SECURE ACCESS FOR THE SMART FACTORY FLOOR

5 Steps to Secure and Service IIOT Devices for Maximizing Uptime

The Business Effects of Unplanned Downtime

Industry 4.0 is using the Industrial Internet of Things, cloud computing, cyber-physical systems and cognitive computing to boost manufacturing efficiency.

The stakes get higher with the rise of the smart factor floor.

82%
of companies have experienced unplanned downtime over the past three years

Unplanned downtime can cost a company as much as
$260,000 /hr

https://www.aberdeen.com/techpro-essentials/stat-of-the-week-the-rising-cost-of-downtime/

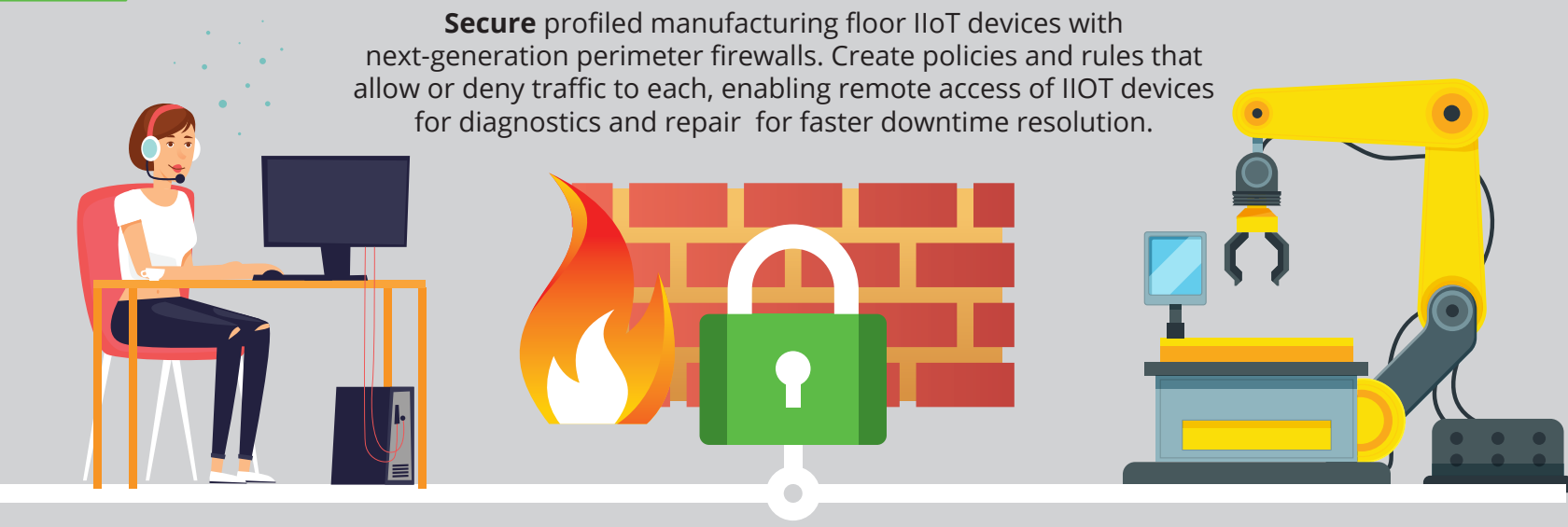
1 Visibility for Industry 4.0

Secure Access starts with device profiling and establishing complete network visibility. This includes IIoT systems on manufacturing floors. Organization production may be blindsided by unknown and unsecured endpoints

A 2016 Deloitte-MAPI study found that one-third of manufacturers have not performed any cyber risk assessments of industrial control systems (ICS) operating on factory floors.[12]

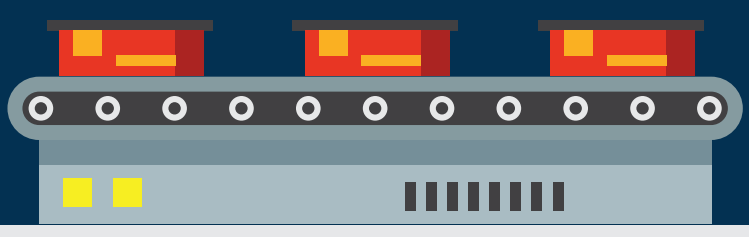
2 Provisioning for Factory Uptime

Secure profiled manufacturing floor IIoT devices with next-generation perimeter firewalls. Create policies and rules that allow or deny traffic to each, enabling remote access of IIOT devices for diagnostics and repair for faster downtime resolution.



