How SWACRIT Secures Its Manufacturing and Simplifies IT Operations with Illumio

Securely powering growth and innovation

For SWACRIT, precision is everything. The Swiss company builds high-accuracy components and mechanical assemblies for sectors where mistakes aren't an option. Medical, aerospace, and semiconductors are just a few of the industries it serves.

As the company grew, so did its focus on security. Protecting customer data and its fast-moving operations became top priorities.

"Our biggest priority is securing our knowledge, especially our customers' sensitive data, so it's only accessible to authorized employees," said Daniel Hofer, the company's head of information technology security. "At the same time, we needed to be protected from cyberattacks inside and outside the organization."

With limited IT resources and bold growth plans, Hofer needed security tools that worked harder without creating more work for his team. Illumio delivered exactly that: stronger protection with less complexity.

SWACRIT systems

Solution
Illumio Segmentation

Industry
Manufacturing

Challenge
- Strengthen security across IT and operational environments
- Protect data
- Secure legacy systems
- Gain network visibility

Use Cases
- Asset mapping and visibility
- IT/OT convergence
- Critical asset protection

Location
Austria, with multiple production plants and office locations.

Results at a glance
- Legacy systems secured, extending equipment lifespan
- Daily firewall checks reduced to weekly reviews
- Instant visibility, making troubleshooting fast and simple

Beyond firewalls: A smarter way to segment

Like many in its industry, SWACRIT first looked at hardware firewalls. The approach was familiar, but it quickly proved too expensive and too complex for what the company needed.

"Most of the products I found were hardware firewalls," Hofer said. "But they didn't provide real segmentation."

What SWACRIT needed was visibility. The team wanted to see how systems communicated and control internal traffic at a more granular level. That was especially important for legacy machines still running Windows XP.

Some production machines cost up to €700,000. Illumio helped the team isolate and protect them — avoiding costly upgrades and boosting security.

Extending protection to OT with help from ROS\\TECH

The network segmentation couldn't stop at IT systems. SWACRIT also needed protection for its operational technology (OT) environment. It labeled unmanaged workloads such as manufacturing equipment and non-Windows devices. From there, it enforced strict communication controls — with no agents needed.

ROS\\TECH, a longtime Illumio partner, played a key role. Its expertise in Active Directory hardening and infrastructure security helped SWACRIT move quickly from planning to execution. Seeing the visibility and control Illumio offers sealed the decision.

"Illumio is the logical next step after Active Directory hardening," explains Rostek. "For me, permission and network segmentation are just a natural fit."

Fast deployment, flexible protection

With help from ROS\\TECH, SWACRIT deployed Illumio in just four full-day sessions. The rollout covered two production plants, three office locations, and a construction site.

The team followed a phased approach:

- First, core services
- Next, high-availability systems
- After that, office networks
- And finally, production environments

> "
> **The key deciding factor was ease of implementation and operation.** Agent deployment proved to be straightforward and efficient."
>
> **Robert Rostek**
> IT Security Architect,
> ROS\\TECH

ROS\\TECH was already familiar with SWACRIT's systems, which helped speed up deployment. Writing policy rules, for instance, was straightforward.

Illumio offered a safe rollout strategy that added confidence. Running in visibility-only mode allowed the team to see network traffic patterns without disrupting anything. Deploying agents was smooth and predictable.

Immediate results and ongoing operational gains

Within the first hour of going live, SWACRIT's IT team found a long-misconfigured NAT rule that had gone unnoticed for years.

Other surprises emerged, such as:

- Spotify was installed on several client machines
- Outdated monitoring agents were still communicating on the network
- A misconfigured firewall was trying to print to a server

The new visibility also revealed new ways to shrink the internal attack surface. SWACRIT quickly blocked unneeded client-to-client communication — a big step toward preventing lateral movement.

Thanks to Illumio Segmentation's label-based policy model, only approved traffic was allowed between clients. Everything else stayed blocked by default.

"

The traffic visualization capabilities have proven invaluable for understanding network communications."

Robert Rostek
IT Security Architect,
ROS\\TECH

Day-to-day simplicity for IT operations

Illumio didn't just improve security. It transformed daily operations. Before the deployment, Hofer checked firewall logs several times a day. Now, Illumio handles traffic enforcement automatically. Hofer checks it once a week, freeing time for more strategic IT projects.

ROS\\TECH saw longer-term benefits too. "Illumio's traffic visualization capabilities are invaluable," Rostek said. "We now have a clearer understanding of how systems communicate — whether it's between sites, across the DMZ, or inside our ERP ecosystem."

He says the combination of visibility, control, and operational efficiency is still paying dividends, keeping SWACRIT secure as it grows.

Benefits and results:

- **Stronger security with Zero Trust.** Isolating critical assets to prevent lateral movement.
- **Reduced IT workload.** Cutting down firewall rule management from daily to weekly.
- **Cost savings.** Avoiding unnecessary infrastructure investments, estimated to save a six-figure amount.
- **Improved visibility.** Real-time insight into network traffic, revealing hidden misconfigurations.
- **Fast deployment.** Fully implemented in four sessions across all SWACRIT sites.

About Illumio

⊠ illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.