Mainframe Under Siege
Real-Time Threat Interception and Automated Recovery

TECH_180s2

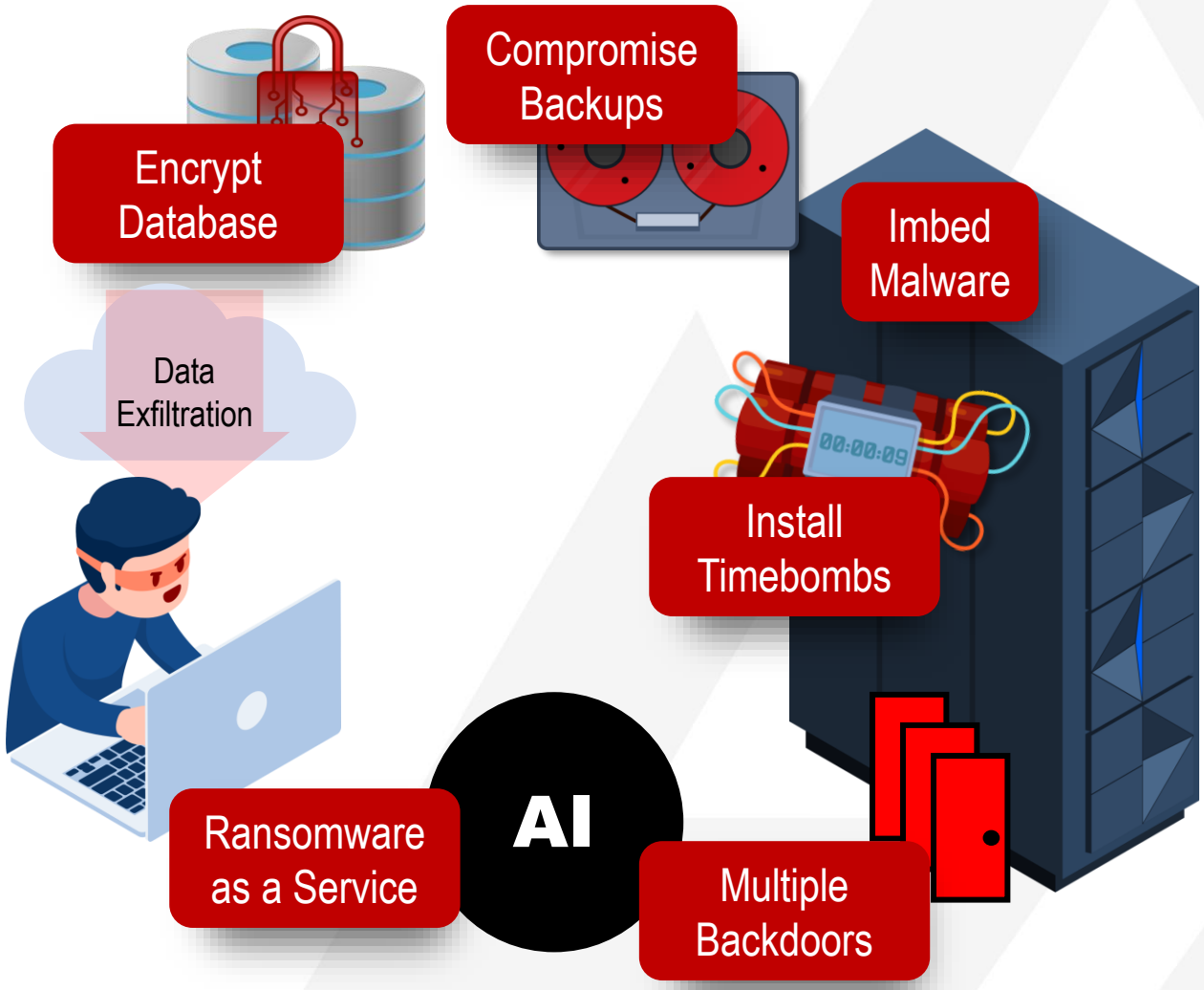
Today we are going to discuss how/why you need to:

