INTRUSION INC
Form 10-K
March 28, 2019

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

FORM 10-K

(Mark One)

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2018

OR

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

COMMISSION FILE NUMBER 0-20191

Intrusion Inc.

(Exact name of registrant as specified in its charter)

DELAWARE (State or other jurisdiction of incorporation or organization)	**75-1911917** (I.R.S. Employer Identification No.)
1101 EAST ARAPAHO ROAD, SUITE 200 **RICHARDSON, TEXAS** (Address of principal executive offices)	**75081** (Zip Code)

Registrant’s telephone number, including area code: **(972) 234-6400**

Securities registered pursuant to Section 12(b) of the Act: **None**

Securities registered pursuant to Section 12(g) of the Act:

Common Stock, $0.01 par value

(Title of class)

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act.

Yes No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the past 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.
No

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes No

Indicate by check mark if disclosure of delinquent filers in response to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	Accelerated filer
Non-accelerated filer	Smaller reporting company
Emerging growth company	

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act).

Yes No

State the aggregate market value of the voting and non-voting common equity held by non-affiliates computed by reference to the price at which the common equity was last sold, or the average bid and asked price of such common equity, as of June 30, 2018: $15,043,000.

As of February 28, 2019, 13,515,236 shares of the issuer’s Common Stock were outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's definitive Proxy Statement filed in connection with the Registrant's 2018 Annual Meeting of Stockholders are incorporated by reference into Part III of this Annual Report on Form 10-K.

INTRUSION INC.

INDEX

PART I

Item 1. Description of Business.

In addition to the historical information contained herein, the discussion in this Annual Report on Form 10-K contains certain forward-looking statements, within the meaning of the Private Securities Litigation Reform Act of 1995, that involve risks and uncertainties, such as statements concerning:

- growth and anticipated operating results;
- developments in our markets and strategic focus;
- new products and product enhancements;
- potential acquisitions and the integration of acquired businesses, products and technologies;
- strategic relationships and future economic and business conditions.

The cautionary statements made in this Form 10-K should be read as being applicable to all related forward-looking statements whenever they appear in this Form 10-K. Our actual results could differ materially from the results discussed in the forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, those discussed under the section captioned “Risk Factors” in Item 1A of this Form 10-K as well as those cautionary statements and other factors set forth elsewhere herein.

General

We develop, market and support a family of entity identification, high speed data mining, cybercrime and advanced persistent threat detection products.

Our product families include:

- TraceCop for entity identification, cybercrime detection and disclosure, and;
- Savant for high speed data mining and analytics, and advanced persistent threat detection.

Intrusion's products help protect critical information assets by quickly detecting, protecting, analyzing and reporting attacks or misuse of classified, private and regulated information for government and enterprise networks.

We market and distribute our products through a direct sales force to:

- end-users, and
- value-added resellers.

Our end-user customers include:

- U.S. federal government entities,
- state and local government entities,
- large and diverse conglomerates,
- manufacturing entities, and
- other customers.

We were organized in Texas in September 1983 and reincorporated in Delaware in October 1995. Our principal executive offices are located at 1101 East Arapaho Road, Suite 200, Richardson, Texas 75081, and our telephone number is (972) 234-6400. Our website URL is www.intrusion.com. References to the "Company", "we", "us", "our", "Intrusion" or "Intrusion Inc." refer to Intrusion Inc. and its subsidiaries. TraceCop and Savant are trademarks of Intrusion Inc.

Government Sales

Sales to U.S. government customers accounted for 83.9% of our revenues for the year ended December 31, 2018, compared to 81.6% of our revenue in 2017. We expect to continue to derive a substantial portion of our revenues from sales to governmental entities in the future as we continue to market our entity identification products and data mining products to the government. Sales to the government present risks in addition to those involved in sales to commercial customers that could adversely affect our revenues, including potential disruption due to irregularities in or interruptions to appropriation and spending patterns, delays in approving a federal budget and the government's reservation of the right to cancel contracts and purchase orders for its convenience.

Generally, we make our sales under purchase orders and contracts. Our customers, including government customers, may cancel their orders or contracts with little or no prior notice and without penalty. Although we transact business with various government entities, we believe that the cancellation of any particular order in itself could have a material adverse effect on our financial results. Because we derive and expect to continue to derive a substantial portion of our revenue from sales to government entities, a large number of cancelled or renegotiated government orders or contracts could have a material adverse effect on our financial results. Currently, we are not aware of any proposed cancellation or renegotiation of any of our existing arrangements with government entities.

