



# INTRUSION

Protect everything. Trust nothing.

Investor Relations Presentation

January 2021

# SAFE HARBOR STATEMENT

## SAFE HARBOR STATEMENT

This presentation has been prepared by INTRUSION Inc. (the “Company”) solely for informational purposes based on its own information, as well as information from public sources. This presentation has been prepared to assist interested parties in making their own evaluation of the Company and does not propose to contain all of the information that may be relevant. In all cases, interested parties should conduct their own investigation and analysis of the Company and the data set forth in the presentation and any other information provided by or on behalf of the Company. This presentation does not constitute an offer to sell, nor a solicitation of an offer to buy, any securities of the Company by any person in any jurisdiction in which it is unlawful for such person to make such an offering or solicitation. Neither the Securities and Exchange Commission nor any other regulatory body has approved or disapproved of the securities of the Company or passed upon the accuracy or adequacy of this presentation. Any representation to the contrary is a criminal offense.

Except as otherwise indicated, this presentation speaks as of the date hereof. The delivery of this presentation shall not, under any circumstances, create any implication that there has been no change in the affairs of the Company after the date hereof.

Certain of the information contained herein may be derived from information provided by industry sources. The Company believes that such information is accurate and that the sources from which it has been obtained are reliable. The Company cannot guarantee the accuracy of such information and has not independently verified such information.

This presentation contains forward-looking statements within the meaning of the federal securities laws. These forward-looking statements can be identified by the use of forward-looking terminology, including the terms “believe,” “estimate,” “project,” “anticipate,” “expect,” “seek,” “predict,” “continue,” “possible,” “intend,” “may,” “might,” “will,” “could,” “would” or “should” or, in each case, their negative, or other variations or comparable terminology. These forward-looking statements include all matters that are not historical facts. They appear in a number of places throughout this presentation and include statements regarding our intentions, beliefs or current expectations concerning, among other things, the performance of our products in the marketplace, the current technological, network, and communication platforms our products operate on and with; our ability to stay current and competitive in our research and development efforts; our ability to protect and enforce our intellectual property rights, the success of our commercialization objectives, and our customer marketing and sales initiatives. We derive many of our forward-looking statements from our operating budgets and forecasts, which are based upon many detailed assumptions. While we believe that our assumptions are reasonable, we caution that it is very difficult to predict the impact of known factors, and, of course, it is impossible for us to anticipate all factors that could affect our actual results. Forward-looking statements should not be read as a guarantee of future performance or results and may not be accurate indications of when such performance or results will be achieved. In light of these risks and uncertainties, the forward-looking events and circumstances discussed in this presentation may not occur and actual results could differ materially from those anticipated or implied in the forward-looking statements. A number of important factors could cause our actual results to differ materially from those indicated in these forward-looking statements, including risks and uncertainties related to product performance, rapidly changing technologies, and the success of our sales and marketing efforts, as well as those set forth in the Company’s filings with the Securities and Exchange Commission under the heading “Risk Factors.”

# INTRUSION LEADERSHIP



**JACK  
BLOUNT**  
President &  
CEO

40 years in technology as a visionary in the personal computer, local area networking, ERP, mobile computing, big data, cybersecurity and AI.

CIO of USDA, the 4th largest data center in federal government

SVP of Business Development at Novell, helping company grow from \$50 million to \$2 billion in 6 years

Served as CEO, CTO, COO of 8 technology companies

Began career as software engineer at IBM

## PRIOR AFFILIATIONS



**JOE HEAD**  
Co-Founder &  
SVP Systems  
Engineering

Recognized by the federal government as a top expert on cyberwar. Integral in the development of both INTRUSION Shield and Savant.

Co-founder of INTRUSION, serving 37+ years as a director

Named Vice Chairman of the BOD in 2000, and VP in 2003

Product Marketing Manager & Marketing Engineer at Honeywell Optoelectronics

## PRIOR AFFILIATIONS



**FRANKLIN  
BYRD**  
CFO

Franklin has more than 25 years of experience in finance, accounting and compliance and scaling experience with early stage and high-growth entities.

Prior to joining INTRUSION, Franklin served as CFO for Peak Nano Systems, LLC. There, he was responsible for completing critical financings and scaling up office operations for the company.

Franklin has also served as vice president of finance for Hunt Power L.P., a division of Hunt Consolidated Inc.

Franklin is a Certified Public Accountant.

