



BRYAN, GARNIER & CO

Critical Protection

EXPLORING THE GROWING MARKET FOR OPERATIONAL TECHNOLOGY (OT) SECURITY



TECHNOLOGY WHITE PAPER JANUARY 2022


Contents

1: AN ACCELERATING USD 2.5BN MARKET

2: REGULATORS ARE INCREASING REQUIREMENTS

3: SPECIALIZED PLAYERS HAVE AN EDGE

4: INTERVIEW WITH DANIEL BREN – OTORIO CEO



In the past two decades, the digitization of business and daily life has led to the emergence of several new players in the cybersecurity market. Industries have been going through a similar phase of digitization, which has blurred the lines between IT and operational technology (OT) as OT has been brought online. The resulting “cyber-physical” systems have created many vulnerabilities and risks that are difficult to identify in these highly complex environments. In response, a new generation of specialized security players that natively support converged IT/OT environments is now emerging to fend off the threats faced by industrial players.

1: An accelerating USD 2.5bn market

After years of underdevelopment, the OT security market was estimated to be worth USD 2.5bn in 2020. It is expected to reach 21% CAGR over the 2020-2025 period, driven by two trends: the rapid convergence of IT and OT environments, and increased market

awareness as security is now among the top priorities of executives and regulators. Early adopters are the most regulated industries, often called critical infrastructure, which have to observe high security standards. In terms of geographical distribution, the main

market is North America, accounting for approximately 40% of spending, followed by Europe (28%), and the most dynamic region in the next five years, APAC (21%).

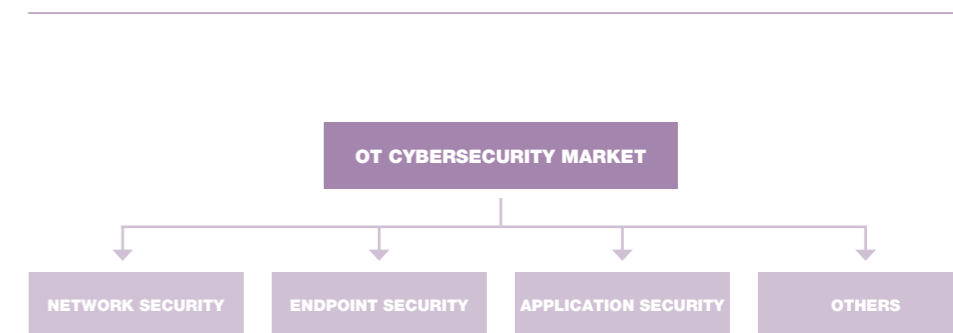
The newly connected OT assets often come from multiple vendors, use different communications protocols and different standards. Last but not least, they were designed for reliability and productivity, not cybersecurity.

These multi-generation, multi-vendor, multi-location environments are inherently insecure. They are the root cause of a significant expansion of the attack surface at industrial sites. And they are also very complex to protect.

This has led to the OT security market being split as follows:

- Network security, to protect the perimeter by monitoring, identifying, alerting and stopping threats to the industrial network. These solutions need to be paired with strong identity and access management (IAM) capabilities/solutions.
- Endpoint security, to secure devices by monitoring their status and activities.
- Application security, to secure industrial control systems such as Supervisory Control and Data Acquisition (SCADA), Manufacturing Execution Systems (MES) and Human-Machine Interfaces (HMI) at the application level.
- Other solutions aimed at very specific needs or only used in some verticals.

