SOLUTION BRIEF

IronNet and CrowdStrike

Reduce the impact of cyber attacks with integrated Endpoint Detection and Response

Why we work better **together**

CROWDSTRIKE

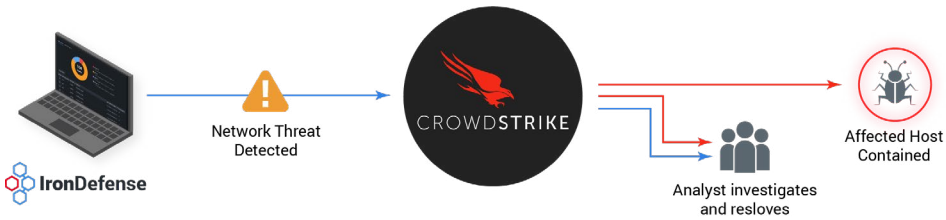
SOLUTION BENEFITS AT A GLANCE

Visibility across the threat landscape
Apply real-time collective threat intelligence, contextual information on new threats, and higher-order analysis of anomalies correlated across communities.

Increase effectiveness of existing SOC resources
Streamline and automate operations by integrating endpoint information and containment actions into a highly effective Network Detection and Response platform.

Reduce the impact of an attack
Lessen business repercussions and security risk by detecting threats across the network and endpoints earlier in the attack lifecycle.

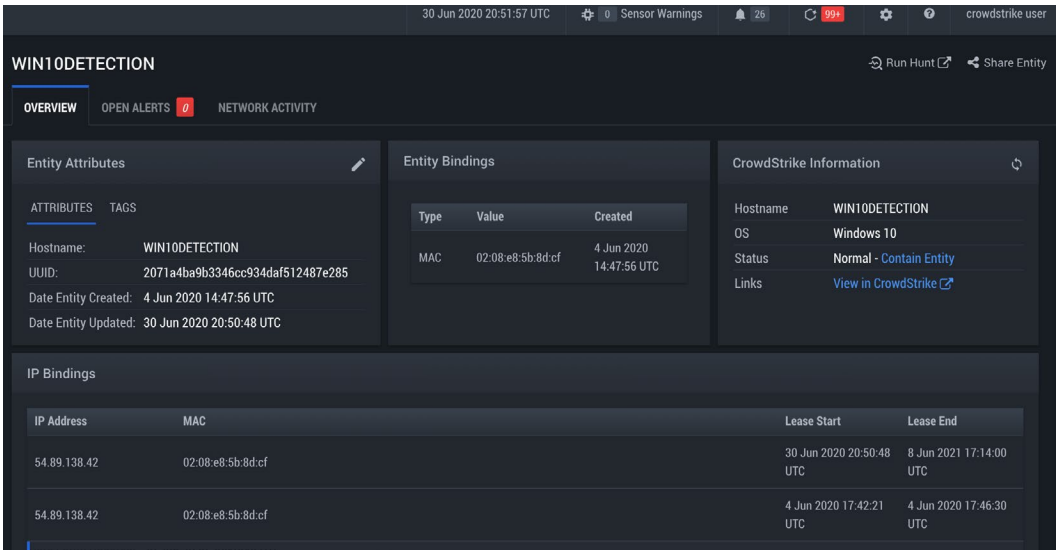
Designed by national security analysts and top intelligence data scientists, IronNet's scalable Network Detection and Response (NDR) solution and Collective Defense platform provide visibility across communities of enterprises at machine-speed. This approach allows peers to identify advanced threats often missed by existing commercial cybersecurity solutions. IronDefense, IronNet's NDR solution, delivers cyber analytics and integrated hunt capabilities to a variety of public and private sector enterprises. IronNet's Collective Defense platform, IronDome, shares these behavior-based detections with communities of similar risk profiles to create a defensive fabric across companies, sectors, and nations.



Network and Endpoint Detection and Response

CrowdStrike provides Endpoint Detection and Response (EDR) capabilities to monitor, block, and remediate threats detected on endpoints, which are devices, such as desktops, laptops, and mobile devices, that serve as entry points to a network. Analysts can also instantly contain compromised endpoints by issuing a network containment action on the affected endpoint directly from IronDefense.

Key Capabilities



Easily view network and endpoint telemetry data on a single pane of glass

IronDefense works natively with CrowdStrike to provide relevant host details through IronDefense's IronVue User Interface (UI), delivering the necessary contextual information that speeds up time to detection by reducing investigative workflow complexity.

Instantly contain threats

Analysts using IronDefense can contain endpoints with one click through IronNet's IronVue interface. This enables security teams to instantly stop threats during an investigation.

Pivot seamlessly from network to endpoint during an investigation

IronDefense users with CrowdStrike permissions can also pivot to the CrowdStrike Falcon interface for deeper investigation, allowing security teams to seamlessly trace suspicious behaviors on the network to the source endpoint.

Leverage the power of IronDome Collective Defense

IronDefense fully integrates with IronDome, the first automated cyber Collective Defense solution, to deliver threat knowledge and intelligence sharing across industries at machine speed. With IronDome, IronDefense and Crowdstrike customers can collaborate with others across industries and sectors to stay ahead of evolving threats.

Contact Us

To learn more about the IronDefense Integration for Crowdstrike, visit IronNet.com or contact us at info@IronNet.com.

ABOUT IRONNET

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprises by delivering the first-ever Collective Defense platform operating at scale. Our solutions leverage our unique offensive and defensive cyber experience to deliver advanced behavioral analysis and collective intelligence to detect known and unknown threats.