

IBM STORAGE FOR DATA RESILIENCE - IBM STORAGE DEFENDER



James Rose
UKI Sales Manager - IBM Storage Technologies
jamesros@uk.ibm.com

IBM Storage Defender

Today's relevance

- Data Protection & Cyber Security MUST be foundational capabilities in any organisation
- New Regulations coming into effect for Operational Resiliency
- Cyber Recovery probability is higher than Disaster Recovery
- Ransomware is big business
- Cyber Attacks YTY is growth is HUGE
- 17% of Cyber Attacks are Ransomware (and that's growing too)
- Every 11s a Ransomware attack is launched (Arctic Wolf website)
- 21% dormant threats, up from 5% YTY
- Average cost of an Attack is rising exponentially
- But you already know this



Tox



Tox
toxicola7qwv37qj.onion

FOR SALE


Ransomware as a Service. The menace!


Contact tox@sigaint.org and make an offer: BeforeCrypt.com

- Platform + virus;
- Platform + virus + database + toxicola7qwv37qj.onion private key.

I'm talking about source code and documentation, you'll have to set up your own server.

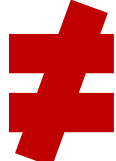
Cyber recovery is very different from Disaster recovery



Category	Disaster Recovery	Cyber Recovery
Recovery Point	Known Point in time	Not known...yet
Recovery Time	RPO/RTO	Trusted and Verified first
Nature of Disaster	Flood, power outage, weather	Targeted
Impact of Disaster	Regional	Global
Recovery	Failback	Based on situation
Data to Recover	Known	Unknown
Topology	Connected Data Centers	Isolated and away from production
Data Volume	Comprehensive, all data	Super selective
Probability	Low	High 

Data Resilient solutions need to cover BOTH

Is YOUR Business Resilient?



Predict attacks
Cyber attack prevention
Respond to Cyber Attacks

Minimize/eliminate downtime
Protect from infrastructure failures
Avoid data loss from disasters

Immutable data copies
Malware scanning
Business Recovery

IBM Cyber Resiliency Assessment
Understand your BLIND SPOTS

Capability Steps to Data Resilience



AUTOMATION

Simplified operations plus ability to test and prove recoverability
Integration between Cyber Security & Cyber Resiliency



RECOVERY

Rapid business recovery in minutes to hours
Avoid paying ransomware



DISCOVERY

Understand when defences have been compromised
Malware scanner and data pattern insights



