

IronNet Wins Major Amazon Web Services (AWS) Global Award

IronNet, an AWS APN Partner, is named Best Cybersecurity Solution for Public Sector Organizations by AWS as part of their 2021 Global AWS Public Sector Partner Awards.

McLean, VA (June 23, 2021) – IronNet announced today that it was named Best Cybersecurity Solution for Public Sector Organizations by Amazon Web Services as part of the 2021 Global Amazon Web Services (AWS) Partner Network (APN) Public Sector Partner Awards

IronNet won the Global Best Cybersecurity Solution award for its unique Collective Defense platform, including its IronDefense network detection and response (NDR) and IronDome real-time threat intelligence sharing solutions.

The AWS Global Public Sector Partner Awards recognize leaders in the channel playing a key role helping customers drive innovation and build solutions using AWS Cloud technology.

IronNet’s Collective Defense platform enables organizations to detect known and unknown threats targeting customers operating on AWS, hybrid cloud, and on-premise infrastructures. IronDefense applies advanced behavioral detection techniques in all environments to detect cyber anomalies often missed by traditional cybersecurity tools. These anomalies are then shared anonymously and in real time among members of an IronDome Collective Defense community — which is composed of a group of related organizations such as a supply chain or an industry sector — providing members with advanced warning of incoming attacks so they can respond proactively. The platform also allows participants to collaborate in real time about threats by sharing context and insights from the participating members. This exponentially increases a security team’s capacity to detect, triage, and respond to threats targeting their organizations and agencies.

Bill Welch, co-CEO of IronNet, said, “As both public and private sector organizations accelerate their digital and cloud transformation efforts to better serve their constituents, they are at the same time battling a major escalation of ransomware and other cyberattacks, which divert critical resources away from their core mission. IronNet is proud to work with AWS to offer a unique level of threat detection and collaboration through Collective Defense, allowing both public and private sector organizations to benefit from a radar-like view of incoming attacks. A Collective Defense approach is the only way to gain the upper hand against attackers and protect organizations in this demanding era of cybersecurity threats.”

IronNet’s Collective Defense platform enables public sector organizations and the private sector contractors that serve them to address President Biden’s May 2021 Executive Order on cybersecurity by:

-
- providing deep visibility into threats to agency networks
 - enabling active threat hunting and identification of anomalies
 - offering broad and consistent sharing of information about attacks on U.S. government and contractors
 - promoting consistent real-time collaboration on cyber and incident response activities across public and private organizations, and
 - enabling the adoption of a zero-trust approach.

“Every year we are impressed by how our Partners continue to innovate using cloud technology, helping their customers raise the bar on mission success, and this year is no different,” said Sandy Carter, Vice President, Worldwide Public Sector Partners and Programs, AWS. “IronNet’s Collective Defense platform is a game-changer that enables groups of organizations in the public sector to collaborate in a truly operational way, share attack intelligence in real time, and add a new layer of proactive protection to their AWS Cloud environments.”

IronNet, along with the other award winners, will be recognized at a special online event hosted by theCUBE on June 30, 2021. To learn more about how IronNet’s Collective Defense platform is adding unique value to public sector organizations, [register](#) to attend The AWS Public Sector Partner Awards 2021 on theCUBE.

About IronNet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet Cybersecurity is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a high number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

In March of 2021, IronNet and LGL Systems Acquisition Corp. (NYSE: DFNS) (“LGL”) announced that they entered into a definitive business combination agreement that will result in IronNet becoming a public company. Upon the closing of the transaction, the combined company will be named “IronNet, Inc.” and is expected to be listed on the New York Stock Exchange and trade under the ticker symbol “IRNT.”

IronNet Contacts:

IronNet Investor Contacts: Michael Bowen and Ryan Gardella: IronNetIR@icrinc.com
IronNet Media Contact: Kate Duchaney: ironnet@matternow.com

Important Information and Where to Find It

This press release relates to a proposed transaction between LGL Systems Acquisition Corp. (“LGL”) and IronNet Cybersecurity, Inc. (“IronNet”). LGL has filed with the Securities and Exchange Commission (“SEC”) a registration statement on Form S-4 (the “Registration Statement”) that includes a proxy statement to be distributed to LGL’s stockholders in connection with LGL’s solicitation of proxies for the vote by LGL’s stockholders in connection with the proposed business combination and other transactions described in the Registration

