Unmanaged Devices

Use Case
Operational Technology

Protecting the attractive attack vector

Operational Technology (OT) is the hardware and software controlling and operating the physical processes of an industry. These systems function to run, automate and manage industrial equipment.

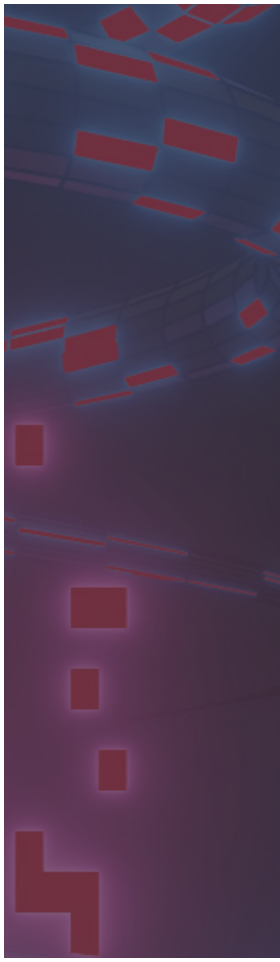
Traditionally, OT was an ‘air-gapped’ environment, meaning that the OT systems were kept distinct and disconnected from IT environments. The assumption was OT networks were never be exposed to threats as they were not connected to the outside world. With the rise of the Industrial Internet of Things (IIoT), this gap rapidly diminishes, and OT environments are exposed to cyber threats.

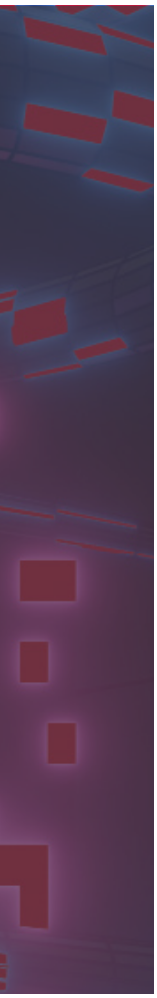
Operational Technology Security

Operational technology (OT) security is mainly designed to meet the unique security needs required for OT environments. OT security is commonly used to protect and control traditional operations, critical infrastructures and assets from cyberattacks.

A trend of the last two decades is 'IT/OT convergence' bringing IT technological advances into OT systems. Though operational and information technologies are becoming more connected, important differences exist. While operational technology (OT) manages and controls industrial operations, information technology (IT) focuses on handling computing and data processing.

IT/OT convergence opens the OT to a vast and advanced cyber-threat landscape despite the benefits. It makes OT devices accessible from the IT network by lateral movement, a technique a cyberattacker uses to move deeper into a network searching for sensitive data or assets to breach. Since OT incidents lead to more destructive outcomes, they have become a new attack vector.





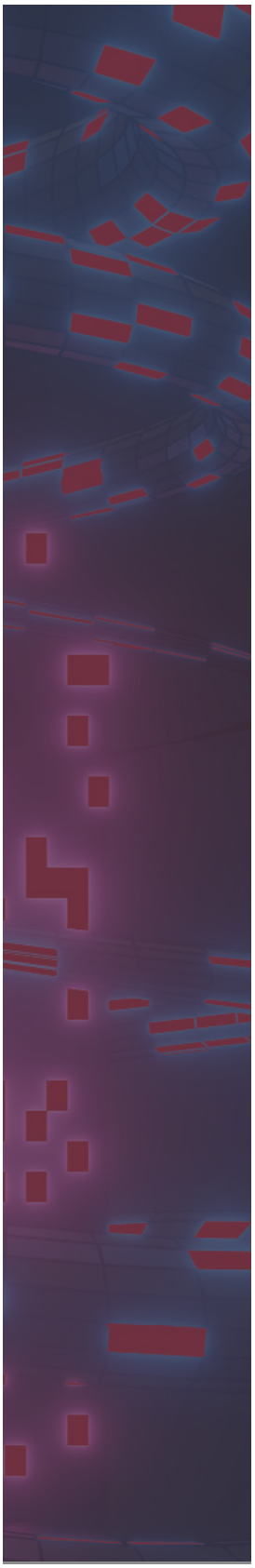
Strong security with Software-defined Perimeter and Zero Trust

Zero Trust is based on the premise that nothing is trusted and assumes a breach is inevitable or has likely already occurred. It means that access to network resources should never be allowed until users and devices are properly authenticated and authorised.

Software-defined Perimeter (SDP) is a security framework that controls resource access based on user identity. Zero Trust enforces identity-based access, ensuring that users are not authenticated once or twice but continually verified upon login.

SPD is unquestionably the best alternative to virtual private networks (VPN) to establish remote access to applications. SDP is designed to enable micro-segment network access effectively. Traditional network security connects various roles or groups to a network segment. SDP solutions create identity-centric perimeters, allowing for more fine-grained access control.

The strongest feature of SDP is that it can 'blacken' any infrastructure and assets connected to the internet. It makes it impossible for external parties or hackers to see, ensuring only authorised users can access certain resources.



The OT threat landscape

Historically, cybercriminals were mainly interested in stealing data or other high-value assets. As the Industrial Internet of Things (IIoT) has grown, almost everything on an OT network now features IoT connectivity. As a result, it increases the potential attack surfaces and challenges endpoint security. Cybercriminals recognise the potential for disruption due to inadequate OT security and increasingly target OT networks.

Industrial Control Systems (ICS) is under the umbrella of OT. ICS is used in almost all industrial processes and enables remote monitoring, upgrading, and servicing systems from a central location. Many industrial organisations and companies use a well-known industrial control system in public and private sectors: Supervisory Control and Data Acquisition (SCADA). SCADA supports organisations in controlling and maintaining efficiency, distributing data for smarter decisions, and communicating system issues to help mitigate downtime. These Industrial Control Systems greatly improve efficiency, increase productivity and expose the OT environment to the same disruptive and destructive attack threats for any internet-connected device.

