



COMPANY PRESENTATION



THE CHALLENGE



Securely connecting IIoT



Real-time knowledge and control of industrial processes, infrastructure and devices can drive higher efficiency, increased productivity and lower costs



Accessing this knowledge (data) is fundamental to the Industrial Internet of Things (IIoT)



Safe, bi-directional data access to IIoT systems is a **difficult** problem, especially while segregating networks



PROBLEM

Safe remote access to
industrial data



Security



Performance



Flexibility

No attack
surfaces

No slow
downs

No costly
integration

SOLUTION



A new data protocol for industrial

We invented a software protocol to network industrial data in a new way that reverses the server-client paradigm



Security



Performance



Flexibility

Closed firewalls at the plant and device

Real time at plant scale, robust QoS

Standards-based solution deployed in minutes, without costly integration

WHAT ARE THE RISKS IN IIoT?



Constant industrial
cyber-attacks

Forbes

BBC

The Washington Post

Honda Hacked:
Japanese Car Giant
Confirms Cyber Attack
On Global
Operations

June 10, 2020

Hacker tries to
poison water supply
in Florida

Feb 8, 2021

Leaked Pentagon
documents claim
hackers breached a
Canadian gas
network

Apr 11, 2023

OT / IT (IN)SECURITY

A growing problem



Connecting Operational Technology (OT) and Information Technology (IT) networks

Victims of hacks failed to implement robust security architecture:

- Poor segmentation between OT and IT networks
- Resulting in Windows-based assets on both the IT and OT networks being compromised:
 - HMI, data historians, and polling servers
- For international companies, impact is not geographically limited

GOVERNMENTS GET INVOLVED



New legislation is requiring
better cybersecurity

October 24, 2020



In a rare joint release
both NSA and CISA
recommend
immediate actions to
reduce exposure
across operational
technologies and
control systems

January 16, 2023



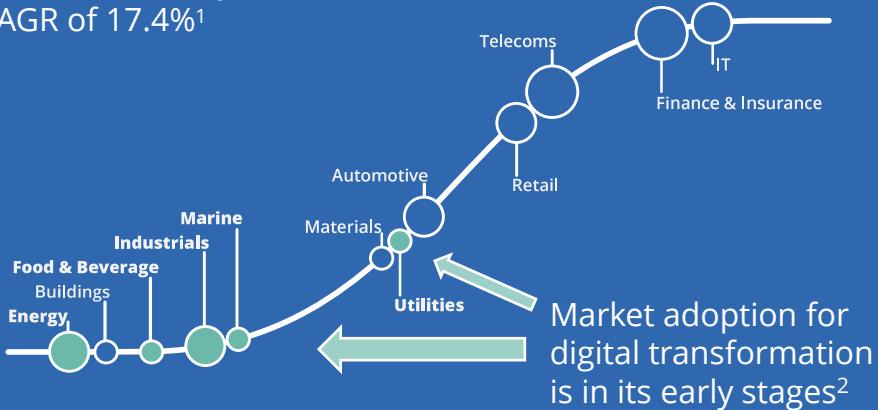
Directive on Security of
Network and Information
Systems (NIS2)

Key Guideline: One or more
DMZs are needed for the
most secure, manageable,
and scalable segregation of
control and corporate
networks – **to become law
in member countries by
Oct 24, 2024**

MARKET GROWTH

Digital transformation
for industrial assets

Industrial IoT spending is
expected to grow from \$209B in
2022 to \$398B by 2026 at a
CAGR of 17.4%¹



BUSINESS MODEL & PRODUCT PORTFOLIO



Hybrid SaaS for secure
IIoT connectivity



On-premise middleware
software (DataHub®)



Cloud-based service for remote
connections (on MS Azure)



Embedded code base for
equipment manufacturers (ETK)

OUR MARKET TRACTION

25+ years of critical infrastructure expertise

27,000+ software installations in 86 countries

Used by 10 of 10 top automation providers worldwide

Certified AVEVA Technology Partner with officially endorsed product

OEM relationships with many hardware and software providers

Covering green energy, discreet manufacturing, water/waste-water, building automation, oil & gas, minerals & mining

Demonstrated effectiveness of solutions with real-world case studies

BUSINESS HIGHLIGHTS



Cash-flow positive and profitable



Track record of double-digit sales growth, at an accelerating rate, across several market segments



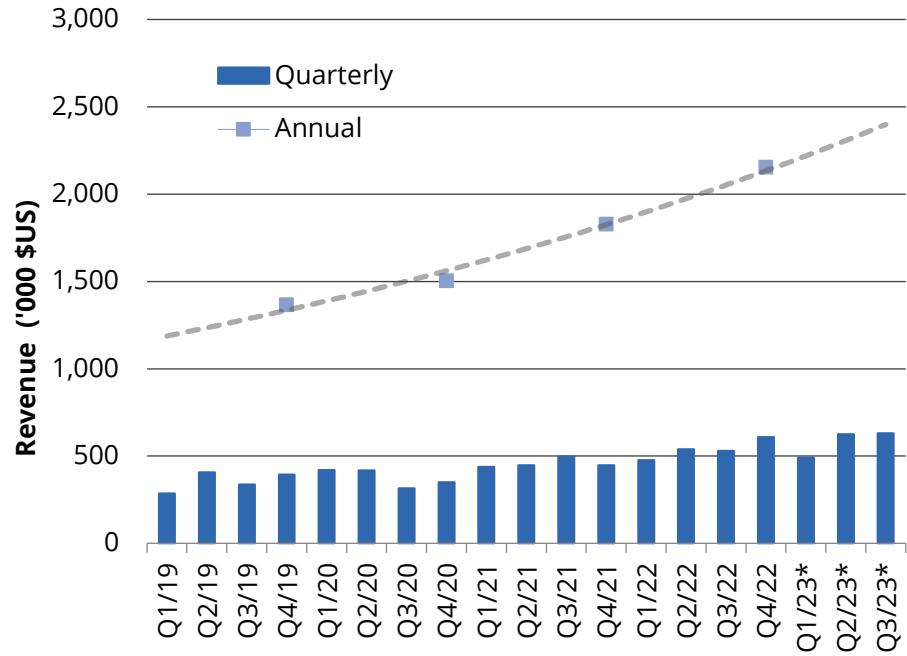
Very sticky, large customer base, including OEMs requesting SaaS pricing model