- Discover and remove ransomware
- Intercept / suspend malicious encryption immediately
- Fight data exfiltration - detect / stop malevolent data transfers
- Freeze offending actors to mitigate damage
- Reduce human reaction time with GUI-driven tools
- Perform surgical recovery

Al Saurette
MainTegrity

Mark Wilson
Vertali

Ransom attacks – Multi-pronged



Attacking as a business

- Persistent, intelligent
- Multiple Backdoors
- Timebombs
- Compromise Backups
- Encrypt Database
- Data Exfiltration
- Ransom Demand

A Brave New World

Mainframes were very secure before being networked

- Mainframes are now attached to everything
- Formerly trusted network nodes get attacked
- Compromised Windows, Linux, Apache, VPNs …
- Lateral movement to the mainframe
- Devices may not even be owned by you – No control
- Specialized Ransomware-as-a-service & AI attacks
- State sponsored, Sophisticated
- APIs, Open Source new threat vectors

Trust but verify

Lateral movement

Network must be monitored 24/7 for behavioral change

Suspected Mainframe Breaches

Jaguar Land Rover (2025)

Exploited social engineering SAS NetWeaver
Moved laterally requiring z/OS shutdown
5 week outage - determine if z/OS impacted
Revenue hit reached over £2 billion
Complete assembly line shutdown

Anthem Health (2015)

Phishing attack, database breach
79 million healthcare records stolen
HIPAA fine $16 million
5 years of litigation, 43 state Attorneys General
Cost $500Million legal, settlement, remediation

Office of Personnel Management (2015)

State-sponsored cyber espionage China?
21.5 million records high security Americans
Fingerprints, security clearance data
Est. $500 million for remediation

Equifax (2017)

Unpatched vulnerability in Apache Struts
147 million individuals' financial data.
Over $1.4 billion, including settlements, remediation, and legal fees.

UnitedHealth Group (2024)

Phishing exploitation of web application
Affected health claims for 1/3 of Americans
Outage for 9 days, full recovery 2 months
Est. Cost $3 Billion

For detailed information go to www.MainTegrity.com/attacks

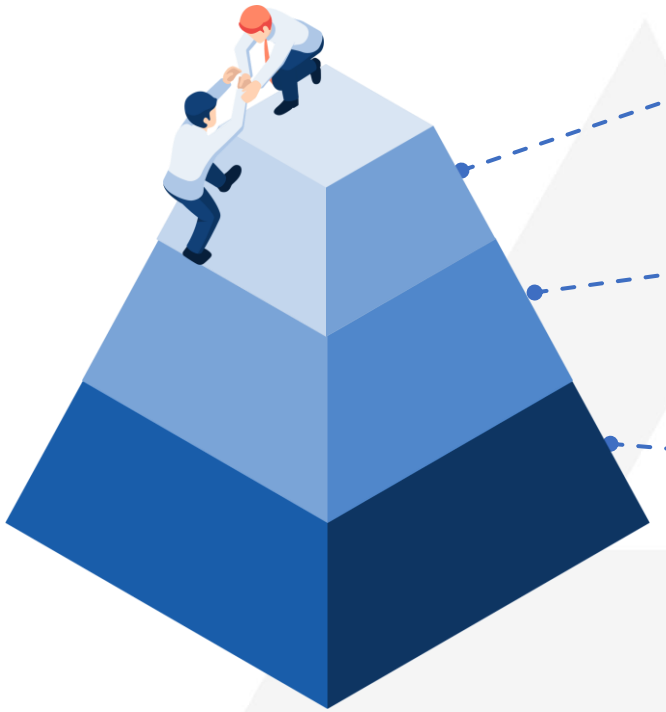
People, Process, Technology

Breakdowns

Process: Unimplemented, Untested, Incomplete

Technology: Security gaps, SMF slow & incomplete, detection missing

People: Slow human response, Lack of knowledge, skills, vigilance



Solutions

People

Time to respond – GUI for staff offload

Instream Recovery Guidance – correct response

Recover System & Data – What was compromised

Technology:

