HEALTHCARE RANSOMWARE IMPACT MAPPING PARTNER PLAYBOOK

For Technology Advisors, MSPs, and Healthcare Integrators

Help hospitals determine which systems, services, departments, and care environments are impacted during ransomware events so teams can prioritize response, reduce downtime confusion, and maintain patient care.

Partner opportunity snapshot

Ransomware response is one of the easiest healthcare conversations for partners to start because the pain is immediate. When hospital systems go down, teams need to know what is affected, which care services are disrupted, and what to restore first.

How WanAware helps

WanAware helps hospitals connect infrastructure, application, identity, and operational records into a connected relationship map so teams can quickly see what systems, services, and care environments are affected during downtime events.

What the first engagement actually looks like

Partners do not need to start with a full ransomware program or enterprise-wide continuity initiative.

Most first engagements begin with:

- One high-priority care service
- One clinical department
- One operational environment
- One downtime scenario
- One ransomware response workflow

The initial engagement helps the client:

- Identify impacted systems
- Map which services or care areas depend on those systems
- Determine what remains operational

- Clarify what must be restored first
- Create a practical next-step roadmap

This gives partners a clear first motion: run a focused impact-readiness assessment, show the impacted-system and care-service map, and deliver a practical findings report.

The operational pain

During a ransomware event, hospitals need fast answers:

- What systems are affected?
- Which departments or care services are disrupted?
- What systems are still working?
- Which services must be restored first?
- Where could disruption spread next?
- Who needs to coordinate the response?

For partners, this creates a focused first engagement that can be delivered as an assessment before expanding into broader continuity, dependency mapping, segmentation, or managed services.

Ideal customer

- Hospitals and health systems
- Downtime or ransomware concerns
- Complex clinical environments
- Manual response coordination
- Patient-care continuity pressure

Ransomware Impact Mapping Assessment

- Pick one care service or environment
- Review the response workflow
- Map impacted systems and dependencies
- Identify restoration priorities
- Create next-step roadmap

Expansion opportunity

- Response roadmap follow-on
- Dependency mapping
- Restoration prioritization support
- Segmentation planning
- Continuity planning services

Why ransomware response visibility is difficult today

The operational problem is simple: when ransomware disrupts hospital operations, teams need to know what is affected and what must be restored first.

Ransomware events are different from recalls or vulnerability alerts because disruption can spread across multiple operational and clinical systems at the same time.

A ransomware event may affect:

- Medical devices
- EHR systems
- Imaging
- Scheduling
- Communications
- Pharmacy
- Billing
- Identity systems
- Network operations

Hospitals may know which systems they own, but quickly understanding what is offline, what services are disrupted, and what must be prioritized first is often far more difficult.

During a ransomware event, teams need to connect systems, services, workflows, dependencies, and care impact across the healthcare environment.

Common operational challenges

- Software and firmware tracking gaps
- Unsupported systems still in operation
- Disconnected security and operational records
- Patch limitations on clinical systems
- Manual validation across teams
- Slow leadership updates
- Unclear next steps after the affected systems are found

Why traditional tracking systems struggle

Many hospital systems were built to manage:

- Equipment
- Applications
- Departments
- Procurement
- Maintenance

Ransomware events create broader operational disruption across:

- Connected devices
- Applications
- Shared infrastructure
- Identity systems
- Network segments

Clinical workflows

- Modern ransomware response often requires:
- Impacted-system identification
- Application dependencies
- Identity dependencies
- Clinical workflow dependencies
- Segmentation context
- Continuity planning

