CROWDSTRIKE FALCON IDENTITY PROTECTION WITH VIJILAN

Unified Identity Threat Detection & Response

DOCUMENT PURPOSE

This technical document describes a co-branded Identity Threat Detection and Response (ITDR) offering that combines CrowdStrike Falcon Identity Protection with Vijilan's 24/7 U.S.-based Security Operations Center (SOC) for continuous detection, investigation, and response to identity-driven attacks across hybrid identity environments.

EXECUTIVE SUMMARY

CrowdStrike Falcon Identity Protection + Vijilan's 24/7 SOC delivers real-time defense against identity-driven attacks across endpoints, cloud, and SaaS. It stops credential compromise, lateral movement, and privilege escalation with a lightweight agent and correlated identity + endpoint insights.

Risk-based authentication and extended MFA protect even legacy systems, while Vijilan ensures rapid threat detection and response—often within minutes. The solution supports Zero Trust, boosts efficiency, and delivers strong ROI.

USE CASE HIGHLIGHTS

Credential Theft and Account Takeover Prevention
Detect suspicious logins and trigger step-up authentication or blocks. Vijilan's SOC validates threats and responds in real time with actions like account lockout or session termination.

Ransomware & Lateral Movement Containment
Detect and stop lateral movement using compromised credentials. Falcon correlates identity and endpoint data, while Vijilan's SOC rapidly isolates threats to prevent ransomware spread.

Privilege Escalation & Insider Threat Detection
Detect unauthorized privilege changes and suspicious admin activity. Vijilan analysts act fast using enriched context to protect critical assets.

Hybrid Identity Protection for Cloud and On-Premises
Gain unified visibility across cloud and on-prem AD. Detect and respond to attacks spanning both environments for consistent identity security.

JOINT VALUE PROPOSITION

CrowdStrike Falcon Identity Protection + Vijilan's 24/7 SOC delivers a unified ITDR solution that boosts identity security while reducing overhead.

Key Benefits:

- 24/7 Threat Monitoring & Response
- Faster Detection & Containment (MTTD/MTTR)
- Zero Trust Enforcement
- Streamlined Identity Threat Management
- Scalable for Hybrid Environments

This partnership offers proactive, real-time defense against identity threats—empowering organizations to stop credential abuse, lateral movement, and privilege escalation while operationalizing Zero Trust across cloud and on-prem systems.

KEY CAPABILITIES

Unified Detection Across Endpoint and Identity
Falcon Identity Protection correlates endpoint telemetry and identity activity to detect full attack chains that typically span multiple domains. This reduces blind spots created by siloed tooling and improves detection fidelity by tying identity anomalies to endpoint behavior and vice versa.

Real-Time Identity Threat Visibility
The platform continuously analyzes authentication activity and detects identity-based attacks in real time without requiring heavy log ingestion pipelines. Built-in machine learning and behavioral analytics identify threats such as credential theft and reuse, directory reconnaissance, lateral movement methods, and privilege escalation patterns as they occur.

Adaptive Risk-Based Authentication Policies
Organizations can define conditional access policies that automatically allow, block, or require step-up MFA based on real-time risk. Legitimate users experience seamless authentication, while high-risk sessions can be challenged or blocked. This helps mitigate modern tactics such as MFA fatigue and session abuse, while extending MFA controls to legacy protocols and systems that traditionally lack modern identity controls.

Integration with AD, Entra ID, and Identity Providers
Falcon Identity Protection integrates with on-premises Active Directory and cloud identity services such as Azure AD and Entra ID, and supports common SSO and federation providers. It also supports a broad set of MFA solutions, allowing consistent enforcement and monitoring across Windows logins, SaaS sign-ins, VPN authentication, and hybrid identity flows.