FIM, Behavior Changes, Ransomware, Exfiltration

Real-time Threat Detection / Alerts - SMF too slow

Damage control – Suspend, Resume, Countermeasures

Process:

NIST CSF V2, PCI, Zero Trust, DORA

Defined, tested, automated processes

Required controls

File Integrity Monitoring

- Detect, Prevent, Remove Malware/Ransomware
- Learn about desired changes so unapproved stand out
- Real time Alerts to support staff, Splunk, ServiceNow, etc

Detect / React to z/OS attacks

- Detect Authority / Privilege Escalation, User Impersonation
- Suspend Rogue Encryption in seconds
- Alerts for suspicious User behavior

Network Awareness

- Eliminate all Non-encrypted connections
- Data Exfiltration – stop too much data (TSO, batch)
- Alert for changed suspicious network behavior

Supply Chain

- Improve release control / approval:
- Enable separation of duties – mentoring, issue resolution
- Certify / Lock changes prior to approval / implementation
- Verify that change deployment was correct

Foundational Elements

Real-time Reaction

- Suspend offending tasks
- Resume if found to be desired
- Cancel / Revoke – Invoke assisted recovery
- Damage Control – offending tasks halted

Human Interface

- Automatically invoked from detection alert
- Web-based UI for easy investigation
- Human response at machine speed