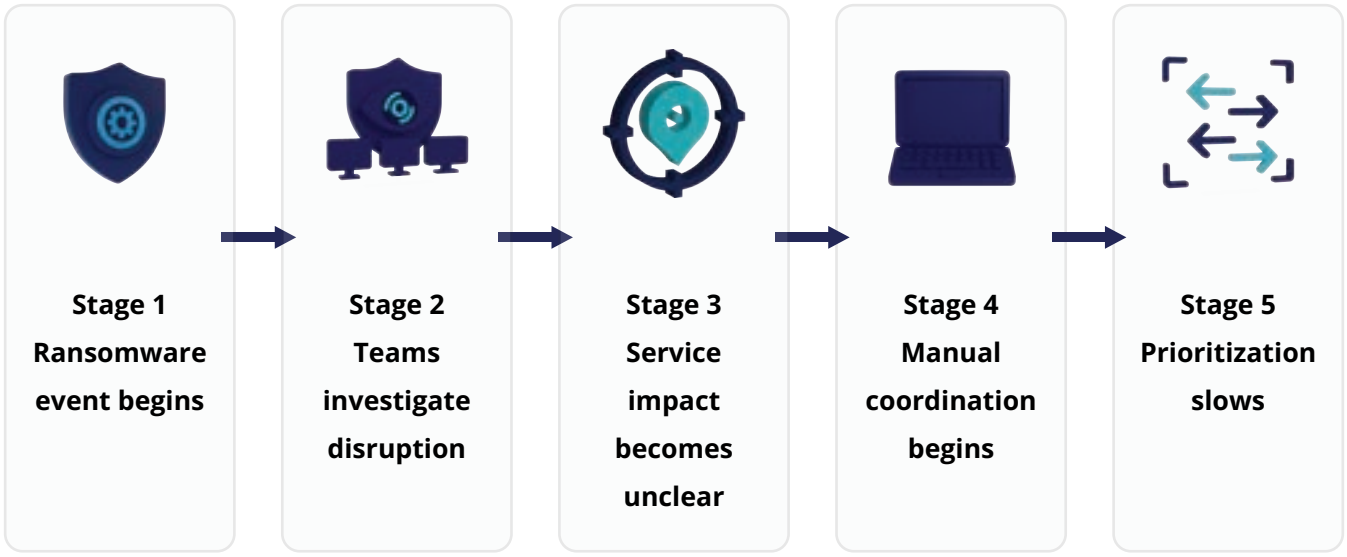
Fragmented vs connected downtime response

Fragmented vulnerability response	Connected vulnerability response
Show disconnected inputs: • FDA or manufacturer alerts • CISA advisories • Security tools • Inventory systems • Firmware records • Vendor patch information • Clinical engineering records	Show WanAware helping connect: • Affected systems • Software and firmware versions • Patchability • Segmentation needs • Unsupported systems • Operational impact • Modernization priorities

What ransomware response looks like in practice

Partners should listen for this pattern when hospitals describe how they manage ransomware disruption today.

Ransomware response workflow



Teams often spend valuable time coordinating across disconnected systems while trying to determine what is affected and what must be restored first.

Common customer pain signals

Partners should listen for statements like:

- "We don't know what systems are affected."
- "We don't know what must be restored first."
- "Clinical teams are reporting outages."
- "We're checking systems manually."
- "We can't determine patient-care impact fast enough."
- "Leadership needs immediate answers."
- "We know the system is down, but not what depends on it."
- "We need to brief leadership before we have clean answers."
- "Restoration priorities are being debated during the event."

These often indicate broader dependency, continuity, coordination, and prioritization gaps.

Client pain signals and service opportunities

What the client says	What it often means	Service opportunity
"We don't know what systems are affected."	Weak impacted-system identification	Ransomware impact mapping
"Clinical teams are reporting outages."	Care-service dependencies are unclear	Dependency mapping
"We're checking systems manually."	Fragmented response workflows	Response workflow consolidation
"We can't determine patient-care impact fast enough."	Weak care-service impact context	Care-service impact mapping
"Leadership needs immediate answers."	Downtime and continuity pressure	Ransomware impact readiness

Questions partners should ask healthcare clients

Primary discovery question

"When ransomware disrupts healthcare operations, how do you determine what is affected, which patient-care services are disrupted, and what must be restored first?"

Partner conversation starter

How to position the service

"Many hospitals have cybersecurity tools and backup plans, but still struggle to answer a practical question during downtime: what is affected, which care services are disrupted, and what should be restored first? We can start with one care service, department, or downtime scenario and help map the systems, dependencies, and restoration priorities."

Good entry points

- After a recent downtime or ransomware event
- During cyber readiness planning
- When leadership is asking about operational continuity
- When IT and clinical teams are manually coordinating response
- When the hospital is reviewing segmentation or recovery priorities

The first engagement includes

- One care service, department, or downtime scenario
- One discovery workshop
- One dependency and impact review
- One findings report
- One next-step roadmap

Discovery and qualification checklist

Discovery Questions

- How do you currently determine ransomware impact?
- Which teams and systems are involved?
- Can you quickly identify impacted systems and services?
- Do you know which care services depend on those systems?
- How do you prioritize restoration?
- What did your last downtime event reveal?
- How much of this process is manual?

Strong Fit Indicators

- Manual impact investigation
- Limited dependency awareness
- Unclear restoration priorities
- Fragmented response workflows
- Care-service disruption concerns
- Slow leadership updates
- Continuity planning pressure

Common objections and responses

Use objections to uncover deeper response and coordination gaps.

