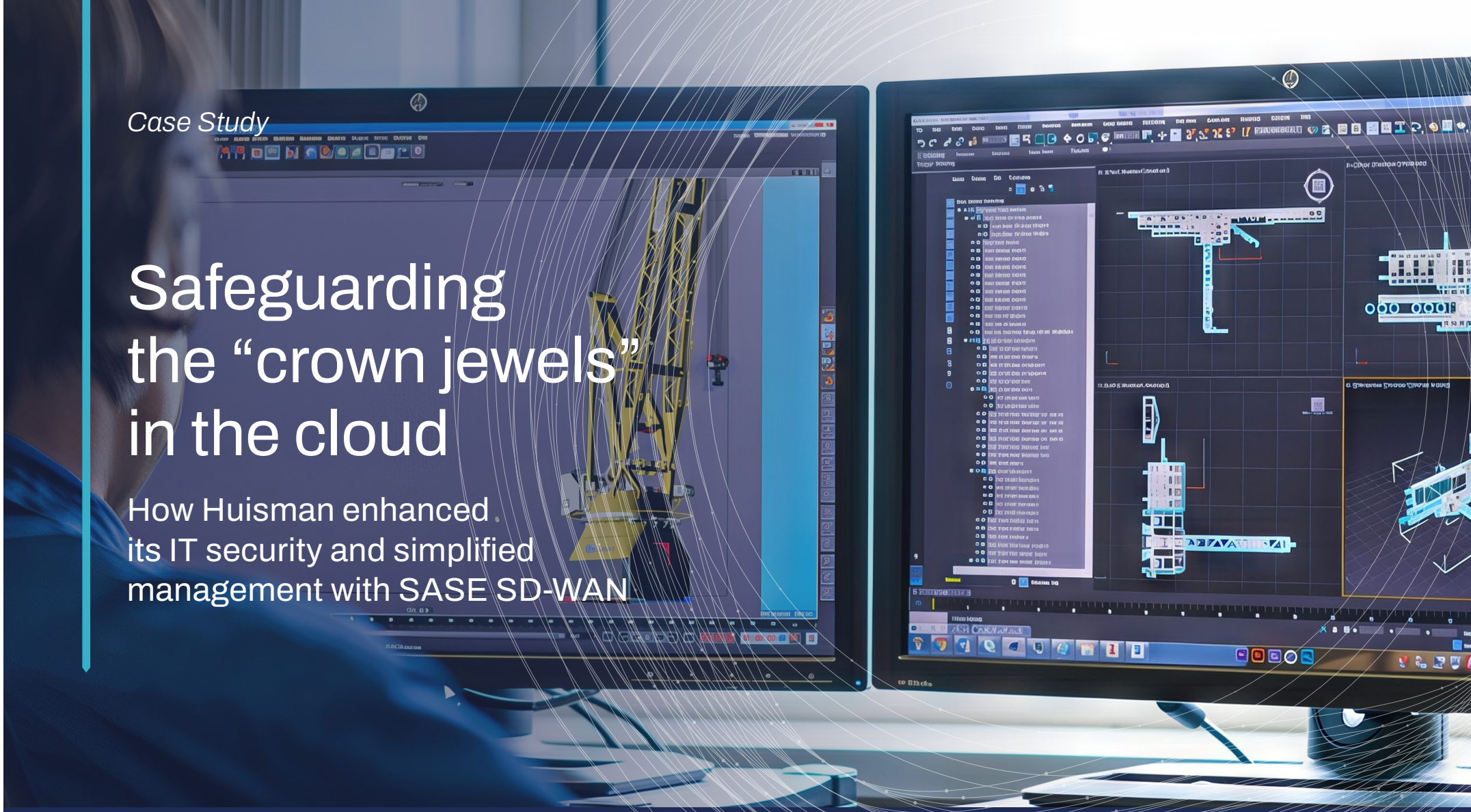
Case Study

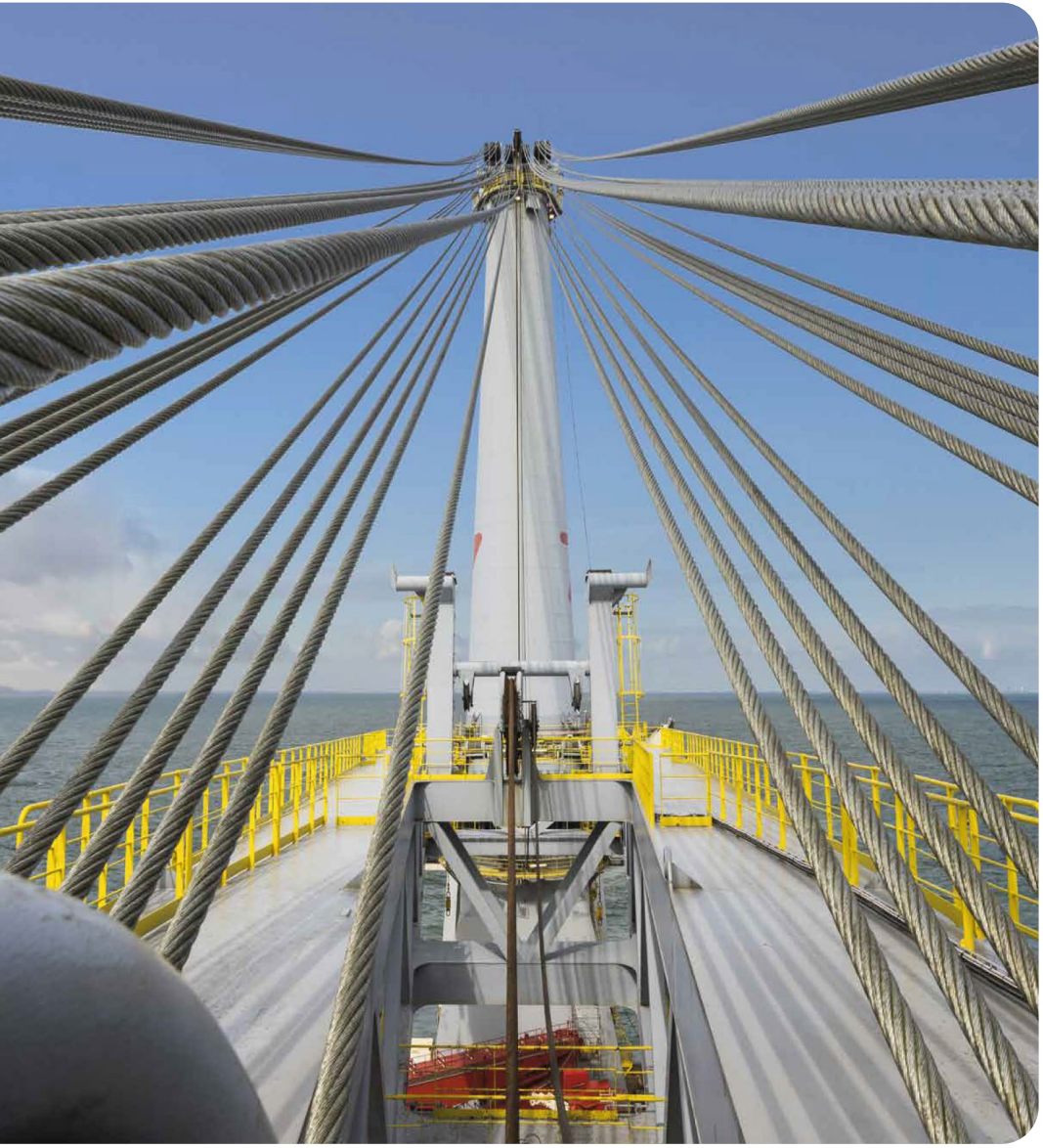
Safeguarding the “crown jewels” in the cloud

How Huisman enhanced its IT security and simplified management with SASE SD-WAN



IP knowledge

Huisman



Customer

Huisman

Industry

Manufacturing

Summary

Founded in 1929, Huisman designs, manufactures, and services heavy lifting and handling equipment for companies active in the renewable energy, oil and gas, port logistics, civil, and entertainment markets worldwide. Operating across four continents, Huisman counts on having a secure and reliable IT environment to support its global operations.

As a knowledge-driven organization, Huisman understood the collaborative benefits of adopting a cloud-first IT environment. At the same time, it was vital that any transition should treat IT security as the top priority.

Adopting a phased approach and a custom migration process, Huisman and IPknowledge implemented a full, organization-wide SASE SD-WAN deployment in less than four months – a major achievement given the project entailed both SASE SD-WAN security and LAN-side security.

Huisman now benefits from:

