IstroSec

# GRYPHON CASE STUDY: PREVENTION STOPPING RANSOMWARE BEFORE IT DETONATES

**Date:** 14/06/2026

# TABLE OF CONTENTS

# ORGANIZATION AT A GLANCE

*Illustrative scenario. "**Example Health**" is a fictional composite created to demonstrate documented GRYPHON capabilities; it is not a real customer. The attack chain is representative of the common healthcare ransomware tradecraft. Every product capability referenced is part of GRYPHON's published feature set.*

| Attribute | Detail |
|---|---|
| **Organization** | Example Health — regional non-profit health system (fictional) |
| **Footprint** | 6 facilities: 1 acute-care hospital, 5 outpatient and specialty clinics |
| **Endpoints** | Approximately 3,200 Windows endpoints across clinical, administrative and OT zones |
| **Estate mix** | Windows 11 clinical workstations and Windows Server; legacy Windows 7 SP1 / Server 2008 R2 on imaging consoles (CT/MRI), lab analyzers, and pharmacy/POS terminals |
| **Incumbent tooling** | Microsoft Defender for Endpoint as primary EDR; on-premises EHR |
| **GRYPHON role** | Behavioral ransomware defense and IR console layered across the estate, including legacy and OT systems the incumbent EDR cannot cover |

# THE PROBLEM FACING US MEDICAL ORGANIZATIONS

Healthcare is the most expensive industry in the world to breach and has been for fourteen consecutive years. The average cost per incident stands at US$7.42 million, against a US national average of US$10.22 million, with healthcare breaches taking around 279 days to identify and contain.[1] For a provider, a ransomware event is not only a financial loss; it is a clinical safety event. Encrypted imaging consoles, downed EHR access, and offline lab analyzers translate directly into diverted ambulances, delayed procedures, and manual charting.

The regulatory exposure is equally concrete. Under the HIPAA Breach Notification Rule, a breach of unsecured protected health information affecting 500 or more individuals must be reported to the HHS Office for Civil Rights within 60 days of discovery, is published on the HHS public breach portal, and triggers an OCR compliance review.[2] The decisive question for a health system is therefore not only "did we detect it?" but "did patient data actually get encrypted or exfiltrated — and can we prove it?"

**Example Health** faced a structural gap shared by most US providers: its modern EDR could not be installed on the legacy OS  Windows 7 and Server 2008 R2 systems running its imaging modalities, lab analyzers and pharmacy terminals. Those certified, frozen, often air-gapped machines hold, and process patient data yet sat outside the EDR's coverage — precisely the soft targets of ransomware operators look for.

# WHY EXAMPLE HEALTH DEPLOYED GRYPHON AHEAD OF TIME

GRYPHON is an agent-based defense and incident response toolkit that complements EDR/XDR rather than replacing it.[3] **Example Health** added it as a second, behavior-based layer with four properties that mattered for a clinical environment:

- **Protection without cloud dependency.** Both detection engines, kernel-level rule evaluation, backup (VSS) protection, autonomous recovery, and anti-malware scanning run on the endpoint. An air-gapped imaging station that never talks to a cloud remains fully protected, and the on-premises console option keeps the management plane inside the hospital's own walls.
- **A second engine that does not rely on signatures.** GRYPHON's behavioral ransomware engine recognizes the operational fingerprint of encryption in progress rather than a known hash — important against the novel and rebranded strains that signature feeds lag by days.
    - **Recovery the attacker cannot delete it first.** Kernel-level backup (Volume Shadow Copy) protection plus automatic backup (VSS) creation gives the system recovery points that ransomware's opening move — deleting backups — cannot be removed.

Deployment was routine: the single **IstroSetup.msi** agent was pushed by GPO and Intune across the modern estate and installed on the systems through standard change control, each registering to the console with an install key. Defender stayed in place; GRYPHON ran alongside it and ingested Defender's own detections into the same console.

# THE ATTACK — AND WHERE GRYPHON INTERVENED

Eight months after deployment, a billing coordinator opened a spear-phishing attachment. The sequence that followed unfolded over roughly forty minutes. At each stage, a specific GRYPHON control fired.

| Step | Stage | What happened and how GRYPHON responded |
|---|---|---|
| 1 | **Initial execution** | A malicious PowerShell loader was launched from the phishing attachment. GRYPHON's integrated anti-malware engine inspected the script through the Windows Antimalware Scan Interface (AMSI) and raised a **MaliciousScriptDetected** alert; while the behavioral Policy engine flagged the spawning pattern. The payload was quarantined rather than merely blocked, preserving its SHA256 and path for later review. |
| 2 | **Living-off-the-land evasion** | The loader pivoted to native Windows binaries (certutil, rundll32 and the PowerShell family) to stay below signature radar. **Example Health** ran GRYPHON's LOLBIN blocking at the **Ransomware level**, halted the most heavily abused binaries outright, each generating a **LolbinUsed** alert that reasoned parent process and command line, not just the binary name. |
| 3 | **Credential access** | The intruder attempted to dump LSASS to harvest domain credentials. GRYPHON's LSASS Protection revoked access at kernel level; the dump attempt outside Windows Error Reporting raised a **MinidumpCreated** alert with automatically elevated severity. A parallel remote DLL-injection attempt surfaced as a **ThreadInjected** alert. |

