TEST-FUCHS sichert hochwertige Prüfgeräte und implementiert vorausschauende Wartung sowie innovative Pay-per-Test-Cycle-Dienste mit Barracuda Secure Connector.

TEST-FUCHS - Über 75 Jahre technische Innovation

Erleben Sie Präzision und Kundenorientierung - TEST-FUCHS ist der Spezialist für maßgeschneiderte Testsysteme und ein leistungsorientierter Hersteller von Komponenten für die zivile und militärische Luft- und Raumfahrt. Das hauseigene Know-how und die Produktionskapazitäten bieten die Flexibilität, um von der Einzelanfertigung bis zur Großserie alles zu realisieren.

Die Kunden vertrauen auf die Zuverlässigkeit und den guten Ruf von TEST-FUCHS in Bezug auf hohe Qualität und Innovation. Zu den Kunden zählen die meisten Fluggesellschaften, Erstausrüster der Luft- und Raumfahrtindustrie (Original Equipment Manufacturers - OEM) sowie Wartungs-, Reparatur- und Revisionsunternehmen (Maintenance, Repair, and Overhaul companies - MRO).

Herausforderungen

Selbst im Normalbetrieb sind spezielle Prüfgeräte in der Luft- und Raumfahrt, z. B. in der Hydraulik, extremen Belastungen und Verschleiß ausgesetzt. Fehlfunktionen der Prüfgeräte müssen vermieden werden, und die Prüfgenauigkeit muss jederzeit gewährleistet sein. Aus diesem Grund sind die Prüfgeräte selbst mit mehreren Sensoren ausgestattet, die ständig überwacht werden. TEST-FUCHS entschied sich für ein vorausschauendes Wartungskonzept für alle Geräte, das ein lokales Edge-Compute-Image benötigt, um die Daten vorzufiltern und sie zuverlässig an den zentral gehosteten Monitoring-Service zu senden. Ein weiterer Anwendungsfall ist die Abrechnung pro Testzyklus. Die Abrechnungslogik wird auf dem eingebauten Management-PC gehostet und ist potenziell anfällig für Manipulationen.

Profil

- Gegründet im Jahr 1946
- Über 500 Mitarbeiter
- Hauptsitz in Österreich
- Servicestandorte in Deutschland, Italien, Großbritannien, Frankreich, China, Singapur und den USA

Herausforderungen

- Implementierung von vorausschauender Wartung zur Vermeidung von Fehlfunktionen und zur Aufrechterhaltung der Genauigkeit der Testsysteme
- Einrichtung einer verschlüsselten Kommunikation und Vorfilterung der Daten vor dem Versand an den zentralen Monitoring-Service
- Schaffung einer klaren Abgrenzung zwischen Testgeräten und umgebenden Netzwerken
- Einführung einer Pay-per-Test-Abrechnungsumgebung

Lösung

- Barracuda Secure Connector 2 Appliances mit Edge-Computing-Funktionalität
- Barracuda Firewall Control Center

Ergebnis

- Edge-Computing-Logik auf einem LXC-Container-Image zur Vorfilterung von Sensordaten
- Manipulationssichere Pay-per-Test-Abrechnungsumgebung
- Remote-Support über eine 24x7 “always on” VPN-Verbindung

Eine weitere Herausforderung, die es zu bewältigen galt, war die Schaffung einer klaren Grenze für jede (IT-/Cyber-) Risikobewertung, die (von Kunden) durchgeführt wird, um das interne Netzwerk der Prüfstände vor den umliegenden Netzwerken zu schützen und umgekehrt.

Lösung

Barracuda Secure Connector 2 Appliances mit WLAN und/oder LTE für Failover sind in jeden Prüfstand eingebaut. Sie bieten einen zentral verwalteten Linux-Container (LXC) für Edge-Intelligenz und manipulationssichere Pay-per-Test-Cycle-Abrechnung.

Die Secure Connector-Geräte terminieren die VPN-Verbindung an den Barracuda Secure Access Controllern, die im privaten Rechenzentrum von TEST-FUCHS gehostet werden.

TEST-FUCHS nutzt außerdem Barracuda CloudGen Firewall-Lösungen für den Netzwerkschutz, die Netzwerksegmentierung in der Produktion und die Anbindung von Remote-Standorten.

Alle Geräte sowie die Edge-Logik auf den LXC-Containern werden über das Barracuda Firewall Control Center gemanagt.