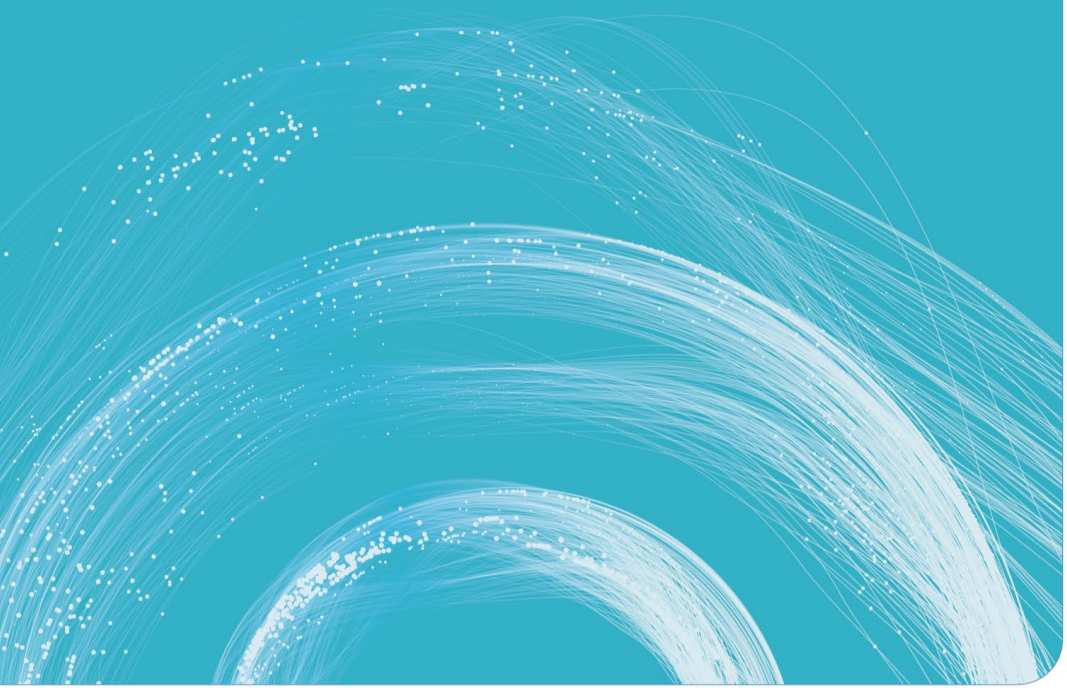
- Consistent data- and intellectual property-protection worldwide thanks to the Zero Trust Network Access (ZTNA)
- End-to-end visibility and 24/7 monitoring, helping the internal IT team shift from reactive firefighting to a more controlled and increasingly predictable way of working
- Regulatory compliance without compliance-related complexity
- Network uptime guarantee up to 99.99%
- Improved user experience with secure, seamless access to applications and resources from any location or device
- More efficient IT operations and cost transparency with a single point of contact through IPknowledge
- A resilient, high-performance IT environment that facilitates the business reliably and effortlessly

Check page 12 for the extended overview of the project deliverables.

This case study describes how IPknowledge worked with Huisman to deliver its goals. At Huisman's headquarters, in Rotterdam, the Netherlands, the IPknowledge team sat down with Arne van Vuuren, Global Manager IT Operations at Huisman. Having enjoyed a successful partnership with IPknowledge in a previous role, van Vuuren chose to work with the Managed Service Provider (MSP) again after joining Huisman. During the interview, he shared the IT challenges he encountered, his rationale for selecting a SASE SD-WAN solution, the implementation journey, and the value he sees in building a long-term partnership with IPknowledge.

Business demand

Safeguard the “crown jewels” in the cloud



Huisman operates in a globally distributed, innovation-driven ecosystem that covers seven countries and four continents. With its headquarters in the Netherlands, sales offices in Norway, the Czech Republic, the US and Singapore, large-scale production facilities in China and Brazil, plus agents in the US, UAE, and Japan, the organization relies on seamless collaboration across borders.

Intellectual property forms the core of this collaboration. Engineering designs, manufacturing expertise, and proprietary processes are the basis of the organization’s competitive advantage and must be protected. Always. As Huisman has evolved to a cloud-first environment, these assets have come to reside in platforms such as Microsoft SharePoint, Microsoft Azure, and other enterprise applications. They are accessed daily by employees worldwide and frequently shared across teams, locations, and partners.

This complex context created a clear business demand for the move to a cloud-first solution: How would Huisman protect its “crown jewels” in a cloud-first, globally distributed environment without putting a brake on collaboration or slowing innovation?

“When I spoke with our CEO, he was very clear about his concerns around intellectual property and that protecting it needed to be my focus.”

Arne van Vuuren, Global Manager IT Operations at Huisman, was in charge of developing an IT strategy to improve security around the organization’s intellectual property.

IT challenge

Securing data while ensuring regulatory compliance

Van Vuuren immediately saw that translating the business's security demands into an effective IT strategy would require a fundamental shift in how the organization approaches security. Security could no longer be static or tied to a single network, location, or device.

Instead, it would have to follow data and user behavior dynamically across applications, systems, and locations. "Just as financial experts track how money flows through an organization, IT professionals must be able to track, control, and protect data anytime, anywhere," he explains. This dynamic security comprised three major requirements:

- Access control across IT environments: Huisman would need stronger, more granular control over access to sensitive data as it moved across cloud platforms, applications, locations, and devices, without relying on implicit network trust.
- Complete visibility and continuous monitoring: By itself, securing data in transit was insufficient. Instead, data protection would have to extend to user behavior and interactions. This would require complete network visibility, continuous monitoring, and early detection of unusual or risky activity.
- Regulatory compliance across borders: Any solution would need to comply with institutional cybersecurity policies, including the EU regulations such as NIS2 and local regulations like China's cybersecurity law, without adding complexity.

Yet Huisman's existing network architecture was not designed to meet these requirements.