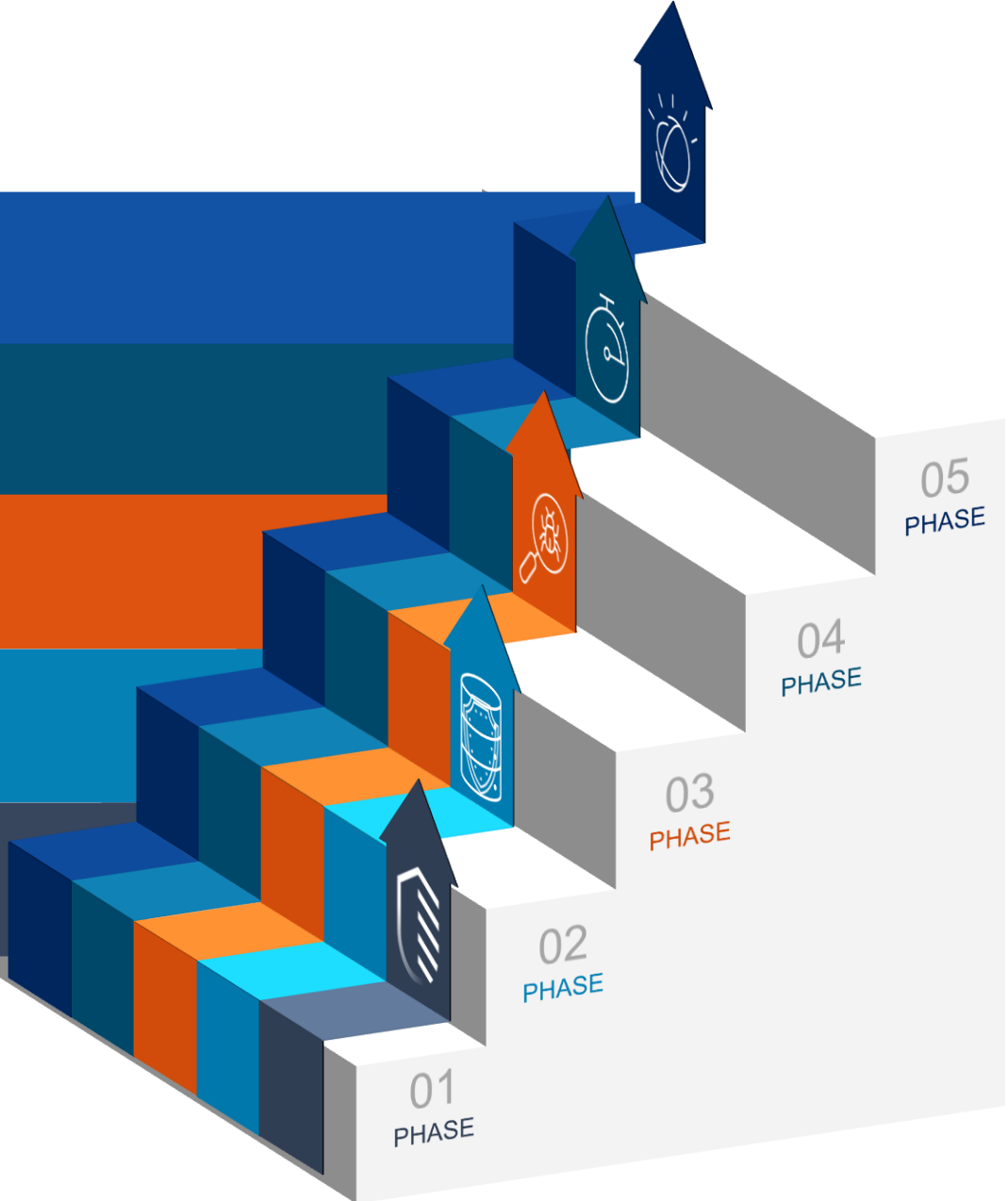
IMMUTABILITY

Recoverable data points
Incorruptible, data can not be deleted



FOUNDATIONAL SECURITY & DATA PROTECTION

Predict, prevent, and respond. SIEM and SOAR implementation.
Protect from infrastructure failures and natural disasters



So why is IBM uniquely positioned ?

- We are a technology company that designs & manufactures its own hardware technologies.
- We are a technology company that codes, designs and supports its own software portfolio.
- We are a technology company that's been helping the world largest organisations protect themselves against cyber threats for decades (before it become fashionable).
- We are a technology company that knows how to integrate both software & hardware.
- We've been doing it a while.
- The technologies we develop and have patented for those large organisations are across our entire range of technologies.
- Its not just the largest banks in the world or government departments we talk to

Just for Big Business?

Started 158 years ago with a horse & cart.



Most likely ended in June 23 by a kid in his parent's basement wearing his pyjamas.

NEWS

Home | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture

England | Local News | Regions | Northamptonshire

Kettering logistics firm enters administration with 730 jobs lost

26 September



KNIGHTS OF OLD/FACEBOOK

Kettering-based Knights of Old was founded in 1865

By Kris Holland

BBC News, Northamptonshire

A logistics and training firm targeted by a "significant" cyber attack has entered administration.

Kettering-based KNP Logistics Group was the parent company of the 158-year-old haulage firm Knights of Old.

It suffered a major ransomware attack in June which affected key systems, processes and financial information.

Minimum Viable Company

Data Resiliency in Depth

Full Company Recovery

Workloads that are costing the business money every second/minute/hour they are non-operational

All workloads including non-critical workloads for back-office etc.