Industry Background

We develop, market and support a family of entity identification, data mining and advanced persistent threat detection products. Our product families include:

The TraceCop™ product line, which includes a number of our proprietary supporting tools, allows our customers and in-house cyber analysts to accurately discover and help identify 'bad actors' associated with cybercrime.

The Savant™ product is a 'purpose-built', very high-speed network data mining and analytics software package that is easily installed on commercial off the shelf platforms.

Our customers use our products as an integral part of protecting their critical infrastructure and data information assets. By quickly detecting, protecting, analyzing and reporting attacks, along with the potential misuse of classified information, we have become a key component to the daily challenges of cyber security for both government and large enterprises.

Products

TraceCop

Our TraceCop product family includes a database of worldwide IP addresses, registrant information and their associations, along with a plurality of related IP information, some dating back nearly two decades. When combined with Intrusion's multitude of cyber security 'global threat feeds', along with our TraceCop family of proprietary supporting tools, this vast and ever expanding capability is used in conjunction with our customer's data to help identify areas of vulnerability and potential cyber security threats. In addition to it's extensive capability, the TraceCop family includes analytical software with a GUI interface to assist the analysts in locating cybercriminals and other potential 'bad actors' or network anomalies. We offer our customers a daily, weekly or monthly enrichment service to assist them in the culling of 'good' data traffic from potential threats.

Intrusion licenses TraceCop to our customers for a yearly fee and offers scheduled updates. Intrusion will either install and update the database at the Intrusion facility or install TraceCop on a customer server onsite. Updates are delivered via secure Internet feed or removable storage devices.

Savant

Savant is a high speed network data mining and analysis product which organizes the data into networks of relationships and associations. Its patented design exceeds performance expectations and ensures 'deep dives' into data-in-motion in order to quickly and accurately detect advanced persistent threats. Savant can operate on networks with data flows of over 20 gigabits per second, and still maintain a 100% inspection rate of all packets.

The Savant solution provides real-time access and insight into a company's own indisputable and quantifiable network data for more effective, unbiased examination of their flows. Uses of the Savant product include data mining, data loss prevention, advanced persistent threat detection and identification of Internet habits of network users. Savant is a software product which we license to our customers for which we sell data updates. We also offer the option to fully implement a server and re-sell to the customer as a turn-key solution.

Third-Party Products

We currently resell standard commercially available computers and servers from various vendors which we integrate with our different software products for implementation into our customer networks. We do not consider any of these third party relationships to be material to the Company's business or results of operations.

Customer Services

Our product sales may include installation and threat data interpretation.

Product Development

The network security industry is characterized by rapidly changing technology standards and customer demands all shaped by the current state of the economy. We believe that our future success depends in large part upon the timely enhancement of existing products as well as the development of new technologically advanced products that meet cybersecurity industry needs and perform successfully and efficiently. We are currently marketing TraceCop and Savant products to meet emerging market requirements and are continuously engaged in testing to ensure that our products interoperate with other manufacturers' products, which comply with industry standards.

During 2018 and 2017, our research and development expenditures were approximately $1.2 and $2.2 million, respectively. All of our expenditures for research and development have been expensed as incurred. At December 31, 2018, we had 21 employees engaged in research, product development and engineering. At certain times during the year, research and development labor expense has been shifted to direct labor to support ongoing projects.

Manufacturing and Supplies

Our internal manufacturing operations consist primarily of software, packaging, testing and quality control of finished units.

The hardware we sell are standard off-the-shelf products.

Intellectual Property and Licenses

Our success and our ability to compete are dependent, in part, upon our proprietary technology. We principally rely on a combination of contractual rights, trade secrets and copyright laws to establish and protect our proprietary rights in our products. In addition, we have received two patents. We have also entered into non-disclosure agreements with our suppliers, resellers and certain customers to limit access to and disclosure of proprietary information. There can be no assurance that the steps taken by us to protect our intellectual property will be adequate to prevent misappropriation of our technology or that our competitors will not independently develop technologies that are substantially equivalent or superior to our technology.

We have entered into software and product license agreements with various suppliers. These license agreements provide us with additional software and hardware components that add value to our security products. These license agreements do not provide proprietary rights that are unique or exclusive to us and are generally available to other parties on the same or similar terms and conditions, subject to payment of applicable license fees and royalties. We do not consider any of the product license, software or supplier agreements to be material to our business, but rather complementary to our business and product offerings.

