ARCHITECT JOURNEY

MAN Energy Solutions

Ensuring Both Internal and External Application Access with a Cloud Security Architecture

Company:	MAN Energy Solutions	**Revenue:**	$4.3 billion
Type:	Manufacturing	**Employees:**	15,000
Driver:	Tony Fergusson	**Countries:**	6
Role:	IT Infrastructure Architect	**Locations:**	100

Company IT Footprint: MAN Energy Solutions has 15,000 people in over 100 locations. It has fleets of engines on ships deployed all over the world. Its main offices are in Germany and Denmark. This entity is actually part of the Volkswagen Group, so it is a part of a larger 650,000 person organization.

"To be successful, you really need to sell this concept of cloud transformation—you need to evolve the organizational mindset. This technology is so disruptive that you need the people inside your company onboard."

Tony Fergusson, IT Infrastructure Architect, MAN Energy Solutions

Excerpt from: Stiennon, Richard "Security Transformation" *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 114-120.

MAN Energy Solutions Journey Overview

Business Objectives

- Reduce risk: Shield internal applications from potential attacks
- Reduce network cost, complexity
- Improve user experience
- Secure seagoing vessel control systems and monitoring access

The Solution

- Establish direct connection access with inline security; eliminate backhauling
- Protect internal apps, systems with ZPA
- Onboard third-party contractors
- Connect, secure access for remote seagoing vessels

Impact

- Improved security:
  - Zero-trust default-deny threat posture
  - Inspection of all traffic, including SSL-encrypted
  - Protection against ransomware threats
- Improved user experience with faster app access
- Better management visibility into traffic, app access
- Reduced costs: sunsetted VPNs, software licensing
- Policy-based management, integration for IoT devices
- Faster M&A systems integration

MAN Energy Solutions is a manufacturer of large engines and turbines with fleets of engines on ships deployed all over the world. Tony Fergusson wanted to move to a model where internal applications were not even visible to attackers. Only authenticated users can see them. He calls this stealth approach the "black cloud," and MAN Energy Solutions uses the concept to securely access engine sensors on its deployed fleet. He shares how the organization truly discovered the flexibility of cloud-delivered security when it had its first experiences with ransomware—thanks to its cloud security service, this was a non-event.

In the words of Tony Fergusson:

Eight years ago, we started our journey to the cloud at MAN Energy Solutions when I went down the path of creating a forward proxy for access to the internet. I have been in the IT industry for over 20 years. I started with IBM in 1995, so really at the beginning of the internet. I worked at an application service provider (ASP) back in New Zealand, kind of the precursor for what the cloud is today. I have been working in Europe for ten years, mostly in Denmark for MAN Energy Solutions. While a lot of my experience is with Microsoft products like SharePoint and Office 365, I am actually a network architect.

Moving to cloud-based proxies for internet and SaaS applications

Our on-premises proxy gateways needed to be replaced, so I went to the market and discovered Zscaler for secure internet access. At the time, 2011, they were very new. Now I can say we have been a long-term customer.

Back then, we backhauled all internet traffic from every location and had one connection to the internet. We saw that the future was direct access to the internet from everywhere, while at the same time, we needed to inspect all that traffic. As a result, over several years, we went to local breakouts everywhere and inspection of all traffic in the Zscaler cloud security platform. From a security perspective, this model has been a huge success for our company. We discovered the flexibility of cloud-delivered security when we had our first experiences with ransomware. We simply enabled Zscaler sandboxing for all of our users and the problem went away.

Secure access to internal data center applications without VPN

Back in 2014, I had a lot of discussions with Zscaler around what I call "black cloud"; the whole idea was that my applications should not even be visible to attackers. In 2015, we started beta testing Zscaler Private Access (ZPA). We first used it for the many consultants we work with around the world. Our old system of VPNs was very hard to manage. It was difficult to onboard people and get the visibility into what they were accessing.

> *“We saw that the future was direct access to the internet from everywhere, while at the same time, we needed to inspect all that traffic.”*

The first proof-of-concept (PoC) with ZPA was to onboard consultants and it was very successful. We quickly brought all of our consultants onto the platform and we went into full production in 2016, going live in April, the same date that Zscaler officially launched the product. That was when it dawned on me just how powerful this solution was, and we could really do a lot with this technology.

