

# Securing the World's Leading Provider of Industrial 3D Printing

## THE CHALLENGE:

With a great number of OT devices in their global technology centers, EOS needed to improve visibility into their OT environments. EOS's security team also needed to automate their asset inventory and gain complete visibility into their external remote connections. Additionally, EOS had to be compliant with their industry's regulation requirements for their industrial 3D printer systems & manufacturing technologies.

## THE OUTCOME:

EOS has real-time visibility into all their OT environments with ongoing monitoring of exposure to risks and predictive warnings, including visibility into their external remote network connections. EOS successfully automated its asset inventory and is continuously monitoring the threat detection of malicious activities within their production environments. They also comply with their industry's strict compliance regulations.

EOS provides responsible manufacturing solutions via industrial 3D printing technology. This is powered by its platform-driven digital value network of machines and a holistic portfolio of services, materials and processes. The company e.g. serves the aerospace, automotive, medical, and tooling industries.

-  Headquarters  
Krailling, Germany
-  Sector  
Additive Manufacturing
-  Industry  
Industrial 3D Printing
-  Production:  
Over 300 industrial 3D printer systems annually

## EVALUATING EOS'S INDUSTRIAL CYBER SECURITY CHALLENGES

After connecting their manufacturing production environments to the Internet and adopting different cloud services, new security risks emerged for EOS's OT networks. EOS's security team understood they needed improved visibility into their OT environments as they increased their awareness of cyber attacks in the manufacturing industry. This fast-tracked their management team to invest the proper amount of resources into improving EOS's overall OT security posture.

EOS's security team understood they needed to increase their visibility and management of OT assets and networks to improve the production and security of the company. Additionally, EOS's products are using many proprietary industrial protocols that are not mainstream, and most OT security vendors are not able to fully decode and translate these protocols into valuable data.

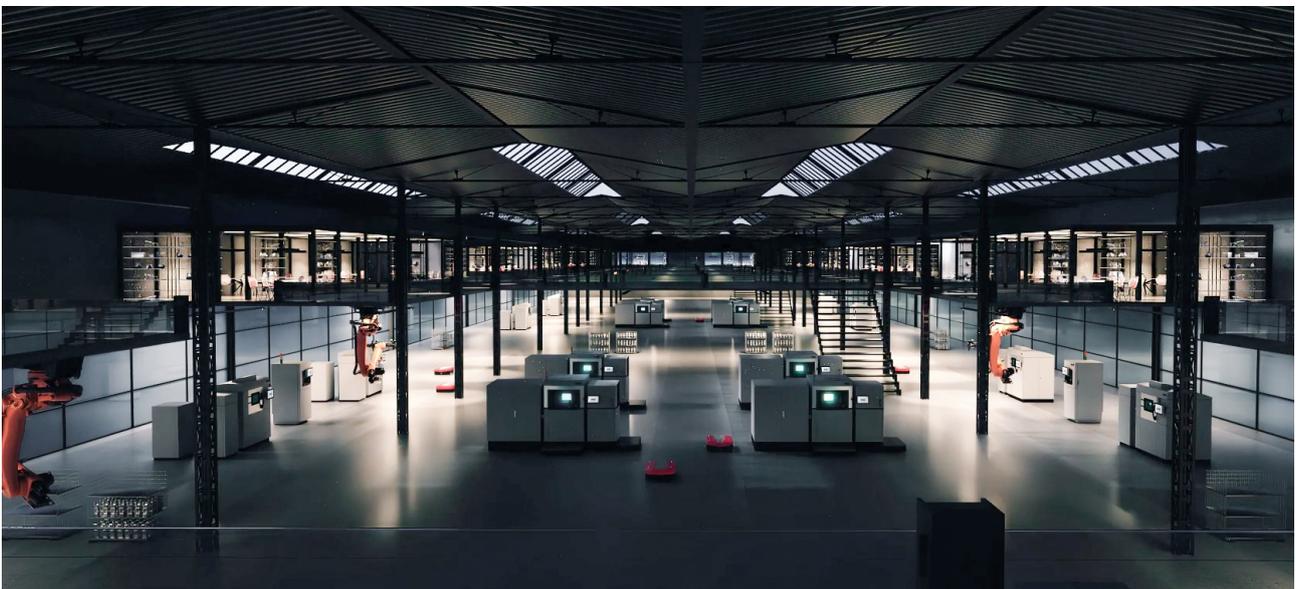
Additionally, EOS needed to monitor and manage the remote connections of their OT networks for suspicious behavior and anomalies to immediately understand if there were any intrusions or malicious activities in their networks. Finally, EOS was seeking a less complex process to become compliant with government and industry compliance regulations.