Sales, Marketing and Customers

Field Sales Force. Our direct sales organization focuses on major account sales, channel partners including distributors, value added resellers (VARs) and integrators; promotes our products to current and potential customers; and monitors evolving customer requirements. The field sales and technical support force provides training and technical support to our resellers and end users and assists our customers in designing cyber secure data networking solutions. We currently conduct sales and marketing efforts from our principal office in Richardson (Dallas), Texas. In addition, we have sales personnel, sales engineers or sales representatives located in Virginia and California.

Resellers. Resellers such as domestic and international system integrators and VARs sell our products as stand-alone solutions to end users and integrate our products with products sold by other vendors into network security systems that are sold to end users. Our field sales force and technical support organization provide support to these resellers. Our agreements with resellers are non-exclusive, and our resellers generally sell other products that may compete with our products. Resellers may place higher priority on products of other suppliers who are larger and have more name recognition, and there can be no assurance that resellers will continue to sell and support our products.

Foreign Sales. Export sales did not account for any revenue in 2018 and 2017. See "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in this report for a geographic breakdown of our revenue in 2018 and 2017.

Marketing. We have implemented several methods to market our products, including participation in trade shows and seminars, distribution of sales literature and product specifications and ongoing communication with our resellers and installed base of end-user customers.

Customers. Our end-user customers include U.S. federal government, state and local government entities, large and diversified conglomerates and manufacturing entities. Sales to certain customers and groups of customers can be impacted by seasonal capital expenditure approval cycles, and sales to customers within certain geographic regions can be subject to seasonal fluctuations in demand.

In 2018, 83.9% of our revenue was derived from a variety of U.S. government entities through direct sales and indirectly through system integrators and resellers. These sales are attributable to ten U.S. Government customers through direct and indirect channels; four exceeded 10% of total revenue individually in 2018. Comparatively, sales to the U.S. Government through direct and indirect channels totaled 81.6% of total revenues for 2017. Those sales were attributable to six U.S. Government customers through direct and indirect channels; three exceeded 10% of total revenue individually in 2017. A reduction in our sales to U.S. government entities could have a material adverse effect on our business and operating results if not replaced.

Backlog. We believe that only a small portion of our order backlog is non-cancelable and that the dollar amount associated with the non-cancelable portion is immaterial. We purchase, or contract for the purchase of, our inventory based upon our forecast of customer demand and we maintain inventories in advance of receiving firm orders from customers. Commercial orders are generally fulfilled within two days to two weeks following receipt of an order. Certain orders may be scheduled over several months, generally not exceeding one year.

Customer Support, Service and Warranty. We service, repair and provide technical support for our products. Our field sales and technical support force works closely with resellers and end-user customers on-site and by telephone to assist with pre- and post-sales support services such as network security design, system installation and technical consulting. By working closely with our customers, our employees increase their understanding of end-user requirements and provide input to the product development process.

We warrant all of our products against defects in materials and workmanship for periods ranging from 90 days to 36 months. Before and after expiration of the product warranty period, we offer both on-site and factory-based support, parts replacement and repair services. Extended warranty services are separately invoiced on a time and materials

basis or under an annual maintenance contract.

Competition

The market for network and data protection security solutions is intensely competitive and subject to frequent product introductions with new technologies, improved price and performance characteristics. Industry suppliers compete in areas such as conformity to existing and emerging industry standards, interoperability with networking and other security products, management and security capabilities, performance, price, ease of use, scalability, reliability, flexibility, product features and technical support. The market for identity identification and data mining is more fragmented and thus allows more opportunities for small companies to compete in.

There are numerous companies competing in various segments of the data security markets. At this time, we have limited competitors for TraceCop; however, we expect competitors to emerge in the future. These competitors perform only a portion of the functions that we currently perform with TraceCop. Also, we have been collecting the TraceCop data continuously for more than ten years. We believe that none of our current or future competitors have the ability to provide this historical data. In our newest market segment, data mining and advanced persistent threat detection, we compete with several companies including Niksun, NetScout, Fireeye and Palo Alto Networks.

Furthermore, some of our competitors have substantially greater financial, technical, sales and marketing resources, better name recognition and a larger customer base than we do. Even if we do introduce advanced products that meet evolving customer requirements in a timely manner, there can be no assurance that our new products will gain market acceptance.

Certain companies in the network security industry have expanded their product lines or technologies in recent years as a result of acquisitions. Further, more companies have developed products which conform to existing and emerging industry standards and have sought to compete on the basis of price. We anticipate increased competition from large networking equipment vendors, which are expanding their capabilities in the network security market. In addition, we anticipate increased competition from private “start-up” companies that have developed, or are developing, advanced security products. Increased competition in the security industry could result in significant price competition, reduced profit margins or loss of market share, any of which could have a material adverse effect on our business, operating results and financial condition. There can be no assurance that we will be able to compete successfully in the future with current or new competitors.

