



Protecting society with cyber-physical security



DIGITAL REPORT 2022

IN ASSOCIATION WITH:







CLAROTY

PROTECTING
SOCIETY WITH
CYBER-PHYSICAL
SECURITY

Simon Chassar, CRO, Claroty, reflects on the last two years, the maturity landscape of those in critical infrastructure sectors and Industry 5.0

In the business of building technology to protect critical infrastructure environments, Claroty's core mission is to secure the cyber-physical systems used to run hospitals, power grids, oil pipelines, water utilities, and many other essential services that we depend on every day.

"We have unique skills and a unique technology platform that is specially designed to detect, manage, and protect all connected devices within the four walls of an operational site, whether it's industrial, medical, or commercial," says Simon Chassar, chief revenue officer, Claroty.

"Claroty has evolved significantly since I joined. When I started, the company was on a growth trajectory. There was an increase in the number of attacks in the critical infrastructure environments and increasing regulation. In the years following 2013, there has been a 3900% increase in ransomware attacks in these environments.

"Since joining, we have established a structured organisation, increased our headcount and client base, and grown our revenue year on year by 100%. All of that growth has helped us to stay ahead of threats and to better serve our customers, protecting them from malactors taking advantage of the weaknesses within the critical infrastructure."





2015

Year
founded

450+

Number of
employees

Simon Chassar



TITLE: CHIEF REVENUE OFFICER

INDUSTRY: INDUSTRIAL CYBERSECURITY

LOCATION: SURREY, UNITED KINGDOM



Simon Chassar is Chief Revenue Officer at Claroty, where he leads the global sales organisation including territories, partnerships, sales engineers, sales development, and revenue operations. He brings more than 20 years of IT industry experience across the go-to-market on hardware, software, and services at multinational organisations such as NTT, Cisco, Avaya, VMware, and Actifio. Prior to joining Claroty, he served as CRO of the security division of NTT, where he ran a sales channel, and marketing organisation of more than 300 people, delivering over \$1.5 billion in revenue across products and services. Chassar is part of the World Economic Forum for Oil & Gas Security.

“Since joining, we have established a structured organisation, increased our headcount and client base, and grown our revenue year on year by 100%”

SIMON CHASSAR
CHIEF REVENUE OFFICER,
CLAROTY





Claroty: protecting society with cyber-physical security

WATCH NOW

On the cusp of a revolution: Industry 5.0

From the mechanisation of production through to automation and connectivity, the industrial sectors are on the cusp of a new evolution: Industry 5.0.

“While Industry 4.0 saw connectivity of the end-to-end processes, Industry 5.0 harnesses all these other smart devices out there to effectively drive the optimisation of factories and production; humans and intelligent devices through connectivity,” says Chassar.

He adds, “Increasingly, we are seeing those in the industry look at how they can optimise further by reducing waste, accelerating production, reducing energy, and improving health and safety through greater connectivity – not only in production, but across different functions and supply

chains, as well as automating functions where possible.

“We are on that cusp now, where more organisations are heading in this direction regarding their future strategies. But, with greater connectivity of machines comes greater exposure to new kinds of cyber threats, which the machines are often not equipped to withstand. Ensuring that connectivity goes hand-in-hand with security is imperative for ensuring the safety and resiliency of the world’s critical infrastructure.”

The maturity landscape of those in the industrial sector

Although most organisations (60%) are only now going through the awareness phase and beginning to understand that they have these connected assets in their industrial environments, many continue to struggle to determine how they communicate or where they are located.

Digital Safety + Process Integrity = Cybersecurity for Industrial Environments

With over 100 years of combined OT/IT Industrial, Enterprise and C-suite experience, Velta Technology helps clients:

- Take proactive steps to protect Operational Technology (OT) from adverse cyber events
- Discover and correct vulnerabilities relating to physical outcome producing equipment
- Facilitate internal discussions between OT, IT, and the C-Suite to ensure cybersecurity ownership on the plant floor

Velta Technology
Get Safer Sooner.





Industrial Environments, IIoT and Digital Safety

Craig Duckworth, President and Co-Founder of Velta Technology, discusses IIoT, cybersecurity and partnering with Claroty to stay on top of the industry

Craig Duckworth is the President and one of the co-founders of **Velta Technology**, providing Digital Safety, operational integrity, and cybersecurity for industrial manufacturing and critical infrastructure environments. "Communication between IT and Operational Technology (OT) teams is vitally important, and we believe OT needs to own the safety and security of the plant floor. IT security tools and solutions can't be overlayed onto equipment in the Industrial Control System (ICS) environment. The two environments and skillsets to successfully manage and protect are very different."

Velta Technology's partnership with Claroty

Velta Technology's leadership team made the strategic decision to work only with top industrial cybersecurity companies – with **Claroty** a leader in asset visibility and

monitoring solutions for industrial networks. "We bring value to Claroty's clients because of our deep understanding of the inner working of OT and IT environments, and the full potential of their industrial security solution. Velta Technology is not an IT cybersecurity technology company trying to move into the OT space. We understand process integrity and the inherent risks of plant floor equipment, which are unique to industrial environments. We help our mutual clients fully embrace what Claroty and our expertise at Velta Technology can offer."