FIG 2: STRUCTURE OF THE OT SECURITY MARKET



Source: Bryan, Garnier & Co

FIG 1: OT SECURITY SPENDING WILL INCREASE AT A FAST PACE



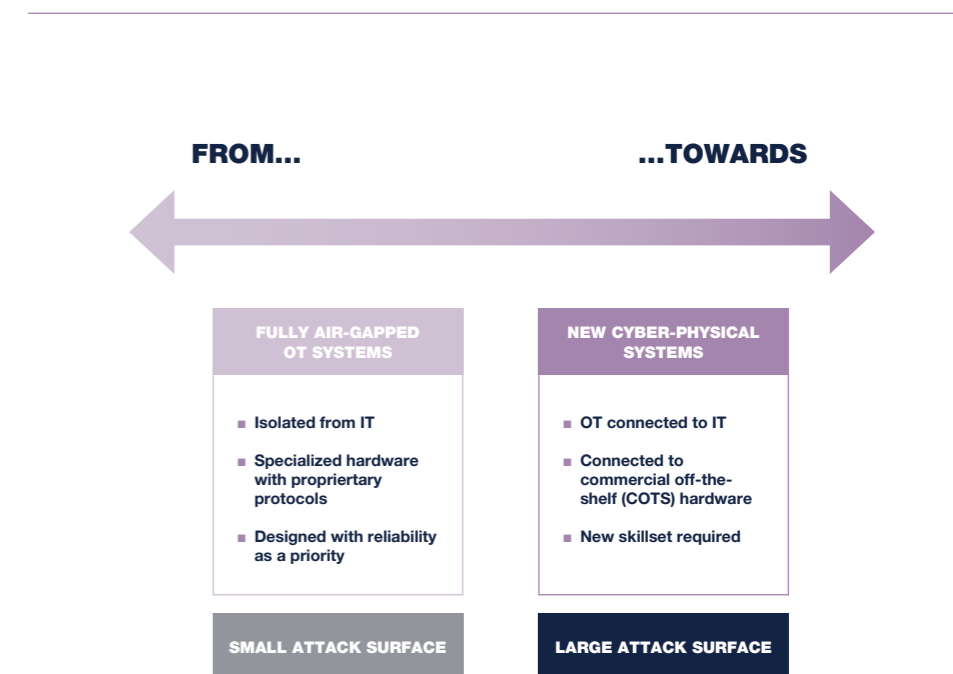
Source: Frost & Sullivan

But why does convergence of IT and OT environments create a need for more security? Traditionally, OT environments were “air-gapped” – completely separated from the IT environments. Protecting that perimeter was relatively easy, as the attack surface was small.

With the advent of Industry 4.0, industrial sites are increasingly connecting OT assets to (often legacy) IT environments to leverage advances such as cloud computing, artificial intelligence, data analysis, or remote operations, maintenance and support.



FIG 3: NEW CYBER-PHYSICAL SYSTEMS HAVE A LARGER ATTACK SURFACE



Source: Bryan, Garnier & Co

2: Regulators are increasing requirements

CASE STUDY:



Colonial Pipeline Company

On May 7, 2021, the Colonial Pipeline, which carries approximately 45% of the gasoline, diesel and jet fuel consumed on the US east coast, suffered a ransomware attack, leading to a six-day shutdown of the pipeline's operations to contain the attack, even though the ransom of 75 bitcoin was paid and the network restored. This resulted in fuel shortages in filling stations in several US states, changed flight schedules, and raised fuel prices in most of the US. Just days after this cyberattack, US President Joe Biden signed Executive Order 14028, charging multiple governmental agencies with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

The consequences of security breaches in OT are extremely serious and more direct than those of conventional cyber security breaches. As cyberattacks on critical infrastructure by state actors and criminals are becoming more and more common, regulators are introducing new regulatory requirements for operators across the globe.

After the Colonial pipeline attack, the US government's Executive Order underlined the importance of securing critical infrastructure for the first time. It emphasized the need to improve awareness among owners and operators, but also acknowledged that these attacks are threats to national security. This Executive Order should result in the introduction of a new special publication, NIST SP 800-161, from the National Institute of Standards and Technology (NIST), the US body

that issues standards and guidelines for federal agencies. In Europe, a new regulation was introduced in 2016: the Network and Information Security (NIS) Directive. The Council of the European Union agreed on the general approach for its successor, the NIS2 directive, in late 2021. In addition to these directives, the regulatory environment has been evolving at several geographical levels (countries, states, regions) or even at the sector level, for example in manufacturing, power, aviation and maritime.

Recent critical infrastructure incidents and the resulting governmental push to prioritize cybersecurity have led market participants to realize that adopting new solutions is a "must-have" and not a "nice-to-have". This is now significantly accelerating growth in this market.



"Compliance is the number 1 driver for investments in OT Cybersecurity (86%)"

Otorio survey

3: A new generation of OT security players is emerging

Although it is still an emerging market, OT security is already going through its second generation of players. The first generation had two characteristics: 1/ they used IT security solutions adapted to industrial environments to focus on legacy industrial platforms and operations-only networks and firewalls; and 2/ their capabilities were limited and largely reactive.