Employees

As of December 31, 2018, we employed a total of 31 full time persons, including 6 in sales, marketing and technical support, 21 in research, product development and engineering, and 4 in administration and finance.

None of our employees are represented by a labor organization, and we are not a party to any collective bargaining agreement. We have not experienced any work stoppages and consider our relations with our employees to be good.

Competition in the recruiting of personnel in the networking and data security industry is intense. We believe that our future success will depend in part on our continued ability to hire, motivate and retain qualified management, sales, marketing, and technical personnel. To date, we have not experienced significant difficulties in attracting or retaining qualified employees.

Item 1A. Risk Factors

In addition to the other information in this Form 10-K, the following factors should be considered in evaluating Intrusion Inc. and our business.

We may not have sufficient cash to operate our business and may not be able to maintain certain liquidity requirements under our existing debt instruments. Additional debt and equity offerings to fund future operations may not be available and, if available, may significantly dilute the value of our currently outstanding common stock.

As of December 31, 2018, we had cash and cash equivalents of approximately $1,652,000, up from approximately $224,000 as of December 31, 2017. We generated a net income of $2,287,000 for the year ended December 31, 2018 compared to net loss of $30,000 for the year ended December 31, 2017. The net loss in 2017 included other income of $928,000, of which $872,000 came from the sale of certain unused IP addresses and $56,000 from the sale of an investment. As of February 28, 2019, in addition to cash and cash equivalents, $885,000 of funding is available from a promissory note to borrow up to $2.7 million from G. Ward Paxton, the Company's Chief Executive Officer. We are obligated to make payments of accrued dividends on all our outstanding shares of preferred stock that will reduce our available cash resources. Based on projections of growth in revenue and net income in the coming quarters, and the borrowings available previously mentioned, we believe that we will have sufficient cash resources to finance our operations and expected capital expenditures through March 31, 2020. We expect to fund our operations through anticipated Company profits, borrowings from the Company's CEO, and possibly additional investments of private equity and debt, which, if we are able to obtain, could have the effect of diluting our existing common stockholders, perhaps significantly. Any equity or debt financings, if available at all, may be on terms which are not favorable to us and, in the case of equity financings, may result in dilution to our stockholders. If our operations do not generate positive cash flow in the upcoming year, or if we are not able to obtain additional debt or equity financing on terms and conditions acceptable to us, if at all, we may be unable to implement our business plan, fund our liquidity needs or even continue our operations.

We had a net income of $2.3 million for the year ended December 31, 2018 and have an accumulated deficit of 59.2 million as of December 31, 2018. To continue profitability, we must continue to generate consistent or increased revenue.

For the year ended December 31, 2018, we had a net income of $2.3 million and had an accumulated deficit of approximately $59.2 million as of December 31, 2018, compared to a net loss of $30 thousand and an accumulated deficit of approximately $61.5 million as of December 31, 2017. We need to continue to generate consistent or greater revenue from the sales of our products and services if we are to continue profitability. If we are unable to generate consistent or greater revenue growth, net losses may occur and we may not be able to generate positive cash flow from operations in the future.

If our products do not achieve market acceptance, our revenue growth may suffer.

Our security products, advanced persistent threat detection and entity identification products have been in the market place for a limited period of time and may have longer sales cycles than our previous products. Accordingly, we may not achieve the meaningful revenue growth needed to sustain operations. We can provide no assurances that sales of our newer products will grow or generate sufficient revenues to sustain our business. If we are unable to recognize revenues due to longer sales cycles or other problems, our results of operations will be adversely affected, perhaps materially.

We have not yet received broad market acceptance for our products. We cannot assure you that our present or future products will achieve market acceptance on a sustained basis. In order to achieve market acceptance and achieve future revenue growth, we must introduce complementary security products, incorporate new technologies into our existing product lines and design, develop and successfully commercialize higher performance products in a timely manner. There is no assurance that we will be able to offer new or complementary products that gain market acceptance quickly enough to avoid decreased revenues during current or future product introductions or transitions.

A large percentage of our revenues are received from U.S. government entities, and the loss of any one of these customers could reduce our revenues and materially harm our business and prospects.

A large percentage of our revenues result from sales to U.S. government entities. If we were to lose one or more of these key relationships, our revenues could decline and our business and prospects may be materially harmed. We expect that even if we are successful in developing relationships with non-governmental customers, our revenues will continue to be concentrated among government entities. For the years ended December 31, 2016, 2017 and 2018, sales to U.S. government entities collectively accounted for 69.3%, 81.6% and 83.9% of our total net revenues, respectively. The loss of any of these key relationships may send a negative message to other U.S. government entities or non-governmental customers concerning our product offering. There is no assurance that U.S. government entities will be customers of ours in future periods or that we will be able to diversify our customer portfolio to adequately mitigate the risk of loss of any of these customers.

