Complete Protection with Full-Coverage EDR and NDR

CrowdStrike is the leader in endpoint detection and response (EDR) solutions. CrowdStrike collects and protects rich endpoint data from every endpoint the platform is installed on.

ThreatWarrior is a leader in network detection and response (NDR). The ThreatWarrior platform sees and secures every network-connected "thing" (whether on-premises, cloud-based, or both), delivering complete network visibility and full-coverage protection for possible gaps left by EDR. ThreatWarrior helps reveal the entire attack surface, including managed and unmanaged devices.

Combining these solutions allows users to identify all network and endpoint attack behaviors and signatures — empowering security teams to stop both conventional and advanced threats.

Better Together: Key Benefits

Full coverage. Complete protection for anything connected to the network, including IoT, OT, legacy technologies, and Industrial Control Systems.

Complete, real-time visibility. Gain 100% visibility of the entire network topology, including cloud, virtual, on-premises, and hybrid environments.

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

Free from human bias. ThreatWarrior's unsupervised neural networks learn free from human bias, ensuring accuracy.

More signal, less noise. ThreatWarrior delivers context to filter out false positives and less severe threats, correlating network data to speed up investigation and response.

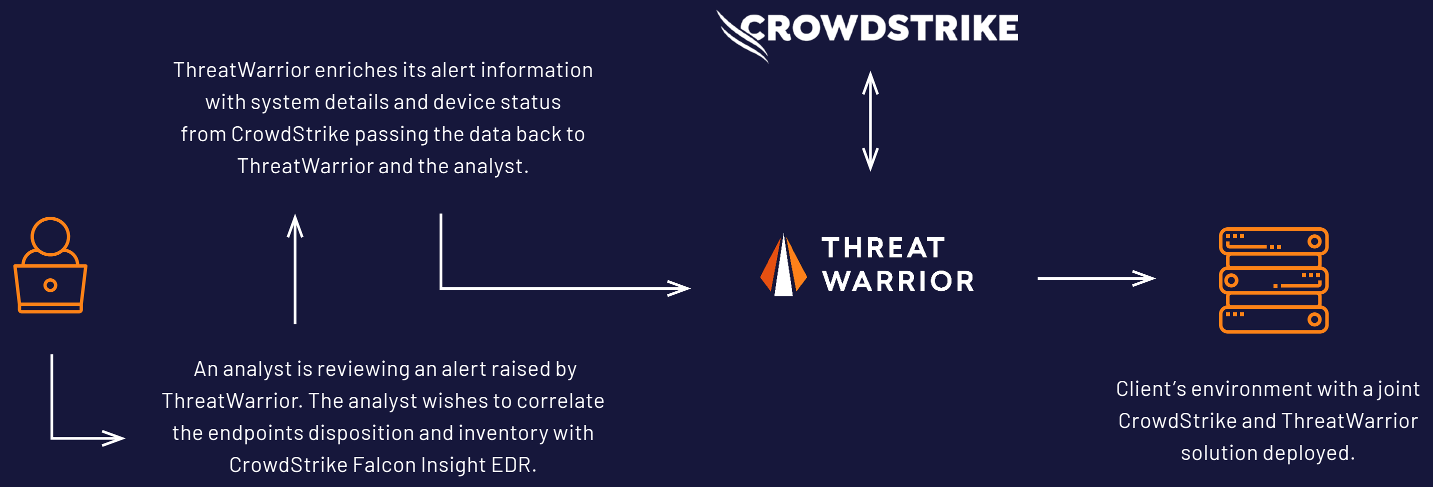
> *ThreatWarrior is helping solve a critical problem in the cybersecurity industry — a lack of contextual intelligence and visibility across the enterprise, including public cloud environments. ThreatWarrior aggregates intelligence, analyzes behavior and correlates context on-premises and in the cloud to identify attacks wherever they occur.*

MICHAEL SENTONAS
Chief Technology Officer, CrowdStrike

Better Together: The Integration

The integration of ThreatWarrior with CrowdStrike Falcon combines complete network visibility, cloud-scale AI, and behavioral anomaly detection with world-class endpoint security. The solution provides powerful detection and response across every attack surface in any infrastructure.

With ThreatWarrior and CrowdStrike, users gain network-wide intelligence with deep endpoint context to see and stop threats faster — a critical ability when every second matters. ThreatWarrior's rapid detection, investigation and response helps stop attackers in real-time by leveraging advanced AI, correlative analysis, and Intelligent Threat Scoring to rank threat severity and prioritize alerts. This keeps analysts focused only on critical threats, enabling customers to achieve CrowdStrike's 1:10:60 challenge.