Diversified enterprise customers base which accelerates growth by a factor of 3-5X due to data sharing to suppliers

BUSINESS HIGHLIGHTS

Cash-flow positive and profitable



* unaudited, reported at sec.gov

COMPETITIVE ADVANTAGES



Reputation, proven product and intellectual property

- Unique software: field-proven code base of 10M+ lines of code representing 25+ years of development, making duplication extremely difficult to achieve
- Patented security architecture model: 10 U.S. patents and counting
- Established reputation for quality products, and trust with industrial vendors

KEY CONSIDERATIONS



In an ever-more connected world, secure data access is key

- We live in an ever-more connected world, dependent on industrial processes, infrastructure and devices
- Knowledge and control of this infrastructure, in the form of real-time data = opportunities for continuous improvement from dynamic process optimization, to lower costs from predictive maintenance, increase speed to market through production chain management, increase reliability and security through anomaly detection, etc.
- There is a clear market need for a safe connectivity solution specifically designed for the IIoT that provides for bi-directional data access and control: it is a complex problem

BUSINESS GOALS IN JAPAN



Growth opportunity

1.

Find new reseller and system integration partners in Japan

2.

Significantly grow Asia sales, and boost product awareness

3.

Attract growth capital investment, potential up-list to NASDAQ

MANAGEMENT

Executive team



Andrew Thomas
CEO, Founder

Inventor of the communication technology, over three decades in process control, system integration and software development of real time data communications systems



Paul Thomas
President, Founder

A patent attorney and engineer with extensive experience in intellectual property development, litigation strategies and protection of patented products and services



Paul Benford
COO, Founder

Process control and applications engineer with deep experience in customer development and communication strategies in a variety of our client industries



Lowell Holden
CFO

Experienced financial manager with broad experience in securing financing, structuring of transactions, and managing relationships with customers, financing institutions and stockholders



Xavier Mesrobian
VP Sales & Marketing

Seasoned sales executive with a strong foundation of focusing on net new business in SaaS business environments, direct experience with cutting edge venture-backed software start-ups, and possesses extensive experience in technical sales

BOARD

Experienced advisors



Norman Evans
Independent Board Member

Former Chief Financial Officer of Cipher Pharmaceuticals Inc (TSX:CPH). Norm has over 30 years of business experience, including roles as VP Finance at MDS Pharma Services, and as a Partner at Ernst & Young



Kenneth Jennings
Independent Board Member

Former VP, Manufacturer Solutions & Consulting, VP of Marketing, and VP of Sales at ADP Dealer Services, a division of ADP Inc. Ken's has over 30 years of experience in business development, strategy, and in leading business-to-business software sales and marketing teams



John Adiletta
Independent Board Member

Former CEO of EMR Technology Solutions, Inc., a U.S. holding company that acquires technology-related products and services. John has vast experience in mergers and acquisitions, and has served on boards for technology companies as a member of audit and corporate governance committees



Dr. José Fernandez
Advisor, Security

Professor at the Department of Computer & Software Engineering at the École Polytechnique de Montréal. José is an expert in computer security for Internet applications and SCADA systems, intrusion detection systems, malicious software and botnets, with over 50 publications



Minoru Yamazaki
Advisor, Japan

Former President of Lantronix (Japan), extensive experience in business development and marketing, having also held various senior positions such as general manager of the wireless data division of Nippon Motorola, and former president of Toyo Microsystems

THANK YOU

Secure Real-Time Data
Communication for the
Industrial IoT and Industry 4.0



SECURE INDUSTRIAL IoT REDEFINED

This presentation may contain "forward-looking statements" that are made pursuant to the "safe harbor" provisions as defined within the Private Securities Litigation Reform Act of 1995. Forward-looking statements may be identified by words including "anticipates," "believes," "intends," "estimates," and similar expressions. These statements are based upon management's current expectations as of the date of this presentation. Such forward-looking statements may include statements regarding the Company's future financial performance or results of operations, including expected revenue growth, cash flow growth, future expenses and other future or expected performances. The Company cautions readers there may be events in the future that the Company is not able to accurately predict or control and the information contained in the forward-looking statements is inherently uncertain and subject to a number of risks that could cause actual results to differ materially from those indicated in the forward-looking statements. Further information on these and other potential factors that could affect the Company's financial results is included in the Company's filings with the SEC under the "Risk Factors" sections and elsewhere in those filings.