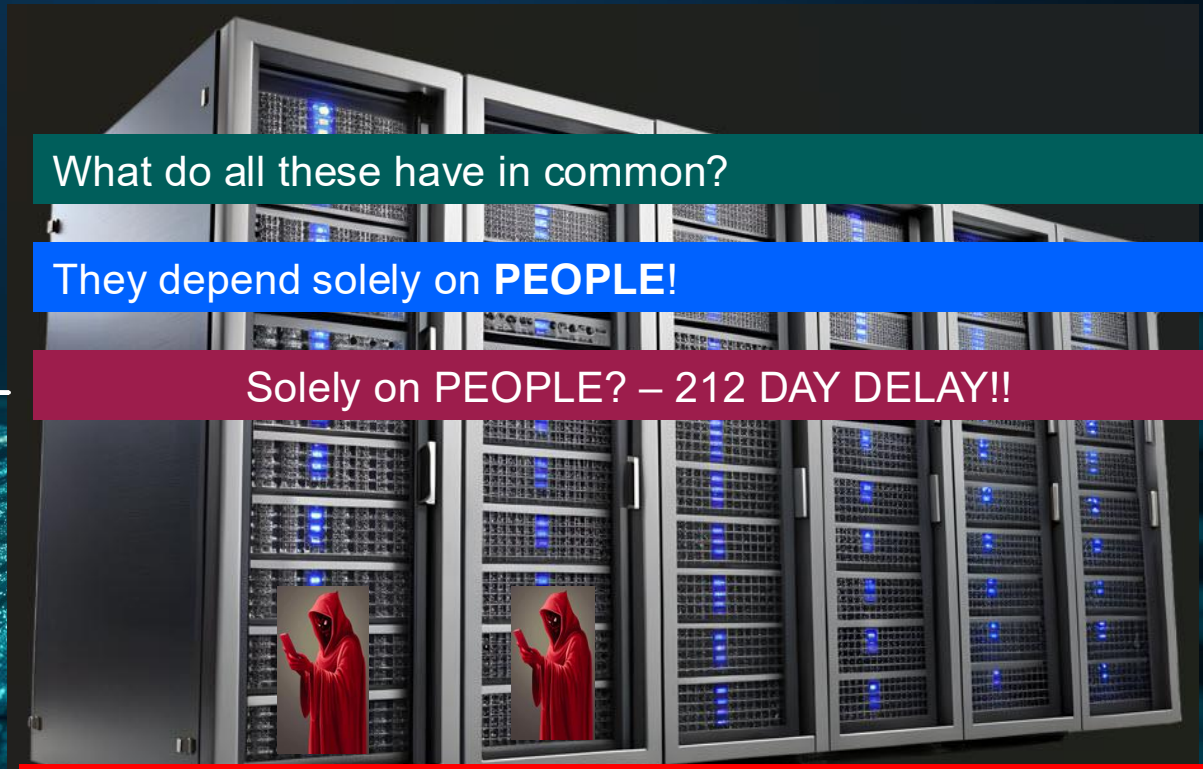
- System
  - Slow
  - Freezing
  - Crashing
- Behavior changes
- New app/icon
- Increased traffic
- Unusual error msg

An attack gets through! How will you know?

- System
  - Slow
  - Freezing
  - Crashing
- Behavior changes
- New app/icon
- Increased traffic
- Unusual error msg

An attack gets through! How will you know?

- System
  - Slow
  - Freezing
  - Crashing
- Behavior changes
- New app/icon
- Increased traffic
- Unusual error msg



What do all these have in common?

They depend solely on **PEOPLE**!

Solely on PEOPLE? – 212 DAY DELAY!!

What can happen in 212 days?

An attack gets through!

- A hacker can do almost anything in 212 days.
- The infection massively spreads
- The bad guys can choose the time to strike.
- Steal many identities.
- Etcetera

Can you wait a ½ year?

Cost of breaches!

- Financial cost: US $10 million per breach
- Reputational Damage
- Legal and Regulatory Consequences
- Loss of Intellectual Property
- Operational Disruption
- Increased Cyber Insurance Premiums
- Erosion of Customer Trust
- Long-term Financial Impact
- Classified environments - Hacking cost