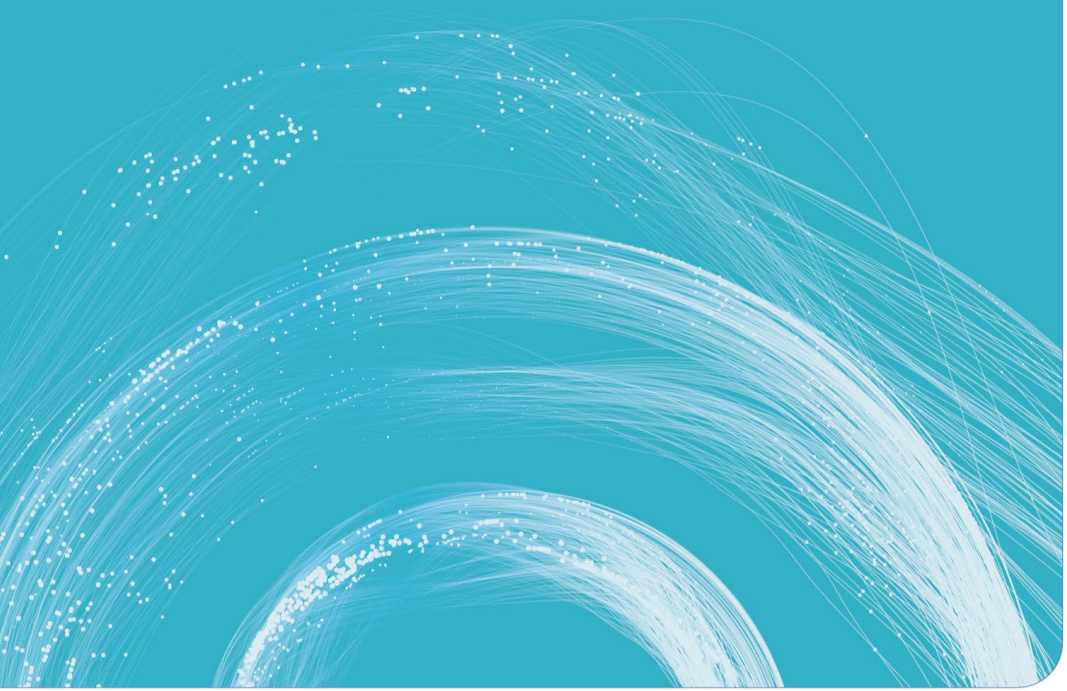
First, the organization relied on a traditional MPLS-based network that was expensive, difficult to scale, and made inefficient use of the available bandwidth. It also offered limited insight into application performance or how data moved across the network, making securing traffic both complex and costly.

The second issue was that Huisman's on-premises datacenter model was not up to the task of supporting a cloud-first strategy. The organization's infrastructure hadn't been built to support cloud-native applications or modern traffic patterns, turning the network into a bottleneck rather than an enabler of digital transformation.

And then there was the legacy Layer 4 firewall. This made security decisions based solely on IP addresses and ports, with no consideration of user identity, device posture, and application context. The static rule model was difficult to manage in cloud-based environments, limiting both visibility and control and constraining Huisman's ability to secure a dynamic IT environment.

Taken together, Huisman clearly needed a fundamentally new approach to networking and security.

