# TEST-FUCHS secures high value testing equipment and implements predictive maintenance as well as innovative pay-per test cycle consumption services with Barracuda Secure Connector.

## TEST-FUCHS - More than 75 years of technical innovation

Experience precision and customer focus - TEST-FUCHS is the specialist in tailor-made test systems and is a performance-driven manufacturer of components for civil and military aerospace companies. It in-house expertise and production capabilities provides the flexibly to handle everything from one-off production up to large series.

Customers rely on TEST-FUCHS' reliability and proven reputation for high quality and innovation. It clients include most airlines, Aerospace Original Equipment Manufacturers (OEM) and Maintenance, Repair and Overhaul companies (MRO).

## Challenges

Even during normal operations, specialized testing equipment in aerospace applications like hydraulics is subject to extreme stress and wear. Malfunction of the test equipment must be avoided, and test accuracy provided at all times. For this reason, the test equipment itself is equipped with multiple sensors that are constantly monitored. TEST-FUCHS decided working towards a predictive maintenance concept for all of their devices that required a local edge compute image to pre-filter the data and reliably send it back to their centrally hosted monitoring service. Other use-cases include a pay-per-test cycle billing. The billing logic is hosted on the built-in management PC and potentially subject to tampering.

## Profile

- Founded in 1946
- Over 500 employees
- Headquartered in Austria
- Service locations in Germany, Italy, United Kingdom, France, China, Singapore, and the USA

## Challenges

- Implement a predictive maintenance to avoid malfunction and maintain test accuracy of testing equipment
- Establish encrypted communication and pre-filter data before sending to central monitoring service
- Create a clear perimeter between test equipment and surrounding networks
- Launch a pay-per-test billing environment

## Solution

- Barracuda Secure Connector 2 appliances with edge computing capabilities
  Barracuda Firewall Control Center

## Results

- Edge compute logic on an LXC container image for pre-filtering of sensor data
- Tamper-proof pay-per-test billing environment
- Remote-hands support via a 24x7 "always on" VPN-connection

Another challenge that needed to be addressed, was to provide a clear boundary for any (IT-/cyber-) risk-assessment conducted (by customers) to protect the test benches' internal network from the surrounding networks and vice versa.

## Solution

Barracuda Secure Connector 2 appliances with Wi-Fi and/or LTE for fail-over are built into every test-stand and provide a centrally managed Linux container (LXC) for edge intelligence and tamper-proof pay-per-test cycle calculation.

The Secure connector devices terminate the VPN connection at the Barracuda Secure Access Controllers hosted in TEST-FUCHS private datacenter.

TEST-FUCHS also uses Barracuda CloudGen Firewall solutions for network protection, network segmentation on the production floor, and connectivity to remote locations.

All devices as well as the edge logic on the LXC containers are managed via Barracuda Firewall Control Center.

> "Barracuda Secure Connector solutions made it easy for us to implement device connectivity and IoT-platform connectivity across our products."
>
> **Ulrich Poeschl**
> Chief Information Security Officer
> TEST-FUCHS GmbH

## Results

Every new test rig is equipped with a Barracuda Secure Connector device protecting the internal network, hosting the TEST-FUCHS standard software, and running edge compute logic on an LXC container image for pre-filtering of sensor data. Multiple connection methods (Wi-Fi client, cable ethernet or LTE) route the pre-filtered sensor data highly encrypted back to the TEST-FUCHS private cloud to continuously monitor device health and test accuracy. For dedicated test devices that are sold or leased with pay-per-test-cycle billing, the LXC image of the Secure Connector device provides the platform to host the billing logic in a way that provides no surface for tampering to any end user. Interconnections to the customers networks are secured via local breakout-configurations and if desired by the customer, remote-hands support is possible via the flexibility of a 24x7 "always on" VPN-connection.

> "Barracuda provided excellent support during implementation phase and reacted quickly to technical challenges that appeared on the way."
>
> **Ulrich Poeschl**
> Chief Information Security Officer
> TEST-FUCHS GmbH

## About TEST-FUCHS

Founded in 1946, TEST-FUCHS has been developing and manufacturing test systems for the aerospace industry for more than 75 years. Today TEST-FUCHS is one of the leading companies for planning and production of highly customized test systems for aircraft in production and maintenance world-wide. Next to the fully customized test solutions TEST-FUCHS also designs, qualifies, manufactures, and maintains airborne systems and components for civil and military applications for fixed-wing and rotary aircraft as well as aerospace solutions. TEST-FUCHS employs over 500 people and in addition to its headquarters in Austria, TEST-FUCHS operates service locations in Germany, Italy, United Kingdom, France, China, Singapore, USA, and partners in many other countries.

## About Barracuda Industrial IoT Solutions

Barracuda CloudGen Firewall solutions for Industrial IoT are a family of highly secure, small form-factor devices for advanced network security, encrypted communications, and cost-effective connectivity. Full integration into Barracuda Firewall Control Center architecture guarantees hassle-free centralized management for tens of thousands of remote devices. The encrypted connection between the security appliance and the data center is established with Barracuda's proprietary, enhanced IPsec protocol TINA. Without relinquishing any security aspects, TINA is significantly more resilient and effective than other competitive VPN solutions. Advanced security functions include application enforcement, IPS, URL filtering, antivirus, sandboxing (ATP), and denial-of-service protection. These functions are provided by a CloudGen Firewall device or on the highly scalable and stackable Secure Access Controller hosted on premises or in the public cloud.

For more information about Barracuda IIoT security, please visit barracuda.com/IoT.

For more information about other Barracuda successes, please visit: blog.barracuda.com

Barracuda®
Your journey, secured.