MGM Grand
$100 / $110 Million

AT&T - $177 Million
class action suite

Tmobile - $350 Million

Federal Government - $26 Billion

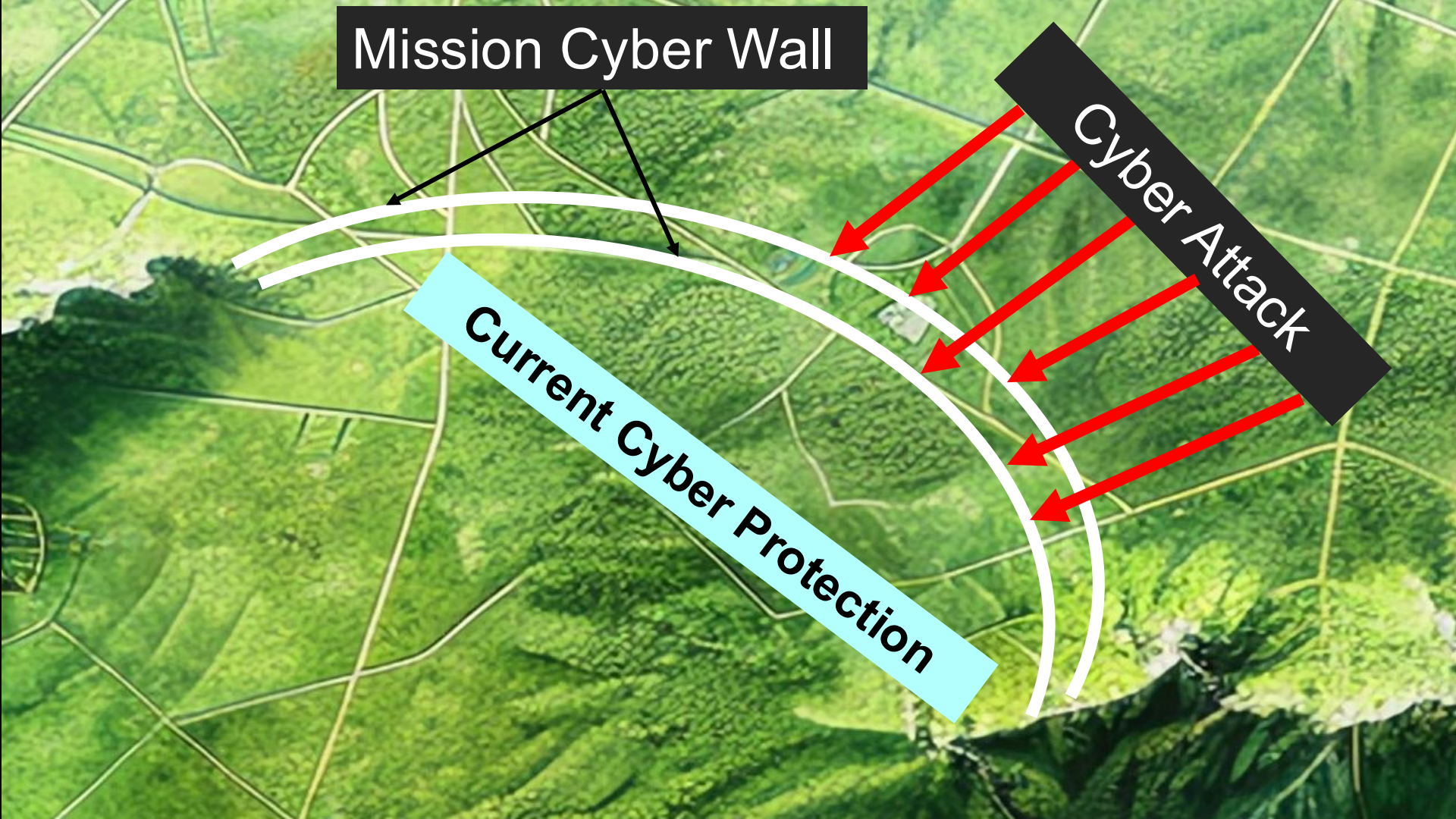
~41% per year

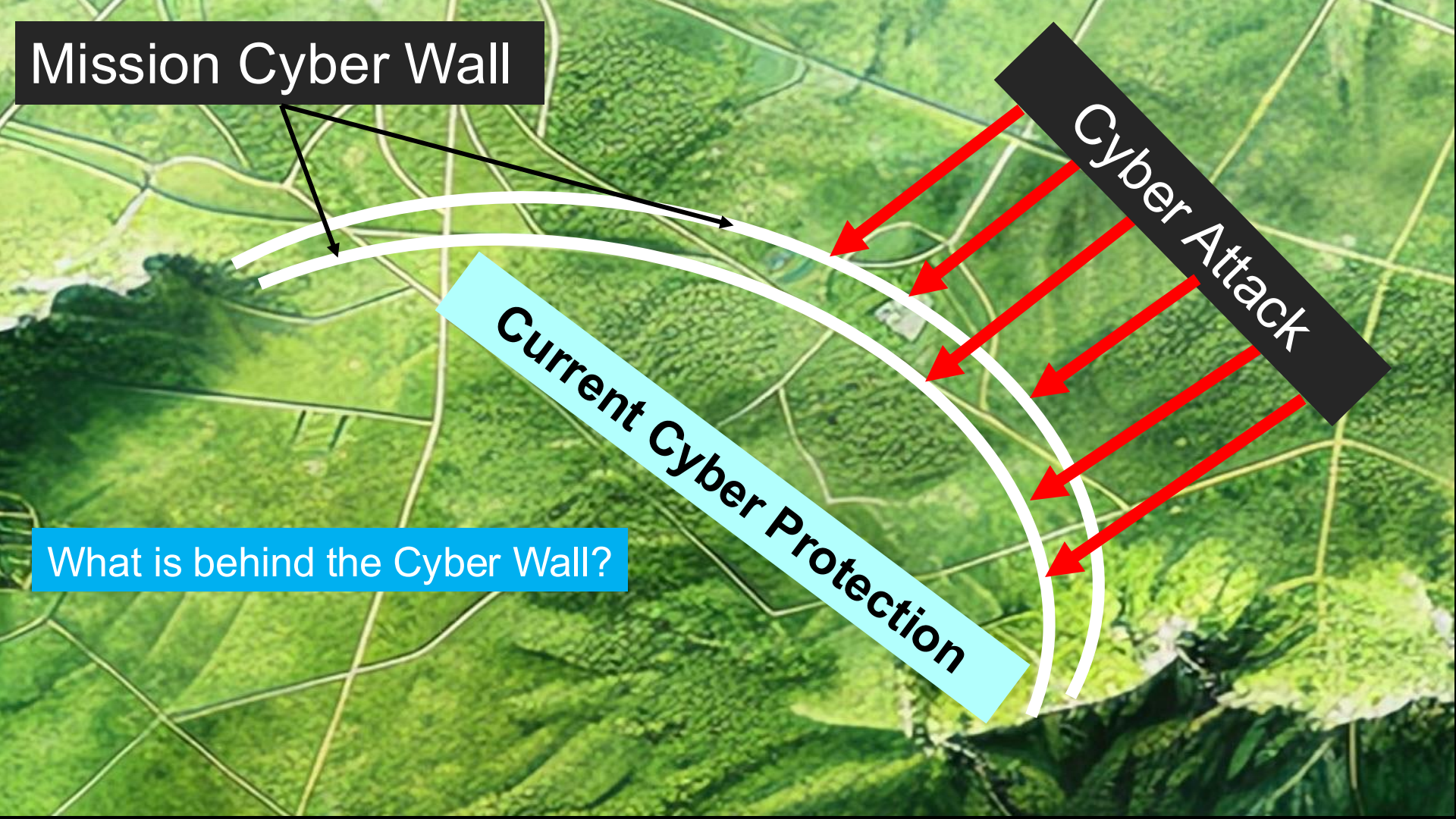
???

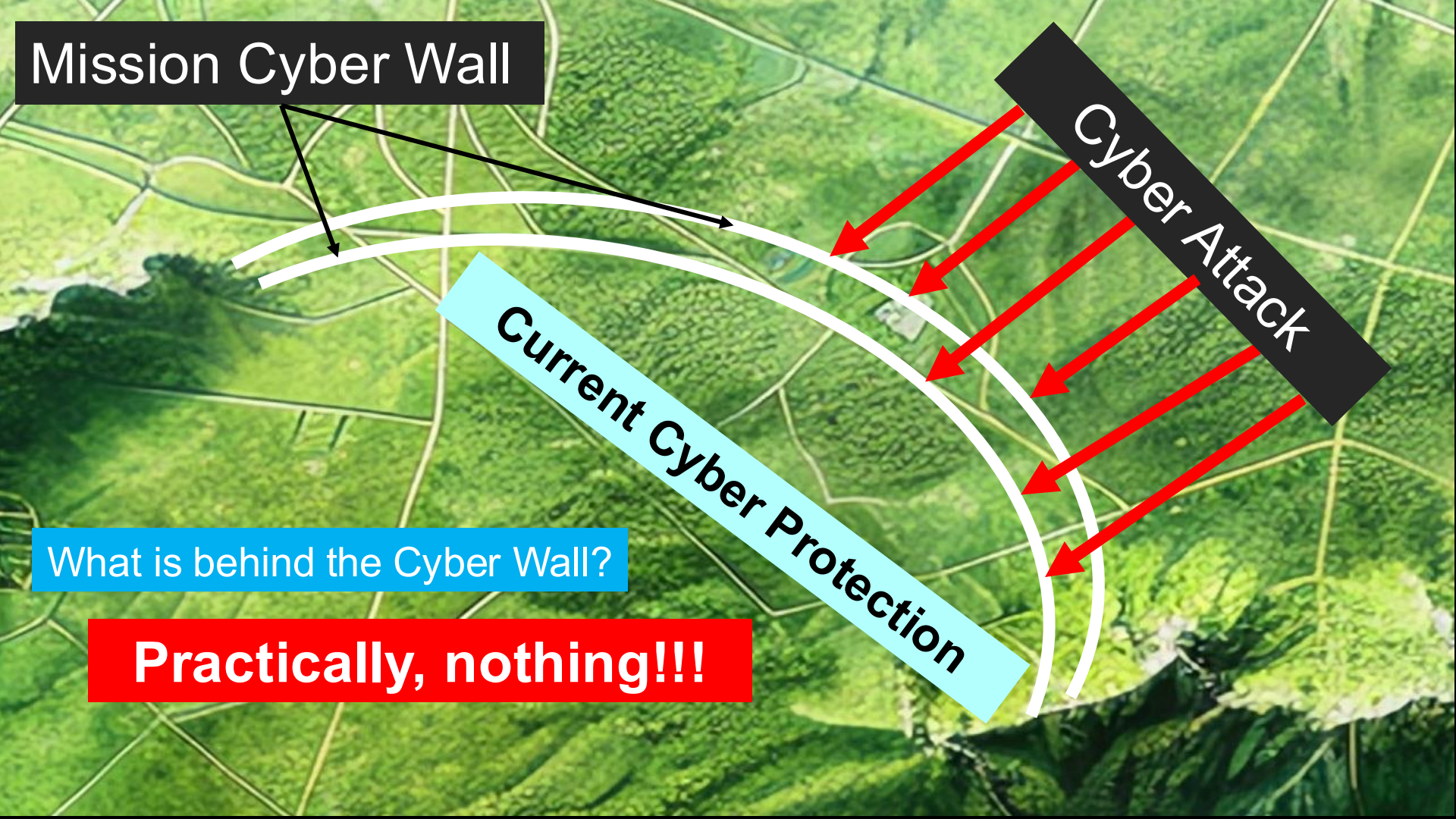
???