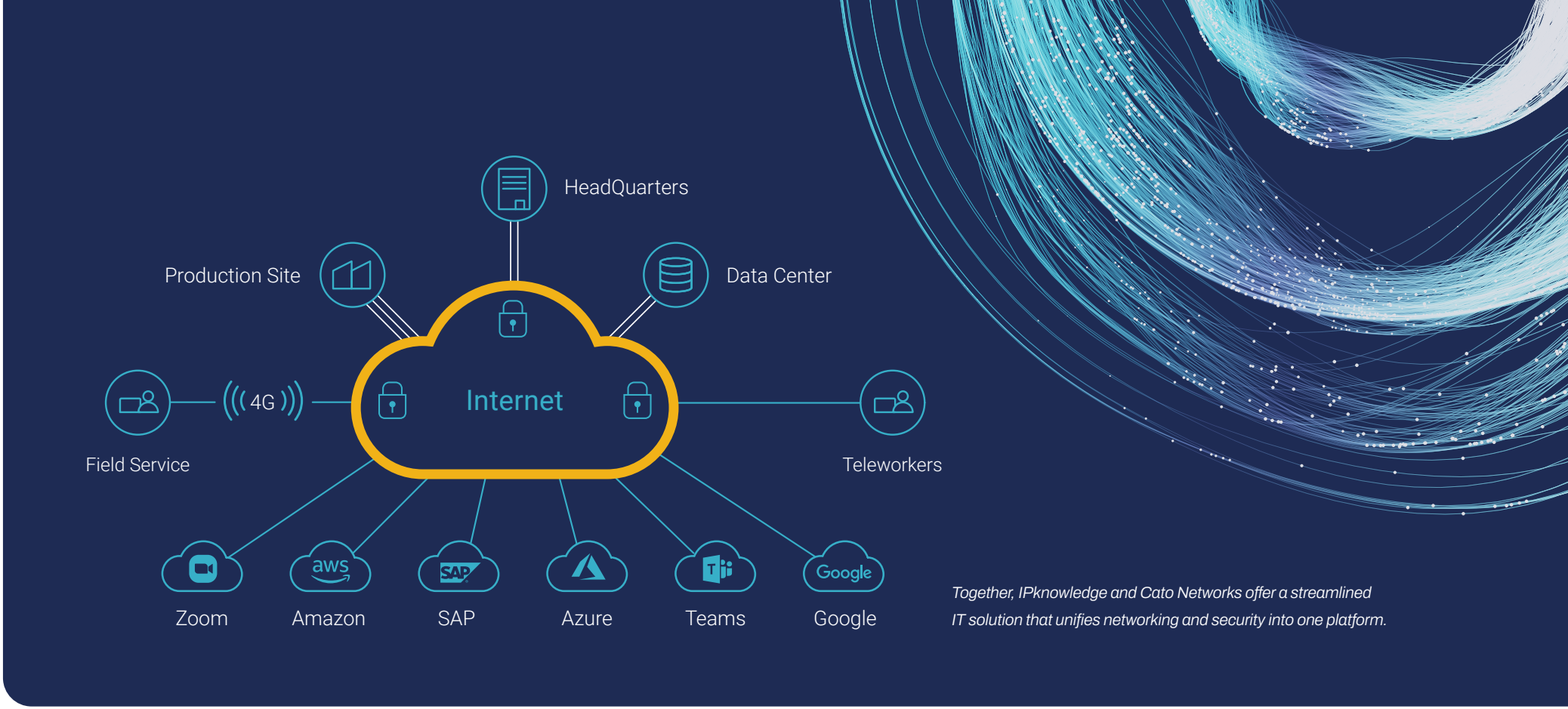
Cutting through the noise to find the right solution



For Arne van Vuuren, switching to a SASE SD-WAN solution was the obvious way to align Huisman's network architecture with a cloud-first strategy. Having previously implemented Cato Networks' SASE SD-WAN in partnership with IPknowledge, he felt confident that the same model would also deliver strong results at Huisman.

Several years ago, van Vuuren had been skeptical of SASE. "Most vendors promised a comprehensive security solution that is, in reality, a collection of disconnected components. Based on my experience, such fragmentation often introduces integration risks and operational challenges, especially in global environments," he explains.

For van Vuuren, the standout differentiator of Cato's SASE solution was its genuinely integrated design. "Networking and security are delivered as a single, unified platform rather than a collection of bits and pieces," he notes. "With a single click, I can have a complete view of WAN security. Cato gives me one unified solution."



Together, IPknowledge and Cato Networks offer a streamlined IT solution that unifies networking and security into one platform.

The Zero Trust component was another decisive factor. Cato goes beyond protecting data in transit to control access based on identity, application, and context. There is clear end-to-end visibility, from user to application. This aligned with van Vuuren's view that security must be end-to-end by design, covering both data protection and user interaction.

Cato's simplification of regulatory compliance further reinforced the decision. New regulations like NIS2 ultimately map back to established frameworks like NIST. Cato's SASE architecture supports these controls by design, making compliance a built-in outcome rather than an additional operational burden.

Equally important was selecting the right implementation partner. Van Vuuren had worked with IPknowledge in the past and trusted its ability to translate network architecture into operational reality.

IPknowledge stood out for two reasons: deep expertise and operational simplicity.

On the one hand, IPknowledge possesses exceptional expertise in Cato Networks and delivering reliable connectivity in challenging internet environments. This specialization is critical to meeting Huisman's uptime requirements. To deliver true redundancy and consistent throughput, IPknowledge recommended that Huisman have at least two independent internet access lines per site, configured in an active-active setup.

"Cato is continuously introducing new features, and IPknowledge has the deep expertise and pragmatic approach to rapidly adopt and deploy those capabilities, ensuring innovation can be implemented quickly and reliably."

For example, at Huisman's site in Shanghai, IPknowledge proposed one line from China Unicom and a second line from China Telecom – two separate local telecom operators with independent networks. If one connection fails, traffic automatically continues over the other, ensuring continuity without downtime. In addition, IPknowledge commits up to a 99.99% SLA (Service Level Agreement) site availability.

On the other hand, IPknowledge removes Huisman's operational burden of managing multiple local Internet Service Providers (ISPs) across regions, each with their own contract terms, local languages, and billing practices such as invoicing in different currencies. With established relationships across 500+ ISPs in more than 100 countries, IPknowledge relies not on third-party intermediaries, but directly sources connectivity from local telecom operators. This gives Huisman faster response times and greater control when issues occur.

Together, Cato's integrated SASE platform and IPknowledge's proven ability to execute to plan would provide Huisman with a secure, scalable, and manageable solution.