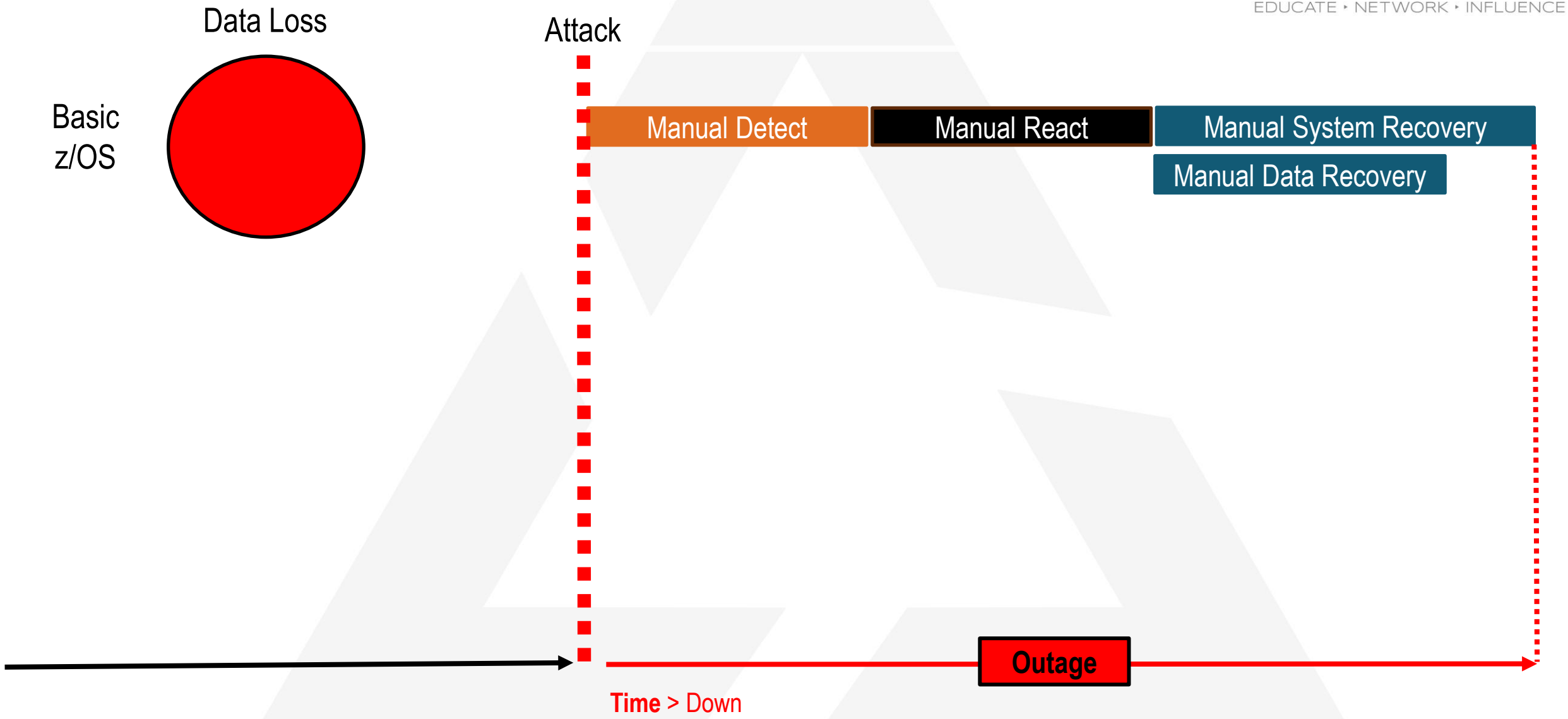
Whitelisting

- Learns about approved workload / activity
- Avoids false positives
- Can exclude certain production user IDs

