



The most effective Cybersecurity offerings in the market, enabled by Human supervised AI Technology

Intrusion Investor Presentation

September 2026

Intrusion

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.”



What We Do

Intrusion + VigilAgent

Integrated cybersecurity intelligence, protection and AI-enabled operations

Intrusion combines proprietary internet intelligence, agentless network protection and managed security expertise to help organizations identify, investigate and respond to cyber threats.

Highly Adaptive Cybersecurity Solutions

Customized cybersecurity consulting and services including attack-surface mapping, critical-infrastructure protection, threat hunting, incident response and custom integrations.

Commercial / Subscription

MSSP offering sold directly and through channel partners utilizing VigilAgents Agentic AI tools integrated with Intrusion Shield technology



PROPRIETARY INTELLIGENCE

TraceCop + threat enrichment

NETWORK + OT PROTECTION

Shield family + OT Defender

AI-ENABLED SECURITY OPERATIONS

OmniViz + ORACLE + MDR

Highly Adaptive Cybersecurity Services (“HACS”)

CUSTOM ARCHITECTED SOLUTIONS



Intrusion Shield



OT Defender



TraceCop



Cybersecurity
Services

-
- **Critical Infrastructure Mapping** – Discover exposed OT devices and map dependencies across public and private infrastructure
 - **High Profile Event Monitoring** – Track threat intelligence and dark web activity around major events
 - **Threat Intelligence and Incident Response** – Deliver intelligence and forensic analysis to support breach investigations
 - **Custom Development** – Build tailored data pipelines and visualizations for complex network and geospatial datasets
 - **Customized Threat Intelligence**



Human Supervised - AI powered Commercial / Subscription

THE ORACLE™

Sees, decides and acts – escalating to humans or initiating response. The core of the agentic digital workforce.

OMNIVIZ

Correlates telemetry, tickets, customer context, analyst knowledge and external enrichment in one investigation view.

INTRUSION SHIELD

Adds proprietary intelligence, network level prevention and agentless coverage for IoT, critical infrastructure and AI activity.

THE COMBINED OFFERING:

- A security fabric that ingests telemetry from across the enterprise attack surface.
- Intrusion Shield technology adds network visibility and enrichment that can expose activity other tools miss.
- An open ecosystem designed to incorporate existing tools and customer data.
- A common back end intended to support scalability and reduce integration management costs.



Tony Scott, President & CEO

CIO | Federal Government

CIO | Microsoft

CIO | The Walt Disney Company

CIO | VMware

CTO | General Motors

Inducted into CIO Magazine's "CIO Hall of Fame"