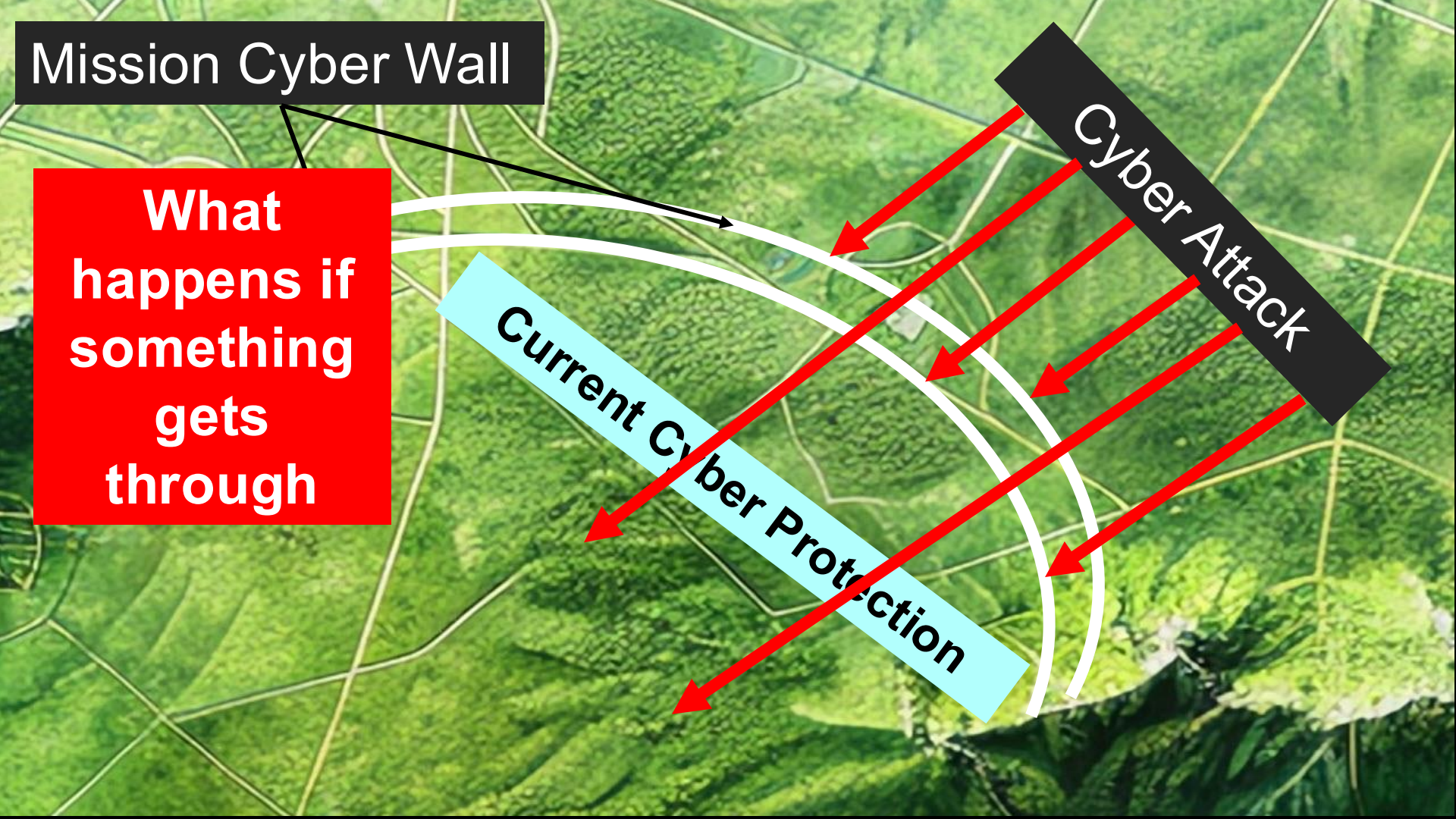
Snowden leaks - Billions

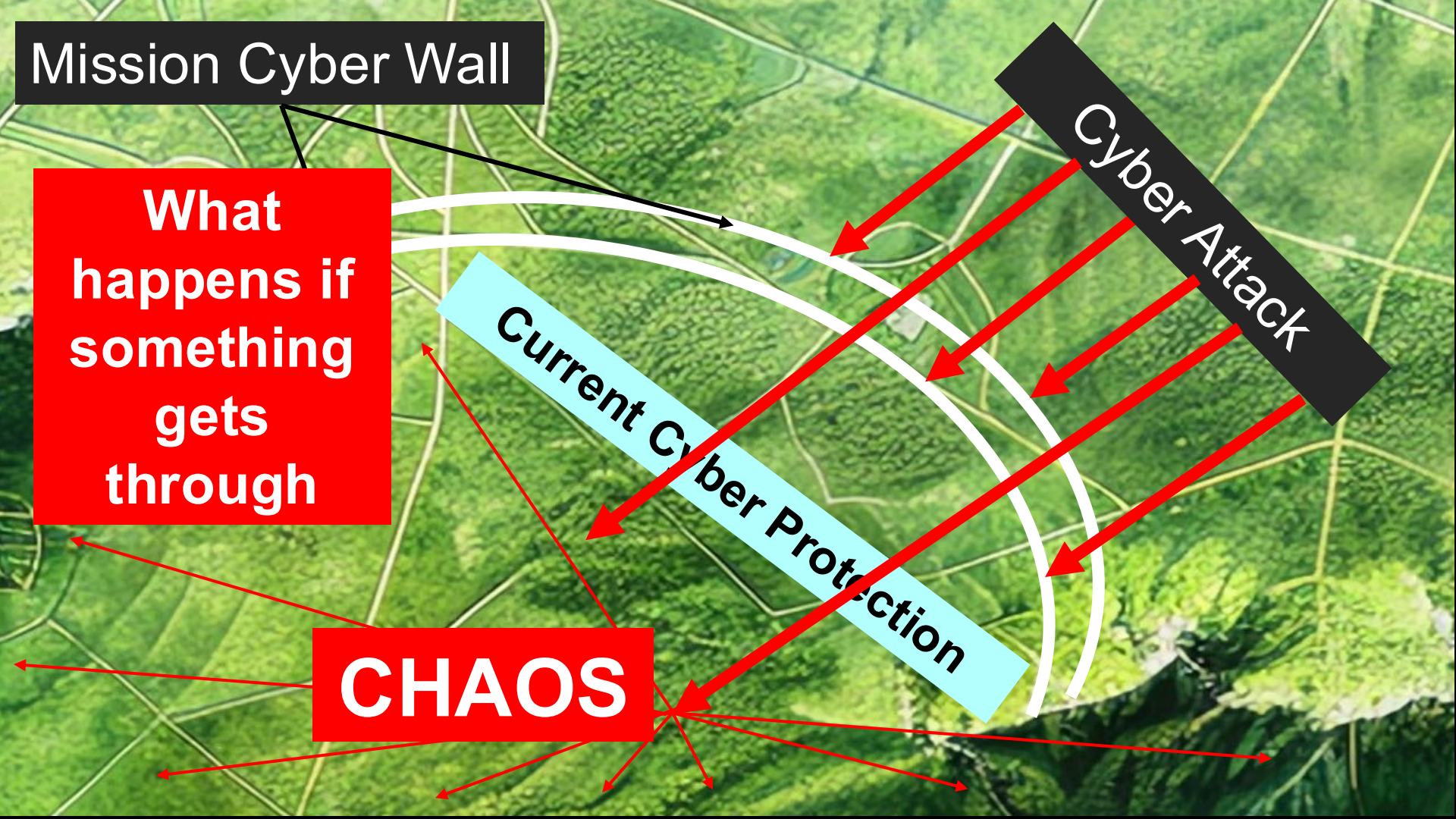

What do you need?
Minimizing the effect
Reducing the COST!


Mission Cyber Wall
Cyber Attack
Current Cyber Protection


Mission Cyber Wall
Cyber Attack
Current Cyber Protection
What is behind the Cyber Wall?


Mission Cyber Wall
Cyber Attack
Current Cyber Protection
What is behind the Cyber Wall?
Practically, nothing!!!


Mission Cyber Wall
What happens if something gets through
Cyber Attack
Current Cyber Protection


Mission Cyber Wall
What happens if something gets through
Cyber Attack
Current Cyber Protection
CHAOS

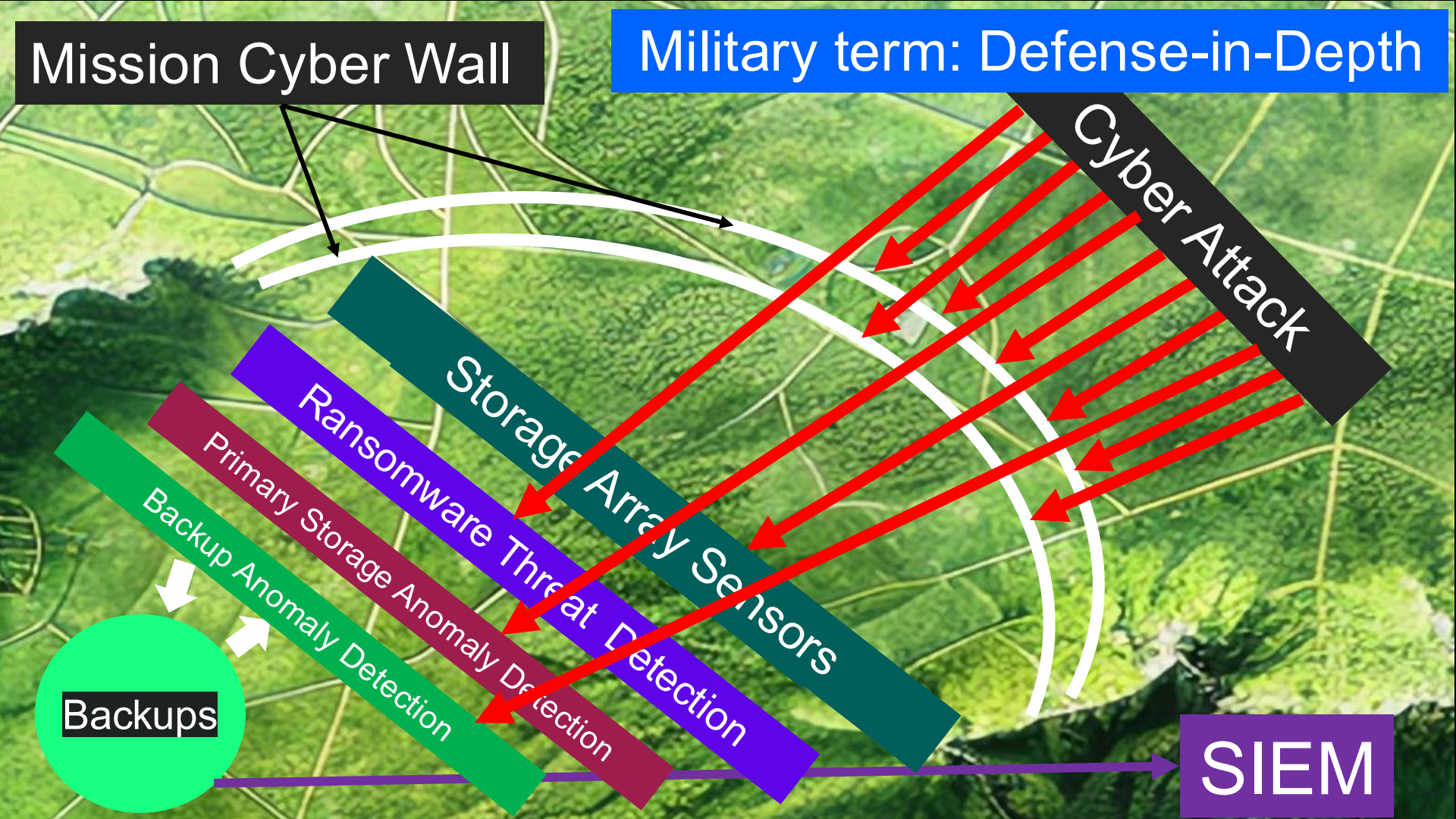
What is needed?

Chaos mitigation

- Security and Storage must coordinate activities.
- Deploy storage sensors and anomaly detection layers within the storage environment.
- The storage layers communicates alerts with Security
- Protect your cloud data!

Military term: Defense-in-Depth

- There are six layers within the Defense-in-Depth
  - Storage Array Sensors
  - Ransomware Threat Detection
  - Storage Anomaly Detection
  - Backup Anomaly Detection
  - Clean room environment
  - Security Information & Event Management (SIEM)


Mission Cyber Wall
Military term: Defense-in-Depth
Cyber Attack
Storage Array Sensors
Ransomware Threat Detection
Primary Storage Anomaly Detection
Backup Anomaly Detection
Backups
SIEM


Additional Information
ctrl
alt

Introducing IBM Storage Defender

Minimizing damage and automating recovery through storage level data monitoring backup, and data anomaly detection.

