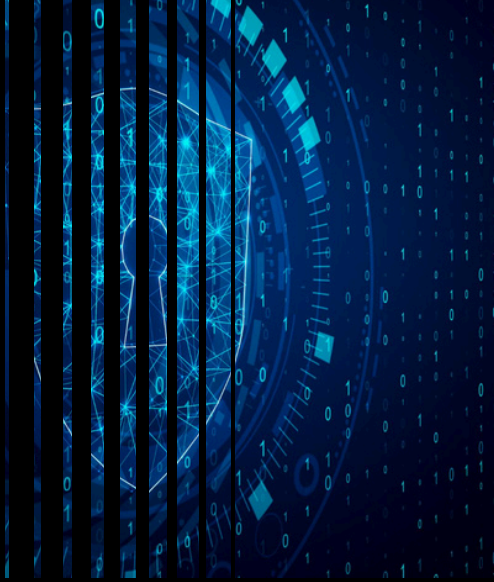
vijilan
IT Security: Enabled

ThreatRespond

Managed Extended Detection & Response

Powered by Vijilan's Information Security Hub, ViSH



ThreatRespond is Vijilan's fully managed extended detection and response (mXDR) service designed for MSPs, MSSPs, and VARs seeking advanced threat visibility, rapid response, and security operations support without needing to build a SOC. It includes 24/7 monitoring, triage, threat validation, and escalated incident response across endpoint, network, identity, and cloud data sources.

Why Vijilan's ThreatRespond?

Multi-cloud log ingestion
Supports multi-cloud log ingestion (AWS, Azure, Google Cloud) and major firewalls, EDR, and IAM tools

Real-time containment
Isolate endpoints, block IPs/domains, disable users, enforce MFA

Built-in SIEM
Built-in SIEM on AWS with index-free search, raw log access, and long-term retention

Prebuilt integrations
Prebuilt integrations with ConnectWise, Autotask, Zendesk, Freshservice, and more

24/7 Protection
U.S.-based 24/7 SOC handling detection, investigation, and containment

Compliance-ready reports
Audited by A-LIGN and aligned to HIPAA, PCI DSS, CMMC, ISO 27001, and NIST 800-53

Key Capabilities for Your Clients

- 24/7 threat detection and response
- Real-time correlation across endpoint, identity, cloud, and network
- Custom dashboards, reporting, and alerting via secure partner portal
- Raw log access with full-text search and export
- Alerts, incidents, and logs retained up to 7 years for auditing

vijilan IT Security: Enabled
info@vijilan.com
+1 (954) 334-9988
vijilan.com

Value to Your MSP

- Operate your own branded SOC-as-a-Service without hiring analysts
- Expand MRR by offering premium monitoring and compliance services
- Get peace of mind with full visibility, escalation workflows, and documentation
- Access our partner portal to onboard, manage, and support clients
- Deliver measurable outcomes with fast time-to-value

Supported Environments

- **Endpoints:** CrowdStrike, Microsoft Defender, SentinelOne, Palo Alto, etc.
- **Firewalls**: Palo Alto, Fortinet, SonicWall, WatchGuard, pfSense
- **Cloud**: Microsoft 365, Google Workspace, AWS, Azure, Okta, Entra ID
- **Identity**: Microsoft Entra, Okta, Duo
- **SIEM**: Falcon LogScale,
- **Migration** from Sentinel, Splunk, and Elastic

Compliance Alignment

ThreatRespond helps organizations achieve and maintain compliance with:

- HIPAA
- PCI-DSS
- GLBA
- SOX
- CMMC 2.0

Deployment & Integration

Deployment within 1-2 hours

- Cribl-based pipeline for log parsing and enrichment
- Custom escalation paths built per partner and its clients
- Native integrations with major PSA and ticketing platforms (Zendesk, ConnectWise, Autotask)

Pricing Model

- Flexible per-device or per-user pricing available
- Pricing depends on scope, integrations, and technologies monitored
- Includes SOC coverage and log management; remediation can be added

Getting Started

Vijilan makes onboarding easy.

We'll help your team activate SOC & SIEM services for your clients with co-branded onboarding, live support, and GTM alignment. Use our portal to manage alerts, generate compliance reports, and provide real-time value to every client under your care.

vijilan IT Security: Enabled
info@vijilan.com
+1 (954) 334-9988
vijilan.com