Personnel and contractors need visibility and access to the OT network for ongoing maintenance and monitoring. Industrial equipment and systems still use VPNs to establish remote access to these systems and applications. This approach inadvertently expands the attack surface and opens the door for intruders to exploit trusted access.

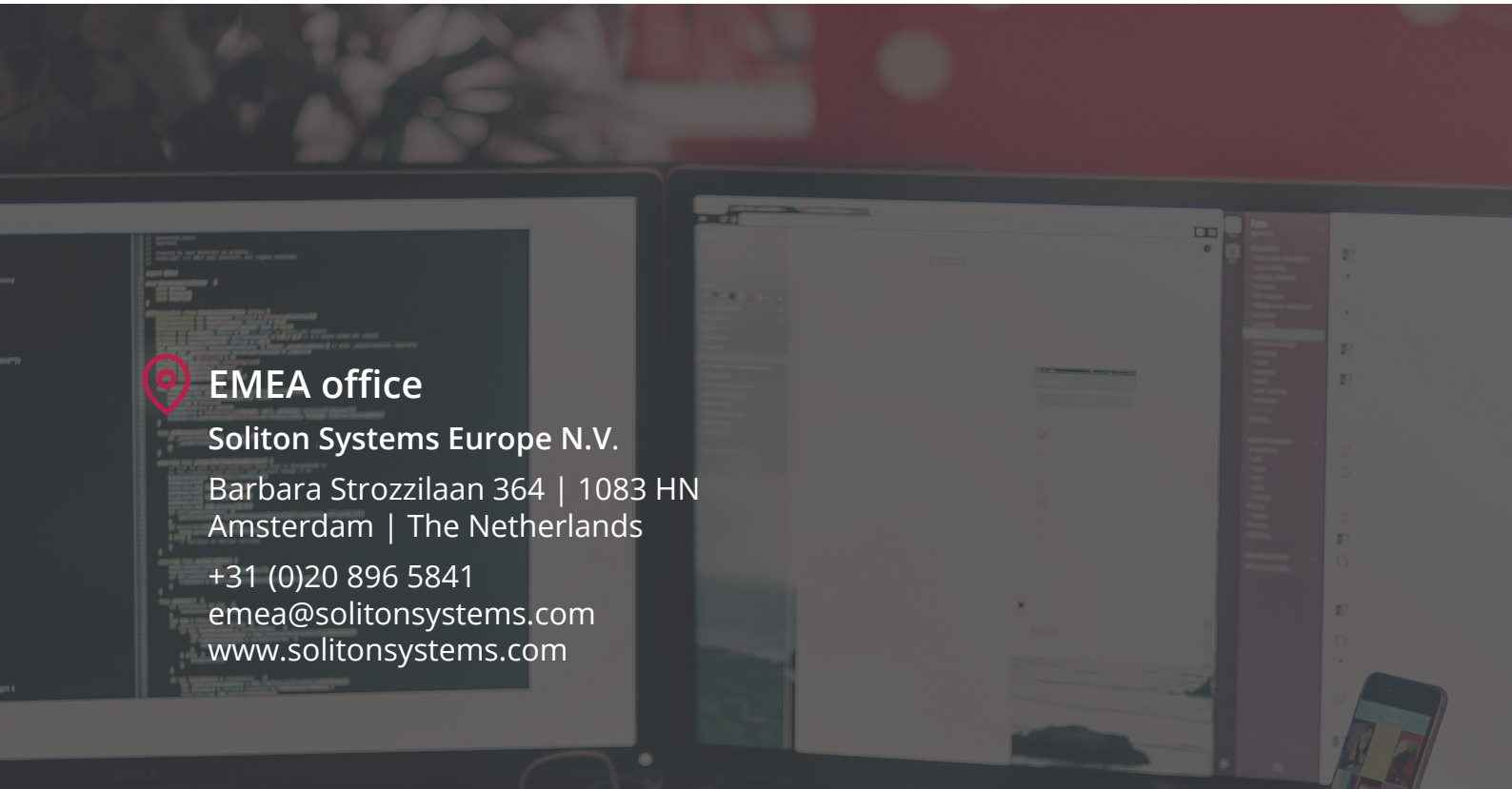
Insider threats are often neglected and underestimated. An insider attack can have a major impact on an organisation. There's the value loss of the breached data or asset and the immediate loss of intrinsic value and lost revenue to consider.

All things IoT

In the current trend toward digitalisation, manufacturers increasingly rely on a range of technology platforms to help streamline and accelerate their production processes. IIoT will be a large contributor in connecting more smart devices and sharing the information they produce to improve existing business models and enable new ones.

SDP will remain an effective security measure protecting IIoT and related systems against cyber threats. Whether they are an employee or third party user, users are only permitted access to specific applications on a need-to-know basis. It means SDP only connects authorised users and devices to the resources they need without connecting a user to the network directly, drastically reducing the risk of a data breach. When authorised, users immediately gain access to the required resources, regardless of their location, delivering a seamless experience and maximising their uptime and productivity.

SDP reduces the cost and complexity of traditional network appliances such as VPN and mitigates the attack surfaces. The network is only visible to authorised users, making it the best defence as hackers can't reach the network.



EMEA office

Soliton Systems Europe N.V.

Barbara Strozzilaan 364 | 1083 HN
Amsterdam | The Netherlands

+31 (0)20 896 5841
emea@solitonsystems.com
www.solitonsystems.com