Filed by LGL Systems Acquisition Corp.
pursuant to Rule 425 under the Securities Act of 1933
and deemed filed pursuant to Rule 14a-12
under the Securities Exchange Act of 1934
Subject Company: LGL Systems Acquisition Corp.
Commission File No. 333-256129

New Research Finds the SolarWinds Cyber Attack Cost Affected Companies in Key Sectors 11% of Total Annual Revenue on Average

Results indicate cyber-related information sharing is increasing, signaling a positive response to national- and industry-level calls to action

June 28, 2021 08:00 AM Eastern Daylight Time

MCLEAN, Va. – (BUSINESS WIRE) **–** IronNet Cybersecurity, in its mission to transform cybersecurity through Collective Defense, released today its 2021 Cybersecurity Impact Report assessing timely topics such as the estimated cost per enterprise of the SolarWinds cyber attack, executive-level engagement in attack responses, and the effect of information sharing on an organization's overall security posture.

IronNet commissioned independent research firm Sapio to survey 473 IT security decision makers in the technology, public services, financial, and utilities sectors across the United States, United Kingdom, and Singapore.

The report revealed a complex relationship between the reported level of confidence organizations have in their cybersecurity posture and their ongoing attack volume and impact: that is, despite rising confidence, incidents are increasing, too. While 92 percent of respondents express confidence in their current security technology stack, adversaries are still evading traditional defensive technologies. Nearly half of respondents cited a rise in cyber incidents in the past 12 months due to the increasing sophistication of attacks; and the SolarWinds attack cost, on average, 11 percent of affected respondents' annual revenue.

What is helping, however, is information sharing: Responses revealed positive effects of cyber-related information sharing on an organization's overall cybersecurity posture.

- 90 percent of respondents indicated that the security posture of their company has improved over the past two years.
- 72 percent of companies who have increased information sharing with industry peers report their overall security posture has improved over the past two years.

Despite the reported benefits of information sharing for improving cybersecurity, respondents indicated that there are still obstacles that limit collaboration among industry peers: concerns about data privacy and liability (53 percent), the lack of an automated or standard mechanism to share information with peers (34 percent), and the fact that shared information is not timely or relevant by the time companies receive it (33 percent).

General (Ret.) Keith Alexander, Founder and Co-CEO of IronNet, said, “Organizations are clearly struggling to keep up with the volume and impact of cyber attacks coming from well-funded and well-organized nation states. We believe that the main reason for this is that every organization is still trying to battle these attacks individually, when they should be working together to create an exponentially stronger defense. Sharing and operationalizing attack intelligence through a Collective Defense model provides that automated, real-time solution that is missing in the market, and can be done securely, using anonymized data. This is the only way to ultimately shift the balance of power away from the attackers. Fortunately, our survey data shows that organizations are starting to increase their information sharing and are seeing benefits from doing so. This is a positive signal towards the adoption of Collective Defense.”

Through the Collective Defense model, IronNet is taking information sharing and collaboration to a new level by enabling anonymized, real-time threat sharing to maximize visibility into the attack landscape and minimize impact on an organization’s operations.

Answering Calls to Action

Calls for faster, more relevant threat information sharing continue to come from industry- and national-level cybersecurity initiatives. Former President Barack Obama initiated momentum on this concept with his 2015 Executive Order on Cybersecurity, which promoted private sector cybersecurity information sharing. In March 2020, the U.S. Cyberspace Solarium Commission report emphasized this same call to action, as did President Biden’s U.S. Presidential Executive Order on Improving the Nation’s Cybersecurity in May 2021, emphasizing threat information sharing as a primary theme and signaling to the public and private sectors that still more of this type of collaboration is needed in a timely, immediate, and relevant way.

The report’s findings related to the SolarWinds/SUNBURST attack revealed that organizations are urgently turning toward a threat-sharing model. The report provided an inside look into the financial damage stemming from this widespread supply chain attack that struck 18,000 companies and nine U.S. government agencies: Among the 85 percent of respondents affected by SolarWinds, nearly one third said their organization felt a significant financial impact from the attack. In fact, on average across all respondents, the attack cost affected companies 11 percent of their annual revenue.

These findings demonstrate the pressing need for a transformative approach to cybersecurity — an approach that operationalizes timely, relevant, and actionable threat sharing among industry peers and with the government. IronNet’s Collective Defense platform includes network detection and response (NDR) capabilities for advanced behavioral detection of unknown cyber threats via its IronDefense solution, and real-time threat intelligence sharing with its IronDome solution. The Collective Defense platform provides a radar-like view of potential incoming attacks; this real-time picture empowers organizations to more proactively defend against cyber attacks — both on-premise and in the cloud.

Visit ironnet.com/collective-defense for more information and view the full 2021 Cybersecurity Impact Report at ironnet.com/cyber-impact-report. The reference to IronNet’s website address does not constitute incorporation by reference of the information contained at or available through IronNet’s website, and you should not consider it to be a part of this press release.

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

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.

###