Renowned speaker and panelist



vmware®



Experienced Leadership



Tony Scott
President & CEO



Kimberly Pinson
CFO



Joe Head
CTO



Mark Porter
President, VigilAgent



Bobby Mikkelsen
VP Strategy &
Corporate Development



Andrew Wildrix
VP, Business
Development



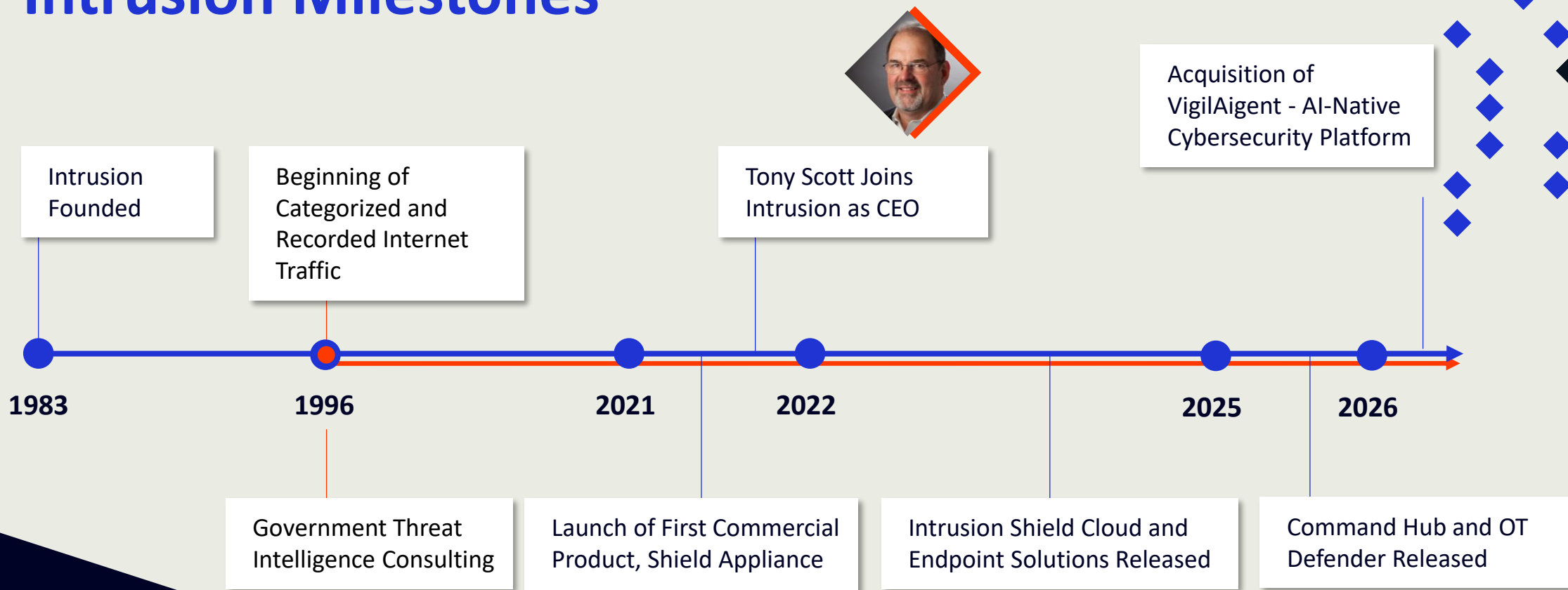
Blake Dumas
VP, Engineering



Mike McClure
VP, Consulting



Intrusion Milestones



30 years
of securing networks,
threat hunting, and analysis expertise



VigilAgent Acquisition

Announced on June 29, 2026

- ◆ Adds an AI-native cybersecurity platform to the Intrusion family of products and services.
- ◆ Immediately adds over \$3.0 million of annual recurring revenue (ARR) backed by a diversified base of multi-year customer contracts.
- ◆ Expands commercial reach by providing access to a broader ecosystem of more than 80 reseller partners and approximately 1,000 customers.
- ◆ Combines complementary cybersecurity technologies to deliver a more comprehensive security platform.
- ◆ Strengthens technical capabilities through the addition of managed detection and response (MDR), proprietary threat intelligence, and experienced cybersecurity professionals.
- ◆ Approximately \$3 million of annualized operating cost savings identified, not yet implemented.



Key Takeaway

The combination of Intrusion and VigilAgent creates an opportunity to drive revenue growth, margin expansion and operating leverage by combining proprietary threat intelligence, agentic AI and an established commercial channel to scale recurring, higher-margin revenue while reducing the cost of alert investigation and response.



Shield - A Cyber Threat Intelligence Engine 30 Years in the Making



Proprietary Threat Intelligence

from decades of networking and government cyber threat consulting



Unique Risk Assessment

based on a combination of reputation, behavior, manual analysis, and historical records



Patented Data Mining and Network Flow Analysis

allows near 100% packet capture at high speeds



Largest Known IP-Related Database

with historical data on over 8.5 billion IPs

Intrusion

8.5+ billion
IPs

Proprietary database with history and intel on billions of IPs and hostnames

Competitors

Product Differentiation

Highly differentiated solution leveraging largest known IP-related threat intelligence dataset and modern AI tools

Historical Data

Leverage the largest known IP dataset of 8.5 billion IP addresses and domain names

Automated and AI based Analysis

Operationalize decades of threat intelligence and observation to understand what IP address and domain owners are doing over time

Association and Inference

Technology includes a reputational and behavior analysis inference engine that allows Intrusion to make connections between known and unknown IPs that may be nefarious