Primary
Workloads

Corruption Discovery
Mins/Hrs/days

Recovery Time
Mins/Hrs/days

Data Retention
Days/weeks/months

Storage Medium
On Array/Off array

Secondary
Workloads

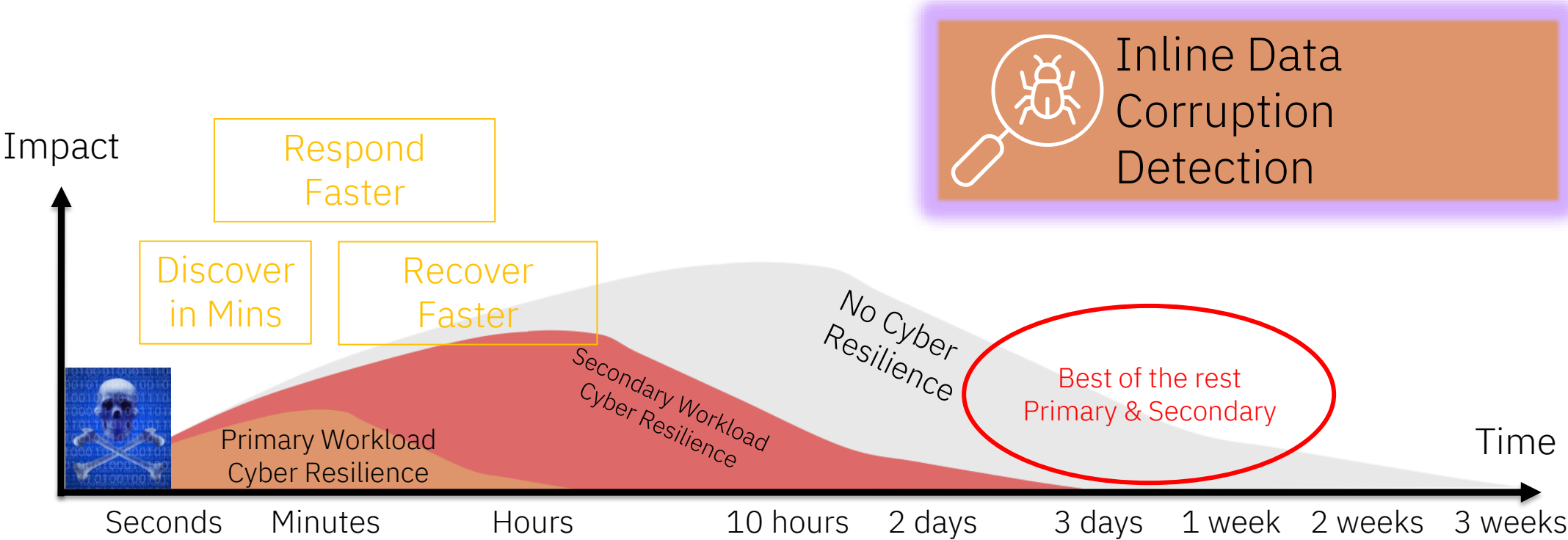
What do we mean by minimal viable company?

- All apps are not born the same.
- What applications are essential to allow your organisation to continue to function?
- Do you have the same policy for recovery should you need to recover data (in the event of something like a ransomware attack)?
- Have you ever calculated how long it will take to restore the critical applications data?