OT security market offerings have now evolved, following patterns similar to those seen in the IT security market. The best solutions are proactive by design rather than reactive, and also feature the emergence of Security Orchestration Automation and Response (SOAR) solutions to limit the workload of security analysts and improve responsiveness to threats. Emerging players also offer:

- Continuous threat monitoring across networks and endpoints, following a similar pattern to the XDR (Extended Detection and Response, spanning network, endpoint, mail, etc.) trend in IT security
- Incident management system for the registration, prioritization, analysis and resolution of OT cyber security incidents
- Risk assessment process to continually review the OT cybersecurity program effectiveness
- Collection and analysis of asset information such as log files and network information to identify anomalies.

FIG 4: COMPARISON OF CONNECTIVITY AND SECURITY REQUIREMENTS BETWEEN IT AND OT

	IT	OT
Connectivity Mechanisms	Via Telco, Wifi	Via Telco, Radio, Satellite, Powerline Carrier, Wi-Fi
Security Priority	Data security with high confidentiality	Operational uptime with high availability, safety, and integrity
Security Patching	Frequent	Slow to impossible
Cyber Forensics	Available	Limited, if any
Overall Impact From Security Breaches	Business impacts	Business impacts, process fluctuations, equipment damage, environmental release, personnel safety

Source: Palo Alto Networks



75% of OT security solutions will be delivered via multifunctional platforms interoperable with IT security solutions by 2025, according to Gartner

4: Specialized players have an edge

Reviewing the competitive environment reveals that the market for OT security is attracting several types of player:

- Specialized OT security players
- IT security specialists going into OT security, either through partnerships, M&A (for example, Microsoft's acquisition of CyberX and Forescout's purchase of SecurityMatters) or minority investments
- Industrial automation players that want to provide a comprehensive solution to their customers, mostly through venture investments (Rockwell's investment in Claroty, Emerson's in Dragos, Schneider's in Claroty via its venture arm) but also through M&A deals (Hexagon's acquisition of PAS Global)
- The complexity of the industrial environment means that the market has high barriers to entry. The need for technological expertise in the domain means it is dominated by a handful of specialized players, which often address only a subset of issues. These specialized players have a strong advantage over others: they are experts in both security and OT environments, a specific skillset that is globally lacking in the industry.

