

CASE STUDY

Truma Sees Clear Roads Ahead with Enhanced Network Visibility and Protection from Infoblox



OVERVIEW

For more than 75 years, **Truma Gerätetechnik** has been the leading specialist for RV and caravan accessories and equipment.

From heating and cooling systems to water heaters and energy solutions, the German company provides top-quality products to support the active outdoor lifestyles of RV enthusiasts around the world. This customer focus has long been a theme throughout the company's history. Even Truma employees, who are avid campers themselves, regularly use the very same products they create.

Headquartered in Putzbruun, Germany, the company has subsidiaries in the U.S., the U.K., and Sweden, with more on the way. Through its robust network of dealerships and service partners spanning over 30 countries, Truma not only offers innovative products but also delivers professional advice and readily available replacement parts, building trust and fostering long-term relationships with customers around the globe.

“With Infoblox, we can close the gap between security and network operations. With one system, we have a view of both worlds.”

Andreas Schmidt,
IT System Engineer,
Truma Gerätetechnik



THE SITUATION

Agile Business Operations Require an Agile Network

Truma's success depends on its ability to fulfill evolving customer needs, from traditional fuel-based units to newer, environmentally friendly technologies, such as electric and solar-powered alternatives. Maintaining that agility requires a network that is adaptable, fast, reliable, and secure. This network must also align with Truma's cloud-first strategy, which enables IT to deploy services in the ways that make the most sense. "If a system is better running in the cloud, we take it to the cloud. If it's better on-premises, we take it on-premises," says Andreas Schmidt, IT System Engineer for Truma.

THE CHALLENGE

Disparate Networking Technologies and Risk Exposure

In recent years, Truma's network has expanded through mergers and acquisitions, adding new subsidiaries and preparing for more in the near future. Running network operations seamlessly across all these locations had become increasingly troublesome, largely due to the diverse legacy infrastructure that newly acquired subsidiaries had in place for critical network services—DNS, DHCP, and IP address management (DDI).

Part of Truma's challenge stemmed from its IT team's limited knowledge of how best to manage DDI across such varied networking environments. "Our network strategy was developed to be scalable," Schmidt says. "We don't have endless people working in IT, and we don't want to spend time on basic tasks, like bringing up a new DNS zone."

And yet, basic tasks like absorbing a new location into the network did indeed take time, many weeks in most cases. Truma's existing DDI implementations also lacked the flexibility required to meet the company's cloud strategy.

The company ran most of its DNS traffic through Microsoft DNS, Active Directory, and various domain controllers. A key challenge was the considerable time and effort required to manage both internal and external DNS through Microsoft. IT staff had to ensure certain internal network resources were accessible only through internal DNS zones while maintaining uninterrupted traffic for public zones. To achieve this, Schmidt and his colleagues had to manually enter terminal commands on Microsoft servers and domain controllers at each location, a time-draining undertaking. "There was no real way to streamline this; there was no dashboard to manage it," Schmidt says.

Schmidt and his team faced the same difficulties when it came to updating changes in DNS records and IP address allocations, a constant issue since DDI data requires frequent updates. The process of updating disparate DDI systems consumed two to three hours a week. It also created unacceptable delays of up to half an hour when employees and customers were unable to access vital network assets while updates were being synchronized in the Microsoft DNS system.

Customer: Truma Gerätetechnik
Industry: Electronics
Location: Putzbrunn, Germany
Partner: 4N IT-Solutions

OBJECTIVES:

- Reduce network disruptions and outages caused by inefficient, legacy implementations
- Improve visibility into network assets and resources to avoid complications
- Increase cloud agility across networking and security

RESULTS:

- Reduction in time from weeks to hours when absorbing infrastructure from new subsidiary locations
- Simplified DDI operations with a consolidated solution and centralized management portal
- Faster problem resolution with contextualized visibility across networking and security

PRODUCTS:

- NIOS DDI
- Infoblox Threat Defense

Moreover, the Active Directory structure of Truma's Microsoft deployment made it very challenging to see how networking resources across the company's distributed infrastructure were connected. This lack of visibility resulted in unplanned downtime. In one notable example, IT, unaware that a DNS entry was set up for a vital service needed by a production line, decommissioned it, deeming it unnecessary. This oversight resulted in a four-hour work stoppage while Schmidt's IT team addressed the problem. For Schmidt, it was a worst-case scenario. "Production was standing still because of an IT issue."

In addition to unplanned downtime, Schmidt and his managers also had to contend with ongoing security threats posed by data exfiltration and ransomware, both of which rely on DNS pathways. Truma had no comprehensive means for effectively stopping these and other threats.

THE SOLUTION

Trusted Expertise and Proven Capabilities

Over time, Schmidt and his co-workers understood that they needed a more efficient way to manage critical network services and to do so in far less time while extending proactive security seamlessly to all users in all locations.

