MARSH

Cyber Catalyst by Marsh

IronNet

IronNet® Collective Defense Platform — Cyber Catalyst 2020 Designation

The IronNet Collective Defense Platform applies network detection and response capabilities and behavioral analytics to detect sophisticated cyber anomalies in a company's network. The platform visually correlates those alerts with what other organizations in the IronDome ecosystem see on their networks, to provide advanced warning and threat intelligence on potential incoming attacks.

The Collective Defense platform addresses risks associated with the potential theft of intellectual property, data manipulation, critical infrastructure compromises, and more that are posed by increasingly sophisticated cyber attacks. Corporate environments and security operations teams are under increasing pressure due to expanded attack surfaces from the shift to remote working, nation-state targeting of COVID-19 care and research facilities, and rising ransomware attacks. But companies cannot expect to defend on their own against nation-state cyber-attacks; they need to both see and share real-time, actionable threat information to defend more efficiently and effectively.

IronNet's Collective Defense Platform combines behavioral analytics at the network level with a real-time threat intelligence sharing platform. The platform is comprised of IronDefense (network detection and response) and IronDome (secure threat intelligence sharing).

Based on machine learning and AI techniques, IronNet's detection capabilities uncover known and unknown cyber threats that signature-based tools often miss, providing companies a more thorough approach to network security. Notifications of these threats, along with comments and contextual information, are immediately shared within an IronDome secure ecosystem, whose members may comprise an industry, supply chain, or other related grouping of organizations.

Alerts are prioritized to emphasize the highest-risk issues and threats that have been correlated across IronDome members, showing the breadth and persistence of the attack and enabling security operations teams to quickly take action. This provides a unique level of increased visibility into the threat landscape, allowing overburdened security operations teams to prioritize the most urgent and pervasive attacks and apply contextual threat intelligence for quick defensive action.

IronNet's Collective Defense platform is suitable for large Fortune 500 companies as well as mid-sized organizations across both the public and private sectors. It adds a level of threat visibility and detection to a CISO's security portfolio, while integrating with SOAR, SIEM and workflow tools. It can be deployed on public or private cloud as well as on-premises.

**Product information provided by IronNet Cybersecurity*

For more information about the IronNet Collective Defense platform, visit www.ironnet.com.

Why the IronNet Collective Defense Platform is a 2020 Cyber Catalyst Designated Solution

ADDRESSES A TOP 5 CYBER RISK:

The 2020 program encouraged the submission of solutions that targeted the top five cyber risks identified by participating insurers: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

IronNet's Collective Defense Platform specifically targets network security risks such as malware attacks, but also has wider utility and applicability in addressing other types of cyber risk.

INSURER RATINGS AND COMMENTARY:

Cyber Catalyst participating insurers rated the IronNet Collective Defense platform highest on the criteria of key performance metrics, efficiency, and differentiation.

In their evaluation, the insurers commented:

- "One of the strongest products in the category. A major issue in incident response and threat hunting is that, by the time an action is classified as malicious and recorded in publicly accessible resources, the threat has likely already changed. This avoids that duplication of effort by creating a collaborative intel platform."
- "A flexible and comprehensive solution. The mind-mapping approach to UI is attractive, appears to scale well, can be used in numerous on-premises and offsite contexts, and is well-documented."
- "Great product that offers actionable industry insights. Industry correlation is a novel solution for SOC workflow."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst designated products and services in accordance with certain "implementation principles" that have been developed by the insurers and product vendors.

The implementation principle for the IronNet Collective Defense platform is:

- The user organization has installed the platform for at least 3 months and there are plans to remediate critical findings within 2 weeks.

Evaluation Process

Applications for evaluation of cybersecurity products and services were accepted from March 10 to May 15, 2020. More than 90 offerings, spanning a broad range of categories, were submitted.

The insurers evaluated eligible solutions along six criteria:

1. Reduction of cyber risk.
2. Key performance metrics.
3. Viability.
4. Efficiency.
5. Flexibility.
6. Differentiation.

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight insurers, which voted independently. Marsh did not participate in the Cyber Catalyst designation decisions.

More Information on Cyber Catalyst

The next Cyber Catalyst program will occur in 2021.

For more information on the 2020 Cyber Catalyst designated solutions, or the 2019 class of Cyber Catalyst solutions, visit the Cyber Catalyst pages on the Marsh website: www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit www.marsh.com, or contact your Marsh representative.