Behavior Updates

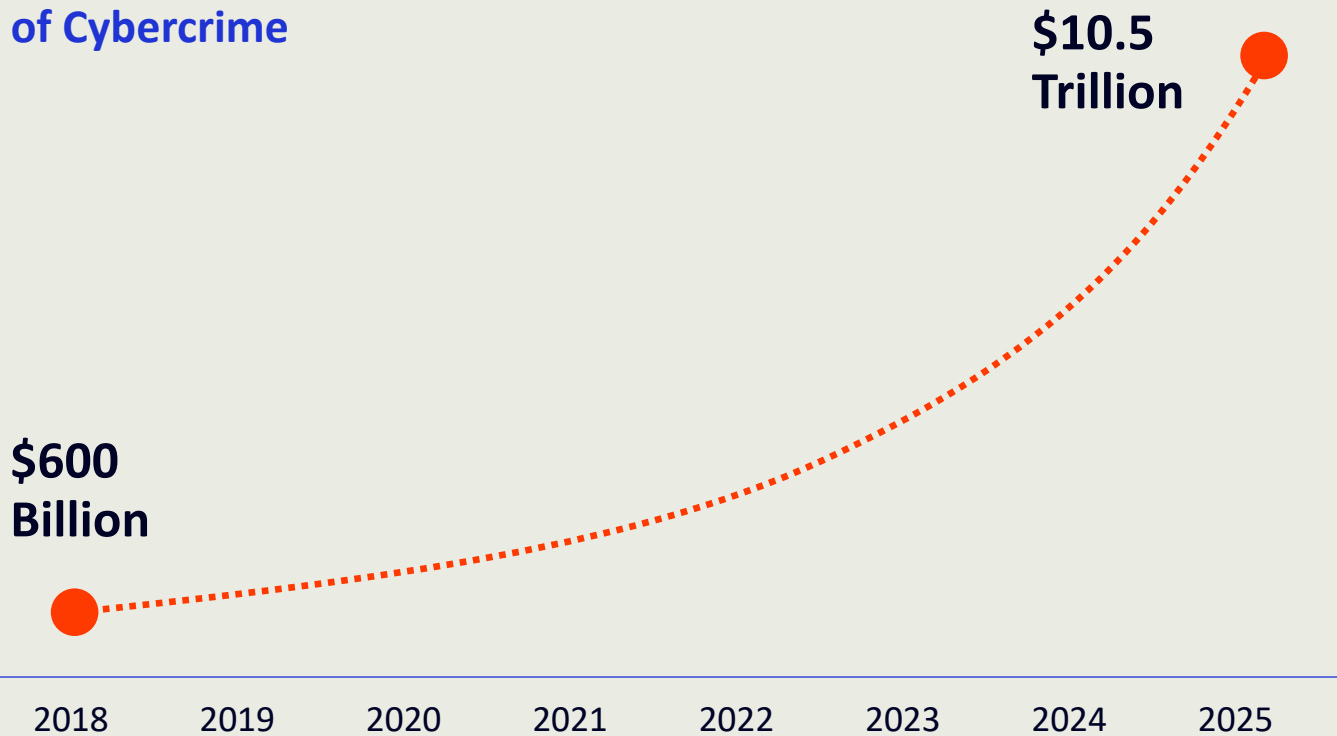
Constantly update behavioral algorithms to create an updated behavioral rule set. This behavioral ruleset creates a unique ability and an unrivaled level of threat intelligence



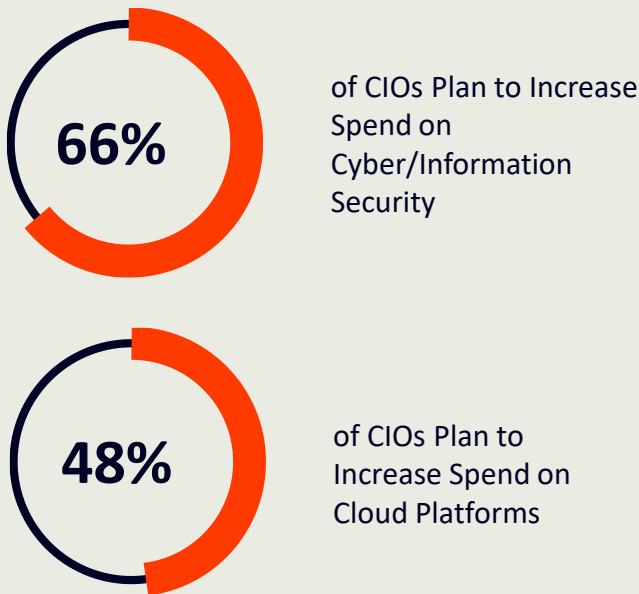
Large and Growing Demand

Cyberattacks are increasing despite growing investment in security infrastructure

Economic Impact of Cybercrime



Spend on Cybersecurity Over Time



Source:
2018: The Economic Impact of Cybercrime: No Slowing Down by Center for Strategic and International Studies (CSIS) McAfee
2019-2025: Cybersecurity Ventures

Source: Gartner



The need for Speed

AI –powered attacks + volume of data that must be examined has changed the game

Cyber Threats

Companies are **attacked every 39 seconds**.⁽¹⁾

Legacy cyber technologies creates two blind spots: **overconfidence** (we haven't been compromised yet) and the **proliferation of alerts** that are not meaningful (the false positives problem).