Government customers involve unique risks, which could adversely impact our revenues.

We expect to continue to derive a substantial portion of our revenues from U.S. government customers in the future. Sales to the government present risks in addition to those involved in sales to commercial customers, including potential disruption due to appropriation and spending patterns, delays in approving a federal budget and the government’s right to cancel contracts and purchase orders for its convenience. General political and economic conditions, which we cannot accurately predict, directly and indirectly may affect the quantity and allocation of

expenditures by federal departments. In addition, obtaining government contracts may involve long purchase and payment cycles, competitive bidding, qualification requirements, delays or changes in funding, budgetary constraints, political agendas, extensive specification development and price negotiations and milestone requirements. Each government entity also maintains its own rules and regulations with which we must comply and which can vary significantly among departments. As a result, cutbacks or re-allocations in the federal budget or losses of government sales due to other factors could have a material adverse effect on our revenues and operating results.

We are highly dependent on sales made through indirect channels, the loss of which would materially adversely affect our operations.

For the years ended December 31, 2016, 2017 and 2018, we derived 70.7%, 81.6% and 83.9% of our revenues from sales through indirect sales channels, such as distributors, value-added resellers, system integrators, original equipment manufacturers and managed service providers. We must expand our sales through these indirect channels in order to increase our revenues. We cannot assure you that our products will gain market acceptance in these indirect sales channels or that sales through these indirect sales channels will increase our revenues. Further, many of our competitors are also trying to sell their products through these indirect sales channels, which could result in lower prices and reduced profit margins for sales of our products.

The payment of dividends on our preferred stock may strain our cash resources.

On March 25, 2004, we completed a $5,000,000 private placement pursuant to which we issued 1,000,000 shares of our 5% Convertible Preferred Stock (the “Series 1 Preferred Stock”) and warrants to acquire 556,619 shares of our common stock. The conversion price for the Series 1 Preferred Stock is $3.144 per share. As of February 28, 2019, there were 200,000 shares of the Series 1 Preferred Stock outstanding, representing approximately 318,065 shares of common stock upon conversion.

On March 28, 2005, we completed a $2,663,000 private placement pursuant to which we issued 1,065,200 shares of our Series 2 5% Convertible Preferred Stock (the “Series 2 Preferred Stock”) and warrants to acquire 532,600 shares of our common stock. The conversion price for the Series 2 Preferred Stock is $2.50 per share. As of February 28, 2019, there were 460,000 shares of the Series 2 Preferred Stock outstanding, representing 460,000 shares of common stock upon conversion.

On December 2, 2005, we completed a $1,230,843 private placement pursuant to which we issued 564,607 shares of our Series 3 5% preferred stock (the "Series 3 Preferred Stock") and warrants to acquire 282,306 shares of our common stock. The conversion price for the Series 3 Preferred Stock is $2.18 per share. As of February 28, 2019, there were 289,377 shares of Series 3 Preferred Stock outstanding, representing 289,377 shares of common stock upon conversion.

If we are unable to pay scheduled dividends on shares of our preferred stock it could potentially result in additional consequences, some of them material.

Delaware law provides that we may only pay dividends out of our capital surplus or, if no surplus is available, out of our net profits for the fiscal year the dividend is declared and/or the preceding fiscal year. We have become delinquent in our dividend payments that became past due because we did not have a capital surplus or fiscal year net profits. However, in light of our net profits for the fiscal year ended December 31, 2018, we are able to and have paid these past due dividends as of the date of this Annual Report. However, dividends continue to accrue on all our outstanding shares of preferred stock, regardless of whether we are legally able to pay them, and we cannot assure you that our net assets will exceed our stated capital or that we will have sufficient net profits in order to pay these dividends as they continue to accrue in the future. If we are unable to pay dividends on our preferred stock, we are required to accrue an additional late fee penalty of 18% per annum on the unpaid dividends for the Series 2 Preferred Stock and Series 3 Preferred Stock. In addition to this late penalty, the holders of our Series 2 Preferred Stock and Series 3 Preferred Stock could elect to present us with written notice of any failure to pay dividends as scheduled, in which case we would have 45 days to cure such a breach. In the event that we failed to cure the breach, the holders of these shares of preferred stock would then have the right to require us to redeem their shares of preferred stock for a cash amount calculated in accordance with their respective certificates of designation.