Together, IPknowledge and Cato Networks offer a streamlined IT solution that unifies networking and security into one platform.

A phased transition

From China pilot to global rollout

IPknowledge developed a phased approach to help Huisman transition to the new network architecture. As the organization's management and IT teams both needed hands-on experience with Cato's SASE SD-WAN, it was decided that a real-world pilot deployment was essential before migrating all the global sites.

China was chosen as the pilot. Due to the Great Firewall of China, the country presents one of the most challenging environments for secure and reliable connectivity. An ideal proving ground, in other words.

The positives were immediate. "For the first time, our staff in China experienced fast and stable access to Microsoft 365, reliable connectivity to Microsoft Azure, and improved performance across other enterprise applications," as Arne van Vuuren puts it. For Huisman, the successful China pilot gave it the confidence to roll out the Cato solution across its global operations.

The full migration was inherently complex. First and foremost, the migration had to be completed without disrupting daily operations: as a manufacturer of heavy cranes and lifting equipment, any interruption to factory systems or end users would directly impact productivity and could introduce safety risks. To reduce risk and disruption, Huisman decided to keep its existing security rules rather than redesign them from scratch. However, these rules had to be carefully converted from the older Layer 4 firewall model (basic

controls like IP addresses, ports, and protocols) to a more advanced Layer 7/ next-generation firewall (NGFW) model (more advanced controls based on applications, users, and content). This required detailed preparation and extra time to ensure the new policy did in fact improve the level of security. Second, the project involved more than deploying SASE SD-WAN; it also included enhancing security across local LAN environments in local office and factory networks. The need to modernize the WAN while also upgrading LAN security increased the project scope and its technical complexity.

Based on the technical complexity of the project, IPknowledge developed a custom implementation plan based on its usual best practices and Huisman's strict requirement for non-disrupted operations. This allowed the reduction of the risks they faced while ensuring the organization's daily business continuity.

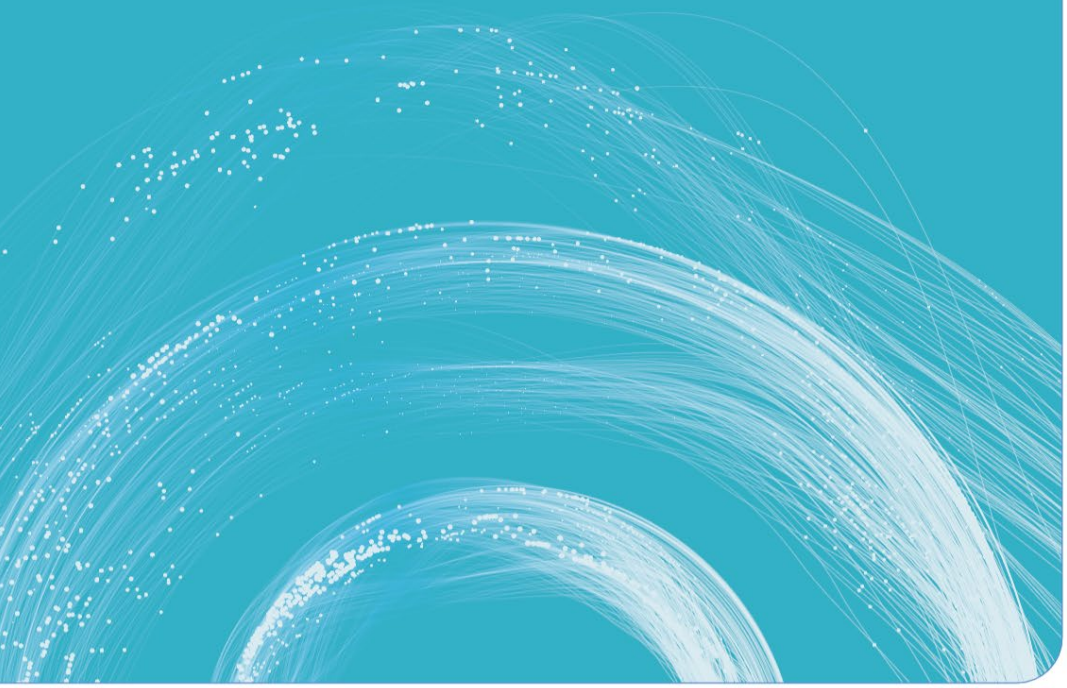
In line with this risk-averse approach, IPknowledge invested additional time in upfront preparation. IPknowledge engineers worked across multiple time zones in Europe, the Americas, and Asia to provide continuous support and a rapid response if issues arose.

The result was that in less than four months, Huisman successfully migrated all its sites across seven countries to the new network architecture, with zero disruption to end users. Existing LAN environments were preserved, while legacy firewalls were replaced with two compact Cato firewall devices per site to provide redundancy and maintain high availability.

For van Vuuren, the transition was fast, controlled, and executed without compromising business continuity. The outcome demonstrates how a phased, risk-aware approach, combined with global coordination and disciplined execution, can enable enterprise-wide transformation with confidence.

