MANAGED EDR SERVICE OVERVIEW

THREATREMEDIATE™ ENDPOINT DETECTION & RESPONSE

THE CHALLENGE

Endpoints are ground zero for attacks. Every ransomware incident, every data breach, every compromise starts with an endpoint. Legacy antivirus can't keep up with modern threats, and even good EDR tools generate thousands of alerts.

The reality:

- 70% of breaches originate at the endpoint
- Legacy AV misses 60%+ of modern malware
- Average EDR generates 10,000+ alerts/week
- Most teams lack time to investigate properly

THE VIJILAN APPROACH

ThreatRemediate EDR combines the industry's best endpoint protection (CrowdStrike Falcon) with 24/7 expert monitoring. We don't just detect threats—we stop them before damage occurs.

PLATFORM: CROWDSTRIKE FALCON INSIGHT

CrowdStrike Falcon is a top-rated, cloud-native endpoint protection platform, consistently recognized by Gartner, Forrester, and independent labs. It uses a single lightweight agent to deliver full protection without the need for on-prem infrastructure. Key features include behavioral IOA (Indicators of Attack) detection, an AI/ML engine for adaptive threat detection, real-time visibility into processes and connections, and built-in remote response capabilities.

Unlike traditional IOC (Indicators of Compromise) methods that rely on known signatures and detect threats after compromise, Falcon's IOA-based detection identifies behavioral patterns during an attack, enabling faster, more effective protection—even against fileless or novel threats. Falcon leverages both IOC and IOA, but its strength lies in stopping what signatures often miss.

WHAT'S INCLUDED

Capability	Description
CrowdStrike Falcon Platform	#1 rated EDR/XDR solution
Behavioral Detection (IOA)	Catches threats signatures miss
24/7 SOC Monitoring	Expert analysts watching every alert
Active Response	Isolate, kill, quarantine—in seconds
Threat Hunting	Proactive searches for hidden threats
Full Remediation	Complete threat removal, not just containment

HOW IT WORKS

PREVENT
Falcon blocks known threats automatically

DETECT
IOA engine identifies suspicious behavior

INVESTIGATE
SOC analysts verify and scope

RESPOND
Isolate, kill process, quarantine

REMEDIATE
Remove malware, close attack vectors

vijilan.com
info@vijilan.com
+1 (954) 334-9988

COMPLIANCE SUPPORT

Our platform helps meet key security requirements across multiple frameworks, including HIPAA (§164.308 and §164.312), PCI DSS v4.0 (Requirements 5 and 10), CMMC 2.0 (SI.2.214, SI.2.216, IR.2.092), NIST CSF (PR.DS, DE.CM, RS.AN), and CIS Controls (Control 10).

INTEGRATIONS

Vijilan integrates seamlessly with leading platforms across your tech stack, including PSA/ITSM tools like ConnectWise Manage, Autotask/Datto, ServiceNow, and Zendesk; SIEM platforms such as CrowdStrike LogScale, Splunk, and Microsoft Sentinel; and identity providers including Active Directory, Microsoft Entra ID, and Okta.

THREAT COVERAGE

We detect and stop a wide range of threats, including ransomware, fileless malware, living-off-the-land attacks, credential theft, lateral movement, persistence mechanisms, rootkits, and zero-days—using advanced techniques like behavioral analysis, memory inspection, and kernel-level detection, without relying solely on signatures.

DEPLOYMENT

Metric	Value
Time to Deploy	24-48 hours
Agent Size	~50 MB
CPU Impact	< 1%
Memory	~40 MB
Deployment Method	GPO, SCCM, Intune, manual
Supported OS	Windows, macOS, Linux

Deployment Options

- Mass deployment via Group Policy, SCCM, Intune
- Manual installation for ad-hoc endpoints
- Golden image inclusion for VDI/new builds

WHY VIJILAN FOR EDR

Vijilan delivers fully managed EDR powered by CrowdStrike Falcon, combining industry-leading technology with 24/7 SOC monitoring, active threat remediation, and a guaranteed 15-minute SLA.

Unlike DIY EDR approaches—where your internal team may only monitor alerts during business hours—Vijilan provides continuous coverage by certified analysts, ensuring faster response and greater peace of mind. Plus, our predictable monthly pricing eliminates the hidden costs of licensing, staffing, and training.

RESPONSE CAPABILITIES

Action	Description	Speed
Network Isolation	Cut endpoint from network	Seconds
Process Kill	Terminate malicious processes	Seconds
File Quarantine	Remove malicious files	Seconds
Registry Cleanup	Remove persistence mechanisms	Minutes
User Lockout	Disable compromised accounts	Minutes
System Restore	Return to known-good state	As needed

Service Tiers

Feature	Essentials	Premium
CrowdStrike Falcon Insight	✓	✓
24/7 Monitoring	✓	✓
Alert Triage	✓	✓
Active Containment	✓	✓
Threat Hunting	Monthly	Continuous
Full Remediation	-	✓
Identity Protection	Add-on	Included
Response SLA	30 min	15 min
Dedicated Analyst	-	✓

FREE ASSESSMENT IDENTIFIES ENDPOINT PROTECTION GAPS.

Uncover Weaknesses in Your Endpoint Security—At No Cost.

vijilan
IT Security. Enabled.

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN