

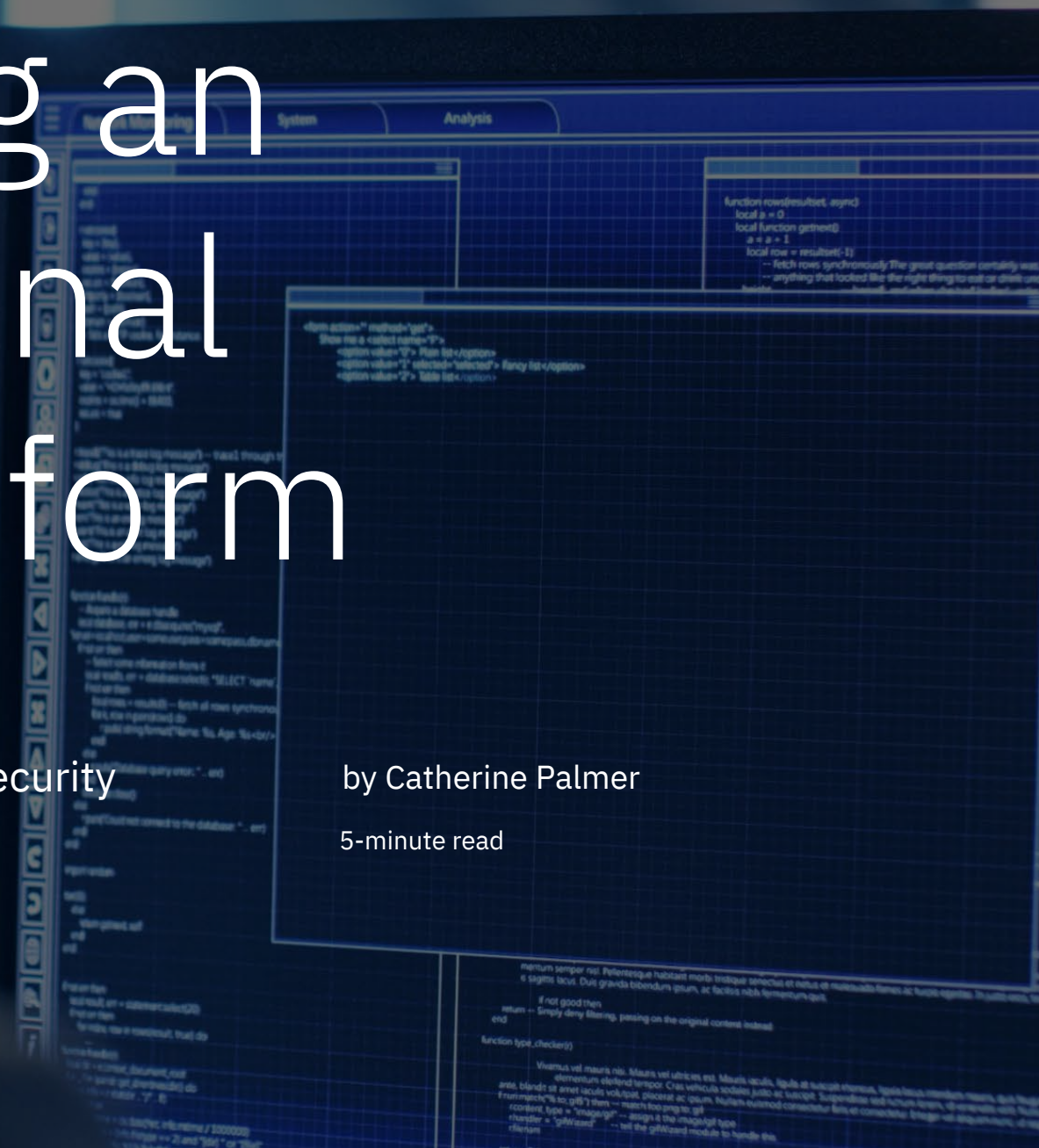


# Protecting an international trade platform

Marco Polo Network adds proactive security measures to its growing network

by Catherine Palmer

5-minute read





**M**arco Polo Network is on a mission to digitize and transform supply chain transactions, payments and financing. Founded in 2017, the business is a fast-growing open account automation and working capital network that is based on blockchain technology.

