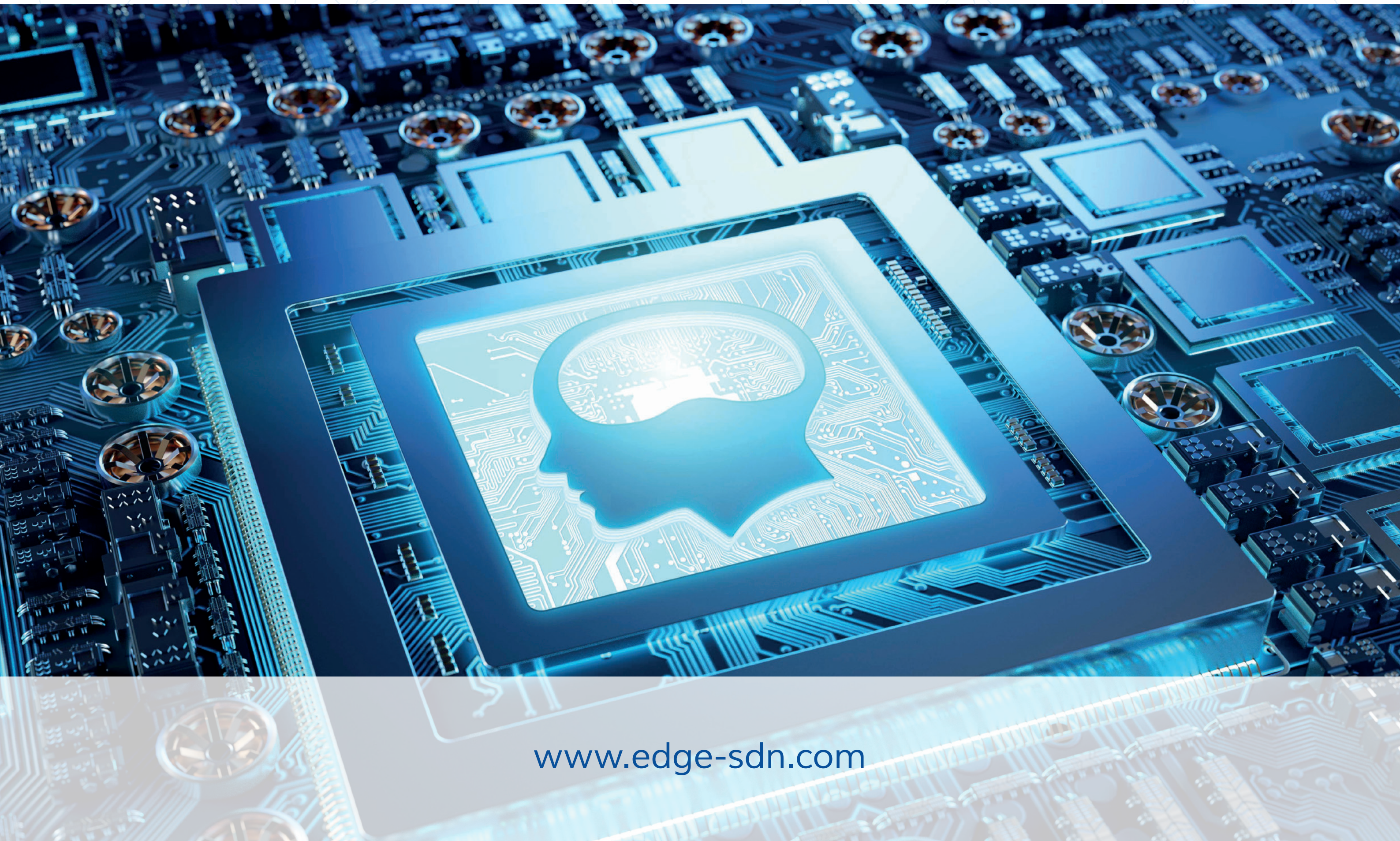
EDGE SDN

CYBER SECURITY Platform for IOT and OT Industrial Network

Software Defined LAN to secure and protect devices, machines, assets, and services

ISO/IEC 62443 NIST 800-82

International Cyber Security Standards



www.edge-sdn.com

EDGE SOFTWARE DEFINED NETWORK

Edge SDN is a **Cyber Security** Platform that secures the **assets** and the **OT** telecommunications **network** according to **ISO/IEC 62443** and **NIST 800-82**. Edge SDN is composed of **SDN Nodes**, to be installed in selected points of the network; a **Central Management Console**, for the IT department to manage **security profiles**; and a Tablet, in the hands of the OT department, that allows them to **implement** security policies **independently**.