We must change the way we think about recovery

Traditional Recovery

Random; power outages, system failures, natural disaster, user error

Local or regional

Backups usually available

Known recovery point with a defined RPO

Depending on amount of data, **minutes to days**

Cyber Recovery

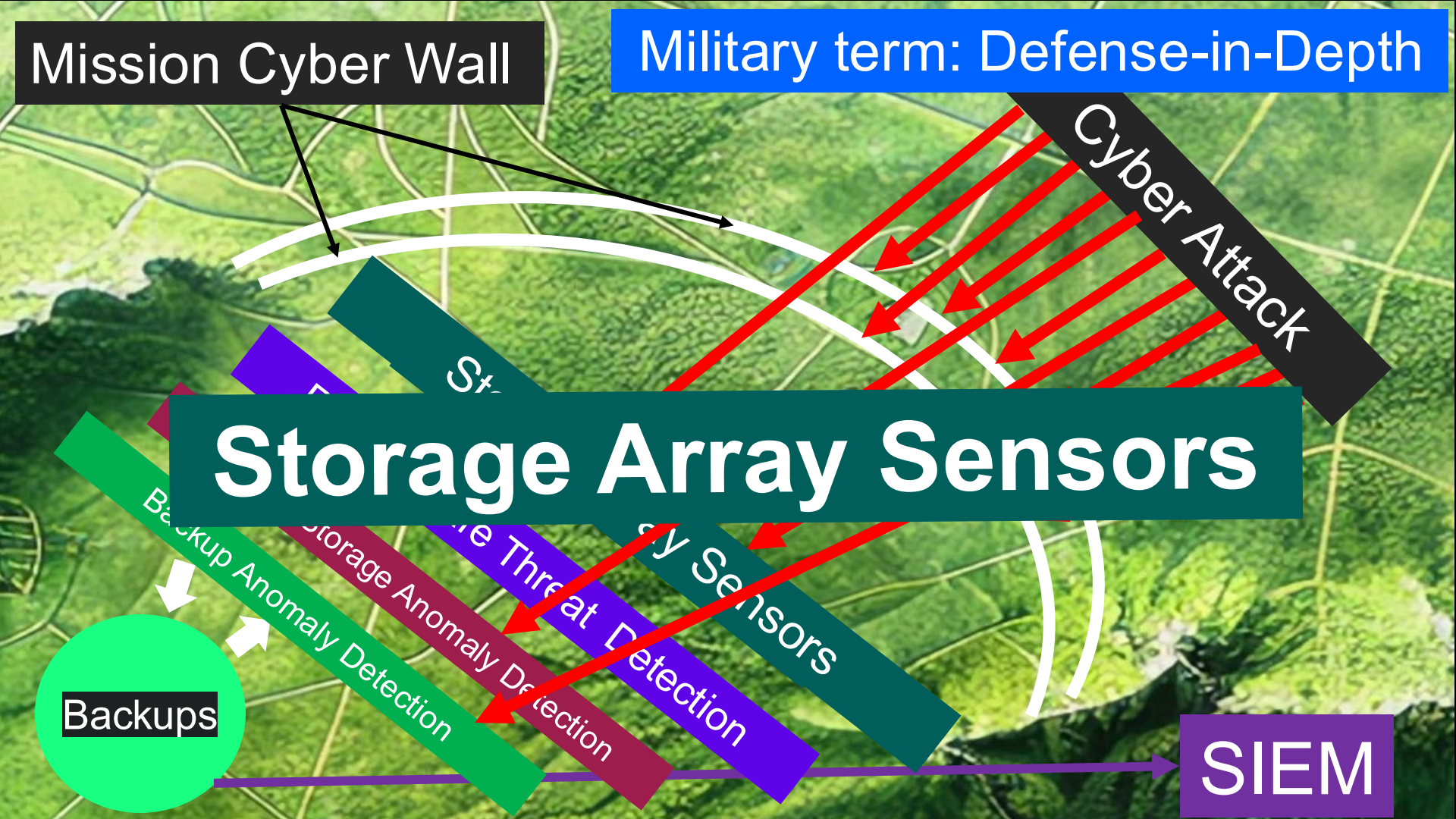
Targeted; well-planned attack, engineered for maximum impact

Global, designed to spread across all connected systems and networks

Backups included in attack and compromised or destroyed

Need to determine a clean recovery point before restore can start

Depending on the size and scope of the attack, **hours to months**


Mission Cyber Wall
Military term: Defense-in-Depth
Cyber Attack
Storage Array Sensors
Backup Anomaly Detection
Storage Anomaly Detection
Threat Detection
Sensors
Backups
SIEM

IBM FCM4
Storage Anomaly Sensors

- Cyber resiliency starts with hardware sensors tasked to look for any changes in data.
  - IBM FCM4s collect and analyze detailed malware statistics from every I/O with no performance impact.
  - The AI engine learns what is normal for the system and detects threats by using data from FCM.