Threat actors have learned how to bypass many current solutions by exploiting gaps in architecture and operational shortcomings.

Lack of Qualified Staff + data overload

62% of organizational cybersecurity teams are **understaffed**.⁽²⁾

78% lack confidence in their company's cybersecurity posture.⁽³⁾

93% of SecOps teams cannot address all security alerts in same day; 83% claim staff has **alert fatigue**.⁽⁴⁾

Increased Complexity

Attack surface has expanded exponentially (wearable devices, cloud, consumer electronics, social media, vehicles, etc.)

94% of malware observed used was **polymorphic** to help avoid detection.⁽⁵⁾

61% of successful attacks use a **Zero-Day**.⁽⁶⁾

34% of successful attacks use **malware-free** techniques.⁽⁶⁾

Sources:

1) University of Maryland 2) ISACA State of Cybersecurity 3) Insight Enterprises Inc. 4) Webroot Threat Report 5) 2020 State of SecOps & Automation report 6) Watchguard



Customers and Segments

Customers across all industries rely on VigilAgent and/or Intrusion Shield to enable a proactive cyber threat intelligence and defense capability



Financial Institutions

Manage vast amounts of client data, which can be at risk for ransomware and are subject to increasing scrutiny by government agencies.



Medical Community

Every appliance that collects patient data has open ports that can be ransomed and exploited, requiring a greater cybersecurity infrastructure.



Hospitality

House vast amounts of sensitive customer data resulting in increased cybersecurity costs.



Government

Local, State and Federal Governments under increased pressure to protect citizens data from increased cyber attacks.



Critical Infrastructure

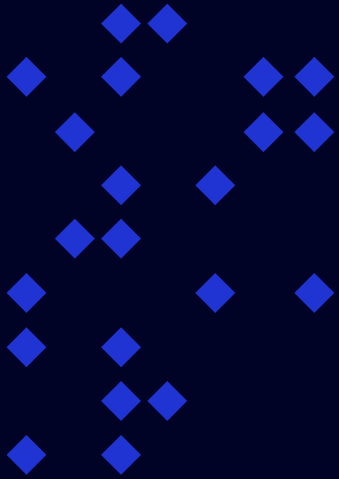
Essential services such as electricity and water are susceptible to malware and cyber attacks and require constant monitoring.



Reasons to Invest in Intrusion

- 1 Experienced management team brings an **emphasis on execution and profitable growth**
- 2 Intrusion's **proprietary database and IP** have historically been under-monetized
- 3 **Cloud and Endpoint solutions** significantly expand the product portfolio and total addressable market
- 4 Transition to **recurring revenue model**, selling through the channel - MSPs, MSSPs, and VARs
- 5 **Long-term roadmap established for product growth** building on core technology assets





Financial Information



Recent Business Highlights

2026

- ◆ Received a \$3.9 million award from the State of Texas to deliver cyber threat intelligence and critical infrastructure protection.
- ◆ Completed the acquisition of VigilAgent to integrate a AI-native cybersecurity platform and improve the Company's top line by adding over \$3.0 million in annual recurring revenue from multi-year contracts.

2025

- ◆ Received additional \$3.0 million for continued U.S. Department of Defense contract support, with funding driving operational deployment of critical infrastructure monitoring tools and deeper research-driven threat analysis capabilities.