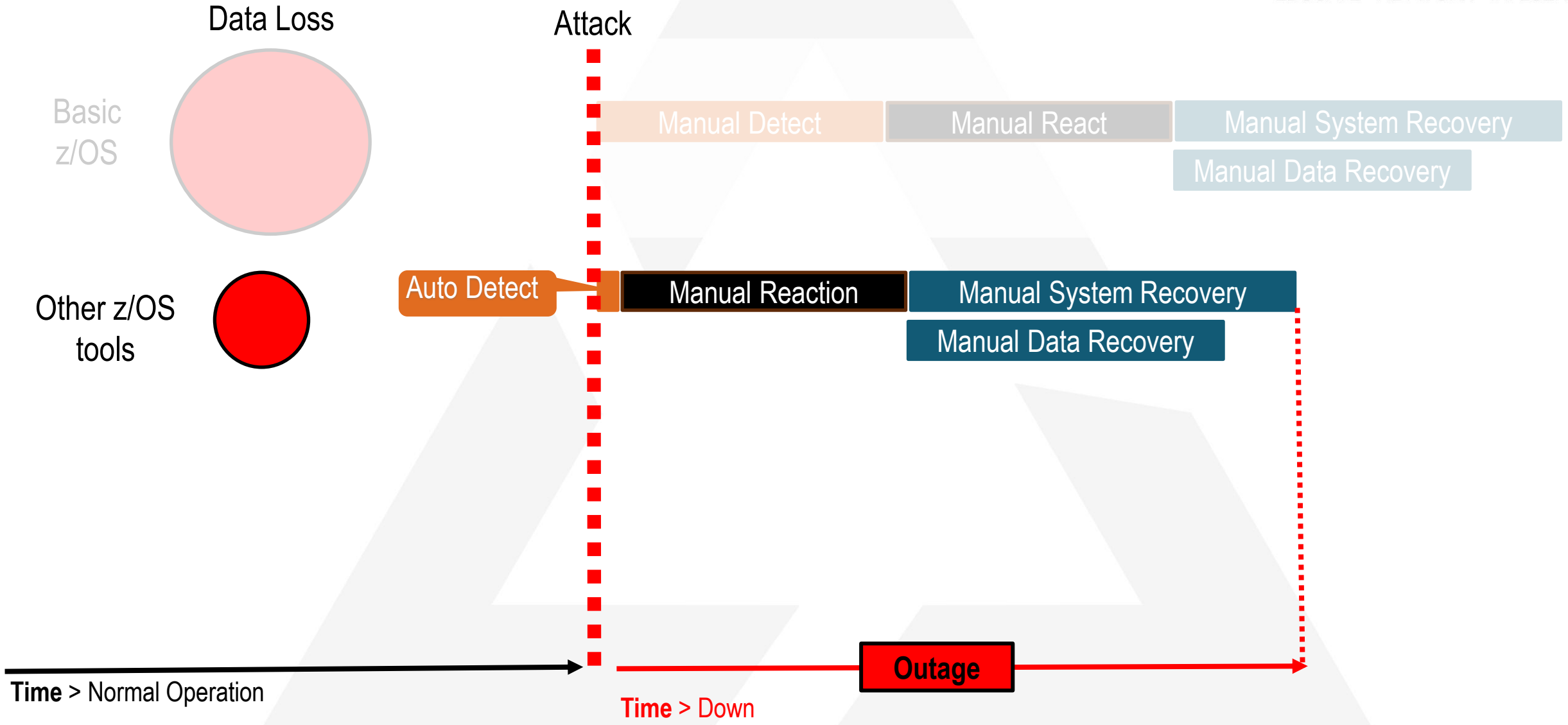
Restore Assist

- Client specific recovery guidance
- Remove Malware & Verify
- Assist Data Recovery – IBM, Dell, HV, immutables
- Conventional backups