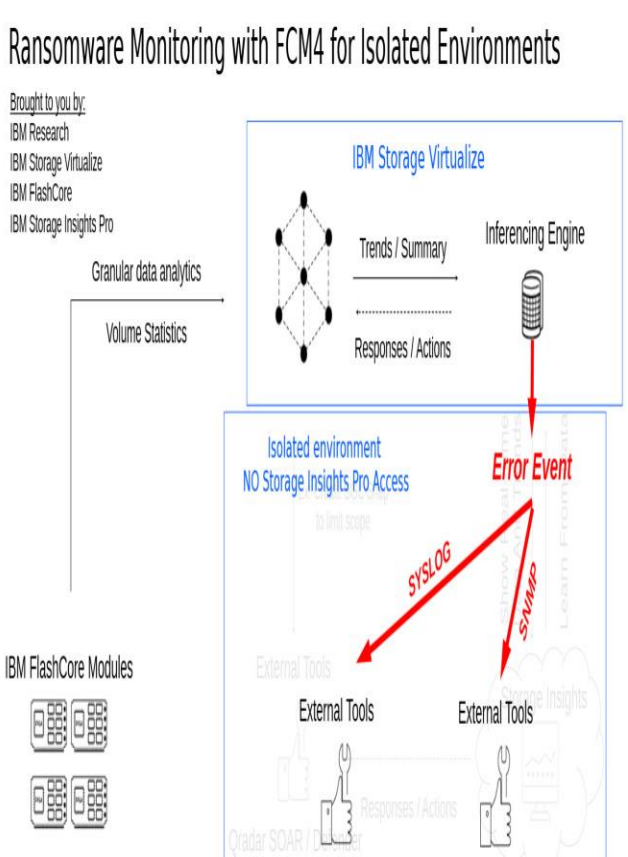
IBM Flash Core Module (FCM) 4

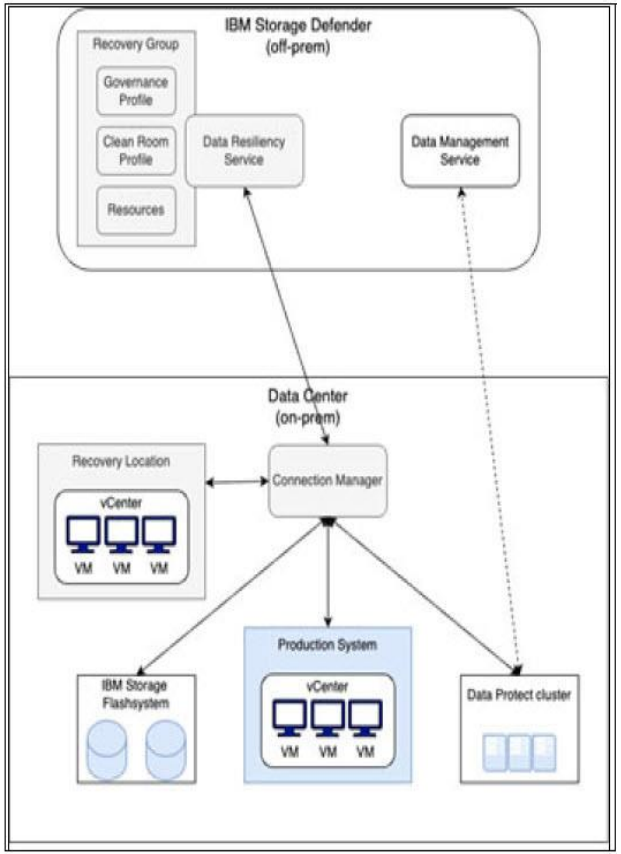
IBM FCM4 Storage Anomaly Sensors

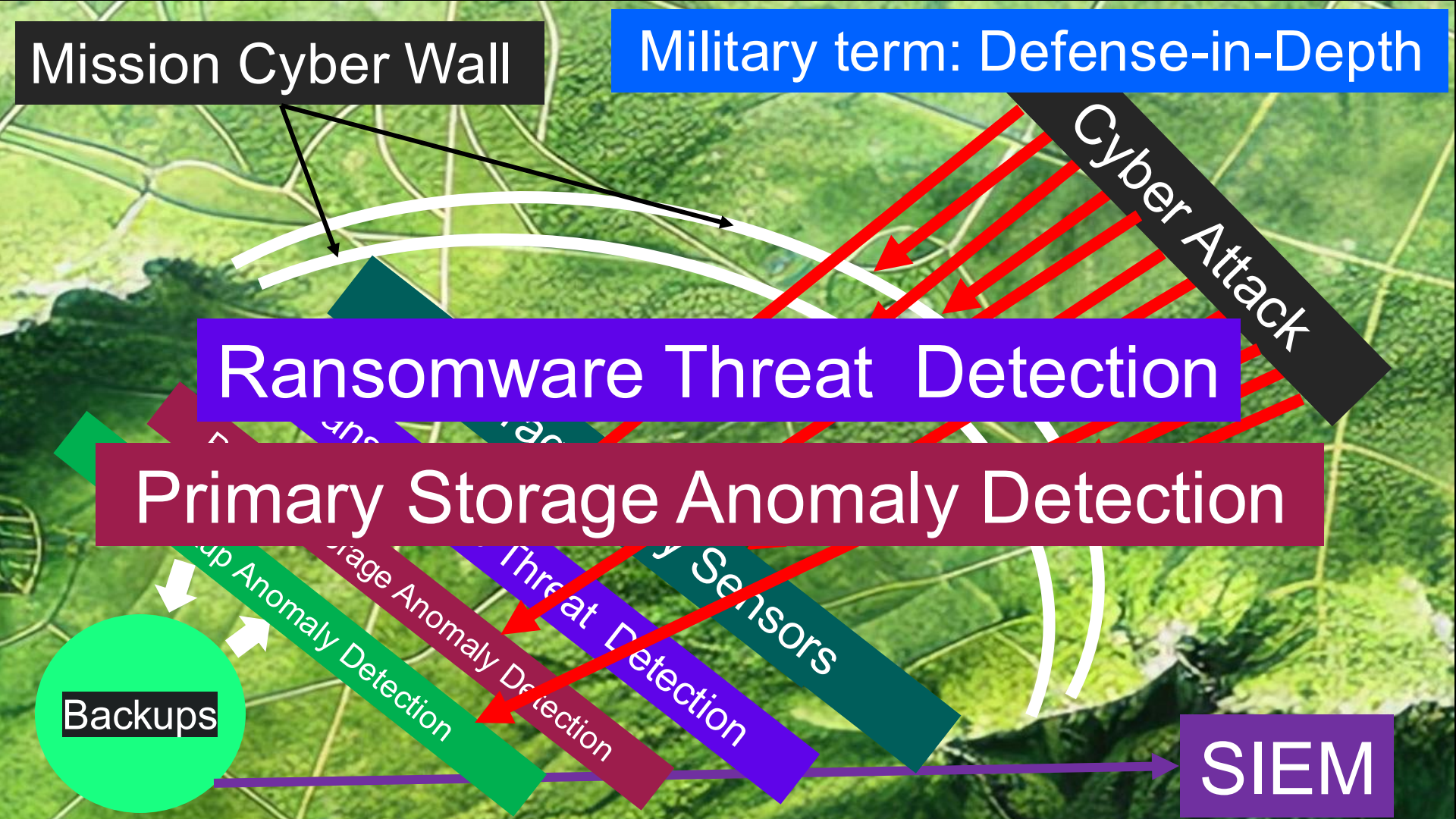
- FCM4 storage sensor detects a data anomaly.
  - This error is forwarded to the Defender central collector.
  - The central collector's AI evaluates all alerts and determines if a user defined threshold has been reached to invoke automated reactions.
  - These automated reactions can include data snapshots of VMs connected to the erroring system. SIEM alerting which can then lock down the effected machine.

IBM FCM4 Storage Connection Manager

- Connection Manager
  - Maintains connections between local storage systems, backup systems, and Data Protect clusters
  - Perform test recoveries
  - Orchestrates directs recovery operations across these resources.