In choosing the right solution, Truma's IT staff also knew they would need ongoing help in improving their know-how of DDI best practices and DNS-based security. "It was important that we implement new technology with strong partners who understand the technology so that we don't need to do so much research on our own," Schmidt says.

With the expertise of Infoblox and partner [4N IT-Solutions](#), Truma seamlessly transitioned its DDI functionality from Microsoft systems to [Infoblox NIOS](#). This migration, leveraging the industry's most deployed DDI solution, was remarkably smoother and more efficient than Schmidt had anticipated. "The implementation was very well planned, worked very smoothly. Honestly, it was one of the best migrations I have seen in my entire career."

Truma's NIOS solution features a redundant setup at its headquarters in Putzbrunn, complemented by additional servers in each of Truma's four subsidiaries. All servers are connected through the Infoblox Grid, which ensures continuous availability of DDI services in the event that a server at any location goes offline.

With Infoblox, Truma gains complete DDI control and visibility over all networking assets, whether on-premises or in hybrid and multi-cloud environments. The solution enables the company's IT staff to manage internal and external DNS across all locations from a single console. The time it takes to update DDI systems has been reduced from a few hours per week down to just minutes. In addition, all updates are replicated almost instantaneously, eliminating the delays that had adversely affected customer service.

For security, Truma relies on [Infoblox Threat Defense](#), the cloud-native solution that protects all users across the enterprise, whether in the office, at home, or roaming. "Every DNS query runs through Infoblox Threat Defense. It's a centralized DNS system," Schmidt says. "Every part of our business, every device, VPN connection, elevator, or production line—everything is secured by Infoblox Threat Defense."

The solution gives Truma consolidated visibility into all devices on the network. In addition, it provides secure DNS resolution and automatically blocks devices from connecting to known malicious destinations. Using AI and machine-learning behavioral threat detection, it also flags zero-day threats in DNS traffic weeks and even months before an attack can become active.

THE RESULT

Simplified Management, Resiliency, and Comprehensive Protection

Simplifying and streamlining DDI functionality with Infoblox NIOS delivered immediate benefits for Truma. For starters, Schmidt and his team were able to eliminate the painstaking work of administering domain controllers across the infrastructure. “Before, we had to go to different portals, to different consoles,” Schmidt says. He and his team now have a single point of truth and a single portal for all network services. “The change to Infoblox improves our confidence in our network. These services are now in very good hands.”

Simplified DDI management also means that Truma’s IT team can now dynamically configure DDI on the fly as its operations grow, on-premises and in the cloud, while avoiding the technology snarls that hindered it in the past. “With Infoblox NIOS, it’s much easier to spin up new subsidiaries, especially if they are in a cloud system,” Schmidt says. “Adding new locations has gone from weeks to just hours or days.”

Truma’s network is now much faster and more resilient, thanks in part to the Infoblox Grid with its automated failover features. Enhanced asset visibility also plays a key role in avoiding the unplanned downtime Truma experienced previously. With Infoblox, Schmidt and his colleagues can see exactly which machines run on which servers. “It is much safer to make changes in production. We no longer have to guess whether a change might interfere with other systems. That is a big improvement in the trust and stability of the system.”

Infoblox provides the company with granular details about each asset all in one central location, such as MAC and IP address, operating system, user information, location, and asset history, facilitating rapid identification and resolution of client issues.

The same asset visibility that helps Truma’s management of critical network services also significantly accelerates its response to security events when they occur. “We see everything on the Infoblox system: which client is using which address, what it’s affecting, what it’s communicating with,” Schmidt notes. The IT team can now quickly pinpoint, isolate, and remediate compromised machines safely without affecting service to other devices and systems.

With Infoblox Threat Defense, Truma achieved comprehensive protection against data exfiltration and ransomware. And should something happen, the forensic tools within the Infoblox solution enable IT to quickly determine the cause and initiate the correct response in a fraction of the time it once took.

In small IT organizations like Truma’s, everyone is responsible for both networking and security. Infoblox makes both jobs easier. “With Infoblox, we can close the gap between security and network operations. With one system, we have a view of both worlds,” Schmidt says. He can easily move between dashboard views of NIOS DDI and Infoblox Threat Defense, allowing him to view rich networking insights in context with security events, which enables his team to respond faster without consuming valuable time.

Looking forward, Schmidt believes that bringing networking and security together with Infoblox carries another important advantage—cloud enablement. “In our cloud strategy, Infoblox is included as an underlying service for every system we will implement, either in the cloud or on-premises.”

For Schmidt, there is one overarching Infoblox benefit that stands out—people across Truma no longer must think about how things work on the network. “They can focus on what they do to satisfy our customers. Infoblox works as a hidden champion in the background every day.”



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