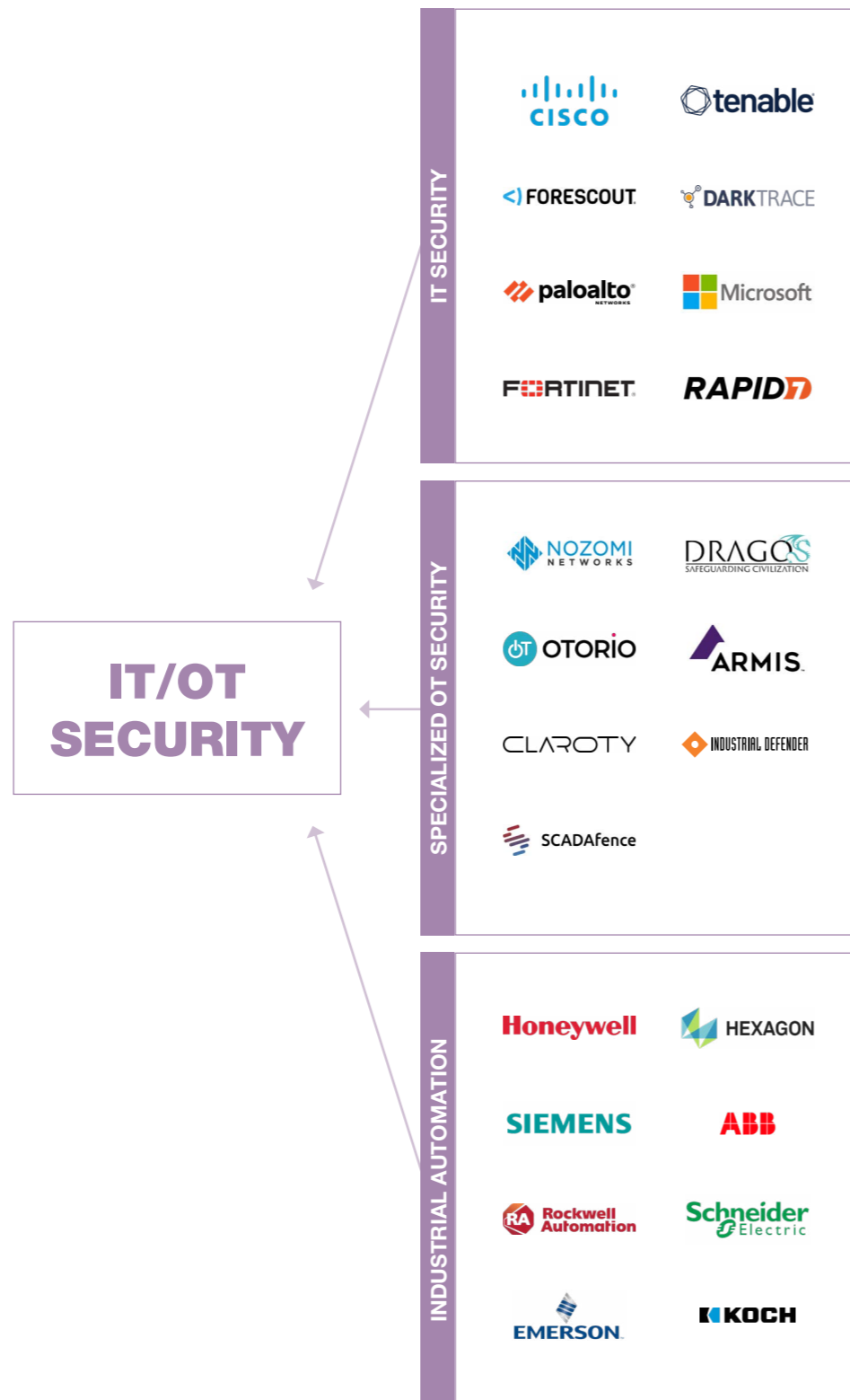


FIG 5: FUNDRAISING AND M&A ACTIVITY

DATE	TARGET	INVESTOR	DEAL VALUE (€M)	TRANSACTION TYPE
Dec-21	Claroty	Softbank	350	Fundraising
Dec-21	Medigate	Claroty	300-400 (rumored)	M&A
Oct-21	Armis	One Equity Partners	260	Fundraising
Oct-21	Dragos	Koch Disruptive Technologies BlackRock	170	Fundraising
Aug-21	Nozomi	Triangle peak	87	Fundraising
Jun-21	Claroty	Bessemer Ventures 40 North	120	Fundraising
Mar-21	SCADAfence	JVP - Rapid7	19	Fundraising
Feb-21	Armis	Brookfield Asset Management	110	Fundraising
Dec-20	Dragos	National Grid Partners Koch Disruptive Technologies	95	Fundraising
Nov-20	PAS Global	Hexagon AB	n.a.	M&A
Jun-20	CyberX	Microsoft	150	M&A
Feb-20	Armis	Insight Partners	950	LBO
Apr-19	Armis	Sequoia Capital Insight Venture	55	Fundraising
Mar-19	CyberX	Qualcomm Ventures Inven Capital	15	Fundraising
Nov-18	Dragos	Canaan Emerson NGP	32	Fundraising
Nov-18	SecurityMatters	Forescout	100	M&A
Oct-18	Nozomi	Planven	26	Fundraising
Jun-18	Claroty	Temasek - Rockwell Schneider (Aster Capital) Siemens (Next47)	50	Fundraising
Apr-18	Armis	Bain Capital Ventures Red Dot Capital	26	Fundraising
Jan-18	CyberX	Norwest	15	Fundraising
Dec-17	Nozomi	Invenergy Future Fund	13	Fundraising
Nov-17	SCADAfence	JVP NexStar Partners	9	Fundraising
Aug-17	Dragos	Energy Impact Partners Allegis Cyber	13	Fundraising
Jun-17	Armis	Sequoia Capital Cerca Partners	15	Fundraising
Oct-16	Nozomi	GGV Capital	6.5	Fundraising
Sep-16	Claroty	Bessemer Ventures	28	Fundraising

Source: Bryan, Garnier & Co

5: Conclusion

All the planets in the OT cyber security market – regulatory, market awareness, availability of new solutions – appear to have now aligned for it to reach its potential. Stakeholders are faced with two key issues in the coming five years: first, adopting new OT security solutions that offer strong capabilities in asset identification, network visibility and continuous risk monitoring; and second, dealing with the talent shortage plaguing cybersecurity – and even more so OT security – due to the specific skillset it requires. This will drive up demand for managed OT security services and also for solutions that have strong automation capabilities.