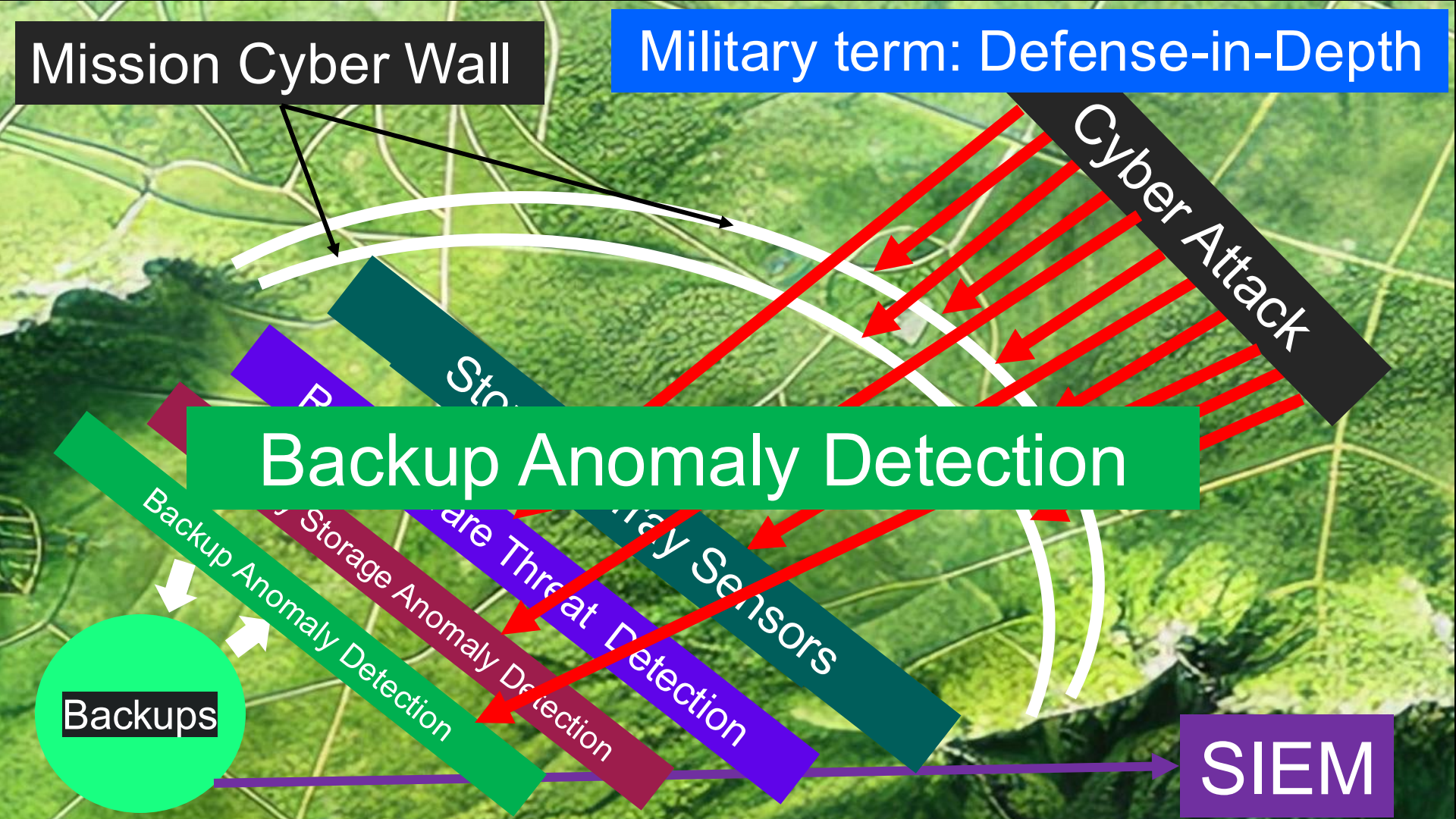





Mission Cyber Wall
Military term: Defense-in-Depth
Cyber Attack
Ransomware Threat Detection
Primary Storage Anomaly Detection
Sensors
Threat Detection
Anomaly Detection
Backups
SIEM

IBM Storage Defender data censors

- IBM Storage Defender sensors are small, lightweight pieces of software that are installed into Virtual machines (VMs)
  - Defender sensors monitor file-pattern activities that resemble ransomware threats.
    - Every 30 seconds, the sensor looks at file-related event information to detect specific file patterns looking for ransomware and other malware.
    - These sensors use AI to identify malware patterns. If malware is suspected a third check that uses file introspection to determine if file is being encrypted
    - If criteria is met the and event is created and passed onto the collection manager to determine if a user defined threshold has been met for further action
- These actions can include data snapshots of VMs connected to the erroring system. SIEM alerting which can then lock down the effected machine.


Mission Cyber Wall
Military term: Defense-in-Depth
Cyber Attack
Backup Anomaly Detection
Backup Anomaly Detection
Storage Anomaly Detection
Threat Detection
Sensors
Backups
SIEM

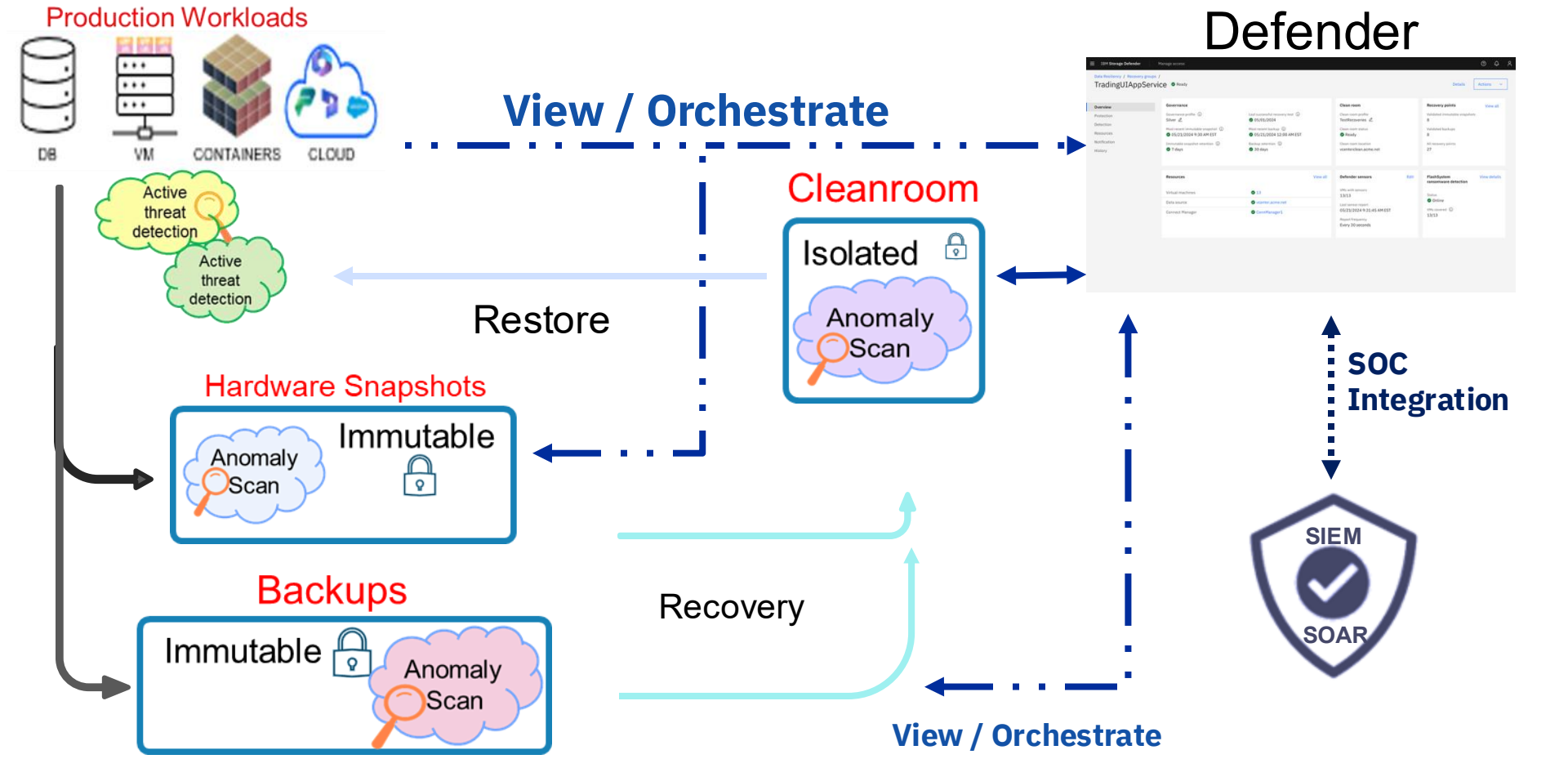
IBM Storage Defender Backup Anomaly Detection

- IBM Storage Defender has an independent backup anomaly detection system designed to use the same techniques and processes as the other previous slides described.
  - This backup and recovery system of Storage Defender can automatically snapshot thousands of Virtual Machines enterprise-wide applying global policies to the backed-up data.
  - During recovery this same solution can instantly recover thousands of servers and allow users back onto their server within minutes.

Clean Room

- A clean room is an isolated environment that can be used to mount VM snapshots into so that final anomaly and malware detection testing can be performed.
  - IBM Storage Defender is designed to help facilitate this mounting and testing of the VMs.
  - The clean room is the final check in this data Defense-in-Depth solution.