| Step | Stage | What happened and how GRYPHON responded |
|---|---|---|
| 4 | **Lateral movement** | With partial credentials, the attacker tried to reach the legacy OT segment over SMB. Three independent controls engaged: **Local Admin Share Protection**, **Remote Execute Protection**, blocked remote access and remote-path execution, and GRYPHON's process-aware firewall enforced a single role-scoped rule blocking unsigned outbound SMB on port 445 not originating from a signed Microsoft binary – across the workstation role. **Lateral Movement Protection** raised the corresponding alerts. |
| 5 | **Backup deletion attempt** | On the one workstation where execution briefly persisted, the malware attempted to delete all backups. GRYPHON blocked this at kernel level: the command failed; recovery infrastructure stayed intact, and a tamper (**VssTamperingDetected**) alert fired. The attacker's standard precondition for irreversible encryption never landed. |
| 6 | **Encryption — stopped mid-stream** | The payload began mass file operations characteristic of encryption. GRYPHON's behavioral engine converged on a ransomware verdict from live behavior (suspicious bulk file writes, double-extension creation, crypto-API usage), raised **RansomwareDetected**, and killed the process. The handful of files altered before the kill were automatically restored from protected shadow copies, on the endpoint, without invoking any external backup system. |

# OUTCOME

| Measure | Result |
|---|---|
| **Spread** | Contained to a single workstation; OT, imaging and lab segments untouched |
| **Encryption** | Stopped mid-stream; the few files touched were automatically restored from protected backups (VSS) |
| **Backup integrity** | Deletion blocked at kernel level — recovery points fully preserved |
| **Clinical operations** | No EHR, imaging or lab downtime; no ambulance diversion |
| **Patient data impact** | No evidence of data (PHI) encryption or exfiltration — no 500-individual HHS-reportable breach |
| **Evidence** | Full alert timeline, process tree and quarantined sample retained in the IR console |

Because GRYPHON stopped the chain before patient data was encrypted or stolen, the event did not meet the threshold for a 500-individual OCR-reportable breach, and the security team had a forensically useful, time-stamped record of exactly what happened — the artefact OCR and counsel ask for first.

# HOW EACH CAPABILITY CONTRIBUTED

| GRYPHON capability | Role in this defense |
|---|---|
| **AMSI script inspection and integrated anti-malware quarantine** | Caught and isolated the PowerShell loader at execution |
| **LOLBIN blocking at ransomware level** | Blocked abuse of native Windows binaries used for evasion |
| **LSASS Protection / MinidumpCreated / ThreadInjected** | Defeated credential dumping and thread injection |
| **Admin-share, remote-execute and lateral-movement protection plus process-aware firewall** | Stopped movement toward the legacy OT segment |
| **Kernel-level backup protection (VSSTamperingDetected)** | Preserved recovery points by blocking backup (shadow-copy) deletion |
| **Behavioral ransomware engine (ransomwareDetected) and autonomous file recovery** | Killed the encryptor and rolled back the files it touched |
| **Legacy and OT platform support, no cloud dependency** | Extended all protections to imaging, lab and pharmacy systems the EDR could not cover |

# WHY IT MATTERED FOR A MEDICAL ORGANIZATION

Organizations that contain incidents faster and operate a tested incident response capability avoid a substantial share of breach cost. A tested IR plan is associated with roughly US$2.66 million in savings per breach. For **Example, Health,** the value was simpler to state: the attack was neutralized on a single endpoint, no patient-care system went dark, and no patient data (PHI) crossed the line that starts the 60-day OCR notification clock.

> ***Prevention here was not an abstraction. It was the difference between an internal security alert and a public breach-portal entry.***

[1]IBM, Cost of a Data Breach Report 2025: healthcare ranked the highest-cost sector for the 14th consecutive year at a US$7.42M average; US organisations averaged US$10.22M; healthcare breaches averaged 279 days to identify and contain. Reported by IBM and secondary coverage (hipaajournal.com, ibm.com/think).

[2]HIPAA Breach Notification Rule (45 CFR §§164.400–414), enforced by the HHS Office for Civil Rights: breaches of unsecured PHI affecting 500+ individuals must be reported to HHS OCR without unreasonable delay and no later than 60 calendar days from discovery, are published on the HHS public breach portal, and trigger an OCR compliance review (hhs.gov; hipaajournal.com).

[3]All GRYPHON capabilities described in this document are drawn from the published product feature set at gryphon.istrosec.com (Features, Incident Response, Advanced Defense, Zero Trust, Deployment, Integrations, and FAQ).