Detect and Stop Threats with ThreatWarrior and CrowdStrike

The Challenge

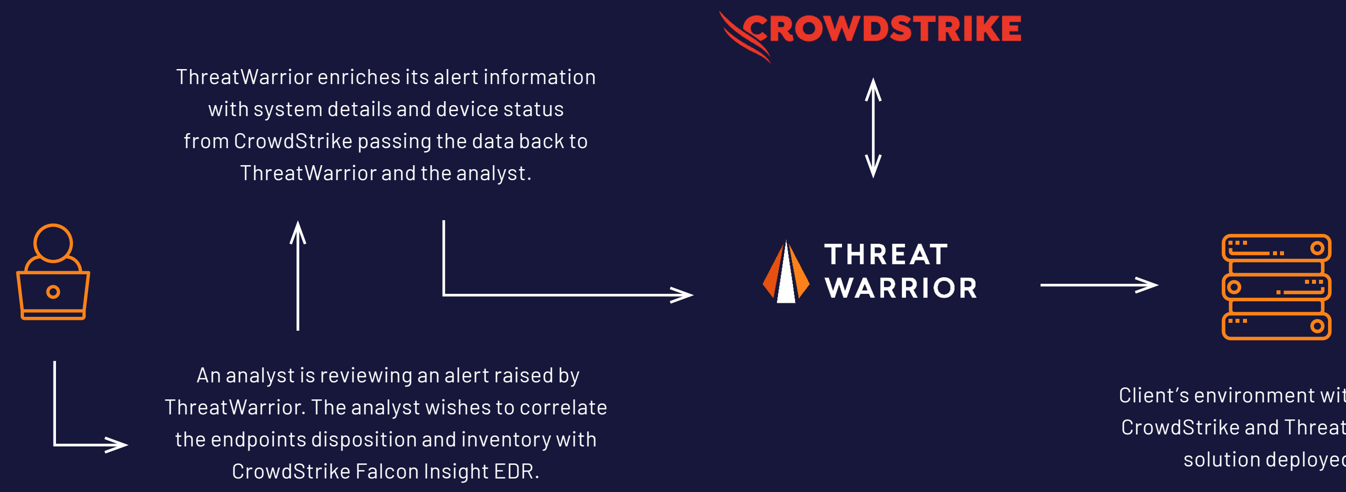
As the threat landscape continues to evolve, organizations are faced with sophisticated threat actors using novel approaches to breach their networks. The threats are everywhere: network, endpoint, cloud, IoT and more. Endpoint security solutions effectively stop threats at the endpoint, but attacks may sneak through at other points in the network.

Businesses need cybersecurity solutions that keep pace with evolving threats. Security analysts need real-time visibility and insight into every connection, managed or unmanaged, to adequately protect themselves.

The Solution

The integration of ThreatWarrior with CrowdStrike Falcon Insight combines complete network visibility, machine learning, and behavioral anomaly detection with powerful endpoint security and rapid response. Extending detection and response across platforms, networks, clouds and endpoints is a new approach to threat protection called XDR. ThreatWarrior extends CrowdStrike detections into new attack surfaces, increasing SOC efficiency and reducing time to resolution.

ThreatWarrior and CrowdStrike deliver a unified view of endpoint and network context, enabling security teams to quickly detect, investigate, and resolve cyber threats — even stealthy, unknown threats.



ThreatWarrior enriches its alert information with system details and device status from CrowdStrike passing the data back to ThreatWarrior and the analyst.

An analyst is reviewing an alert raised by ThreatWarrior. The analyst wishes to correlate the endpoints disposition and inventory with CrowdStrike Falcon Insight EDR.

Client's environment with a joint CrowdStrike and ThreatWarrior solution deployed.

ThreatWarrior analyzes in real-time all network traffic across on-premises and cloud environments to monitor behaviors, detect indicators of compromise, and stop active threats. The platform ingests endpoint telemetry from CrowdStrike Falcon, as well as other data sources, and correlates that information to deliver complete context and situational awareness across the enterprise.

Users can take manual or autonomous action to immediately respond to suspicious activity. When this activity requires investigation, with a single click, Falcon Insight delivers deep endpoint data displayed in ThreatWarrior's intuitive UI.

With ThreatWarrior and CrowdStrike, organizations can save time and resources by increasing SOC efficiency. The integration reduces response and investigation time, enabling security teams to take action against threats as they happen.

Key Benefits

Complete, real-time visibility
See everything happening across your environment from the network to the endpoint.

Continuous device inventory
Track all devices including managed, unmanaged, IoT and remote connections, identifying those not yet protected by endpoint security.

Deep context and insights
Unifying endpoint and network data provides insight and contextual information for all observed activity.

Instant response
Take manual or automated response to increase SOC efficiency and reduce time to resolution.

THREAT WARRIOR

ThreatWarrior is a leader in cloud-native network detection and response, helping organizations see, learn about, and act to stop cyber threats before they cause damage. The cyber defense platform delivers true signal to eliminate alert fatigue and keep analysts focused on critical threats. ThreatWarrior escalates the most serious threats , filters out low-value events, and helps cybersecurity professionals prioritize their work with far greater efficiency.

ThreatWarrior combines unsupervised neural networks, continuous deep packet inspection, complete network visibility, and behavioral anomaly detection in a single platform. Leading organizations use ThreatWarrior to defend against APTs, zero-day exploits, digital supply chain attacks and more across on-premises, cloud, and hybrid infrastructures.

CROWDSTRIKE

CrowdStrike is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud, the Falcon platform enables partners to rapidly build best-in-class integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.