## PRIOR AFFILIATIONS



# OUR HISTORY



# KEY BUSINESS HIGHLIGHTS

Differentiated cybersecurity vendor undergoing dramatic TAM expansion under new leadership

1 New management team brings emphasis on growth and vision for **INTRUSION**

2 **INTRUSION** has an irreplaceable, proprietary data asset that has historically been under-monetized

3 Highly differentiated, custom business in federal network forensics

4 New solution for commercial cybersecurity market significantly expands **INTRUSION**'s TAM

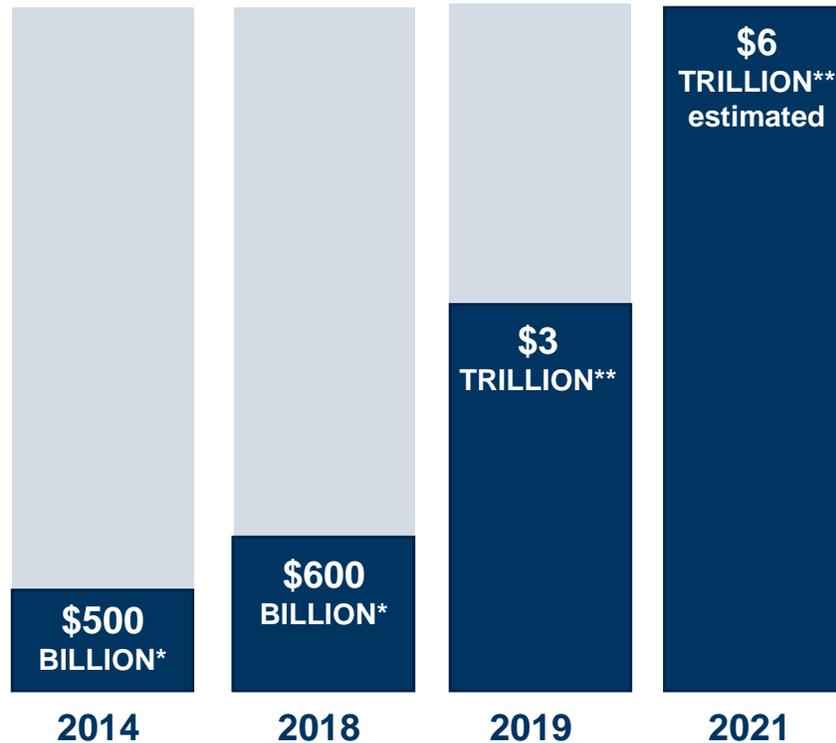
5 Transitioning company to recurring revenue model, focused on new solutions and Enterprise business

6 Long-term roadmap with several releases building on core technology assets

# SIZE OF PROBLEM & OPPORTUNITY

\$3 trillion in global cybercrime losses in 2019, projected to grow to \$6 trillion by 2021

## GROWTH OF LOSSES RESULTING FROM CYBERCRIME (BY YEAR)



\*The Economic Impact of Cybercrime: No Slowing Down by Center for Strategic and International Studies (CSIS) McAfee

\*\*CyberSecurity Ventures

## TOTAL GOVERNMENT AND ENTERPRISE SPENDING ON SECURITY SOFTWARE AND HARDWARE

CYBERSECURITY VENTURES PREDICTS GLOBAL SPENDING ON CYBERSECURITY PRODUCTS AND SERVICES WILL EXCEED

**\$1 TRILLION CUMULATIVELY**

OVER THE FIVE-YEAR PERIOD FROM 2017 TO 2021

## Average Annual Cybersecurity Spend per Employee



Source: Gartner

# COMMON MISCONCEPTIONS ABOUT CYBERSECURITY THREATS

## *Myths...*

“If our firewalls stay updated, the network will stay protected”

“Software and hardware from trusted vendors are secure when delivered”

“Bad actors can be locked out with the right tools”

“My network is clean and free from malware”



## *...Realities*

Firewalls are breached everyday by armies of attackers employed by nation-states using AI and Supercomputing

Malicious code is routinely embedded on all types of IT hardware shipping from China

The average time to identify a network breach in 2019 was 206 days; the average lifecycle of a breach is 314 days from breach to containment

Every company's network is infected with malware living on your network every second of every day

# EXISTING SOLUTIONS



# INTRUSION *TraceCop*™

Monetized over 25 years as a Network Forensics Tool for Federal Customers

- ✔ World's only database of 25 years of Internet traffic and specifically cyber crime
- ✔ **INTRUSION** constantly expands the data in *TraceCop* with dozens of international data feeds