Statement, as well as a preliminary prospectus relating to the offer of LGL's securities to be issued to IronNet's stockholders in connection with the completion of the proposed business combination described in the Registration Statement. After the Registration Statement is declared effective, LGL will mail the definitive proxy statement/prospectus to stockholders of LGL as of a record date to be established for voting on the proposed business combination. LGL also will file other relevant documents from time to time regarding the proposed transaction with the SEC. INVESTORS AND SECURITY HOLDERS OF LGL ARE URGED TO READ THE PRELIMINARY PROXY STATEMENT/PROSPECTUS AND, ONCE AVAILABLE, THE DEFINITIVE PROXY STATEMENT/PROSPECTUS AND OTHER RELEVANT DOCUMENTS THAT HAVE BEEN OR WILL BE FILED BY LGL FROM TIME TO TIME WITH THE SEC CAREFULLY AND IN THEIR ENTIRETY WHEN THEY BECOME AVAILABLE BECAUSE THEY CONTAIN OR WILL CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION. Investors and security holders will be able to obtain free copies of the proxy statement/prospectus and other documents containing important information about LGL and IronNet once such documents are filed with the SEC, through the website maintained by the SEC at <http://www.sec.gov>. Copies of the documents filed with the SEC by LGL when and if available, can be obtained free of charge on LGL's website at <https://www.dfns.ai> or by directing a written request to LGL Systems Acquisition Corp., 165 Liberty St., Suite 220, Reno, NV 89501 or to info@dfnsi.ai.

Participants in the Solicitation

LGL and IronNet and their respective directors and executive officers, under SEC rules, may be deemed to be participants in the solicitation of proxies of LGL's stockholders in connection with the proposed transactions. Information regarding the persons who may, under SEC rules, be deemed to be participants in the solicitation of proxies from LGL's stockholders in connection with the proposed transactions described in the Registration Statement and the interests that such persons have in the proposed business combination are set forth in the proxy statement/prospectus included in the Registration Statement.

No Offer or Solicitation

This communication shall neither constitute an offer to sell or the solicitation of an offer to buy any securities, nor shall there be any sale of securities in any jurisdiction in which the offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such jurisdiction.

Forward Looking Statements

This press release includes "forward looking statements" within the meaning of the "safe harbor" provisions of the United States Private Securities Litigation Reform Act of 1995, including, without limitation, statements regarding IronNet's business combination with LGL. When used in this Report, the words "estimates," "projected," "expects," "anticipates," "forecasts," "plans," "intends," "believes," "seeks," "may," "will," "should," "future," "propose" and variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements, including statements relating to IronNet's future financial performance. These forward-looking statements are not guarantees of future performance, conditions or results, and involve a number of known and unknown risks,

uncertainties, assumptions and other important factors, many of which are outside LGL's or IronNet's management's control, that could cause actual results or outcomes to differ materially from those discussed in the forward-looking statements. Important factors, among others, that may affect actual results or outcomes include: the inability to complete the transactions contemplated by the proposed business combination; the inability to recognize the anticipated benefits of the proposed business combination, which may be affected by, among other things, the amount of cash available following any redemptions by LGL stockholders; the ability to meet the NYSE's listing standards following the consummation of the transactions contemplated by the proposed business combination; costs related to the proposed business combination; IronNet's ability to execute on its plans to develop and market new products and the timing of these development programs; IronNet's estimates of the size of the markets for its products; the rate and degree of market acceptance of IronNet's products; the success of other competing technologies that may become available; IronNet's ability to identify and integrate acquisitions; the performance of IronNet's products; potential litigation involving LGL or IronNet; and general economic and market conditions impacting demand for IronNet's products. Other factors include the possibility that the proposed transaction does not close, including due to the failure to receive required security holder approvals, or the failure of other closing conditions. The foregoing list of factors is not exhaustive. You should carefully consider the foregoing factors and the other risks and uncertainties described under the heading "Risk Factors" in the proxy statement/prospectus included in the Registration Statement, LGL's Annual Report on Form 10-K (as amended), Quarterly Reports on Form 10-Q, and other documents filed by LGL from time to time with the SEC. These filings identify and address other important risks and uncertainties that could cause actual events and results to differ materially from those contained in the forward-looking statements. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and neither LGL nor IronNet undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.