Key outcomes

from firefighting to control and predictability



Today, in addition to improving the way Huisman collaborates, the transition has introduced a fundamental change in the way its IT team operates. Despite having only two network engineers in-house, the organization now has far greater control and visibility across its global environment. The reactive firefighting of the past has been replaced with a controlled and increasingly predictable way of working.

This increased control is the result of moving security and access decisions from the network layer to the application layer. Zero Trust Network Access (ZTNA) has replaced implicit trust with explicit approval by granting access based on user identity, the specific application, and the relevant security context, enabling consistent, policy-driven enforcement. Meanwhile, because Cato's SASE SD-WAN is built natively around a Layer 7 firewall, application-aware security is designed into the platform. Replacing Layer 4 firewall's IP- and port-based controls with application-level policies makes it easier to understand traffic movements across cloud and remote environments. This reduces exceptions, guesswork, and the need for manual interventions.

Centralized management and real-time visibility have further turned control into predictability. Through a single interface, Cato provides Huisman with a real-time, global view of end-user behavior, network performance, and traffic.

“It’s a very successful project that has delivered awesome, awesome results.”

As van Vuuren notes, the end-user monitoring makes it easy to pinpoint where issues occur. “Whether a problem originates in the underlay network, along the routing path, or at a user’s home connection, we can identify it very quickly.” This consistent insight reveals recurring patterns such as latency or unstable last-mile connections, allowing issues to be addressed before users are affected.

Predictability also enables more effective user support, even when problems lie outside the corporate infrastructure. “Sometimes, the issue is with a home ISP (Internet Service Provider),” says van Vuuren. “Even though it’s not our responsibility to manage it, we can clearly identify the root cause and guide users on how to resolve it by, for example, making a call to the ISP to fix it.”

At the same time, centrally enforced security policies and unified visibility have simplified compliance with regulatory frameworks such as NIS2 and internal controls like CIS, which can now be measured and monitored more easily.

For van Vuuren, IT success is measured not just by technical metrics but also business impact. “IT should facilitate business like water from the tap or power from a socket. If my CFO or directors don’t notice any end-user disruption, then I know I’ve done a good job.”

Together, these results delivered what mattered most: high availability, stronger security, regulatory compliance, and an IT environment that facilitates the business.

Reflection

Outsourcing to a trusted team for business goals

With decades of experience across large enterprises, multiple industries, and in different roles, including IT leadership, company ownership, and freelance work, Arne van Vuuren has a clear perspective on what effective IT truly requires. For him, IT goes beyond technology; it starts with understanding how the business operates, how teams collaborate, how resources are deployed, and how realities and limitations impact day-to-day operations.

Van Vuuren's conclusion is that building and maintaining deep network expertise in-house is both time-consuming and difficult to scale. "Developing a strong network team takes years, and sustaining that expertise requires ongoing training and investment, often at the expense of speed and efficiency," he says.

For these reasons, van Vuuren views outsourcing to a skilled and reliable partner as the most effective way to optimize business outcomes. "Working with IPknowledge has given Huisman access to an agile team with deep network expertise, allowing us to adapt more quickly to new technologies," he comments.

Equally important is the way IPknowledge worked alongside Huisman's IT team. Clear communication, open discussions, and close collaboration ensures that complex challenges could always be addressed constructively and resolved together. "They are my single external point of contact for managing the entire network, from deployment and monitoring to invoicing," van Vuuren states.

For van Vuuren, IPknowledge is a trusted partner behind the entire foundation of Huisman's global network. "We are still moving toward the cloud, but that only works with very stable connectivity. Delivering a robust, reliable network worldwide without issues is how I would best describe the added value of our collaboration," he concludes.

"If I were to describe our collaboration with a song, it would be the Beatles' *We Can Work It Out*. We can always work it out together, regardless of pressure or difficulty."

About Huisman

Huisman is a global industrial machinery manufacturing company founded in 1929. It designs, manufactures, and services heavy lifting and handling equipment for the world's leading companies in the markets of renewable energy, oil and gas, port logistics, civil, and entertainment.

Headquartered in Schiedam, the Netherlands, Huisman operates worldwide with production sites and sales, service, and engineering offices across the globe. The company employs approximately 2,500 professionals in seven countries. Huisman's product portfolio includes cranes, offshore wind tools, pipelay and drilling equipment, as well as specialized custom solutions.

All relevant images in this case study are courtesy of Huisman.

Faces behind IPknowledge

"I've known Arne for years from another project. As an IT leader, he sets the bar exceptionally high; and as a like-minded person, I think that's exactly what makes working with him so valuable. Arne cares deeply about having full control of IT and being able to verify it at any moment. It's not always easy, but that pressure pushes us to improve every single day. In the end, it's not about being perfect, but striving for perfection, one step at a time."