A unique Velta Technology advantage is their team. "Our leadership team has over a hundred years of OT practitioner experience, and team members are degreed engineers that understand process integrity, ICS environments, and how to maximize **Claroty's** solutions within the OT space," said Duckworth.

The Future of IIoT and OT according to Velta Technology

Over the next year, Duckworth sees Velta Technology poised for continued growth as a market leader. "Our deep understanding of the Claroty platforms combined with our rich knowledge of Industrial Control Systems, allows Velta Technology to highlight the value of Claroty and what they do for the OT space."

[Learn more](#)



“Because of this, many organisations were not prepared for the last few years and remain unprepared for the years to come,” explains Chassar.

“Currently, only 30% of organisations actually understand their assets, know how they communicate, and where they are located – and even fewer, 10%, have full vulnerability awareness of every single asset within their production and operational environments, understanding how they communicate and how they can mitigate threats,” he adds.

While awareness is on the rise, the industry needs to be quicker if it is to successfully tackle malactors as they enhance their sophistication and maturity level.

“In most cases, malactors or cyber criminals are effectively mimicking what would be a normal OT operator: they get inside the environment, start to learn and understand it – and, in most cases, more so than the companies themselves. So the discussion now at a boardroom level is how the industry can mitigate these risks because it is now a question of business continuity,” says Chassar.



“Compliance and governance are also driving this need for organisations to take action and develop a standard framework.”

Innovations in cybersecurity

When it comes to innovation, Chassar is seeing clear investments being made in Claroty’s deep domain expertise area within industrial environments.

“Organisations are innovating in network policy segmentation, user identity permissions, and network policy management to mitigate risks,” he says.

“While Industry 4.0 saw connectivity of the end-to-end processes, Industry 5.0 harnesses all these other smart devices out there to effectively drive the optimisation of factories and production between humans and machines”

SIMON CHASSAR
CHIEF REVENUE OFFICER,
CLAROTY

“I’ve also started to see more innovation in secure access, making sure that organisations have specific tools to access the physical systems’ environment for every user and that can only be accessed by that user. This reduces the possibility of back door risks to the industrial environment.”

Being prepared for a cyber attack

“If an organisation doesn’t have a policy or project underway, then they should start one immediately,” says Chassar.

He explains that it is imperative to understand where the assets are, how they communicate, and where they are most vulnerable. Once they start this process, the organisation needs to get to at least the same level of understanding as the criminals in order to manage this risk.



