GRYPHON
SECURITY

Ransomware Preparedness Assessment

Clear Ransomware Risk Insight. Defensible Recovery Decisions.

A focused ransomware resilience assessment designed for organizations where operational continuity, sensitive data protection, and post-incident defensibility are non-negotiable.

Organizations across all sectors face significant ransomware risk. Modern environments concentrate high-value data, rely heavily on identity-driven access, and are frequent targets for extortion-based attacks. This service provides leadership with a clear, defensible understanding of the organization's ability to prevent, detect, respond to, and recover from ransomware using a structured, risk-based methodology.

What We Do

Gryphon Security conducts a structured ransomware preparedness assessment evaluating the administrative, technical, and operational safeguards that directly affect ransomware resilience.

The assessment combines a targeted review of ransomware-relevant NIST Cybersecurity Framework (CSF) controls with authorized hands-on technical testing of identity, endpoint, logging, and recovery defenses. Rather than applying generic enterprise checklists, we evaluate how controls function in real conditions, how identities are protected, how endpoints behave, how malicious activity would be detected, and how recovery would actually occur.

The result is an evidence-based evaluation of ransomware readiness, not a theoretical maturity score.

Why This Matters

Ransomware incidents create consequences beyond system downtime. Failures can expose sensitive data, disrupt critical operations, jeopardize insurance coverage, and place leadership decisions under scrutiny after the fact.

This assessment identifies where ransomware-specific risk truly exists, distinguishes material exposures from low-value findings, and equips leadership with a defensible basis for prevention, response, and recovery decisions before those decisions must be made under pressure.

Our Assessment Approach

This service uses a NIST-based ransomware methodology.

We apply nationally recognized security principles while deliberately avoiding compliance theater. This is not a certification, attestation, or regulatory audit. Instead, it is a focused risk evaluation supported by hands-on technical validation, designed to answer one core question:

“If ransomware occurs, can leadership demonstrate that preparedness, response, and recovery decisions were informed, reasonable, and defensible?”

Findings are contextualized to the organization’s size, staffing model, technology stack, and threat exposure so recommendations remain achievable and relevant.

What’s Evaluated

The assessment focuses on control areas most likely to fail during real ransomware incidents, including:

Identity & Access Protection
Authentication strength, MFA enforcement, privileged access, and user lifecycle controls

Endpoint, Logging & Detection
EDR coverage, logging visibility, alerting capability, and ransomware indicator detection

Backup & Recovery Readiness
Backup scope, immutability, restore testing, and recovery feasibility

Incident Response Capability
Response procedures, decision authority, communication workflows, and containment readiness

Data Protection
Protection of privileged and sensitive information before, during, and after an incident

Governance & Preparedness
Policies, roles, training, and leadership oversight affecting ransomware outcomes

Each area is evaluated against NIST CSF expectations and translated into clear, operational risk language.

What You Receive

At the conclusion of the engagement, clients receive a comprehensive Ransomware Preparedness Assessment Report, including:

- Executive-level ransomware readiness findings in plain English
- Risk-rated gaps (High / Medium / Low) tied to realistic attack scenarios
- Evidence-based recommendations grounded in observed conditions and testing results
- Screenshots and artifacts supporting each tested technique
- A prioritized Remediation Roadmap (30 / 60 / 90-day recommendations)

Reports are suitable for executive briefings, internal remediation planning, and compliance or audit support.

Who This Service Is Designed For

This service is designed for:

- Organizations with material ransomware exposure
- Environments dependent on identity, endpoint, and cloud services
- Organizations preparing for insurance renewal or third-party risk reviews

This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance assessment
- Organizations looking for managed SOC services or tool resale
- Environments without leadership commitment to remediation and risk ownership

Gryphon Security focuses on clarity, independence, and defensible outcomes.

Why Gryphon Security

- **Real-World Tradecraft:** Testing reflects active adversary behavior
- **Defensible Reporting:** Clear, evidence-based reports for executives and technical teams
- **Risk-Focused Execution**: Emphasis on outcomes that affect ransomware impact
- **Independent & Vendor-Neutral**: No resale pressure, no product bias

Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm scope and technical testing boundaries
- Discuss key risk concerns
- Explain exactly what the assessment will and will not cover

We will not pressure you into tools, managed services, or long-term contracts.

Gryphon Security, LLC
Ransomware Preparedness & Resilience Assessments
info@gryphonsec.com | www.gryphonsec.com