# INTRUSION *Savant*™

FOR REAL-TIME PROCESS FLOW ANALYSIS

Patented network appliance designed to carryout bidirectional protocol decoding in RAM

- ✔ Patented Packet File Systems for recording at line rates
- ✔ Patented, Concise Summaries for mass-enrichment, analysis and indefinite storage

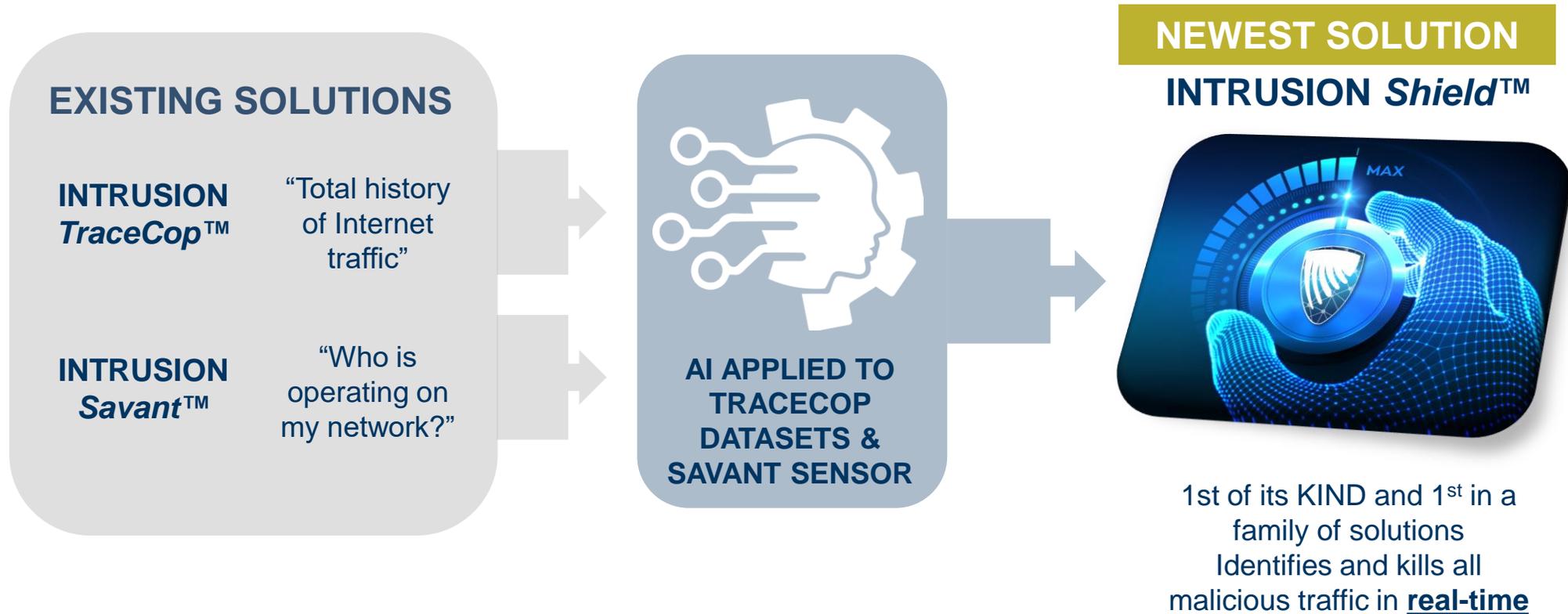
# A NEW FAMILY OF SOLUTIONS



# INTRUSION *Shield*™

## FAMILY REPRESENTS A NEW PARADIGM FOR CYBERSECURITY

Leverage foundational *TraceCop* and *Savant* platforms in expanded new solutions for the Enterprise