OTORIO

INTERVIEW WITH DANIEL BREN – OTORIO CEO :

1. Could you please tell us what, in your opinion, are the key factors that are critical for success in the IT/OT security market?

In order to successfully address the OT security challenge you first need to understand that IT security and IT/OT security are not the same. There are inherent challenges to OT security. First, this is a multi-vendor environment that is using multiple protocols and multiple communication techniques, so it is very difficult to tailor a generic solution that will fit all. Second, an IT environment is, in most cases, three to five years old. In an OT environment, technologies can be 20-25 years old. Third, not all assets are born equal. The same technology, with the same vulnerabilities, in two different places on the same production floor can carry different roles. Therefore, their criticality will be different.

To deal with IT/OT security, the operational use case of the asset needs to be understood. To provide a cohesive holistic protection, the risk needs to be continuously monitored and contextualized according to the impact on the operations and on the business. Another thing that is more challenging in an OT environment: patching. Some

technologies are very old and patches may not be available. However, even when patches are available, patching may not be an option because production would need to be taken down outside the traditional maintenance window. Therefore, the ability to suggest alternatives to patching, which are feasible within the constraints of the operational environment, is very important (as it related to the ability).

2. How are OT security players dealing with the complexity of industrial sites?

There are two ways of dealing with the challenging complexity of industrial environments:

- One way is to connect, work and do the heavy lifting on the cloud. This is very challenging in a legacy environment, and industrials are very sensitive about connecting production sites to the cloud, especially in countries like Germany and Sweden, where they are very strict about connectivity and attack surface.
- The second way is based on a well-known industrial concept called the digital twin (adapted to cyber). If the digital twin is generic enough, it can be used in different industries by applying two sets of tailored layers: one is data collection - different

industries have different data systems and protocols but it is a relatively easy task to develop a new data collector - and the other is to apply the vertical tailored use case on the cyber process itself. That way, the solution does not only serve a niche vertical or industrial organizations within a narrow range of cybersecurity maturity, but a much broader group.

3. Is OT security different from IT security?

There are similarities in the titles, but differences in operations.

The first key concept of security is to keep basic hygiene. 90% of the successful attacks of the last 18 months would have been avoided if companies had kept basic hygiene. For that, companies need to move from reactive to proactive. Companies need to proactively assess their cyber security controls, find where they're not good and then improve that. They should not spend a lot only on the post-breach detection and response, because we've seen that in most cases this is very costly. Now it is much more complex in an OT environment, but if it's smartly tailored, and a risk-based approach is implemented, then it'll be more successful.

A second critical theme is the supply chain and the risk it puts you under. In the past, OT environments were air-gapped, nobody could reach the production floor. Today, especially after COVID, when both employees and suppliers need to be able to work remotely, the production floor is more open. Today, nobody is governing the supply chain and assessing the suppliers' basic cyber hygiene. This is exposing production floors.

We've seen a lot of very successful (i.e. disruptive) supply chain attacks and water infrastructures attack during the last 18 months. We understand that in an OT environment this is much more challenging because you don't have the resources, you don't have the manpower, you don't have the cybersecurity know-how. Whether you generate electricity, manufacture cars, pharma, drugs or food, you need to leverage a platform that automates and manages all the ongoing risk management and assessment, and then alerts you when there's something going wrong.

4. How do you see the competitive environment evolving? Are IT security specialists entering the OT security market? And how

about industrial software vendors?

Large IT security technology vendors have been trying to enter OT security for several years, but the OT environment is unique. For an IT platform, it will take a lot of effort to adapt. It's not just "let's collect data, put it in the same processing unit". The analysts need to understand and contextualize the use cases. There is a very large spectrum of technologies, levels of maturity and differentiation between verticals within process industries and verticals within discrete industries. It is a very heavy lifting task for those players.