Marco Polo Network connects data silos and supply chain systems that are scattered around the world. Rather than having a single destination application, the company provides a distributed ledger-based platform that connects all of its users to the network.

Marco Polo Network is essentially modernizing supply chain transaction processes by providing seamless integration and data exchange between trading parties, such as linking a large corporate buyer to their entire supply chain, as well as to their logistics and banking partners. The value of the network grows for every existing participant whenever a new organization joins, so the business has ambitious plans for growth.

It took just

# 12 weeks

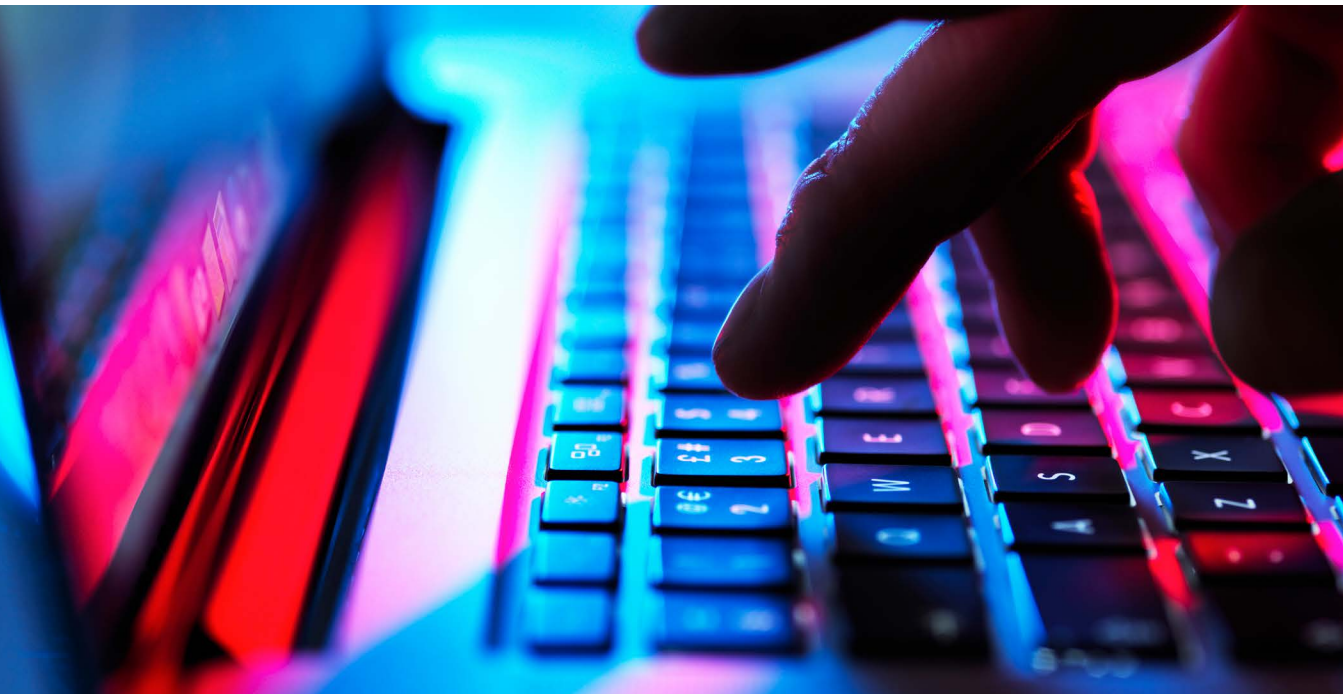
from solution implementation to results

The IBM solution analyzed

# thousands

of security events per hour

# Addressing security in the cloud



To support its growing business, Marco Polo Network moved its infrastructure to the cloud. The cloud provides advantages and opportunities, such as scalability and flexibility. However, because financial data is so sensitive, the company needed to make sure that it was taking a very proactive approach to security.

“Our customers trust us to keep their data safe,” says Ray Gallagher, Director Information Security, at Marco Polo Network. “They trust us to ensure that the systems on which they transact are secure and protected from the attackers that are out there in the world.”

By all accounts, security threats are on the rise around the world. Marco Polo Network needed to find a solution that would help it add security functionality to its cloud infrastructure.

# Identifying security criteria

As Marco Polo Network began to look for a partner to help it implement a security solution, it had several key criteria. The business needed a solution that could provide:

- A security operations center (SOC) operating on a 24x7 basis to reinforce its own security team.
- Operational defense capabilities against cyberattacks.
- Threat intelligence against zero-day attacks, which are attacks that exploit vulnerabilities the software vendor is unaware of. These types of attacks are

particularly concerning because they are more likely to succeed than known vulnerabilities, for which patches exist.

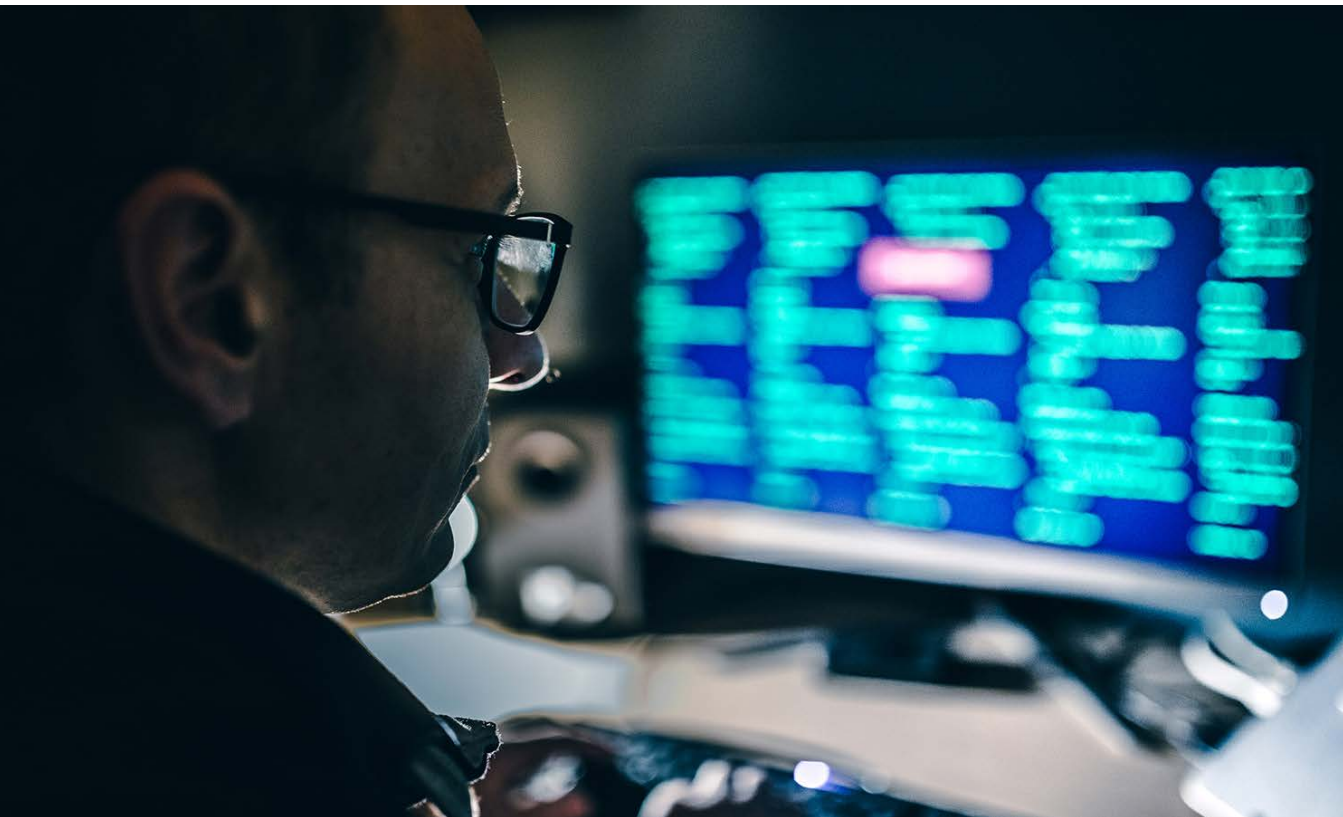
- The capacity to ingest cloud-based logs. Because the business's solution runs on the cloud, ingesting and analyzing cloud-based logs was essential to Marco Polo Network's security strategy.
- Scalability to support Marco Polo Network's growth. The more members that join the network, the greater the value of the network to all its participants. So Marco Polo Network needed to make sure it adopted a highly scalable security solution.