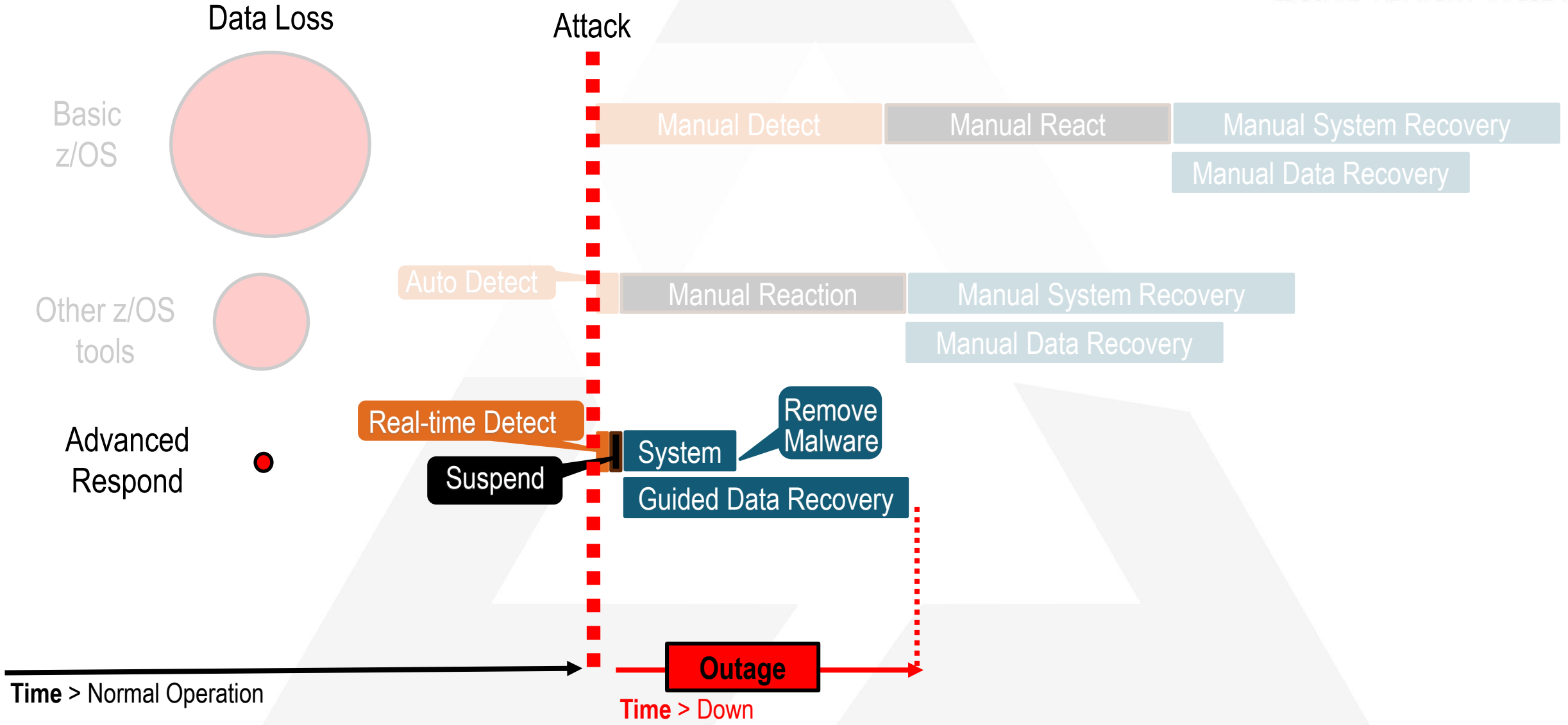
Response Time Line / Damage



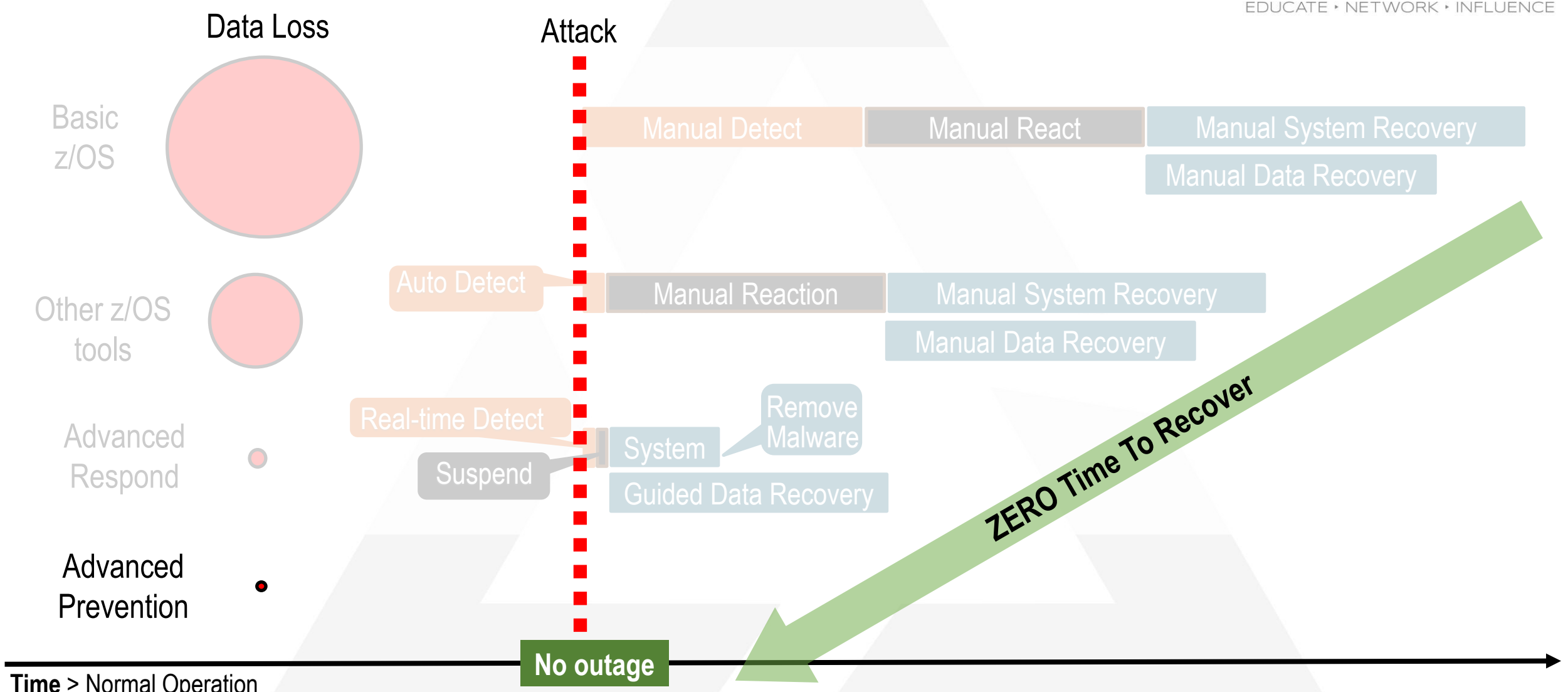
Minimal Damage Control



Maximum Damage Control



No Damage



Integration with AI - IBM TDz / Splunk …

AI can not work without current / complete data

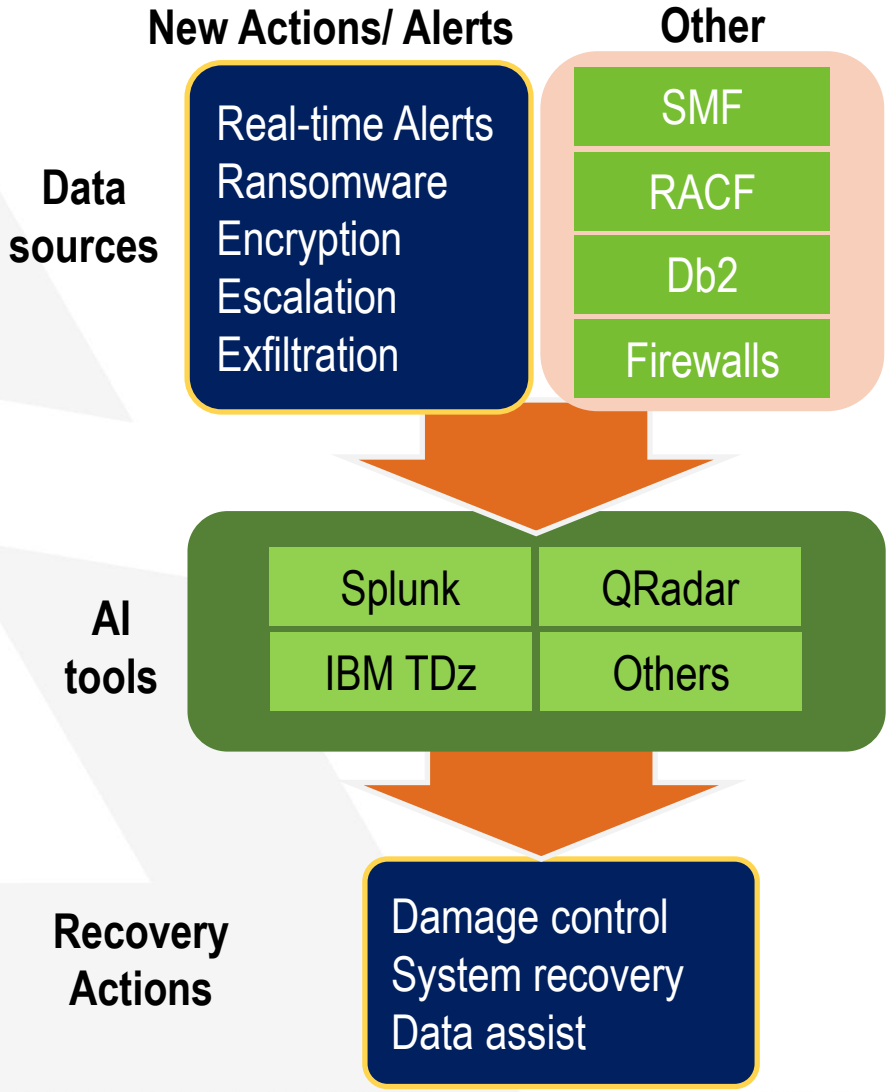
- SMF misses critical information due to incomplete detection
- Loading SMF to an offline processor is slow, therefore analysis delayed
- AI tools don't take needed actions – recovery, ransomware removal on z/OS

Better tools can:

- Detect authority tampering, rogue encryption, ransomware insertion, 40 others
- Improve clarity of suspicious actions before attack
- Send real-time alerts for reaction in milliseconds not hours
- Take Action - Damage control, countermeasures, suspend/resume
- Provide recovery assist for fasted more precise restore

Customer value:

- Timely and precise security processes that prevent outages
- Customer specific recovery processes imbedded in UI
- Better info + AI = compliance with ZeroTrust, NIST, DORA, PCI, ISO …



Network Vigilance

Endpoint monitoring – 7/24 (inboard)
- Discover z/OS attached networks
- Learn what is normal for transfer jobs and device behavior
- Alert or kill nodes with abnormal usage patterns

Data Breach Protection
- Detect data transfers exceeding thresholds
- Monitor TSO, batch, FTP, SSH, IND$FILE
- Disallow secondary links in TSO