Intrusion Detection System with data analysis in every point of the network

Isolate the machines and **micro-segment** the data traffic of the OT network

IT department **oversees** the threats and **security level** of the OT network

Self-learning Artificial Intelligence System for threat assessment

SDN Edge Platform integration without modifying the existing network

OT operators work **independently** by modifying the functions of the system

HOW IT WORKS

INTERNAL PROTECTION

IoT and **OT networks** must be **protected from the inside** and not only in single network points such as Firewall or IDS at the border. Industrial networks are borderless.

UNPLUG YOUR ASSETS

Isolate hosts, **devices**, **machines**, and **services** from the network. **Allowed applications can exchange** traffic while threats and malwares are segregated and ineffective.

OPERATIONALLY INDEPENDENT OT DEPARTMENT

The **OT department** manages the operation of network security in **complete autonomy** with a simple click on the tablet for each **operating condition**.

NETWORKMICRO-SEGMENTATION

Prevent unplanned traffic **avoiding malicious activities**; allow communication only between well-known and authorized recipients, preventing any illegal or misused communication.

FULL CONTROL OF THE IT DEPARTMENT

The IT department creates network **operation profiles** with the desired **security levels** and supervises operation and detected alarms.

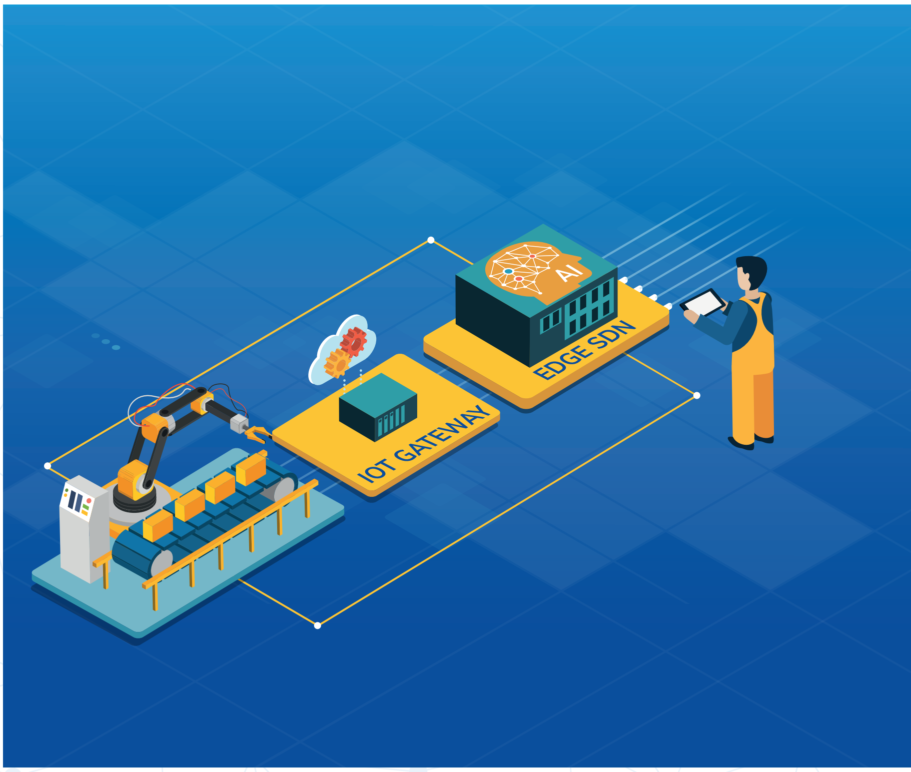
DETECT DANGERS BEFORE THEY BECOME PROBLEMS

The IDS present in each network node evaluates each detected threat using an **AI self-learning** algorithm in order to report only **concrete dangers**.

SOLUTIONS FOR OEMS

The **Edge SDN platform** secures individual **machines** according to the international standard on **Cyber Security ISO/IEC 62443** and **NIST 802-82**. Manufacturers can create **customized operating profiles for each condition of use** of the machine, ensuring their customers operate with a **predefined level of security**.