IBM Storage Defender solution - Workflow



Real World Results

Fast Recovery: Real Customer Example

The bank established recovery time objectives for their critical workloads

Scenario	Scope of VMs	Time to Recover Today	Time to Recover Goal
Deleted or Corrupted File	1	Variable based on file-count	**Variable** based on file-count
Single VM Corruption	1	2 hours	**<10 minutes**
Storage Volume Corruption	30-50	3 hours	**<10 minutes**
Storage Array Corruption	300-1,200	8 hours	**8 hours**
Application Upgrade Rollback	1-50	30 minutes	**<10 minutes**
OS Patching Goes Wrong	300-1,000	5 Days	**< 1 hour**
Large-Scale Malware Attack	1,000-16,000	4 Weeks	**< 24 hours**

Recovery Time Objectives

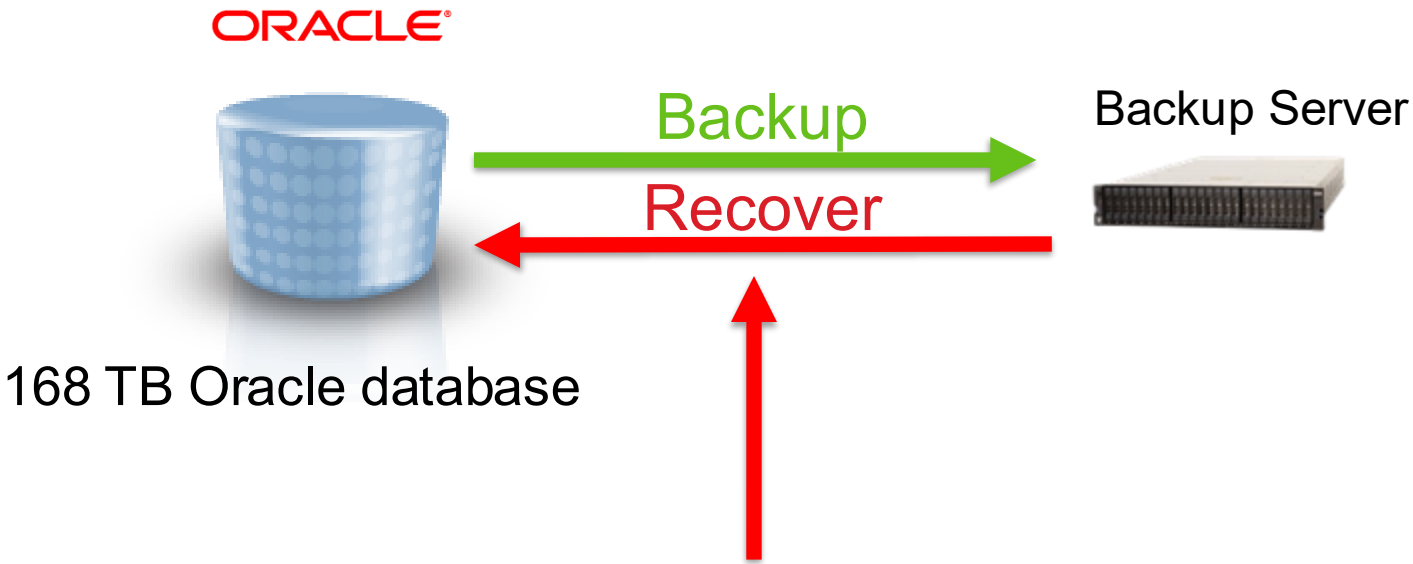
Fast Recovery: Results

Defender's instant mass recovery enables recovery at scale in minutes, not hours, days or weeks

Scenario	Scope of VMs	Time to Recover Today	Time to Recover Goal	Results
Deleted or Corrupted File	1	Variable based on file-count	Variable based on file-count	Global Search with flexible restore options. **< 1 minute**
Single VM Corruption	1	2 hours	<10 minutes	Instant VM Restore **< 1 minute**
Storage Volume Corruption	30-50	3 hours	<10 minutes	Instant VM Restore of **50 VMs** **< 3 minutes**
Storage Array Corruption	300-1,200	8 hours	8 hours	Instant Recovery of **1,000 VMs** **39 minutes**
Application Upgrade Rollback	1-50	30 minutes	<10 minutes	Instant VM Restore of **50 VMs** **< 3 minutes**
OS Patching Goes Wrong	300-1,000	5 Days	< 1 hour	Instant VM Restore of **250** Randomly selected VMs **<7 minutes**
Large-Scale Malware Attack	1,000-16,000	4 Weeks	< 24 hours	**2,200 VMs** Powered on and available **47 Minutes** Back on primary storage = 4 hours

Fast Recovery from HW Snapshot – Real Customer Use Case

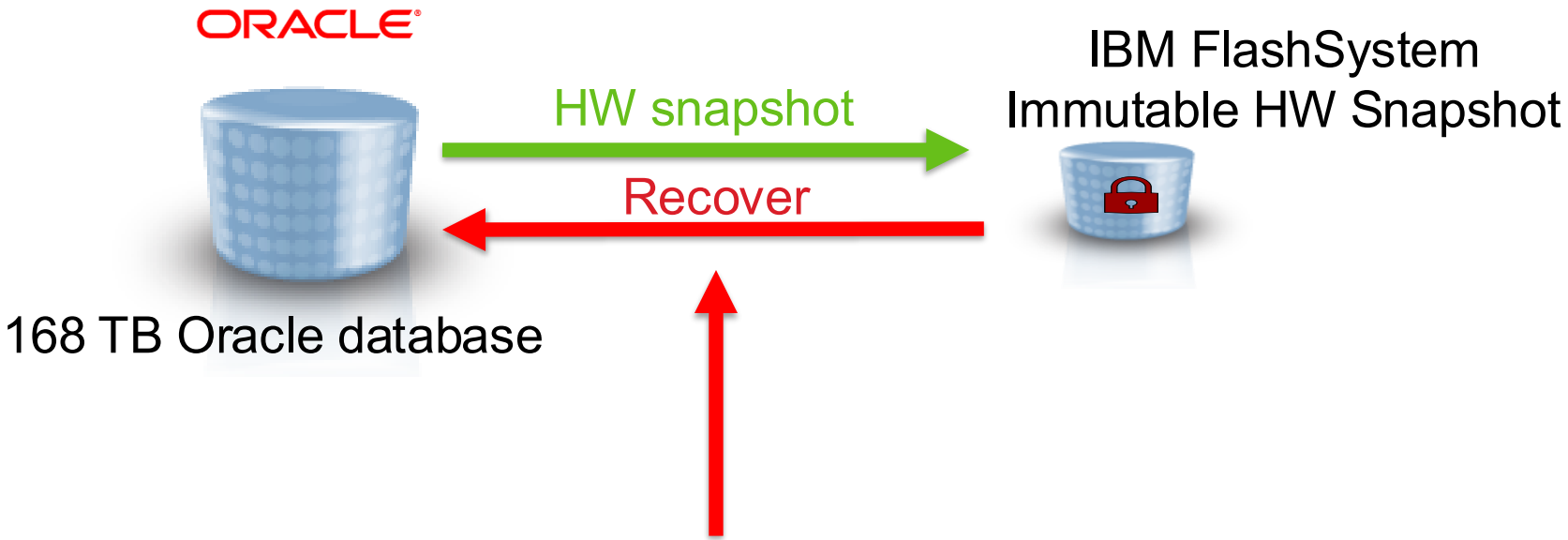
A large financial company could not restore fast enough …



Recovery from a backup took **12+ hours**!

Fast Recovery from HW Snapshot – Real Customer Use Case

A large financial company leveraged hardware snapshots for near instant recovery …



Recovery from a HW snapshot only took **minutes**!

IBM Storage Defender summary

- The overall goal of IBM Storage Defender is to enhance and compliment the cyber health of all data enterprise-wide.
- The layered approach to continually test the in-flight and at rest data for any anomalous behavioral changes is a must for any mission critical enterprise-wide environment.
- The “Cyber Wall” prevents and blocks most of the incoming attacks.
- IBM Storage Defender continually detects, facilitates data cleaning, and greatly reduces the time to recover.

IBM Storage Defender can reduce 212 day to mere minutes!

Thank you!

For more information

Contact Dave Larimer
dlarimer@us.ibm.com