Objection-handling guide

Client question or objection	Better response	Follow-up question
"We already have cybersecurity tools."	Many hospitals do. The challenge is often understanding which systems, services, and patient-care environments are actually disrupted.	Can your team quickly determine which clinical services are impacted during downtime?
"We already have backups."	Backups matter, but response speed also depends on knowing what systems and services need to be restored first.	How clearly can your team prioritize restoration across mission-critical services?
"We already track inventory."	Inventory helps, but ransomware events require system, service, dependency, and care-impact context.	Do you know which workflows depend on your highest-risk systems?
"This sounds overwhelming."	The goal is to start small, often with one care service, one department, or one downtime scenario.	Would it help to focus first on one high-priority environment?
"We can't overhaul everything."	Exactly. The first step is not an overhaul. It is a focused assessment that identifies what is affected, what depends on it, and what should be prioritized next.	Do you know which systems create the greatest downtime risk today?

Recommended first engagement

Ransomware Impact Mapping Assessment

The best first project is a focused Ransomware Impact Mapping Assessment for one care service, one clinical department, one operational environment, or one downtime scenario.

This gives healthcare clients a practical way to evaluate how they identify impacted systems, understand care-service disruption, and prioritize restoration without starting a large cybersecurity or continuity transformation project.

Section 1
Stakeholders

- Security teams
- IT operations
- Infrastructure teams
- Clinical Engineering
- Operational leadership
- Continuity leaders

Section 2
Assessment Scope

- Impacted-system identification
- Care-service dependencies
- Systems still operational
- Restoration priorities
- Manual response steps
- Coordination gaps

Section 3
Deliverables

- Impact map
- Dependency findings
- Restoration priorities
- Coordination risks
- Next-step roadmap

Section 4
Customer Outcomes

- Faster impact identification
- Clearer care-service disruption view
- Reduced downtime confusion
- Better restoration prioritization
- Practical next-step plan

Example customer deliverables

Impacted-system relationship map
Shows which systems, applications, and care environments are affected during downtime.

Care-service dependency map
Shows which patient-care services rely on affected systems.

Restoration priority worksheet
Helps teams determine what should be restored first.

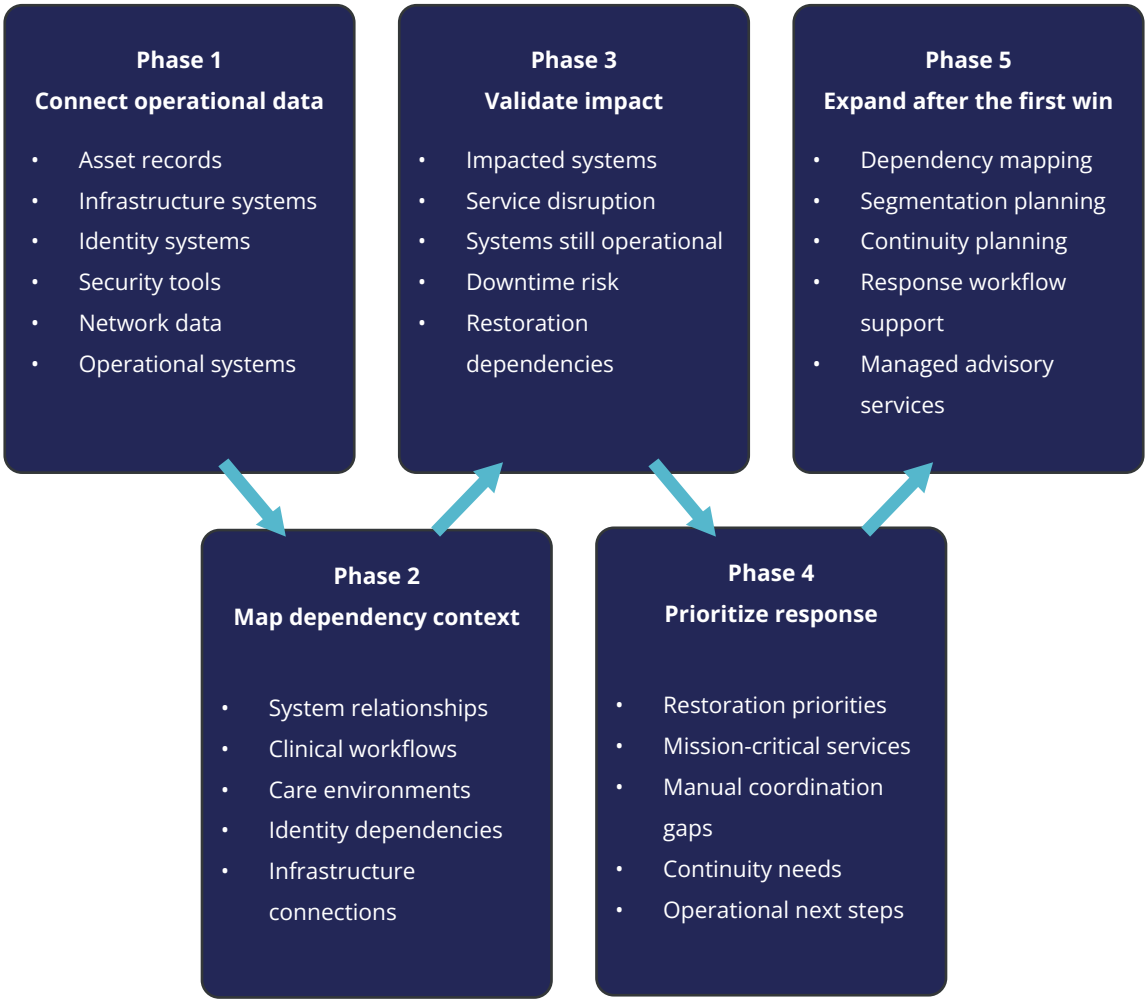
Downtime coordination findings
Highlights manual coordination bottlenecks and operational risks.