The next cluster is the first generation of OT security solutions. Those are network-based reactive behavioral analysis-driven solutions. We are hearing from customers that these solutions offer a subset of asset inventory and detection capabilities but do not contextualize the OT environment. This is primarily because they were developed on an IT-driven concept. In a survey OTORIO conducted in Q4 2021 that covered 200 CISOs from the energy and utility sectors, respondents claimed that first-generation solutions tend to require high level of skillset that they do not have (57%); that the mitigation steps they propose are not feasible (49%) that they lead to alert fatigue (44%) and are too complicated to use (33%)

Some of the industrial software vendors are also looking at what to do. Schneider, ABB, Siemens, and Rockwell invested in the first-generation solutions and at the end of the day, they did not acquire those companies. We are in discussions with a lot of those players and they are looking at how to go forward, whether to partner with companies like ourselves or to try and acquire. I think that the valuation of companies like Nozomi Networks and Claroty today exceeds what is reasonable for companies like Hexagon and the others. These large players are probably going to go for an IPO. Industrial software vendors will have to partner or to acquire a small, new-generation player.

I do believe that we are in a unique place, and we see that from partners and other ecosystem players. We are the first OT-native proactive cyber security platform. We did not start by building a cyber security platform, we started by contextualizing the OT environment. We used that as a basis to perform cyber risk management. Lastly, we put a lot of emphasis on simplifying usability by reducing the "noise", providing clear context to alerts and delivering simple mitigation steps.

5. Has the COVID-19 pandemic impacted the adoption of OT security? Have you seen an acceleration?

Without a doubt. It's not only the acceleration of the capacity and volume, but also the maturity of requirements. Three years ago, the main requirement was asset inventory and then vulnerability databases or vulnerability lifecycle management. I would say that today the main task is risk identification.

6. What are the bottlenecks for the adoption of OT security solutions?

In this case, it's not the executives, it's the operational teams. They are very protective of their environment, and there are language and terminology gaps, conceptual gaps and sometimes

even geographical gaps between the CISO teams and the operations team on site. So until this gap is closed, it is very difficult for CISOs to implement cyber security in the operational environment because this is not their jurisdiction. For example, at a large oil and gas company where the CISO asked us to deploy our solution, it took four months for him to convince the OT engineer of the need.

And the second thing is the complexity of deployment. Most of the deployments in OT environments require heavy lifting, and if security vendors are not prepared for such a journey, the bottleneck will be engineering and delivery. It is easier in new factories as built-in is always easier than bolt-on. The problem, however, is that new factories are almost always connected to the existing enterprise, and therefore to the old factories. The strength of the chain is the weakest link.

7. What are the key trends in IT/OT security?

We see more companies realize that they cannot handle their own IT/OT cyber security, and they outsource that to partners. The large ones are very slow-moving and very costly. This is why there is a new trend where mid-market cyber security providers are entering the OT environment. Companies like Arctic Wolf, Advens, Nomios, Kudelski etc. In the survey I mentioned earlier, 53% of respondents say they either fully outsource OT security (41%) or partially outsource it (12%).

Security service providers are expanding into the OT convergence and they're looking for converging platforms and technologies as well.



White Paper Authors

Sanjin Goglia
Managing Director
Investment Banking
sgoglia@bryangarnier.com

David Vignon
Equity Research Analyst
Software & Payments
dvignon@bryangarnier.com

Gregory Ramirez
Equity Research Analyst
Software & Payments
gramirez@bryangarnier.com

Technology Team

INVESTMENT BANKING

Olivier Beaudouin
Partner
Paris
obeaudouin@bryangarnier.com

Tor Berthelius
Partner
Stockholm
tberthelius@bryangarnier.com

Stanislas de Gmeline
Partner
Paris
sdegmeline@bryangarnier.com

Thibaut de Smedt
Partner
Paris
tdesmedt@bryangarnier.com

Falk Müller-Veerse
Partner
Munich
fmueellerveerse@bryangarnier.com

Sanjin Goglia
Managing Director
Investment Banking
sgoglia@bryangarnier.com

Erik Furnes
Managing Director
Oslo
efurnes@bryangarnier.com

Charlie Pujo
Director
Paris
cpujo@bryangarnier.com

Khalid Ibrahim
Director
Paris
kibrahim@bryangarnier.com

EQUITY RESEARCH ANALYST TEAM

Thomas Coudry
Managing Director
Telecoms & Media
tcoudry@bryangarnier.com

Paul de Froment
Cleantech & Energy
Transition
pdefroment@bryangarnier.com

Bruno de La Rochebrochard
Business and Tech-enabled
Services
bdelarochebrochard@bryangarnier.com