Steven de Graaf

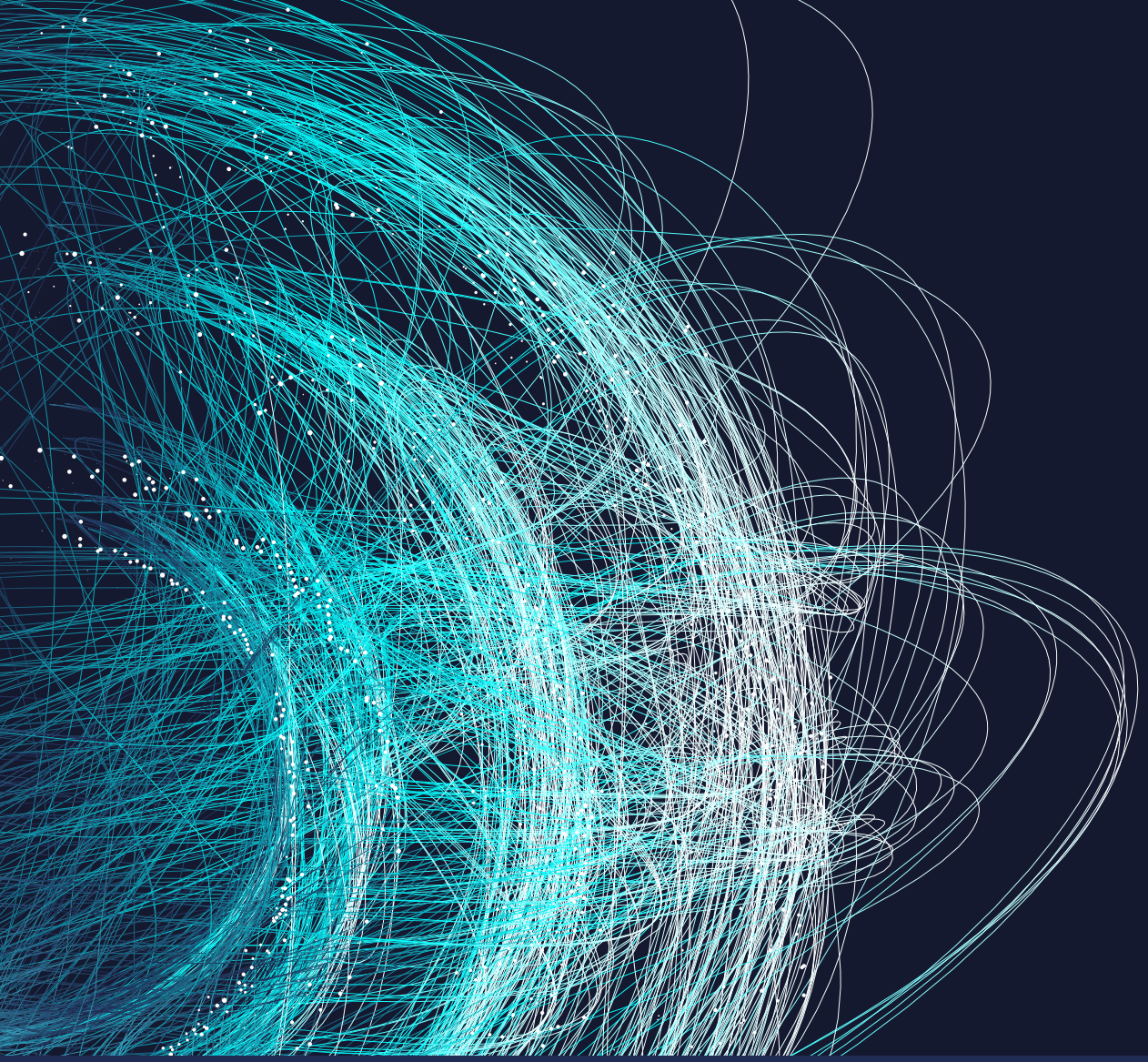
Chief Executive Officer

“Huisman sets a high bar and keeps us on our toes. Supporting complex cloud transitions and production sites in challenging regions such as China demands constant attention, deep expertise, and unwavering commitment to our promises.”

Rob de Vuijst
Head of Operations

“For me, every journey with a customer is a truly unique story. It begins with understanding who they are, identifying their challenges and needs and delivering solution. Huisman is a powerful example of a customer who not only challenges us, but helps us grow and elevate our service. Through demanding questions, high standards, and honest feedback, they push us to continuously improve and perform at our best.”

Tatyana Bilotserkovska
Customer Success Manager



IPknowledge B.V. (HQ)
H.J.E. Wenckebachweg 123
1096 AM Amsterdam
The Netherlands
T +31 88 08 82 600

IPknowledge Alps AG
Brown Boveri Platz 3b
5400 Baden
Switzerland
T +41 56 511 27 90

IPknowledge.net

EMEA MSP of the Year 2024 CATO

EMEA PARTNER of the Year 2025 CATO

IPknowledge