Executive summary and next-step roadmap
Summarizes findings, priorities, and recommended next actions.

How WanAware supports ransomware response visibility

WanAware helps partners connect the information healthcare teams need during ransomware events.

Instead of forcing hospitals to replace existing systems, WanAware helps teams quickly connect impacted systems, operational dependencies, care-service relationships, systems still working, and restoration priorities.



Why this is partner-friendly

WanAware supports a no rip-and-replace approach.

Partners can start with one care service, one environment, or one downtime scenario. The first service does not need to be positioned as a full ransomware program. It can be positioned as a focused assessment that produces three concrete outputs:

- Impacted-system and care-service map
- Restoration priority findings
- Next-step roadmap

That makes the first conversation easier, the first project smaller, and the expansion path more natural after the customer sees value.

Why WanAware is different

WanAware is built for operational healthcare environments where infrastructure, application, identity, operational, and dependency information exists across disconnected systems.

WanAware differentiators

Differentiator	Why it matters for ransomware response
Agentless deployment	Supports visibility across connected healthcare environments without disrupting operations.
Schemaless architecture	Helps connect operational, infrastructure, and security data from varied systems.
Relationship graph	Shows how systems, services, workflows, and dependencies relate.
Response prioritization context	Shows which impacted systems and services matter most during disruption.
No rip and replace	Works with existing healthcare infrastructure and operational systems.