Thibault Morel
Hardware & Semiconductors
tmorel@bryangarnier.com

Gregory Ramirez
Software & IT Services
gramirez@bryangarnier.com

Xavier Regnard
Cleantech & Energy
Transition
xregnard@bryangarnier.com

David Vignon
Equity Research Analyst
Software & Payments
dvignon@bryangarnier.com

Paul Charpentier
Research Associate
pcharpentier@bryangarnier.com

EQUITY CAPITAL MARKETS

Pierre Kiecolt-Wahl
Partner
Co-head of ECM
pkiecoltwahl@bryangarnier.com

Christophe Alleman
Co-head of ECM
calleman@bryangarnier.com

EQUITY DISTRIBUTION

Nicolas d'Halluin
Partner
Head of US Distribution
ndhalluin@bryangarnier.com

Guillaume Hannebelle
Managing Director
Head of European Distribution
ghannebelle@bryangarnier.com

Recent Transactions

Bryan, Garnier & Co leverage in-depth sector expertise to create fruitful and long-lasting relationships between investors and sector leading growth companies.

 Acquired by Financial Advisor	 Acquired by PARQUEST CAPITAL Financial Advisor	 Private Placement TIKEHAU CAPITAL Sole Placement Agent	 Acquired by Financial Advisor	 Private Placement Sole Placement Agent
--	--	--	--	---

About Bryan, Garnier & Co

Bryan, Garnier & Co is a European, full service growth-focused independent investment banking partnership founded in 1996. The firm provides equity research, sales and trading, private and public capital raising as well as M&A services to growth companies and their investors. It focuses on key growth sectors of the economy including Technology, Healthcare, Consumer and Business Services. Bryan, Garnier & Co is a fully registered broker dealer authorized and regulated by the FCA in Europe and the FINRA in the U.S. Bryan, Garnier & Co is headquartered in London, with additional offices in Paris, Munich, Zurich and New York. The firm is a member of the London Stock Exchange and Euronext.

Bryan, Garnier & Co Technology Equity Research Coverage

8 Analysts | 70+ Stocks Covered

With more than 150 professionals based in London, Paris, Munich, Stockholm, Oslo and Reykjavik as well as New York and Palo Alto, Bryan, Garnier & Co combines the services and expertise of a top-tier investment bank with a long-term client focus.



BRYAN, GARNIER & CO

LONDON

Beaufort House
15 St. Botolph Street
London, EC3A 7BB
UK

T: +44 (0) 207 332 2500

Authorized and regulated by the Financial
Conduct Authority (FCA)

PARIS

92 Avenue des Champs Elysées
75008 Paris
France

T: +33 (0) 1 56 68 75 00

Regulated by the Financial Conduct
Authority (FCA) and the Autorité de Contrôle
prudentiel et de résolution (ACPR)

MUNICH

Königinstrasse 9
80539 Munich
Germany

T: +49 89 2422 62 11

NEW YORK

750 Lexington Avenue
New York, NY 10022
USA

T: +1 (0) 212 337 7000

FINRA and SIPC member

STOCKHOLM

Nybrokajen 5
111 48 Stockholm
Sweden

T: +46 722 401 080

OSLO

Beddingen 8, Aker Brygge
0250 Oslo
Norway

T: +47 22 01 64 00

Regulated by the Norwegian Financial
Supervisory Authority (Norwegian FSA)

REYKJAVIK

Höfðatorg, Katrínartún 2
105 Reykjavik
Iceland

T: +354 554 78 00

VISIT OUR WEBSITE



DISCLAIMER

This document is based on information available to the public and other sources deemed reliable. No representation or warranty, express or implied, is or will be made in relation to, and no responsibility or reliability is or will be accepted by Bryan Garnier & Company or any of its officers, employees or advisers as to the accuracy or completeness of this document or any other written or verbal information available to the recipient or its advisers. While all reasonable care has been taken to ensure that the facts stated are accurate and the opinions given are fair and reasonable, neither we nor any of our affiliated companies nor any of our, or their directors, representatives or employees, accepts responsibility or liability for any loss or expense arising directly or indirectly from the use of this document or its or its contents. This document is not and should not be construed as an offer, or a solicitation of any offer, to buy or sell securities. Bryan, Garnier & Co is authorised and regulated by the Financial Conduct Authority (FCA) in the United Kingdom.