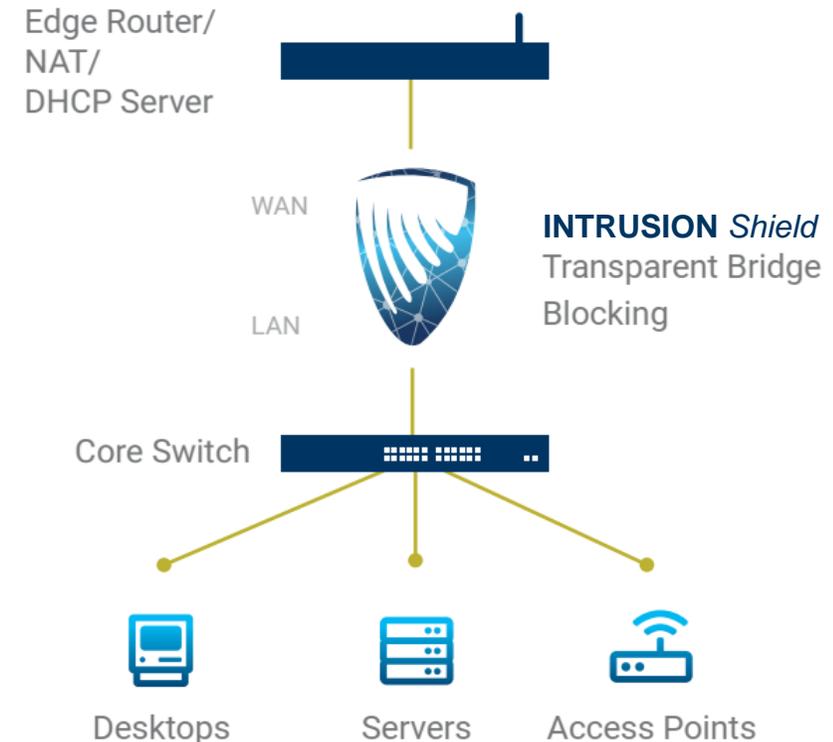
# INTRUSION *Shield*™ OFFERS REAL NETWORK SECURITY FROM THE INSIDE-OUT

Patented technology layers AI on top of *TraceCop* and *Savant*, enabling real-time killing of malicious traffic

## VALUE PROPOSITION

- ✓ Does not replace existing network elements; rather, *Shield* is positioned as an new network security layer
- ✓ Only solution on the market that identifies and kills malicious agents in *real-time* operating on your network
- ✓ No Change Management; Plug-n-Play technology
- ✓ Daily System Updates as *TraceCop* database continues to grow
- ✓ Multiple Provisional patents filed covering *Shield* technology
- ✓ 1<sup>st</sup> in a family of solutions

## PLUG-N'-PLAY IMPLEMENTATION



INTRUSION *SHIELD*™  
DOES NOT SEND  
THOUSANDS  
OF ALERTS,

*Shield* USES  
AI TO *KILL*  
MALICIOUS  
TRAFFIC



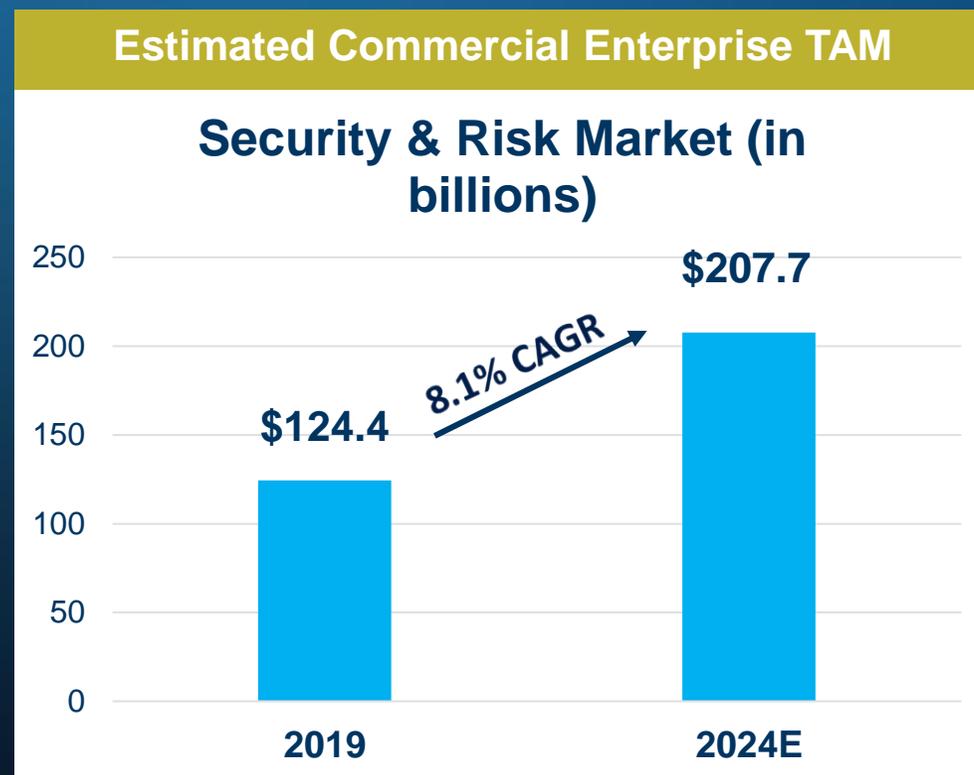
# Shield STRATEGY & MARKET SIZE: SECURITY-AS-A-SERVICE (SAAS)