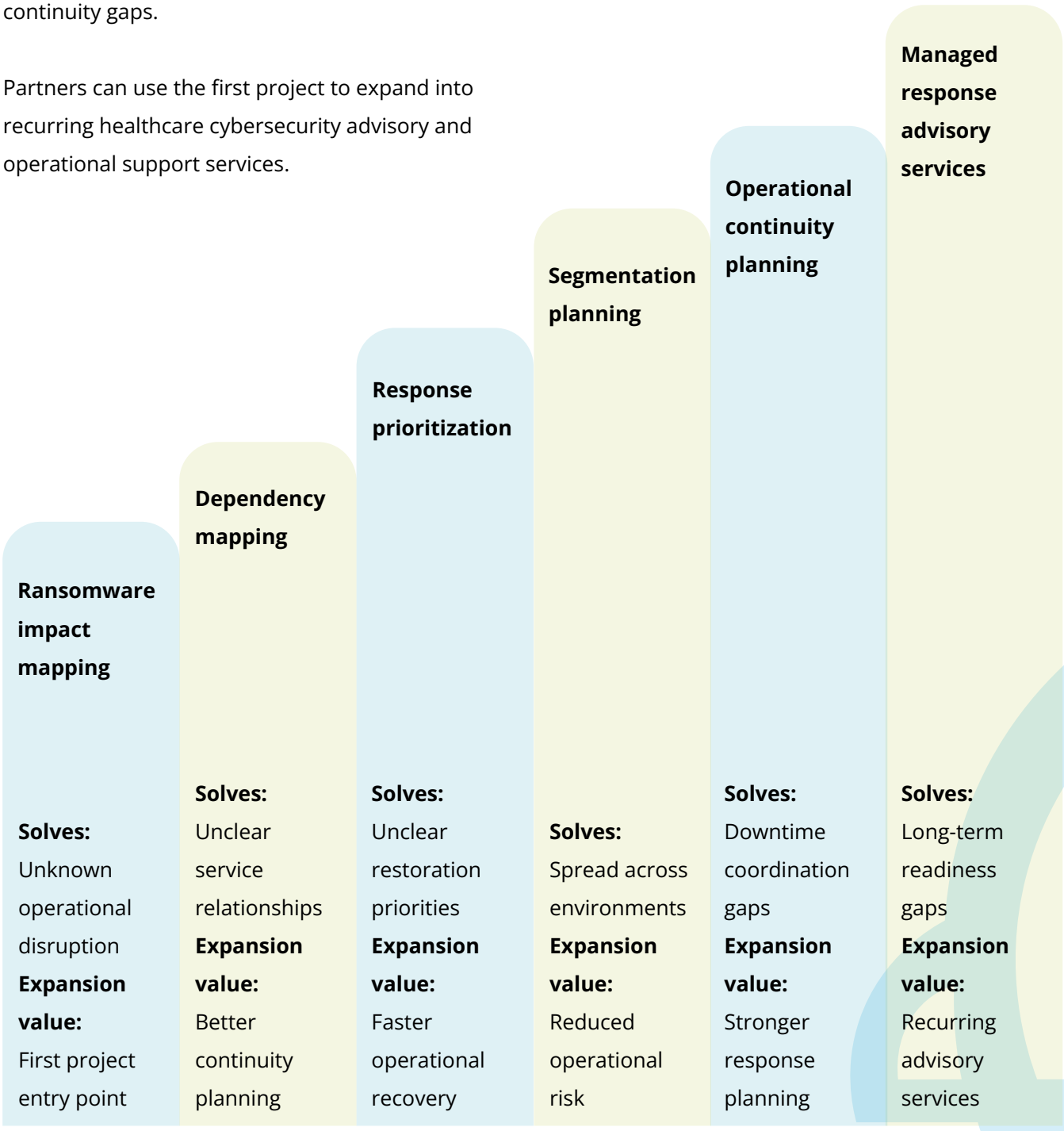
Healthcare organizations need more than outage alerts. They need connected operational context that helps teams prioritize restoration and continuity decisions.

Expansion roadmap

Do not lead with these services in the first conversation. Lead with the urgent question: what is affected and what must be restored first?

After the first assessment, a ransomware event often reveals broader dependency, segmentation, and continuity gaps.

Partners can use the first project to expand into recurring healthcare cybersecurity advisory and operational support services.



Expansion message for partners

Start with one ransomware response problem. Show the customer what is affected and what must be restored first. Deliver the findings and next-step roadmap. Then expand into dependency mapping, segmentation planning, continuity planning, and recurring advisory services only after the customer sees the first win.

White-labeled service opportunities

WanAware gives partners a way to package ransomware response and continuity services under their own brand.

- **Ransomware impact mapping**
- **Care-service dependency mapping**
- **Restoration prioritization support**
- **Segmentation planning services**
- **Continuity planning**
- **Response workflow advisory**
- **Managed response advisory services**

Why this creates recurring revenue

Ransomware readiness is not a one-time project.

Operational environments change, dependencies shift, restoration priorities evolve, and continuity plans need updates.

That creates a natural path into recurring dependency mapping, response workflow advisory, segmentation planning, and continuity support services.

Quick-start delivery motion

Use this 30-day motion to make the first service feel easy to sell and easy to deliver.

The motion is intentionally contained:

- One care service, clinical department, or downtime scenario
- One discovery workshop
- One dependency and impact review
- One findings report
- One roadmap for next steps

Week 1	Week 2	Week 3	Week 4
Discovery workshop • Ransomware response workflow review • Stakeholder identification • Current systems review • Downtime examples	**Dependency and impact review** • System review • Dependency identification • Care-service mapping • Manual coordination review	**Ransomware impact assessment** • Impact validation • Restoration priority review • Continuity needs • Coordination gaps	**Findings and roadmap** • Impact mapping findings • Restoration priority findings • Workflow recommendations • Priority next steps • Optional follow-on service opportunities

Already a WanAware partner?

Use this playbook to start healthcare ransomware response visibility conversations and identify first-project opportunities.

Not yet a partner?

Become a WanAware Partner to deliver ransomware impact mapping, restoration prioritization, dependency mapping, and continuity planning services for healthcare clients.

Become a Partner

www.wanaware.com