During the year ended December 31, 2018, we accrued $50,000 in dividends to the holders of our 5% Preferred Stock, $57,000 in dividends to the holders of our Series 2 5% Preferred Stock and $32,000 in dividends to the holders of our Series 3 5% Preferred Stock. As of December 31, 2018 and 2017, we had $594,000 and $447,000 in accrued and unpaid dividends included in other current liabilities. Delaware law provides that we may only pay dividends out of our capital surplus or, if no surplus is available, out of our net profits for the fiscal year the dividend is declared and/or the preceding fiscal year. This has been in effect since December 31, 2014. However, in light of our net profits for the fiscal year ended December 31, 2018, we are able to and have paid these past due dividends as of the date of this Annual Report. However, dividends continue to accrue on all our outstanding shares of preferred stock, regardless of whether we are legally able to pay them, and we cannot assure you that our net assets will exceed our stated capital or that we will have sufficient net profits in order to pay these dividends as they continue to accrue in the future. If we are unable to pay dividends on our preferred stock, we will be required to accrue an additional late fee penalty of 18% per annum on the unpaid dividends for the Series 2 Preferred Stock and Series 3 Preferred Stock.

You will experience substantial dilution upon the conversion or redemption of the shares of preferred stock or in the event we raise additional funds through the issuance of new shares of our common stock or securities convertible or exercisable into shares of common stock.

On February 28, 2019, we had 13,515,236 shares of common stock outstanding. Upon conversion of all outstanding shares of preferred stock, we would have 14,582,679 shares of common stock outstanding, approximately an 7.9% increase in the number of shares of our common stock outstanding.

In addition, management may issue additional shares of common stock or securities exercisable or convertible into shares of common stock in order to finance our continuing operations. Any future issuances of such securities would have additional dilutive effects on the existing holders of our Common Stock.

Further, the occurrence of certain events could entitle holders of our Series 2 Preferred Stock and Series 3 Preferred Stock to require us to redeem their shares for a certain number of shares of our common stock. Assuming (i) we have paid all liquidated damages and other amounts to the holders, (ii) paid all outstanding dividends, (iii) a volume weighted average price of $4.08, which was the ten-day volume weighted average closing price of our common stock on March 1, 2019, and (iv) our 13,515,236 shares of common stock outstanding on February 28, 2019, upon exercise of their redemption right by the holders of the Series 3 Preferred Stock and the Series 2 Preferred Stock, we would be obligated to issue approximately 107,000 shares of our common stock. This would represent an increase of approximately 0.8% in the number of shares of our common stock as of February 28, 2019.

The conversion of preferred stock we issued in the private placements may cause the price of our common stock to decline.

The holders of the shares of our 5% Preferred Stock may freely convert their shares of preferred stock and sell the underlying shares of common stock pursuant to Rule 144 of the Securities and Exchange Commission. As of February 28, 2019, 800,000 shares of our 5% Preferred Stock had converted into 1,272,263 shares of common stock.

The holders of the shares of Series 2 5% Preferred Stock may freely convert their shares of preferred stock and sell the underlying shares of common stock pursuant to Rule 144 of the Securities and Exchange Commission. As of February 28, 2019, 605,200 shares of Series 2 Preferred Stock had converted into 605,200 shares of common stock.

The holders of the shares of Series 3 5% Preferred Stock may freely convert their shares of Series 3 Preferred Stock and sell the underlying shares of common stock pursuant to Rule 144 of the Securities and Exchange Commission. As of February 28, 2019, 275,230 shares of Series 3 Preferred Stock had converted into 275,230 shares of common stock.

For the four weeks ended on March 1, 2019, the average daily trading volume of our common stock on the OTCQB was 23,134 shares. Consequently, if holders of preferred stock elect to convert their remaining shares and sell a material amount of their underlying shares of common stock on the open market, the increase in selling activity could cause a decline in the market price of our common stock. Furthermore, these sales, or the potential for these sales, could encourage short sales, causing additional downward pressure on the market price of our common stock.

Certain rights of the holders of our preferred stock and the terms of our secured credit line may hinder our ability to raise additional financing.

Under the terms of our preferred stock instruments, we cannot issue shares of capital stock with rights senior to those of our existing 5% Preferred Stock, Series 2 5% Preferred Stock or Series 3 5% Preferred Stock without the approval of at least a majority of the holders of our 5% Preferred Stock, all of the holders of our Series 2 5% Preferred Stock, and holders of at least 75% of our Series 3 5% Preferred Stock voting or acting as separate classes. We also cannot incur certain indebtedness without the approval of at least a majority of the holders of each class of our Preferred Stock.

