SOLUTION BRIEF

IronNet and Palo Alto

Reduce the impact of cyber attacks with integrated perimeter detection and response

Why we work better **together**

SOLUTION BENEFITS AT A GLANCE

Gain 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.

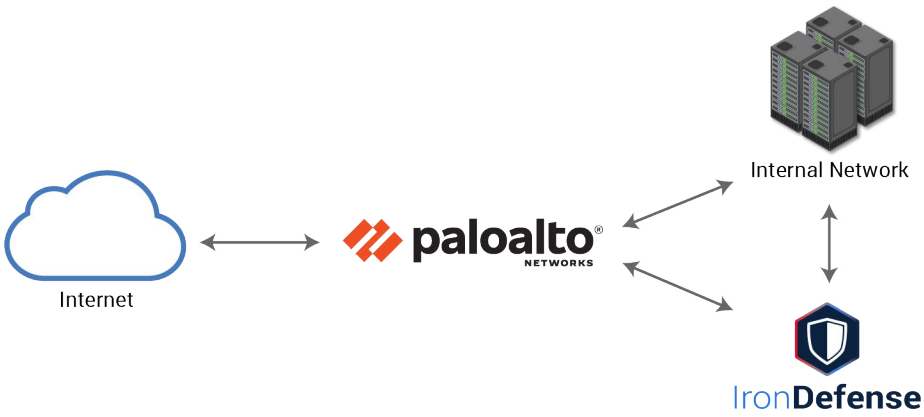
Increased effectiveness of existing SOC resources

Streamline and automate operations by integrating perimeter threat detection and blocking actions into a highly effective Network Detection and Response platform.

Reduce impact of an attack

Lessen business repercussions and security risk by detecting threats across the network and the perimeter 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 enterprise communities 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, states, and nations.



Network and Endpoint Detection and Response

Palo Alto Networks provides centralized management of firewall protection for your entire network perimeter. With Palo Alto Networks' next-generation firewall (NGFW), you can safely enable the use of applications and maintain complete visibility and control over content to stop threats. When used together, IronDefense creates domain and IP block lists that will be synced with the Palo Alto Networks firewall. This ensures that Indicators of Compromise (IoC) that were discovered in the enterprise environment, or other IronNet customer environments, will be dropped at the firewall before posing any risk to the network.

HOW IT WORKS

Detection

IronDefense identifies a malicious IP(s) or domain(s) through behavioral analytics.

Trigger

Analysts triage the appropriate alert and select any associated IP or Domain to add to the NGFW blocklist.

Mitigation

IronNet and Palo Alto Networks NGFW work together to block traffic that threatens to compromise the network. IronDefense sends an updated blocklist to the NGFW, and Palo Alto policies are updated.

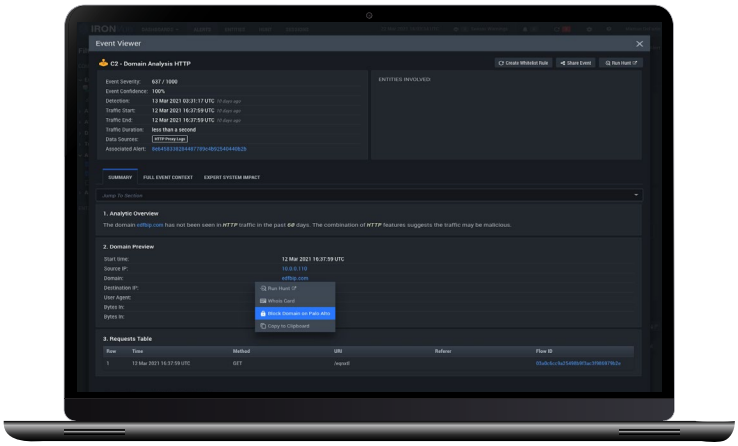
ABOUT IRONNET

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.

Contact Us

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

Key Capabilities



Full visibility

IronDefense seamlessly integrates with Palo Alto Networks NGFW to provide complete lateral (East-West) and perimeter (North-South) visibility of all network traffic and perimeter devices. IronDefense provides the expertise to identify and block advanced attacker behaviors at the firewall and within the enterprise network.

Streamlined response

The combination of IronDefense with Palo Alto Networks NGFW simplifies network defense by combining behavior-based threat detection with real-time mitigation. IronDefense uses advanced behavioral analysis of real-time traffic data to provide complete visibility, detection, and investigation. In addition, IronDefense supplies unique correlation rules for detecting malicious perimeter and network events, which can then be prioritized to expedite triage and response.

Instantly block potential threats

Analysts can use IronDefense's user interface, IronVue, to drop unwanted traffic at the firewall with one click by selecting any IP or domain associated with an alert and adding it to the drop list. This enables security teams to instantly stop threats as soon as they are identified.

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 Palo Alto Networks, customers can collaborate with others across industries and sectors to stay ahead of evolving threats.