> "Die Barracuda Secure Connector-Lösung hat es uns leicht gemacht, Gerätekonnektivität und IoT-Plattform-Konnektivität in unseren Produkten zu implementieren."
>
> **Ulrich Pöschl**
> Chief Information Security Officer
> TEST-FUCHS GmbH

Ergebnis

Jeder neue Prüfstand ist mit einer Barracuda Secure Connector Appliance ausgestattet, die das interne Netzwerk schützt, die TEST-FUCHS-Standardsoftware hostet und die Edge-Compute-Logik auf einem LXC-Container-Image zur Vorfilterung der Sensordaten ausführt. Mehrere Verbindungsmethoden (WLAN-Client, kabelgebundenes Ethernet oder LTE) leiten die vorgefilterten Sensordaten hochgradig verschlüsselt an die TEST-FUCHS Private Cloud zurück, um den Gerätezustand und die Testgenauigkeit kontinuierlich zu überwachen.

Für dedizierte Testgeräte, die über das "Abrechnung pro Testzyklus" Modell verkauft oder verleast werden, bietet das LXC-Image des Secure Connector-Geräts die Plattform, um die Abrechnungslogik auf eine Weise zu hosten, die keine Angriffsfläche für Manipulationen bietet. Die Verbindungen zu den Kundennetzwerken werden über lokale Breakout-Konfigurationen gesichert, und (wenn vom Kunden gewünscht) ist ein Remote-Support über die Flexibilität einer 24x7 "always on" VPN-Verbindung möglich.

> "Barracuda leistete während der Implementierungsphase hervorragende Unterstützung und reagierte schnell auf technische Herausforderungen, die auf dem Weg auftauchten."
>
> **Ulrich Pöschl**
> Chief Information Security Officer
> TEST-FUCHS GmbH

Über TEST-FUCHS

1946 gegründet, entwickelt und fertigt TEST-FUCHS seit mehr als 75 Jahren Testsysteme für die Luft- und Raumfahrtindustrie. Heute ist TEST-FUCHS eines der führenden Unternehmen für die Planung und Produktion von hochgradig kundenspezifischen Testsystemen für Flugzeuge in Produktion und Wartung weltweit. Neben den maßgeschneiderten Testlösungen entwickelt, prüft, fertigt und wartet TEST-FUCHS auch TEST-FUCHS entwickelt, qualifiziert, fertigt und wartet luftgestützte Systeme und Komponenten für zivile und militärische Anwendungen für Starrflügler und Drehflügler sowie Lösungen für die Raumfahrt. TEST-FUCHS beschäftigt über 500 Mitarbeiter und verfügt neben dem Hauptsitz in Österreich über Servicestandorte in Deutschland, Italien, Großbritannien, Frankreich, China, Singapur, USA und Partner in vielen anderen Ländern.

Über Barracuda Industrial IoT Lösungen

Barracuda CloudGen Firewall-Lösungen für das industrielle IoT sind eine Familie von hochsicheren Geräten mit kleinem Formfaktor für erweiterte Netzwerksicherheit, verschlüsselte Kommunikation und kostengünstige Konnektivität. Die vollständige Integration in die Barracuda Firewall Control Center-Architektur garantiert eine problemlose zentralisierte Administration für Zehntausende von Remote-Geräten. Die verschlüsselte Verbindung zwischen der Security Appliance und dem Rechenzentrum wird mit Barracudas proprietärem, erweiterten IPsec-Protokoll TINA hergestellt. Ohne auf Sicherheitsaspekte verzichten zu müssen, ist TINA deutlich belastbarer und effektiver als andere VPN-Lösungen der Konkurrenz. Zu den erweiterten Sicherheitsfunktionen gehören Application Enforcement, IPS, URL-Filter, Antivirus, Sandboxing (ATP) und Denial-of-Service-Schutz. Diese Funktionen werden von einem CloudGen Firewall-Gerät oder auf dem hoch skalierbaren und stapelbaren Secure Access Controller bereitgestellt, der lokal oder in der Public Cloud gehostet wird.

Weitere Informationen zum Thema Barracuda IIoT Security, finden Sie auf barracuda.com/IoT.

Weitere Informationen über Barracuda Erfolge finden Sie auf blog.barracuda.com

Barracuda
Your journey, secured.