\$20 per seat, per month pricing model designed to drive mass adoption in commercial enterprise market

## AGGRESSIVE RAMP UP OF RECURRING REVENUE

- ✓ Leverage established distributor network and channel reach of roughly 12,000 U.S. resellers\*
- ✓ No upfront cost or contracts for customers
- ✓ Appliance drop-shipped direct to customers with software pre-installed by DELL (no inventory)
- ✓ Validation from early adoption by 12 'beta' customer as Shield killed 77,539,801 threats in 90 days
- ✓ Drive increased momentum with rapid expansion of **Shield** family with introduction of 6 solutions

\*Channel Futures



Source: Gartner

# INTRUSION *Shield*<sup>™</sup> PRELIMINARY BETA RESULTS

3 additional Beta customers comment on their experience with our solution

## Customer A

“This product just does not exist in the market today and is sorely needed,” said Aaron, CISCO for B. Riley Financial.

## Customer B

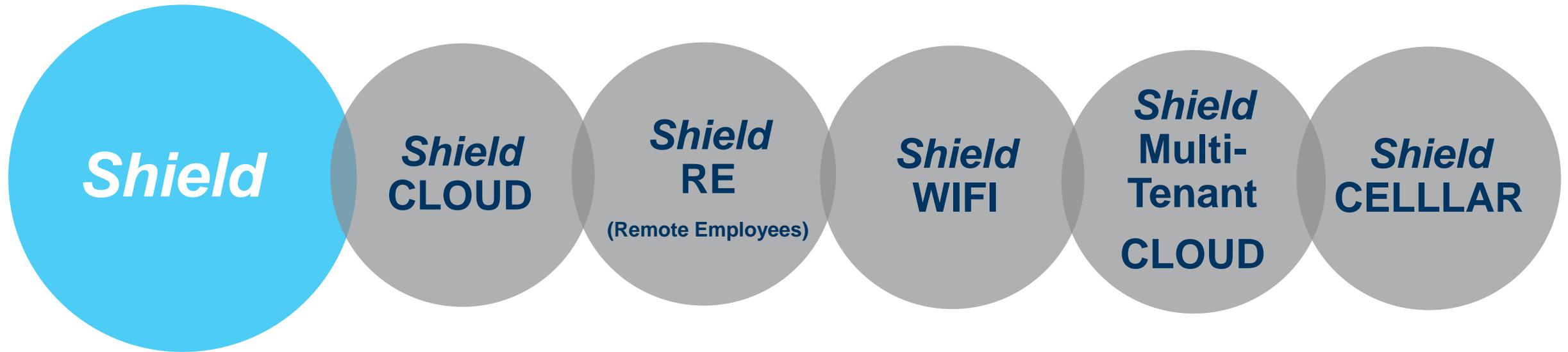
“The *Shield* solution has shown us that virtually every network is already infected, and front-end protection is not possible. The understanding that networks are already compromised and that the only means of protection is to monitor and restrict outgoing traffic is the breakthrough of the *Shield* philosophy,” said Richard, President of NovaTech.

## Customer C

“The ease and instant protection of Shield has been great,” said Michael, Portfolio Manager for Bard Associates. “It’s so simple to implement and run, yet highly effective.”

# INTRUSION *Shield*<sup>™</sup> FAMILY OF SOLUTIONS ROADMAP

A new family of solutions targeting important sub-segments the Enterprise & SMB markets



# KEY INVESTMENT HIGHLIGHTS

Differentiated cybersecurity vendor undergoing dramatic TAM expansion under new leadership

1

New management team with CEO that has repeated success in technology turnarounds

2

**INTRUSION** has a uniquely valuable, dynamically growing, threat-enriched Big Data Cloud of databases

3

AI based solution using ML&NN technology to protect business and government

4

Moving **INTRUSION** into the commercial market significantly expands our TAM

5

Leveraging modern, SaaS revenue model greatly shortens sell cycle and encourages rapid growth

6

Developed, strategic solutions roadmap is designed to enable long-term growth



# INTRUSION

Protect everything. Trust nothing.



CYBERSECURITY AS AN INDUSTRY HAS  
**FAILED!**

**INVEST IN A CYBER DEFENSE  
SOLUTION THAT *WORKS!***