Secure access to engine applications in large ships

The next use case was to start looking at protecting our engines deployed in all of our seagoing vessels. There were only certain people that should be allowed access to the control systems and monitoring software on those vessels so we deployed ZPA.

One of the interesting things about ZPA is that it fulfills my vision of the black cloud. Basically, ZPA acts as a broker for connections. The client software does not know the IP address of the end system. A request is sent and if the requester is properly identified and authorized to get access to the application—or, in this case, the software running on the engine management platform—ZPA initiates the session. It’s like the call-back setting on modems back in the day. The whole platform is based on DNS, so you essentially extract the whole network from the equation. Before ZPA, we were assigning a class-C network space to each engine on every ship. With ZPA, we basically created a namespace routing in between us and the customer. This allowed us to monitor hundreds of ships without looking for a new IP address range.

Now we can secure each connection, which we can define per user per application. We have access control to each engine and we could add strong authentication through identity federation. That led to a thought—why not just replace all of our VPNs with ZPA for all users? After taking that step, it became quite apparent that the next step was to determine what our corporate wide area network was for and if we even needed a corporate network. Why not just put everyone on the internet and secure the access through some sort of software-defined perimeter?

Certainly, we are not there yet but I think within the next few years we will be. Look at WannaCry and NotPetya. Making the corporate campus one big open network is a mistake. In the past, if users wanted access to unsanctioned things we could

not support, we just told them no. Now we tell them if you want access to those applications, you have to go through the Zscaler fabric.

We're starting to migrate applications to AWS, and we have to deploy connectors up there, so we'll get connectivity for people to access them. I think of it as the company making its own black cloud. I don't care where the user is or what device they are on. I don't care whether you are at the office or at home. I just need you to get to the application. If you go through this secure fabric, I know who you are and I know that you actually should have access to this app.

This is the top priority model I have been creating for the company. It is a complete shift in thinking and has taken a couple of years to even solidify it in my head.

Securing the Internet of Things

The biggest problem with IoT is that these devices are generally not patched. They are not complying with standards. They are a security risk. What we are doing is putting this secure fabric between the people who need to access them and the IoT devices themselves.

To accomplish this, we found we needed to create a DNS naming structure. Now our policy is set by DNS names, not IP addresses. I can have an A Record for a device and several different CNAMES, and I can apply policy based on these. The DNS becomes my policy catalog and manager. There is still a lot of thinking we have to do about what this all means.

Better security against ransomware

I remember my management coming to talk to me after NotPetya did so much damage to Maersk. Management was rightfully very concerned. I just looked at them and said, "We're OK. Everything is closed. Every client is closed. We closed the firewalls to everything. The only way you can get to one of our engines is through Zscaler, through this black cloud. So everything is black. The malware has nowhere to go."

"To be successful, you really need to sell this concept of cloud transformation—you need to evolve the organizational mindset."

Cloud security for integrating M&A

Think about how this fabric applies during M&A. We did one acquisition in Zurich and to onboard the new company, I just gave everyone the Zscaler client. As soon as they had Zscaler Internet Access (ZIA), they were at the same security level as we were. Then, when they got Zscaler Private Access (ZPA) they could access our private apps. The whole process took just two weeks.

Advice to infrastructure leaders

To be successful, you really need to sell this concept of cloud transformation—you need to evolve the organizational mindset. This technology is so innovative that you need the people inside your company onboard. I spent a huge amount of time internally evangelizing to my CSO, my management, and everyone on why this is different, and why this works. To further validate, I pointed to them why I was confident that we were protected, and was able to reassure them when they came down to me worried about NotPetya.

Because of this technology, I was able to call a halt to a big 802.1x project we had been working on for Network Access Control (NAC). NAC does nothing for me when I go home or on the road. On the contrary, it can authorize someone infected with NotPetya to get on the network and the next thing you know, everyone is infected.

What not to do

Don't allow people to build direct IP connectivity into their applications. I wish I had acted earlier to keep that from happening. Get your application developers onboard earlier in the project cycle so they understand the new architecture. ”

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US

REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.