

# THREATREMIATE ENDPOINT DETECTION & RESPONSE

Endpoints are the first line of defense—and often the first target. Vijilan's ThreatRemediate Endpoint Detection & Response, powered by CrowdStrike Falcon EDR/XDR, delivers continuous protection, real-time detection, and rapid containment across every endpoint. Modern attackers use stealthy tactics like fileless malware and credential theft. This solution stops them before damage spreads.

## Business Impact



- Reduce dwell time and stop breaches before they escalate
- Simplify endpoint protection and reduce agent sprawl
- Gain compliance visibility with detailed audit trails and detection logs
- Accelerate investigations and response using automation and playbooks
- Rely on Vijilan's 24/7 Resilient SOC for managed containment and remediation

## Key Capabilities



Real-time detection using behavioral indicators of Attack (IOAs)



Lightweight Falcon agent with minimal system impact



Remote response to isolate hosts, kill processes, or quarantine files



Threat correlation across endpoint, identity, and network telemetry



Integrated threat intelligence and enriched telemetry for investigations



## Use Cases



- Contain ransomware in real time before it spreads
- Detect insider threats and unauthorized activity
- Execute remote response actions on infected endpoints
- Meet compliance requirements with continuous endpoint monitoring
- Support threat hunting and digital forensics investigations

## Compliance Alignment



- HIPAA: Continuous visibility and access control validation
- PCI DSS v4.0: System hardening and threat detection
- CMMC 2.0: Risk-based prioritization and mitigation
- NIST 800-53: Controls CA-7, RA-5, SI-2 for assessment and response

## Part of the ThreatRemediate Ecosystem



### Falcon EDR/XDR

Correlate exposures with endpoint activity



### Falcon Identity Protection

Correlate user behavior with endpoint activity



### Resilient SOC

24/7 containment, escalation, and response from Vijilan



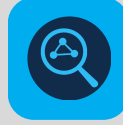
### Falcon LogScale

Ingest exposure data into SIEM for analytics



### Falcon Exposure Management

Remediate vulnerable endpoints faster



### Falcon Discover

Monitor device and application changes in real time

