infoblox

CASE STUDY

Port of Antwerp, the gateway to Europe, relies on Infoblox to keep shipping lanes open 24x7x365

SUMMARY – A UNIQUE HISTORY OF INNOVATION

Thanks to its location 80 kilometers inland from Belgium's coast on the North Sea, the Port of Antwerp offers the fastest and most sustainable connection for delivering goods deep into the European hinterland.

The 14th largest container shipping port in the world, Antwerp handles more than 231 million metric tons of freight per year and more than 14,000 sea trade ships, double the volumes it handled just 20 years ago.

Antwerp's central location within the Scheldt estuary, with easy access to Atlantic shipping lanes and north central Europe, made it a center of shipping activity as far back as the 12th century. From these historic beginnings, the Port of Antwerp has grown steadily through the centuries and now stands as one of the most technologically advanced port facilities today. Its vast digital infrastructure includes two onsite data centers and more than 170 kilometers in dark fiber connecting over 50 sites within the port and thousands of endpoints.

Infoblox has long been a key element in the port's networking fabric, supporting essential DNS, DHCP and IPAM (DDI) processes for more than a decade. The port's extensive digital infrastructure supports its duties as a port operator, regulator, landlord and community builder and has strategically positioned the organization to carry out its vision for the "Port of the Future."

Customer: *Port of Antwerp*
Industry: *Shipping / Transportation*
Location: *Antwerp, Belgium*

INITIATIVES:

- Maintain DDI for continuous operation
- Support a work-from-anywhere workforce
- Provide security for remote workers equal to on-premises security

OUTCOMES:

- Stronger security posture through optimized security stack
- Seamless transition to a distributed workforce
- Many years of excellent, reliable network performance with Infoblox

SOLUTIONS:

- Infoblox NIOS DDI
- BloxOne® Threat Defense
- Trinzic appliances

Port of Antwerp

THE CHALLENGE

Maintaining progress toward the port of the future

Transportation and shipping are at or near the top of nearly every list of the industries investing most in the Internet of Things. The Port of Antwerp is very much emblematic of that trend and has adopted many of the technologies and best practices that have shaped the early stages of the IoT. In recent years the port's IT team has, to the greatest extent possible, digitized core port operations around vessel traffic management. These efforts have driven steady and significant advancements in key metrics, to the point where Antwerp is now recognized around the world for its superior tonnage throughput.

Embracing technological innovations while keeping risks under control is a key business priority for Yannick Herrebaut, Cyber Resilience manager at the Port of Antwerp. He sees this progress as simply the beginning of a continuum that will bring expansion of digital innovation into virtually every facet of port operation—for example, by the usage of drones, autonomous ships and a digital twin. "Our Chief Digital and Information Officer has outlined a vision for the Port of the Future that emphasizes challenging the status quo, seeing opportunities instead of problems and using technology as a lever for a sustainable future. With our competencies, we want to connect the entire port community via different ecosystems," he explains. "Speaking of this path forward, our CEO has characterized our mission as 'We want to be a world port that reconciles people, economy and climate'."

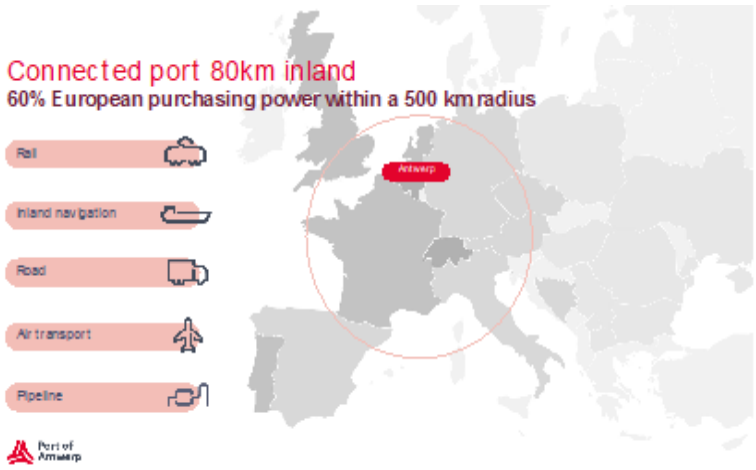

Figure 1. The Port of Antwerp's strategic location in the heart of Europe has propelled it to become Belgium's largest economic engine.

Herrebaut and the port's IT team believe that to really foster and enable this kind of innovation, they'll need to position the port as a digital playground for all kinds of solutions to be implemented and tested. To that end, the port's efforts to roll out 5G technology and various smart IoT devices—like drones, autonomous ships, smart lifebuoys and other types of digital equipment—constitute the Port of the Future's technological underpinning. Yet as Herrebaut points out, IoT devices and appliances have a spotty reputation of often lacking the kind of cyber security protections necessary for deployment in a critical environment such as the port.