You will experience substantial dilution upon the exercise of certain stock options currently outstanding.

On February 28, 2019, we had 13,515,236 shares of common stock outstanding. Upon the exercising of current options issued at or below the exercise price of $2.73, we will have approximately 14,421,000 shares of common stock outstanding, a 6.7% increase in the number of shares of our common stock outstanding.

We resemble a developmental stage company and our business strategy may not be successful.

We depend exclusively on revenues generated from the sale of our network security/advanced persistent threat detection products (Savant), which have received limited market acceptance and our entity identification, data mining and analytic product (TraceCop). We can provide no assurances that our products will ever achieve widespread market acceptance or that an adequate market for these products will ever emerge. Consequently, we resemble a developmental stage company and will face the following inherent risks and uncertainties:

- the need for our entity identification, data mining and advanced persistent threat detection products to achieve market acceptance and produce a sustainable revenue stream;
- our ability to manage costs and expenses;
- our dependence on key personnel;
- our ability to obtain financing on acceptable terms; and
- our ability to offer greater value than our competitors.

Our business strategy may not successfully address these risks. If we fail to recognize significant revenues from the sales of our entity identification, data mining and advanced persistent threat detection products, our business, financial condition and operating results would be materially adversely affected.

If we fail to respond to rapid technological changes in the network security industry, we may lose customers or our products may become obsolete.

The network security industry is characterized by frequent product introductions, rapidly changing technology and continued evolution of new industry standards. We must also introduce upgrades to our products rapidly in response to customer needs such as new computer viruses or other novel external attacks on computer networks. In addition, the nature of the network security industry requires our products to be compatible and interoperable with numerous security products, networking products, workstation and personal computer architectures and computer and network operating systems offered by various vendors, including our competitors. As a result, our success depends upon our ability to develop and introduce in a timely manner new products and enhancements to our existing products that meet changing customer requirements and evolving industry standards. The development of technologically advanced network security products is a complex and uncertain process requiring high levels of innovation, rapid response and accurate anticipation of technological and market trends. We cannot assure you that we will be able to identify, develop, manufacture, market or support new or enhanced products successfully in a timely manner. Further, we or our competitors may introduce new products or product enhancements that shorten the life cycle of our existing products or cause our existing products to become obsolete.

We face intense competition from both start-up and established companies that may have significant advantages over us and our products.

The market for our products is intensely competitive. There are numerous companies competing with us in various segments of the data security markets, and their products may have advantages over our products in areas such as conformity to existing and emerging industry standards, interoperability with networking and other security products, management and security capabilities, performance, price, ease of use, scalability, reliability, flexibility, product features and technical support.

Our principal competitors in the data mining and advanced persistent threat market include Niksun, NetScout, Fireeye (Mandiant) and Palo Alto Networks. Our current and potential competitors may have one or more of the following significant advantages over us:

- greater financial, technical and marketing resources;

- better name recognition;

more comprehensive security solutions;

better or more extensive cooperative relationships; and

larger customer base.

We cannot assure you that we will be able to compete successfully with our existing or new competitors. Some of our competitors may have, in relation to us, one or more of the following: longer operating histories, longer-standing relationships with OEM and end-user customers and greater customer service, public relations and other resources. As a result, these competitors may be able to more quickly develop or adapt to new or emerging technologies and changes in customer requirements, or devote greater resources to the development, promotion and sale of their products. Additionally, it is likely that new competitors or alliances among existing competitors could emerge and rapidly acquire significant market share.

Our management and larger stockholders exercise significant control over our Company and have the ability to approve or take actions that may be in conflict to your interests.

As of February 28, 2019, our executive officers, directors and preferred stockholders beneficially own approximately 31% of our voting power. In addition, other related parties control approximately 27% of our voting power. As a result, these stockholders will be able to exercise significant control over all matters requiring stockholder approval, including the election of directors and approval of significant corporate transactions, which could delay or prevent someone from acquiring or merging with us. These stockholders may use their influence to approve or take actions that may be adverse to the interests of other holders of our Common Stock. Further, we contemplate the possible issuance of shares of our Common Stock or of securities exercisable or convertible into shares of our Common Stock in the future to our Chief Executive Officer and Chief Financial Officer. Any such issuance will increase the percentage of stock our Chief Executive Officer, Chief Financial Officer and our management group beneficially hold.

Our products are highly technical and if they contain undetected errors, our business could be adversely affected and we might have to defend lawsuits or pay damages in connection with any alleged or actual failure of our products and services.