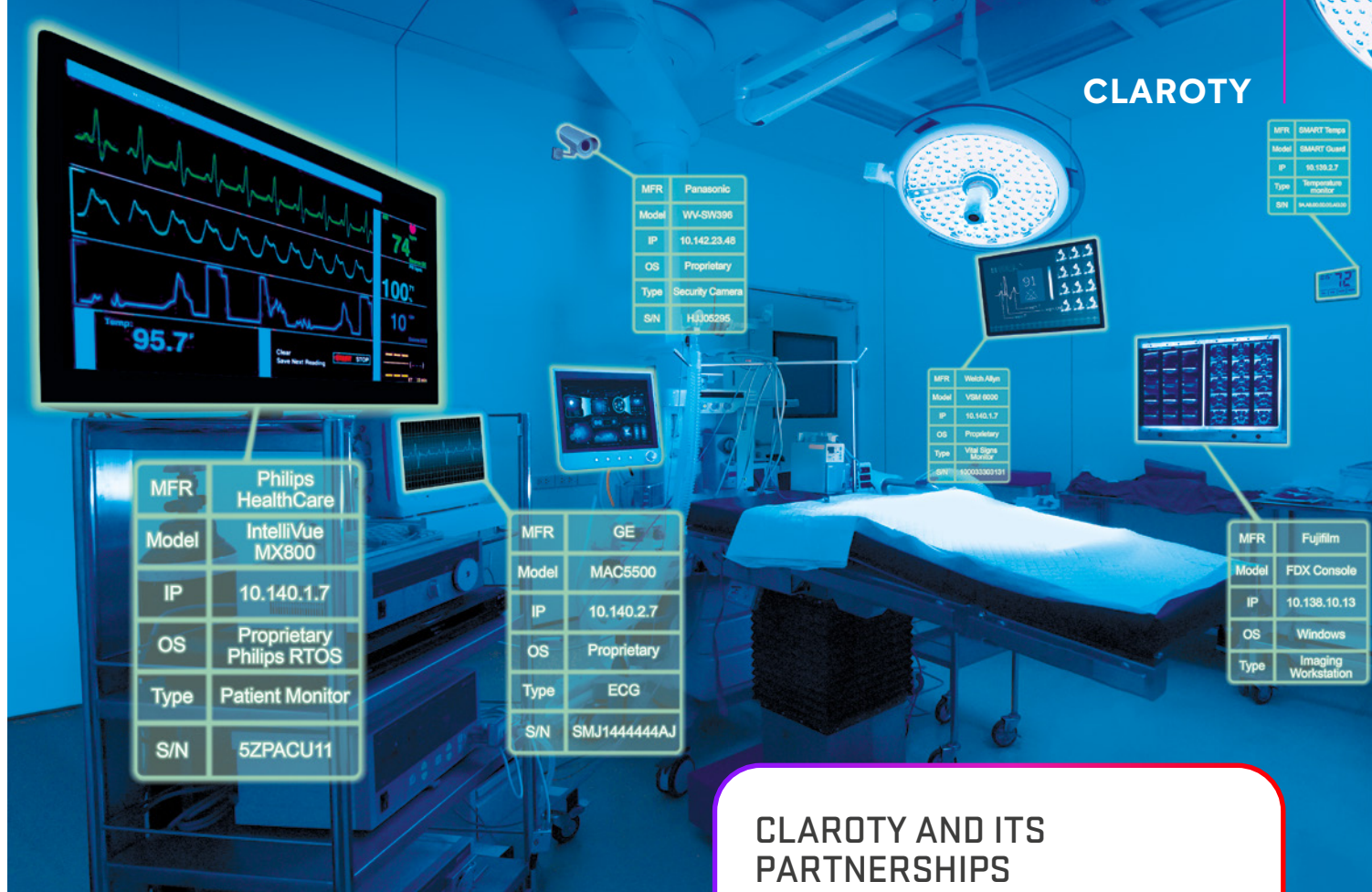
Intelligent Cybersecurity since 2012

OT/ICS, IT, CLOUD

We've got you covered.

[Download eBook](#)

[Kudelski Security OT/ICS Solutions](#)



CLAROTY AND ITS PARTNERSHIPS

Dedicated to building a safer society and protecting all critical infrastructures and industries, Claroty strives to build the best technologies to maintain the supply of essential products and services – healthcare, fuel, energy, food, water – by protecting them from threats as they become increasingly interconnected.

“Our aim is to build the best technology and provide the best research to make everyone aware of the vulnerabilities out there and report on what the cyber criminals are up to, so our partners are critical to our delivery. We have an array of partners working with us, from advisors to system integrators, managed services and automation vendors,” says Chassar.


“We have a broad range of partners that help our customers to protect themselves against the adversaries out there to create a safer society.”

“The next step on from this is to look at who has access to the environment and control that access. Knowing who’s connected, when, where, and to what system is critical. Then organisations should look at how to respond to and recover from potential attacks, and, finally, look at how they can detect attacks,” explains Chassar.

Chassar also emphasises the importance of deploying the best technology. “With one hour of downtime having the potential to cost

“With this greater interconnectivity of machines comes greater exposure to risk, so we have to make sure that we protect these newly formed connections”

SIMON CHASSAR
CHIEF REVENUE OFFICER,
CLAROTY



“Currently, only 30% of organisations actually understand their assets, know how they communicate, and where they are located – and even fewer, 10%, have full awareness of the risks and vulnerabilities affecting these assets and how to mitigate them”

SIMON CHASSAR
CHIEF REVENUE OFFICER,
CLAROTY



80%

of respondents experienced an attack

47%

reported an impact on their OT/industrial control system environment
More than 60% paid the ransom

52%

paid more than US\$500,000

90%

disclosed the incident to their shareholders or authorities

60%

are centralising both OT and IT governance under their CISO

62%

are supportive of government regulators enforcing mandatory and timely reporting of cybersecurity incidents that affect IT or OT/ICS/XIOT systems

The global state of industrial cybersecurity independent survey results, 2021:
Resilience amid disruption, Claroty

a manufacturer £5mn, deploying the best technology that you can helps you gain a full understanding of the risks and vulnerabilities within your environment. It can also help to identify early signs of anomalous behaviour, so that you can find out if a process is not operating as it should be before any damage is done,” says Chassar.

What does the future hold?

Over the next 12 to 18 months, Chassar expects to see an increase in the volume of regulations centred around critical infrastructure environments. “There are already many regulations underway in the United States, Australia, and Germany, and I believe that this will, in turn, drive the next wave of reporting compliance,” says Chassar.

“I expect to see more innovation when it comes to the Extended IoT (XIOT) which will drive IT security and control vendors to partner with domain specialists – like Claroty – to deliver a much more holistic cybersecurity strategy.

“Collaboration and shared knowledge will be a key trend in the future to enrich each other's understanding of a very complex environment.

“I also see society placing more demand on factories to be faster and more efficient in the way they produce goods, as well as being more eco-aware by using less energy and reducing waste. With this, though, an increasing number of physical systems will become connected that will need protecting. Finally, I see a greater use of cloud technology as we see Industry 5.0 accelerate and organisations look to how they can be more interconnected with end-to-end efficiency, as well as be more energy efficient.”





Claroty Ltd

5 New Street Square
London
United Kingdom
EC4A 3TW

—
6-9 The Square
Stockley Park
Uxbridge
UB11 1FW

T 1 212-937-9095 | claroty.com

POWERED BY:

