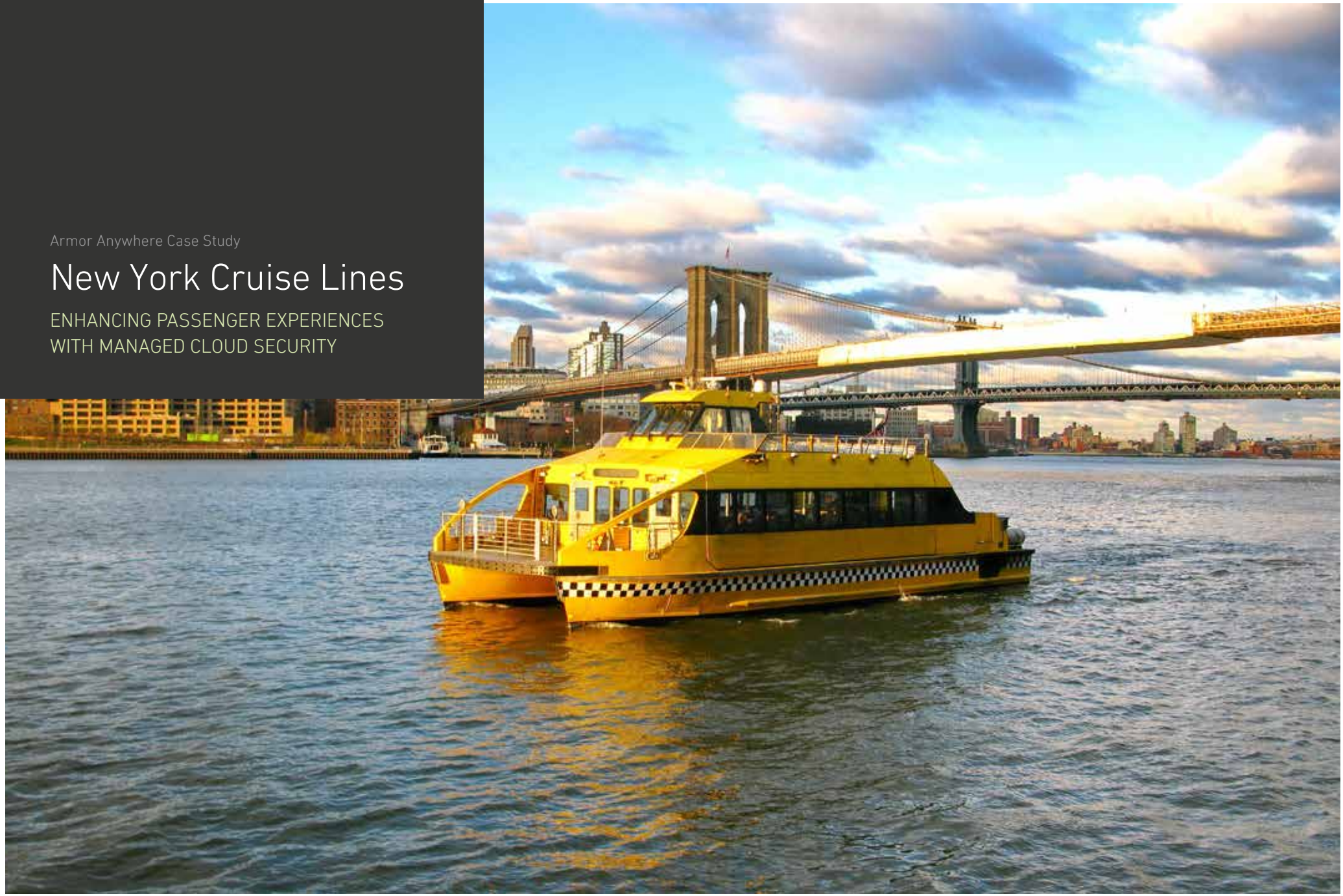
Armor Anywhere Case Study

New York Cruise Lines

ENHANCING PASSENGER EXPERIENCES WITH MANAGED CLOUD SECURITY



Armor Anywhere Case Study

New York Cruise Lines

ENHANCING PASSENGER EXPERIENCES WITH MANAGED CLOUD SECURITY

Company	New York Cruise Lines
Industry:	Travel/Tourism
Armor Solutions:	Armor Anywhere
Cloud provider:	Hybrid
Website:	www.nycl.com

Overview

Operating in the tourism industry is a very customer-centric proposition. Ensuring each passenger has a great experience is key to attracting repeat business and generating referrals. In our internet-enabled world, this also takes on additional mandatory elements – particularly around the necessity to provide guests with online resources so they can plan, book and pay from any device.

However, with every new web-facing resource, there's an increased risk of a data breach. So, it becomes a balancing act between maintaining user-friendliness of your online resources and data security.

It's a proposition that can keep any organization up at night - especially those responsible for implementing the security strategies to keep their network safe.

Security challenge

For New York Cruise Lines, the parent company of industry-leading travel, tourism, entertainment and restaurant businesses, those sleepless nights belonged to Director of Technology, Tanvir Azad.

It was up to him and his team to secure their hybrid cloud infrastructure, comprised of 25 virtual machines. However, initially, this task would prove to be challenging.

"I really didn't have much control over the security situation," he said. "I needed a specific tool to manage and secure our environments."

Fortunately, they didn't have to do it alone. Understanding the difficulty of this task, he began looking for a managed security solution that could reduce their security and compliance burden.

Finding the right solution

This is where Armor stepped in to help protect critical aspects of their hybrid environment. Their managed security solution, Armor Anywhere, provides 24/7/365 monitoring of NYCL's payment processing workloads. It also delivers key security tools, such as host-based intrusion dection, malware protection, vulnerability scans and other security tools – all of which are monitored by Armor's security operations center. By integrating multiple layers of protection and log management, Tanvir and his team reduced their security and compliance burden – especially for their PCI-DSS compliance audits.

Armor Anywhere delivered an effective means of gaining transparency into the vital portions of their IT network.

"After Armor stepped in, I was able to understand that there are various activities taking place in the environments specific to those two servers. I was able to utilize that information to get a better understanding of server behavior and what changes I needed to make to the environments."

Why Armor

For Tanvir, the benefit of extending his team and security resources with Armor Anywhere, is that NYCL has the threat detection and monitoring needed to keep its critical data secure. By sharing this burden with Armor, he can focus on business objectives - instead of managing the complexity of a cloud security program.

"With Armor, someone is always keeping an eye on our servers that require constant monitoring, especially the devices that are processing credit cards."

For Tanvir, one example of this reliable and constant monitoring stands out:

"There was an instance when one of our vendors created a local adim on a server that is critical to payment processing. We would'n't have known it was there without Armor's vigilance," he said. "My consultants were impressed that we received an alert so quickly after it was triggered."

Given the solution's seamless integration into his operating environments, Tanvir feels that Armor was a natural fit for his existing hybrid infrastructure.

"The experience has been great," he said. "I'm able to call in 24/7, even in the middle of the night. Sometimes when I'm going through reports, and I see something I don't understand, I'll call Armor's service agents and ask them questions about specific triggers and how the reports are generated."

What's next

When working with a security vendor, Tanvir looks at a company's current technology and where that technology is heading, along with the quality of the relationship between his team and the vendor. He points out that it's a lot easier to fix problems if you have a great working relationship. He has seen all of these aspects in their relationship with Armor.

"They're great to work with, and I'm looking forward to seeing where Armor is going to go with the technology we are using right now," he said.

"With Armor, someone is always keeping an eye on our servers that require constant monitoring, especially the devices that are processing credit cards."

Tanvir Azad, | Director of Technology, NYCL

NEW YORK CRUISE LINES | ARMOR