Marco Polo Network also needed to be able to demonstrate industry and regulatory compliance, including compliance with the ISO 27000 international security standard. And finally, Marco Polo Network is part of the International Chamber of Commerce (ICC) Digital Trade Standards Initiative (DSI). This initiative supports the development of open trade standards to enable interoperability between digital trade systems, applications and networks. Marco Polo Network needed to make sure that any solution it adopted could adhere to these standards as well.

“Our customers trust us to keep their data safe. They trust us to ensure that the systems on which they transact are secure and protected from the attackers that are out there in the world.”

**Ray Gallagher**, Director Information Security, Marco Polo Network

# An experienced security partner



Marco Polo Network partnered with IBM Business Partner Smarttech247, a managed detection and response (MDR) company and a market leader in security operations for global organizations. “We chose Smarttech247 because they could provide IBM Security® QRadar® SIEM, a known, trusted security solution that correlates thousands of events and searches for threats and attacks,” says Gallagher.

Smarttech247 has extensive experience dealing with the kinds of issues that Marco Polo Network is facing. “At Smarttech247, we’ve seen a growing demand in monitoring solutions, in world-class technologies such as QRadar SIEM,” says Raluca Saceanu, General Manager at Smarttech247. “And we have seen a shift in mindset, whereby organizations are adopting a more risk-based approach to their security, to their vulnerability management and to their monitoring. They are also adopting a more proactive defense strategy.”

# End-to-end visibility

Smarttech247 worked with the IBM Security team in Ireland and Marco Polo Network to implement the solution, which includes the QRadar SIEM and IBM Security X-Force® Threat Intelligence software. Smarttech247 integrated the IBM applications with Marco Polo Network's Microsoft Azure cloud platform.

The QRadar SIEM solution provides end-to-end visibility into Marco Polo Network's entire cloud environment and

analyzes thousands of potential security events per hour. And the X-Force Threat Intelligence application gives Marco Polo Network access to up-to-the-minute security research expertise and global threat intelligence so it can stay ahead of zero-day attacks. Using the comprehensive insights gained from the two IBM applications, the Marco Polo Network team can investigate and respond to any potential threats, helping to protect the network and the customer data flowing

across it. The QRadar software also helps Marco Polo Network manage industry and regulatory compliance.

The Smarttech247 team provides a 24x7 SOC to support Marco Polo Network's own security team. "Having the SOC in place helps us maintain our ISO 27000 international security standard and allows us to monitor and protect customer data sitting on the Marco Polo Network platform," Gallagher says.

# Rapid results

Implementing the entire solution took just 12 weeks. During the project, the teams experienced no major roadblocks. Even the process of ingesting Marco Polo Network's internal log sources went smoothly. "QRadar is very flexible. We managed to change our log sources, including many

that are open source, and QRadar was able to cope with all of them and to ingest the logs quite seamlessly," says Gallagher.

Gallagher credits this quick turnaround to the commitment and dedication of everyone involved in the effort. "It's very

important for all parties to understand the functionality and pain points or gaps you need to close," he says. "Once you share that information with your security partner, you can work together as one team to close any gaps and ensure that you've got the highest and best possible security."



### About Marco Polo Network

Marco Polo Network (link resides outside of ibm.com) is one of the world's fastest-growing digital networks for supply chain transactions and payments. Founded in 2017 and headquartered in Ireland, Marco Polo Network utilizes the latest technologies to provide the most forward-thinking supply chain digitization and automation solutions for corporations and their financial service providers.

### Solution components

- IBM Security® QRadar® SIEM
- IBM Security X-Force® Threat Intelligence



### About Smarttech247

IBM Business Partner Smarttech247 (link resides outside of ibm.com) is a multi-award-winning managed detection and response (MDR) company and a market leader in security operations for global organizations. Geared toward proactive prevention, its services include 24x7x365 SOC, cloud security and threat and vulnerability management.

© Copyright IBM Corporation 2022. IBM Corporation, IBM Security, New Orchard Road, Armonk, NY 10504

Produced in the United States of America, December 2022.

IBM, the IBM logo, ibm.com, IBM Security, QRadar, and X-Force, are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.