Minimize Your Business Exposure from a Cyber Attack

Minimum Viable Company Recovery – Primary Workloads

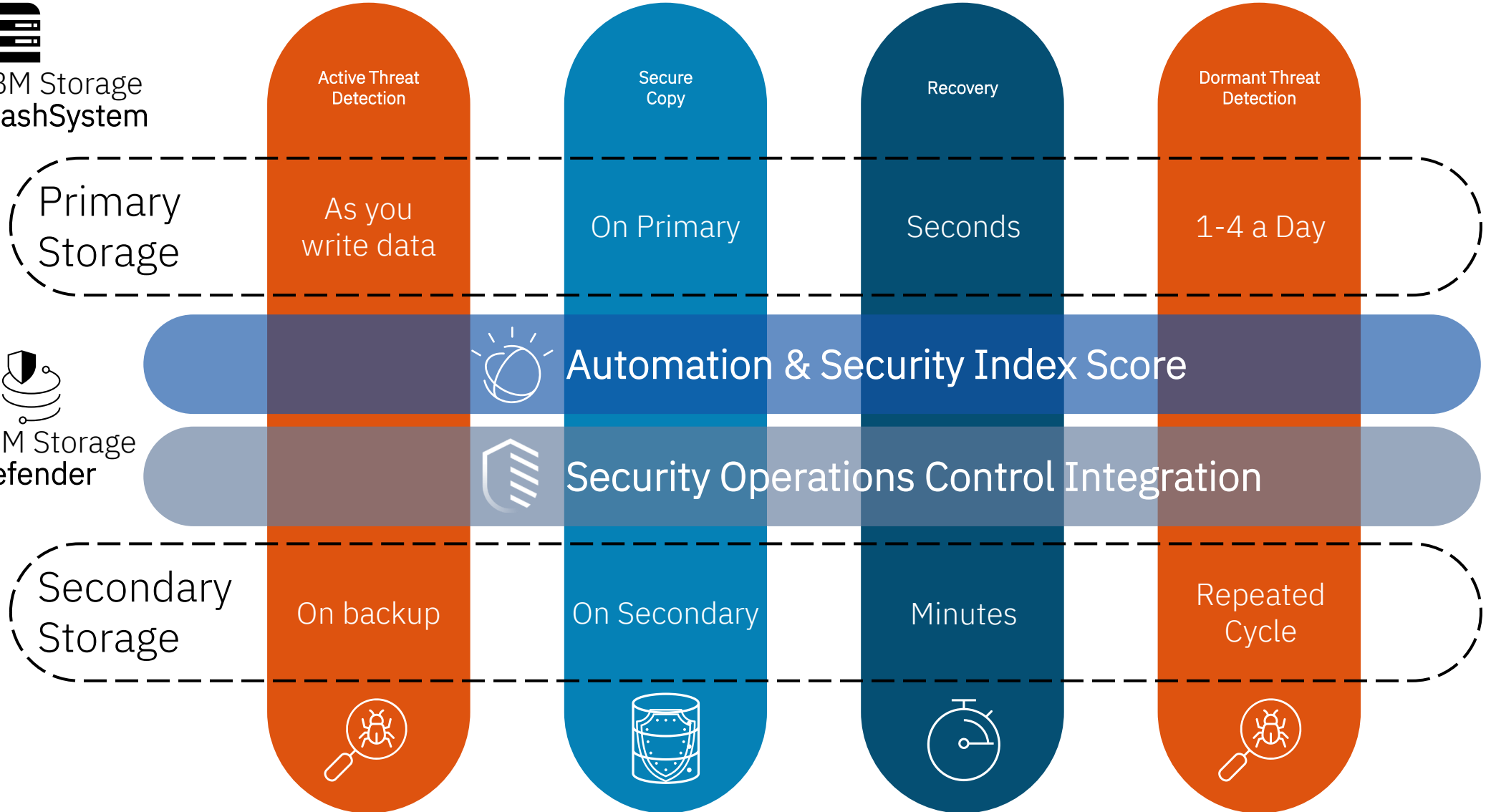


Primary Workloads
Discovery in minutes, contain the spread
Limit Workloads impacted
Recover FASTER

Prevent, Minimize impact, Recover Quickly



IBM Storage
FlashSystem



IBM Storage
Defender

Cyber Resiliency Foundations



- ✓ Capacity for your critical workloads
- ✓ Capacity for immutable copies
- ✓ Inline data corruption detection
- ✓ Integration into your own security monitoring tools
- ✓ IBM Defender Clean Room
- ✓ Could capacity (3rd copy?)
- ✓ 3 years full support with IBM

Your Cyber Resiliency 'Starter Pack'

~£20K₍₁₎

1) Set config, prices vary as capacities increase

IBM Storage for Data Resiliency Workflow

A hub which will assess the data security level from a storage perspective and provide an integrated solution to protect, detect, and recover from cyberattack



Early Threat Detection



Safe Recovery



SOC Integration