Our products are highly technical and complex, are critical to the operation of many networks and, in the case of our security products, provide and monitor network security and may protect valuable information. Our products have contained and may contain one or more undetected errors, defects or security vulnerabilities. Some errors in our products may only be discovered after a product has been installed and used by end customers. Any errors or security vulnerabilities discovered in our products after commercial release could result in loss of revenues or delay in revenue recognition, loss of customers and increased service and warranty cost, any of which could adversely affect our business and results of operations. In addition, we could face claims for product liability, tort or breach of warranty. Defending a lawsuit, regardless of its merit, is costly and may divert management's attention. In addition, if our business liability insurance coverage is inadequate or future coverage is unavailable on acceptable terms or at all, our financial condition could be harmed.

A breach of network security could harm public perception of our security products, which could cause us to lose revenues.

If an actual or perceived breach of network security occurs in the network of a customer of our security products, regardless of whether the breach is attributable to our products, the market perception of the effectiveness of our products could be harmed. This could cause us to lose current and potential end customers or cause us to lose current and potential value-added resellers and distributors. Because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, we may be unable to anticipate these techniques.

If our products do not interoperate with our customers' networks, installations will be delayed or cancelled and could harm our business.

Our products are designed to interface with our customers' existing networks, each of which have different specifications and utilize multiple protocol standards and products from other vendors. Many of our customers' networks contain multiple generations of products that have been added over time as these networks have grown and evolved. Our products will be required to interoperate with many or all of the products within these networks as well as future products in order to meet our customers' requirements. If we find errors in the existing software or defects in the hardware used in our customers' networks, we may have to modify our software or hardware to fix or overcome these errors so that our products will interoperate and scale with the existing software and hardware, which could be costly and negatively impact our operating results. In addition, if our products do not interoperate with those of our customers' networks, demand for our products could be adversely affected, orders for our products could be cancelled or our products could be returned. This could hurt our operating results, damage our reputation and seriously harm our

business and prospects.

Our products can have long sales and implementation cycles, which may result in us incurring substantial expenses before realizing any associated revenues.

The sale and implementation of our products to large companies and government entities typically involves a lengthy education process and a significant technical evaluation and commitment of capital and other resources. This process is also subject to the risk of delays associated with customers' internal budgeting and other procedures for approving capital expenditures, deploying new technologies within their networks and testing and accepting new technologies that affect key operations. As a result, sales and implementation cycles for our products can be lengthy, and we may expend significant time and resources before we receive any revenues from a customer or potential customer. Our quarterly and annual operating results could be materially harmed if orders forecast for a specific customer and for a particular period are not realized.

Consolidation in the network security industry may limit market acceptance of our products.

Several of our competitors have acquired security companies with complementary technologies in the past. We expect consolidation in the network security industry to continue in the future. These acquisitions may permit our competitors to accelerate the development and commercialization of broader product lines and more comprehensive solutions than we currently offer. Acquisitions of vendors or other companies with which we have a strategic relationship by our competitors may limit our access to commercially significant technologies. Further, business combinations in the network security industry are creating companies with larger market shares, customer bases, sales forces, product offerings and technology and marketing expertise, which may make it more difficult for us to compete.

We must adequately protect our intellectual property in order to prevent loss of valuable proprietary information.

We rely primarily on a combination of patent, copyright, trademark and trade secret laws, confidentiality procedures and non-disclosure agreements to protect our proprietary technology. However, unauthorized parties may attempt to copy or reverse-engineer aspects of our products or to obtain and use information that we regard as proprietary. Policing unauthorized use of our products is difficult, and we cannot be certain that the steps we have taken will prevent misappropriation of our intellectual property. This is particularly true in foreign countries where the laws may not protect proprietary rights to the same extent as the laws of the United States and may not provide us with an effective remedy against unauthorized use. If our protection of our intellectual property proves to be inadequate or unenforceable, others may be able to use our proprietary developments without compensation to us, resulting in potential cost advantages to our competitors.

We may incur substantial expenses defending ourselves against claims of infringement.

There are numerous patents held by many companies relating to the design and manufacture of network security systems. Third parties may claim that our products infringe on their intellectual property rights. Any claim, with or without merit, could consume our management's time, result in costly litigation, cause delays in sales or implementations of our products or require us to enter into royalty or licensing agreements. Royalty and licensing agreements, if required and available, may be on terms unacceptable to us or detrimental to our business. Moreover, a successful claim of product infringement against us or our failure or inability to license the infringed or similar technology on commercially reasonable terms could seriously harm our business.

Fluctuations in our quarterly revenues may cause the price of our common stock to decline.