EDGE SDN™

ICOS

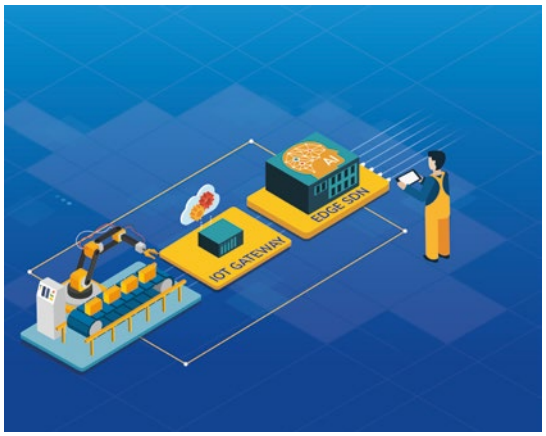
# Edge SDN - Die Cybersecurity-Lösung für IoT und OT Industrienetzwerke

Edge SDN von Stoorm5 ist eine Cybersicherheitsplattform, die die Anlagen und das OT-Telekommunikationsnetz gemäß ISO/IEC 62443 und NIST 800-82 sichert. Edge SDN besteht aus SDN-Knoten, die an ausgewählten Punkten des Netzwerks installiert werden, einer zentralen Verwaltungskonsole für die IT-Abteilung zur Verwaltung von Sicherheitsprofilen und einem Tablet in den Händen der OT-Abteilung, mit dem diese Sicherheitsrichtlinien unabhängig umsetzen kann.

IoT- und OT-Netzwerke müssen von innen geschützt werden und nicht nur an einzelnen Netzwerkpunkten wie Firewall oder IDS an der Grenze. Industrienetzwerke sind grenzenlos. Isolieren Sie die Maschinen und segmentieren Sie den Datenverkehr des OT-Netzwerks. Intrusion Detection System mit Datenanalyse an jedem Punkt des Netzwerks. OT-Betreiber arbeiten unabhängig, indem sie die Funktionen des Systems modifizieren. Ein selbstlernendes künstliche Intelligenzsystem zur Bedrohungsbeurteilung. Die IT-Abteilung überwacht Bedrohungen und Sicherheitsstufen des OT-Netzwerks.

## Für OEMs:

Maßgeschneiderte Sicherheitsprofile für Maschinen gemäß ISO/IEC 62443 und NIST 802-82.




## Für IT- und OT-Abteilungen:

Trennung der Verantwortlichkeiten und Unterstützung der OT-Abteilung.


## Für wen?

Die Plattform richtet sich an verschiedene Industrien, darunter Fertigungsindustrie, Gesundheitswesen, Smart Cities, Transport und Logistik, Energiemanagement, Einzelhandel, Finanznetzwerke, Luft- und Raumfahrt sowie Verteidigung.

**ISO/IEC 62443**
**NIST 800-82**

EDGE SDN™

ICOS

## Trennen Sie Ihre Vermögenswerte:
Isolieren Sie Hosts, Geräte, Maschinen und Dienste vom Netzwerk.

## Frühzeitige Bedrohungserkennung:
Das IDS bewertet Bedrohungen mithilfe eines KI-Algorithmus, um nur konkrete Gefahren zu melden.

## Unabhängigkeit der OT-Abteilung:
OT-Abteilung kann die Netzwerksicherheit eigenständig verwalten.

## Mikrosegmentierung:
Verhindern Sie nicht autorisierten Datenverkehr und ermöglichen Sie nur Kommunikation zwischen bekannten und autorisierten Empfängern.

## Kontrolle durch IT-Abteilung:
Erstellen Sie Sicherheitsprofile und überwachen Sie den Betrieb und erkannte Alarme.

Die herkömmliche Herangehensweise an die Sicherheit besteht oft darin, Sicherheitsgeräte wie Firewalls, IPS, Antivirensoftware und VLANs mit verwalteten Switches zu erwerben. Diese Verteidigungsstrategien sind zwar für IT-Dienste geeignet, aber weniger effektiv in IoT-Netzwerken.

# VORTEILE

- Wettbewerbsvorteil: Integration von IT-Sicherheit.
- Compliance: ISO/IEC 62443 und NIST 802-82.
- Weniger Störungen: Schutz vor Schwachstellen.
- Sicherheitsbewusstsein: Keine Verbreitung von Bedrohungen während der Wartung.
- Zugang zu Märkten: Sicherheit und Zuverlässigkeit.
- Höhere OT-Sicherheit: IEC 62443 und NIST 800-82.
- Weniger IT-Support-Besuche: OT- und IoT-Netzwerke autonom verwalten.
- Schutz von Ressourcen: Segmentierung und Isolation vor Zero-Day-Schwachstellen.
- Compliance mit IT-Sicherheitsregeln: OT-Abteilung.

**ICOS Deutschland GmbH**
Paul-Heyse-Str. 28
D-80336 München
Phone: (+49) 89 326764-0
www.icosvad.de

Für weitere Informationen, wie Partnerprogramm, POCs, Presalesgespräche, Preisinformationen, usw. wenden Sie sich an: info@icosvad.de oder scannen den QR Code.