

ThreatRemediate

IDENTITY PROTECTION ITDR

ENFORCING ZERO TRUST AT THE IDENTITY LAYER

Cybercriminals no longer break in—they log in. Identity is the new attack surface, and traditional defenses aren't built to stop today's threats. That's why ThreatRemediate Identity, powered by CrowdStrike Falcon Identity Protection, brings real-time visibility and enforcement across every identity, account, and access attempt—on-prem and in the cloud.

Developed by CrowdStrike and delivered by Vijilan, this solution enables organizations to enforce Zero Trust where it matters most.

The Identity Crisis

Modern cyberattacks thrive on identity-based exploitation:

- ✓ Stolen or reused credentials
- ✓ MFA fatigue and push-bombing
- ✓ Lateral movement through Active Directory
- ✓ Privileged account misuse

80%

of breaches now involve identity compromise. Most tools detect policy violations. Very few detect active exploitation. ThreatRemediate changes that.

ThreatRemediate Identity Built to Stop What IAM Misses

While traditional IAM and Identity Threat Detection and Response, ITDR, govern who can access what, ThreatRemediate managed ITDR, powered by CrowdStrike Falcon Identity Protection, focuses on how users behave once they're inside—detecting real-time identity threats and enforcing risk-based controls before damage is done.

Key Capabilities

- ✓ Behavioral Analytics across AD and Azure AD
- ✓ Real-Time Detection of credential abuse and privilege escalation
- ✓ Risk-Based Access Controls that adapt dynamically
- ✓ Agentless Deployment—fully operational in hours
- ✓ Privileged Account Monitoring for insider and external abuse

Business Impact for Vijilan's MSP Partners

With ThreatRemediate Identity, organizations gain:

- ✓ Ransomware Prevention at the Identity Layer
- ✓ Adaptive MFA Enforcement to prevent session hijacking and phishing
- ✓ Reduced Dwell Time through identity-aware SOC workflows
- ✓ Visibility into Every Login, Privilege, and Movement



Use Cases

- ✓ Stop ransomware at the login stage—detect lateral movement early
- ✓ Prevent MFA fatigue attacks with behavioral context
- ✓ Ensure compliance through real-time identity monitoring and reporting
- ✓ Detect rogue access to sensitive systems and assets

Part of the ThreatRemediate Premium

Falcon Identity is just one piece of the full ThreatRemediate Complete cybersecurity stack, delivered by Vijilan. Together, they provide holistic, real-time protection across:

Compliance Mapped

ThreatRemediate Identity, powered by Falcon Identity, aligns with key security frameworks:

- ✓ HIPAA Security Rule: §164.312(d), §164.308(a)(3)
- ✓ CMMC 2.0: AC.1.001, IA.2.078
- ✓ NIST 800-53: AC-2, AC-6, IA-4
- ✓ PCI DSS v4.0: 8.4.2, 8.6.2

- ✓ Endpoints with Falcon EDR/XDR
- ✓ Users with Falcon Identity
- ✓ Vulnerabilities with Falcon Spotlight
- ✓ Assets & Applications with Falcon Discover
- ✓ Security Data with Falcon LogScale and Cribl pipelines
- ✓ SOC Operations with continuous monitoring, threat hunting, and rapid remediation

Make Identity Your Strongest Defense

With ThreatRemediate Managed ITDR, powered by CrowdStrike Falcon Identity Protection, identity security is no longer just a checkbox—it's a real-time, adaptive shield against modern attacks. Delivered by Vijilan, this solution helps you shift from reactive to proactive identity protection—without complexity.

Ready to stop identity-based threats before they spread?

Contact Vijilan today to activate ThreatRemediate Identity with Falcon Identity Protection.