"Top of mind for us is that these are newer technologies that have not always been made with security as an essential aspect but rather as an afterthought," he says. "We encourage proof-of-value cases to take place, but properly isolated from our core network. Very promising cases will be operationalized in time, but then they have to adhere to our security policies. The goal is to safeguard the confidentiality, integrity and availability of our core network, of which Infoblox is a critical element. By adding BloxOne Threat Defense to our cyber security stack, we can increase the security level of all our managed endpoints, including all the laptops of our employees who are working mostly from home these days."

THE SITUATION

Maintaining a secure work environment in the Ransomware Age

Since the beginning of the COVID pandemic, the team at the Port of Antwerp has been facing the same challenges that cyber security decision makers around the world have been grappling with: an increasingly mobile, work-from home staff and an alarming rise in malicious data breaches and ransomware. “We’re an operational company, so the real enemy, the worst-case scenario is downtime,” Herrebaut says. “So obviously we’re very much looking to avoid downtime induced by ransomware at all costs.”

According to the Infoblox Q2 2021 Cyber Threat Intelligence Report, the total damage associated with ransomware is estimated to be as high as $20 billion annually, with more than 10 percent of all cyber attacks now involving ransomware. Cyber security researchers attribute much of this increase to the massive expansion in attack surfaces brought about by COVID-induced work-from-anywhere practices. For the port, work from home has been somewhat restricted by the realities of the shipping industry, but it’s still been a significant trend.

In total, Antwerp maintains a workforce of around 1,600 employees: a thousand of them designated as knowledge workers, the other 600 being mechanical engineers, sailors, ship officers and boatmen. Still, up to 700 of the port’s employees worked from home during the height of the lockdown. For Herrebaut and his team, bolstering the port’s security posture given its dispersed workforce became an imperative, and BloxOne Threat Defense from Infoblox was a natural fit.

THE SOLUTION

BloxOne Threat Defense

BloxOne Threat Defense is a proven solution for improving security effectiveness and resiliency. It operates at the DNS level to uncover threats that other solutions do not and stops attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integration, it drives efficiencies in SecOps, boosts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts and lowers the total cost for cyber security. For organizations in the transportation sector—a prime target of ransomware criminals—BloxOne Threat Defense provides comprehensive protection against today’s evolving threats. It uniquely combines advanced analytics based on machine learning, highly accurate and aggregated threat intelligence and automation to detect and prevent a broad range of threats, including DGA families, data exfiltration, look-alike domain use, fast flux and many others.

“BloxOne Threat Defense was the ideal solution at the right time for the port,” explains Herrebaut. “As a cloud-based offering—and because we already had Infoblox NIOS in place—the implementation time was very short. The only thing we needed to do to get up and running was define policies and then deploy the agents to our endpoints. It was all very quickly put in place, which was a great advantage given the lockdown situation.”

THE RESULTS

Strong security posture, continuous uptime

When the full lockdown edicts came down in 2020, Herrebaut and the team felt that they were in good shape to protect their remote workers and, by extension, their core network assets and operations. An upgrade to a full-scale extended detection and response (EDR) solution was underway, the port had long maintained a secure VPN and all company laptops were equipped with anti-malware applications. “While we were confident we had strong security measures in place, we were also aware that EDR systems and anti-malware can still miss certain threats, which is why felt we needed an additional layer of security,” Herrebaut says. “What BloxOne Threat Defense offered was that we could provide the same level of protection to our remote users that they would have when working on-premises.”

BloxOne Threat Defense enabled the port to enact the same kind of content restrictions that were applicable on the corporate network—such as categories of sites that should not be visited on a company device or anything related to the dark web. The unique hybrid security of BloxOne Threat Defense uses the power of the cloud to detect a broad range of threats while tightly integrating with the on-premises ecosystem. BloxOne Threat Defense also enables the port team to optimize the performance and effectiveness of their existing security stack. “BloxOne Threat Defense, in addition to our existing security tools, makes it possible for our team to better identify and remediate threats. Now, we’re able to source information out of the Infoblox solution and get it into our SIEM solution, which will then point us in the right direction to uncover threats or to intervene to prevent negative things from happening.”

As the Port of Antwerp expands its relationship with Infoblox through its BloxOne Threat Defense implementation, the team’s appreciation for the reliability and flexibility of their original NIOS DDI solution continues to resonate. “If I look at how Infoblox contributes to the core success of the business by providing reliable, performant and secure IT services, I would say greatly,” explains Herrebaut. “Without robust, always-on DHCP, DNS and IPAM, a lot of our core services would stop working and we would have a lot of angry colleagues. With Infoblox, we’re able to keep the port running continuously, which keeps our customershappy and profitable.”

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).