NIBE Builds Cyber Resilience in Six Months With Illumio

Heating manufacturer reduces risk and improves IT agility with Illumio Zero Trust Segmentation

Business Goals

For manufacturers, maintaining operational uptime is critical. If they cannot build, ship, or invoice their goods, the potential losses can be catastrophic. NIBE recognized this and took proactive steps to boost its cyber resilience.

NIBE Group is a global organization that develops and manufactures a wide range of eco-friendly, energy-efficient solutions for indoor climate comfort, heating, and control. Comprised of over 140 independent companies and 20,000 employees across 30 countries, NIBE has a complex IT environment. Each company has its own set of applications and systems, all of which were migrated and now reside on the group network. However, understanding the interconnections between users, devices, and systems was a challenge. Without visibility and segmentation in place, a breach in one business could quickly lead to a compromise of the whole group.

“We needed to ensure that different companies within the group couldn’t access each other’s assets,” said Fredrik Olandersson, Network Administrator at NIBE. “At the same time, we also recognized the growing ransomware risk facing manufacturers and wanted to strengthen our defenses.”

Technology Challenge

With a sprawling IT environment, spanning production to the office and IT and OT, NIBE knew it needed to quickly regain control and visibility over traffic flows in its server network. The ultimate goal was limiting unauthorized access between companies – they identified least-privilege access and Zero Trust Segmentation (ZTS) as the solution.

But this was no easy feat. To strengthen resilience, NIBE wanted to segment to the most granular extent possible.
This meant not only delivering microsegmentation between the different companies within the group, but also applications and departments.

Industry: Manufacturing

Challenge: Reducing risk by understanding traffic flows and limiting server-to-server interactions

Solution: Illumio Core & Illumio Endpoint

Use cases: Environmental separation, asset mapping and visibility, IT/OT convergence, risk reduction

Benefits:

- **Comprehensive visibility of network communications**
  Understanding communication across environments enables NIBE to quickly identify and reduce risk.
- **Increased IT agility**
  Real-time application insights from Illumio support troubleshooting, enabling NIBE to resolve issues faster.
- **Strengthened cyber resilience**
  Separating the network into segments gives NIBE confidence that it can quickly contain inevitable breaches.
- **Rapid time to value**
  Illumio shows the impact of new policies before enforcing them, so NIBE can move quickly without the risk of breaking applications.

> We have a huge environment made up of IT, OT, and endpoint devices. We also have a huge network of external contractors who regularly access our environment using devices outside of our control, so we need continued confidence that they can only access the systems and applications that are absolutely necessary.
>
> Frederik Olandersson
> Network Administrator, NIBE

How Illumio Helped

NIBE quickly realized that this level of segmentation would simply not be feasible with a traditional firewall-based approach. Enter Illumio Core.

With Illumio Core, NIBE now has complete visibility over the traffic flows within its server network – something not possible previously. Illumio Core illustrates network communications in an easy-to-understand map, enabling NIBE to quickly identify and block unnecessary traffic, reduce unauthorized access, and stop breaches spreading to critical assets.

Illumio Core also helps support teams with troubleshooting – support can now identify resolutions quicker and easier by seeing and understanding what applications are doing and the interdependencies between them.

"Illumio was simple to deploy, didn't require any big investments in hardware, and is really easy to manage. It's also a great choice if you want to get microsegmentation in place and add value quickly. We were in full enforcement of 90 to 95 percent of our estate within six months."

> We identified over 500 different applications that we wanted to segment, which would have been difficult to execute and would require a lot of manual work for our team using our existing firewalls. We would not have been able to get this granular level of segmentation and protection without Illumio.
>
> Fredrik Olandersson
> Network Administrator
> **NIBE**

Looking Forward

NIBE is now extending the benefits of ZTS to 6,000 endpoint devices for office workers with Illumio Endpoint. By leveraging existing rules already created in Illumio Core, the company can quickly limit and control access between user devices and specific servers or applications, providing another level of cyber resilience in a single platform.

As the group expands, NIBE is also looking to use Illumio to support the migration of new companies onto the hosting network.

"We can see how Illumio could be valuable prior to a migration because it provides an easy-to-understand view of all the traffic flows and different applications in advance."

Results and Benefits

NIBE continues to see benefits from implementing Illumio Zero Trust Segmentation including:

- **Deployment of ZTS at scale**: As the group continues to expand, NIBE can quickly segment new environments and enforce policies to keep assets and data safe.
- **Saving time and resources**: NIBE can now automatically block unnecessary connections — all without writing cumbersome firewall rules or touching the network.
- **Increased cyber confidence**: By gaining a holistic view of its server and endpoint environment, NIBE can more confidently respond to any downtime or cyberattacks.
- **Quick time to value**: Because Illumio was simple to deploy and allowed NIBE to move at their own pace, NIBE was able to reach nearly 100 per cent enforcement in six months.

About Illumio

illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.