Stop Attack Instantly
- Real-time suspend of offending data transfers
- Improved network knowledge & investigation tools
- Revoke offending user IDs to lock out other attacks

NIST, DORA, PCI, ZeroTrust …

SHARE
EDUCATE • NETWORK • INFLUENCE

End-to-End, Multi-Vendor, GUI-based Solution

Identify

Asset Management
Business Environment
Risk Management
Strategy, Recovery Plan

- New Information Sources
- Security Info Sharing
- Imbedded Recovery Plan
- Compliance Reporting

Protect

Access Control
Data Security
Info Protection Processes
Protective Technology

- Monitor Network Endpoints
- File Integrity Monitoring
- Learn Approved Changes
- AI Integration
- Behavior Changes

Detect

Anomaly & Event Security
Continuous Monitoring
Detection Processes
Alert processing

- Data Exfiltration
- Encryption Detection
- Authorization Escalation
- Countermeasures
- Anomaly Scans

Respond

Response Planning
Communication
Analysis
Mitigate / Improve

- Immediate Damage Control
- Real-time Alerts
- What / When Attacked
- GUI-based Investigation
- Integrated Cyber Plan

Recover

Recovery Plan
Improvement
Communication

- Ransomware removal
- Automated System Recovery
- Immutable Backup Recovery
- Verify Restore Trusted State
- Faster / Precise Recovery

Governance

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

Mainframe Under Siege
Real-Time Threat Interception and Automated Recovery
TECH_180s2

2½ min game changer

Detect / Stop encryption attack in under 1 sec

https://media.maintegrity.com/news-media/demos/csf-mainframe-encryption-detection-demo

MainTegrity CSF can do the same for:

- Data Exfiltration
- z/OS authority / security tampering
- Ransomware removal and recovery

Key differentiators:

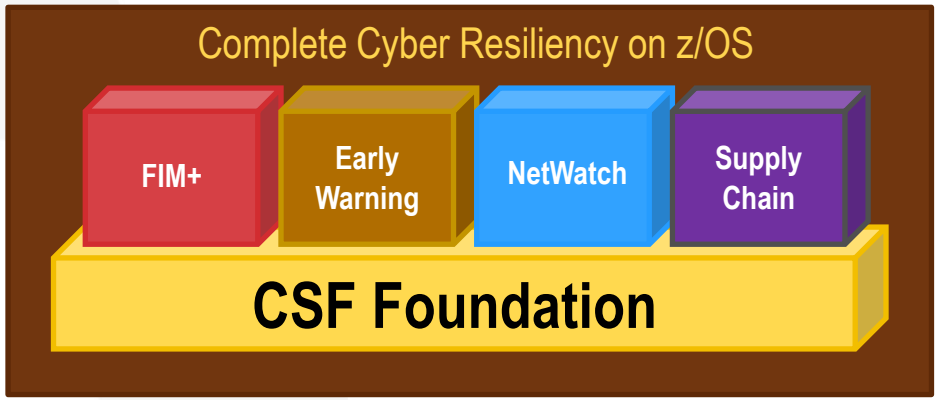
- Learn what is normal to detect what is abnormal
- Stop damage immediately, so people have time to react precisely

MainTegrity CSF

Supports prevention and recovery in automated manner (guides support staff)

Provides features no other mainframe product can:

- Discover and remove ransomware with CSF
- Intercept / suspend malicious encryption in seconds
- Fight data exfiltration - detect / stop malevolent data transfers
- Freeze offending actors to mitigate damage and reduce human reaction time
- Respond to attacks with GUI-driven end-to-end cyber resiliency process
- Surgical recovery for compromised software, parms, etc.
- Restore from IBM SGC, Dell or HV snapshots, or conventional
- Comply with DORA, PCI, HIPPA, NIST, FISMA, ZeroTrust, etc.
- Send real-time alerts with automate actions to assist support staff
- Integrate with ServiceNow, Splunk, Rocket, Vertali, IBM, Dell, Hitachi, BMC ...



Mainframes aren't immune to hacks

Can you risk doing nothing?