Q2 2026 Snapshot

\$1.5M	66%	\$3.5M	\$2.6M	\$0.2M	\$4.1M
Revenue	Gross margin	Operating expense	Net loss	Cash, 30 Jun	Stockholders' equity
+64% sequential -22% YoY	10-Q: 66.4% Q1 74% Q2'25 76% Mix-driven	-\$0.8M sequential	\$(0.13) per share Q2'25: \$2.0M / \$(0.10)	YE'25: \$3.6M	YE'25: \$7.277M

Highlights from Ongoing Transformation

VigilAigent Acquisition – June 29th	State of Texas \$4 million Award	\$3 million annualized Operating Cost Savings
Adds > \$3 million ARR from multi-year contracts	Began contributing in Q2	Cost savings identified, not yet implemented



Financing

S-3 Shelf Registration

\$100M effective February 10, 2025; \$50M unallocated
ATM \$50M capacity

2026 Financings

\$4.5M Secured Note Financing (April & August 2026)
\$1.3M Warrant Inducement (August 2026)

2025 Financings

\$7.5M Registered Direct Offering January 2025

(\$ in millions)	as of 6/30/26
Cash and cash equivalents	\$0.2
Notes payable	\$3.3
Net equity	\$4.1



Cap Table as of 6/30/26

Total common stock outstanding	22,757,075	
Shares held by affiliates (management and 10% holders)	3,383,689	14.86%
Shares held by non - affiliates	19,373,386	
Warrants outstanding	3,198,085	
Average exercise price	\$ 3.26	
Average remaining term	2.85 Yrs	
Options outstanding (including management affiliates)	49,753	
Average exercise price	\$ 42.38	
Average remaining term	7.13 Yrs	
Restricted stock awards (including management affiliates)	897,858	
Fully dilutive shares outstanding	26,902,771	

Note: Does not reflect Recent Warrant Inducement.



Income Statement Snapshot

(in millions, except EPS)	1Q'24	2Q'24	3Q'24	4Q'24	FY'24	1Q'25	2Q'25	3Q'25	4Q'25	FY'25	1Q'26	2Q'26
Revenue	\$1.1	\$1.5	\$1.5	\$1.7	\$5.8	\$1.8	\$1.9	\$2.0	\$1.5	\$7.1	\$0.9	\$1.5
Gross Margin (%)	80.0%	77.8%	77.1%	74.8%	76.8%	75.7%	76.4%	76.6%	74.4%	75.8%	74.2%	66.4%
Operating Expenses	\$3.4	\$3.1	\$3.2	\$3.2	\$12.9	\$3.4	\$3.5	\$3.6	\$4.0	\$14.5	\$4.2	\$3.5
Operating Loss	(\$2.5)	(\$2.0)	(\$2.0)	(\$1.9)	(\$8.4)	(\$2.1)	(\$2.1)	(\$2.1)	(\$2.8)	(\$9.1)	(\$3.6)	(\$2.6)
GAAP EPS	(\$0.94)	(\$0.53)	(\$0.35)	(\$0.36)	(\$1.63)	(\$0.11)	(\$0.10)	(\$0.10)	(\$0.14)	(\$0.46)	(\$0.18)	(\$0.13)
Weighted Average Share Count	1.8	4.3	6.6	6.2	5.3	19.2	19.9	20.0	20.1	19.8	20.3	20.4



Balance Sheet Snapshot

(\$ in millions)	1Q'24	2Q'24	3Q'24	4Q'24	1Q'25	2Q'25	3Q'25	4Q'25	1Q'26	2Q'26
Current Assets	\$0.7	\$2.6	\$2.5	\$5.5	\$12.0	\$10.5	\$7.6	\$4.2	\$2.0	\$2.3
Noncurrent Assets	\$5.0	\$4.8	\$4.9	\$6.0	\$5.9	\$5.9	\$6.1	\$6.2	\$5.9	\$10.2
Total Assets	\$5.7	\$7.4	\$7.4	\$11.5	\$17.9	\$16.4	\$13.7	\$10.4	\$7.9	\$12.5
Current Liabilities	\$5.4	\$3.1	\$3.5	\$3.7	\$3.1	\$3.3	\$2.5	\$1.8	\$2.9	\$6.0
Noncurrent Liabilities	\$1.5	\$1.4	\$1.4	\$1.6	\$1.5	\$1.5	\$1.4	\$1.3	\$1.4	\$2.4
Total Liabilities	\$6.9	\$4.5	\$4.9	\$5.3	\$4.6	\$4.8	\$3.9	\$3.1	\$4.2	\$8.4
Stockholders' Equity	(\$1.2)	\$2.9	\$2.6	\$6.2	\$13.4	\$11.6	\$9.8	\$7.3	\$3.7	\$4.1





Thank you

Intrusion