Due to the many OT security challenges and the awareness of a potential attack on their production sites, EOS's security team proactively searched for a solution that would provide them with complete visibility and security into their inter-connected OT environments.



*"It's quite difficult to find a security platform that can easily secure IT and OT environments properly, but with SCADAfence and their integration with Rapid7, it has allowed us to have complete visibility into our production environments all in one dashboard."*

**Wasim Darwiche**, Product and Operational Cyber Security Officer at EOS



## FINDING THE RIGHT SOLUTION

After evaluating several solutions and receiving many recommendations from their colleagues and analyst firms such as [Gartner](#), EOS's security team chose the [SCADAfence Platform](#) for their OT security needs. They feel the SCADAfence Platform provides them with the most accurate real-time OT asset visibility, continuous monitoring of their OT environments, the ability to manage their industrial compliance regulations and provides them with visibility into remote connections within their OT networks.

Additionally, EOS decided SCADAfence was the ideal solution for their integration needs as they were able to easily integrate SCADAfence [into the Rapid7 solution ecosystem](#), and have their IT and OT security management in one unified dashboard.

After deploying the SCADAfence Platform in their production environment, EOS immediately discovered all of the devices within their networks, and obtained real-time visibility into their OT environments, improving their compliance processes and securing their manufacturing sites. The SCADAfence Platform digitalized their entire asset inventory and reduced their risk from attacks on their OT networks. This has allowed EOS to be more efficient, productive and secure with their OT environments which has led to an increase in their production numbers.

In addition, the EOS security team now has interactive network maps that allow them to explore and get a better understanding of the remote connections between their OT assets and networks. The network maps and diagrams from the SCADAfence Platform allow EOS to improve its anomaly detection. The maps show which behaviors are happening on the network and if there are suspicious behaviors where the attack vectors are located in their manufacturing equipment.



*“SCADAfence’s user experience is very user-intuitive and easy to use. In minutes, we had a complete overview of what’s happening in our OT networks and industrial assets. This is especially a game-changer as SCADAfence is one of the few vendors that can visually show what’s occurring on our network so quickly.”*

**Wasim Darwiche**, Product and Operational Cyber Security Officer at EOS



## PREVENTING THE RANSOMWARE ATTACK

Sometime after the SCADAfence Platform was implemented in the production environment, EOS was targeted by cyber attackers who attempted a ransomware attack on EOS's systems. The SCADAfence Platform quickly alerted EOS's security team of the attempted attack and provided in-depth details of which machines were being targeted. The SCADAfence Platform also provided deep insights into the attackers' exploitation methods.

This allowed EOS's security team to immediately respond to the incoming threat before the cybercriminals could materialize the ransomware attack. With the help of the SCADAfence Platform, they knew exactly how to remediate the situation. EOS's quick remediation of the attack resulted in no downtime in production and enhanced the security to their complex OT environments.



*"Thanks to the simple usability of the SCADAfence Platform we were quickly able to understand where the attack was coming from and take the right steps to remediate the potential exposure points in our production environment. Now, we are tracking the SCADAfence Platform as part of our daily work routine."*

**Wasim Darwiche**, Product and Operational Cyber Security Officer at EOS



### About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing and building management industries to operate securely, reliably and efficiently. To learn more, visit our [website](#), check out our [blog](#), or follow us on [LinkedIn](#).

**GET STARTED TODAY**

See how EOS uses SCADAfence to achieve these results

See it live