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

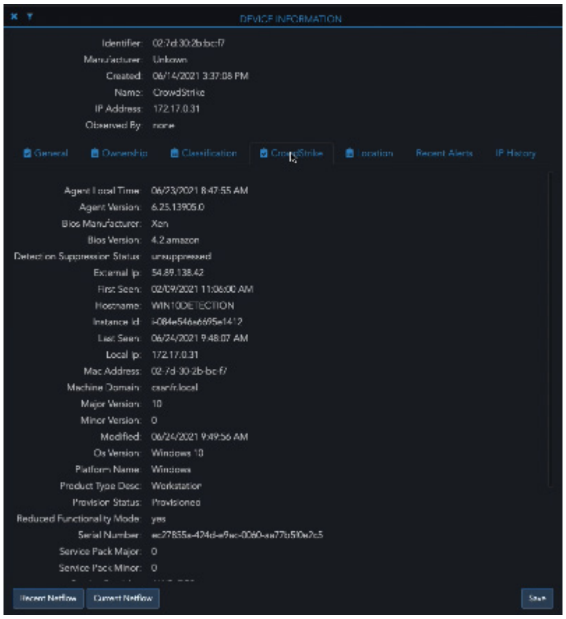
An analyst is reviewing an alert raised by ThreatWarrior. The analyst wishes to correlate the endpoints disposition and inventory with CrowdStrike Falcon Insight EDR.

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

Endpoint + Network Context

This integration automatically displays endpoint data from Falcon Insight in the ThreatWarrior platform. Security teams can quickly gather endpoint and network context to minimize risk and make fast, data-driven decisions.

With a single click, analysts can view device specifics and explore endpoint activity. This unified view allows users to quickly investigate endpoints for indicators of compromise and accelerates time to resolution by reducing unnessecary switches between interfaces.



Identifier: 02:7d:30:2b:bc:f7
Manufacturer: Unkown
Created: 06/14/2021 3:37:08 PM
Name: CrowdStrike
IP Address: 172.17.0.31
Observed By: none

Agent Local Time: 06/23/2021 8:47:55 AM
Agent Version: 6.25.13905.0
Bios Manufacturer: Xen
Bios Version: 4.2.amazon
Detection Suppression Status: unsuppressed
External Ip: 54.89.138.42
First Seen: 02/09/2021 11:06:00 AM
Hostname: WIN10DETECTION
Instance Id: i-084e546a6695e1412
Last Seen: 06/24/2021 9:48:07 AM
Local Ip: 172.17.0.31
Mac Address: 02-7d-30-2b-bc-f7
Machine Domain: csanfr.local
Major Version: 10
Minor Version: 0
Modified: 06/24/2021 9:49:56 AM
Os Version: Windows 10
Platform Name: Windows
Product Type Desc: Workstation
Provision Status: Provisioned
Reduced Functionality Mode: yes
Serial Number: ec27835a-424d-e9ec-0060-ea77b510e2c5
Service Pack Major: 0
Service Pack Minor: 0

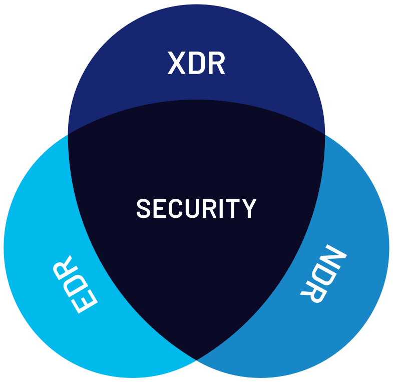
Why ThreatWarrior?

ThreatWarrior is a cloud-native network detection and response platform that analyzes in real-time all network traffic to monitor behaviors, detect indicators of compromise, and stop active threats.

Our approach to security **unifies many different defense engines into a single platform**. ThreatWarrior correlates and analyzes information across these engines, unifying that data with threat intelligence reports and enriched context to deliver true signal through the noise produced by threat volume and other cybersecurity solutions. The platform escalates the most serious threats to the people who need to see them, filters out low-value events from being a distraction, and helps cybersecurity professionals prioritize their work with far greater efficiency.

ThreatWarrior's 3D Universe provides an immersive, real-time visualization of all network data flow. The interface allows users to explore an enormous amount of information all at once, while retaining important features of that information. Plus, the graphical display enables analysts to quickly search for and expose anomalous activity, suspicious communication, and more. When this activity requires investigation, with a single click, Falcon delivers deep endpoint data displayed in ThreatWarrior's intuitive user experience.

Additionally, **ThreatWarrior is passive and agentless**. It is obscured from sight by the network switch so it remains stealth on the network. As nation-state actors become more sophisticated, they often build their malware to lie dormant while being actively observed. Because ThreatWarrior is invisible, the bad actors will never know that ThreatWarrior is watching, enabling the platform to quickly detect the attack.



EDR
Protects endpoints with agents installed, delivering visibility and rich context for all endpoint activity.

NDR
Protects the network to stop known and unknown threats and provides full-network visibility. Passive and agentless.

XDR
Extends over multiple security layers including endpoint, network and cloud workloads. Delivers higher visibility.

THREAT WARRIOR

ThreatWarrior is a leader in cloud-native network detection and response, helping organizations stop advanced threats before they cause damage. Our AI-powered platform performs real-time analysis on data-in-flight and helps identify malicious behavior, empower threat hunting initiatives, and forensically investigate cyber incidents. By combining complete visibility, deep packet inspection, behavioral anomaly detection, analysis, forensics and threat hunting, ThreatWarrior delivers the network-wide context and insight analysts need to take immediate, confident action. Leading organizations use ThreatWarrior to defend against APTs, zero-day exploits, digital supply chain attacks and more across on-premises, cloud, and hybrid infrastructures.

Copyright © 2022 ThreatWarrior, Inc.