# IronNet Cybersecurity is on a mission to protect critical IT infrastructures

**Analysts - Eric Ogren**

Publication date: Tuesday, April 2 2019

## Summary

IT operations learned its lesson long ago that proactive maintenance practices are far more effective and less disruptive than reactive 'break and fix' approaches. Security operations, deeply mired in frustrating 'detect and fix' cycles, has yet to find the answer to being able to predict and ward off threats. Machine learning for security use cases gets very interesting when it can predict the arrival of threats with sufficient lead time for security operations to deploy protective mechanisms. IronNet Cybersecurity, with its IronDefense Network visibility, detection and response (NVDR) product line and IronDome collective defense service that applies machine learning predictive services across behavioral events from enterprises within an industry, is aiming to protect large infrastructures from network-borne attacks.

## The 451 Take

IronNet is embarking on a big mission – a commercial vendor protecting critical IT infrastructures with a vertical industry approach that sounds appropriate as a government undertaking. The concept of IronDome is unique – grouping data from companies related by vertical industry or infrastructure profile, focusing machine learning on those data sets to detect threats, and then communicating the derived intelligence to subscribers, allowing for preventive actions.

To achieve its vision, the company has to fight a war on multiple fronts. It must first promote IronDefense as an NVDR product line that can bolster customers' security programs and serve as the preferred data source to share information in real time with IronDome, and then IronDome must deliver on its promise to empower security operations with the information it needs to deflect incoming threats. IronDome is the key as we envision predictive alerts becoming more valuable to the customer business than traditional historical alerts.

## Context

Baltimore-based IronNet Cybersecurity was founded in 2014. Founders include a team lead by Keith Alexander, former director of the US National Security Agency. Bill Welch, former COO of Zscaler and

an executive at Duo Security, recently joined Alexander as co-CEO. The vendor has completed two major funding rounds, raising over $110m. Lead investors include C5 Capital, ForgePoint Capital and Kleiner Perkins. In addition to Alexander, Don Dixon of Trident, Andre Pienaar of C5and Ted Schlein of Kleiner Perkins, the board of directors is stocked with former government defense executives such as Mike McConell (NSA), Mike Rogers (chairman committee on intelligence) and Jack Keane (former vice chief of staff, US Army).

The management team and IronNet's location in the Washington beltway would imply a vendor designed to cater to the needs of the federal government. However, the company reports that the majority of its revenue comes from the commercial segment. We believe the addition of Welch as co-CEO reflects the need to instill experiences in growing security businesses within the private sector.

## Products

IronNet's product line consists of IronDefense and IronDome. The architecture resembles the generally acceptable NVDR scheme of real-time appliance sensors deployed throughout the network feeding powerful analytic engines hosted in cloud-based datacenters, and then sending high-value alerts to security operations for remediation.

The company's key differentiator will be its IronDome collective defense analytics that bring high-value predictive alerts to its customer base. IronDome is building toward industry-sector threat analysis. The vendor reports significant traction within the energy sector, where each customer delivers threat data from on-premises IronDefense sensors up to the IronDome. IronNet reports enterprise deployments across the US utilities supplying their energy-sector IronDome with information. The company plans to launch multiple IronDomes in 2019 across the financial services, healthcare, defense, and government verticals, with major Fortune 500 customers already in place to serve as anchor enterprises.

IronDefense captures packets from a copy of network traffic to look for evidence of threats utilizing the network at all parts of the attack lifecycle. The heart of IronDefense is its expert system layer that looks into every analytics event, enriching the data when necessary, prioritizing the items of interest, and aggregating alerts for efficient handling. Captured packets are retained for several days to provide detailed information for remediation efforts. IronDefense's machine learning is designed to secure networks without dependencies on IronDome services.

For us, IronDome is where it gets exciting. Residing in Amazon Web Services, IronDome correlates observed behaviors across multiple companies on the prowl for spreading attacks. Competitors may upload traffic to apply analytics, but IronNet is unique in processing vertical industry views to catch campaigns against an infrastructure segment. For example, IronNet claims strength among utility providers, where detected attacks against one can help predict attack details against others. IronDome is positioned to effectively introduce predictive alerts as opposed to alerts on events that have already happened.

## Competition

Every IronDome customer agrees to allow the US Department of Homeland Security and Department of Defense an anonymized view into its corporate data in real time to provide visibility in support of US national cybersecurity. This may be a good example of public-private sector partnership in certain national industries such as utilities – however, we can see that even the prospect of US government involvement would make IronNet a nonstarter for international enterprises. The vendor is clear about its mission to secure American infrastructure – this coupling does open doors for NVDR competitors. IronNet is working with select countries in Asia and EMEA on developing regional IronDomes with their governments to deliver public-private partnerships,

most recently announcing a joint venture with Singapore-based Ensign Infosecurity that is backed by Temasek, Singapore's sovereign wealth fund, to bring IronDome to the region.

Privately held NVDR providers draw inferences from network traffic to detect and act on advanced threats that are active in the network. Firms that capture packets such as Awake Security, ExtraHop and RSA NetWitness will be the most direct rivals for IronDefense. As a rule of thumb, the packet capture-oriented providers are strong in detection, but also generally appeal to hunting and supporting incident response as they have access to detailed application-level data. Competing NVDR vendors emphasizing enriched flow data, including Bitdefender NTSA, Corelight, Darktrace, FireEye, Gigamon, Kaspersky ATA, Lastline and Vectra Networks, are generally optimized for performance around detection and visibility into device behaviors.

## SWOT Analysis

| Strengths | Weaknesses |
|---|---|
| IronNet's ability to look across industry peers, or potentially across IT infrastructures of similar profiles, adds critical context to design defenses. | Responses to alerts, whether signaled by IronDefense or IronDome, add to the response burdens of security operations staff. |
| **Opportunities** | **Threats** |
| IronDome's predictive alerts allowing organizations to mobilize and deflect incoming attacks can change security operations team's expectations for machine learning. | International organizations may be wary of sharing even anonymized proprietary security data with US government agencies. |

*Source: 451 Research, LLC*