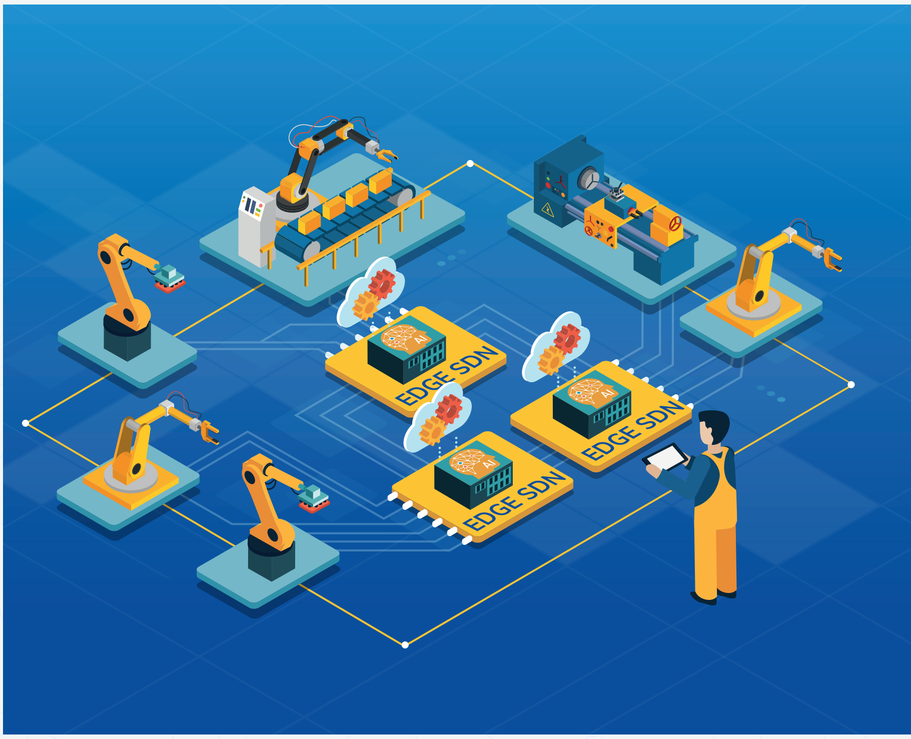
- STAND OUT FROM THE COMPETITION by creating an offer in which IT security is integrated.
- Make your MACHINES COMPLIANT with the international standard ISO/IEC 62443 and NIST 802-82.
- FEWER ASSISTANCE INTERVENTIONS thanks to protection from possible vulnerabilities.
- During maintenance, THREATS on the maintainer's PC CANNOT SPREAD throughout the company.
- RECTIFY VULNERABILITIES IN MACHINES before update patches are released.
- ACCESS TO HIGH VALUE MARKETS, where safety and reliability are essential.



SOLUTIONS FOR IT AND OT DEPARTMENTS

The **cybersecurity** of a company involves both the IT and OT departments. The **IT department** is responsible for IT security, while the **OT department** is responsible for business continuity. The Edge SDN platform allows **the separation of roles** giving the IT department the tools to **support** and **control** the OT department that can work in **full autonomy**.

- INCREASES THE LEVEL OF OT SECURITY in accordance with IEC 62443 and NIST 800-82.
- FEWER IT SUPPORT VISITS to the OT and IOT networks.
- The OT DEPARTMENT INDEPENDENTLY MANAGES DAILY PROBLEMS with predefined security levels.
- PROTECTION OF RESOURCES from zero-day vulnerabilities by segmenting and isolating them.
- Ensure that the OT DEPARTMENT COMPLIES WITH IT SECURITY RULES.
- HIGH-VALUE NETWORK DATA and OT operating procedures.



INTEGRATE THE EDGE SDN PLATFORM INTO YOUR SECURITY STRATEGY

Whatever your **OT cybersecurity** strategy, use of VLAN, Firewall or border IDS, the **Edge SDN platform** can help you **increase** the level of security and **automate** the necessary OT operations in any **operational condition**.
The **Edge SDN platform** can be integrated without making any changes to the existing network. We evaluate which of the functions of the Edge SDN **platform** fills an existing security gap for each **zone** or **network point**.

- ✓ Machine isolation
- ✓ Communication micro-segmentation
- ✓ Intrusion Detection System with Self-learning AI

ANALYSES

We start with the **risk analysis** of the current system, identifying the **areas** and the necessary interventions to achieve the desired **Security Level** of the **ISO/IEC 62443** and **NIST 802-82** standard.

INSTALLATION AND CONFIGURATION

Edge SDN nodes* are installed in the network locations identified in the analysis and network **operation profiles** are created for each **operating condition**.

OT DEPARTMENT TRAINING

The **tablet** used by the **OT department** has individual buttons that allow operators to **apply** the operating profiles of the network in full autonomy.

GO LIVE

The system is now complete. The **IT department** through the **Central Management Console** supervises the IT security level of the **OT department** in real time.

* Any **SDN switch** compatible with the **OpenFlow** protocol version 1.3 can be used

ADVANTAGES

INFORMATION TECHNOLOGY (IT)

- ✓ **Certainty** of the IT security level of the **OT department**
- ✓ **Remote control** of operating conditions in **real-time**
- ✓ Alarms from the network with risk **assessment** through **self-learning AI**

OPERATIONAL TECHNOLOGY (OT)

- ✓ **Operational independence** from the IT department
- ✓ Modification of network operation **profiles** based on **working conditions**
- ✓ **Cyber Security** management even by **inexperienced operators**

powered by
stoorm5®

STOORM5 SRL
LEGAL & OPERATIONAL HEADQUARTERS

Via Natalino Corazza 7/7
40128, Bologna (BO) - Italy
VAT 03450101203

Phone: +39 051 3512525
Email: info@stoorm5.com
www.stoorm5.com