3 Automation for IT and OT

Discovered and profiled manufacturing floor IIoT systems (SCADAs, PLCs, HMIs) are automatically provisioned to next-generation firewalls. This process dramatically reduces operational IT/OT overhead while helping improve production uptime.



‘As more companies work toward IT/OT alignment, the CIO and the IT organization will be at the forefront of fostering relationships and changing the culture of the organization.'. 'This will require a hybrid of traditional IT and OT skills and development of new intellectual property...'

Kristian Steenstrup, distinguished analyst and Gartner Fellow.

https://www.prnewswire.com/news-releases/averna-becomes-a-ptc-platinum-partner-300520643.html

4 Authentication for Factory Repair

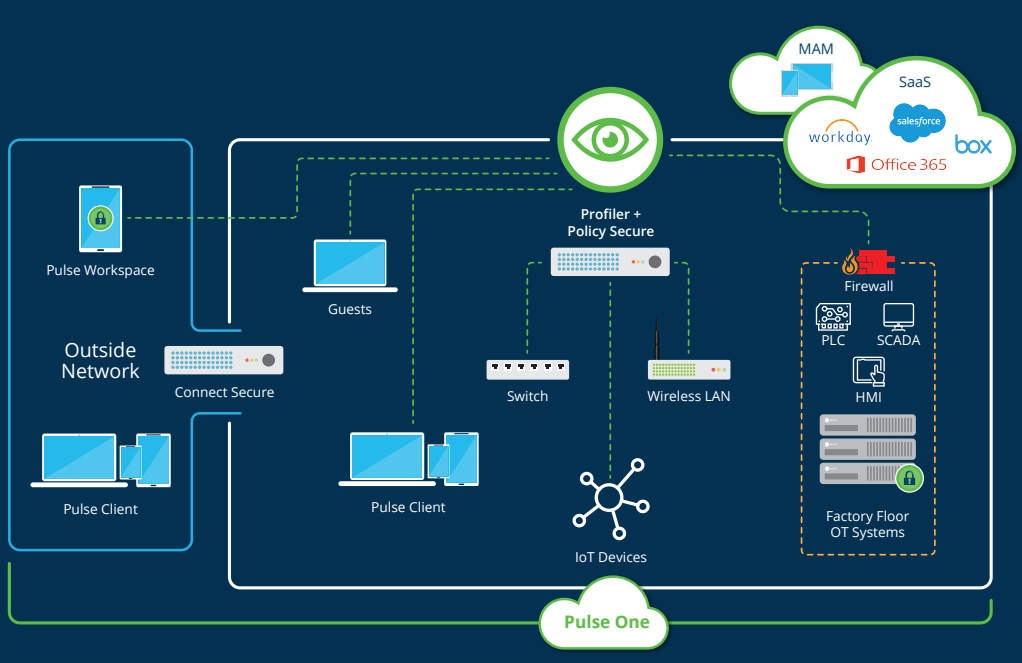
Users and devices requiring access to manufacturing floor IIoT devices are authenticated based on endpoint and technician role before connected to the network.

5 Secure Access by Policy

Support contractors gain remote secure access to troubled floor SCADA, PLC, and other IIoT sensors.

Policies for local and remote access are based on user role, device used, type of access needed and targeted IIOT-based resource.

Secure Access Solution



Pulse Policy Secure and Pulse Connect Secure tie contextual user data to network and application access, addressing regulatory compliance and audit demands. Pulse Secure Profiler finds factory floor devices and performs pre-connect security compliance. When deployed with popular next-generation firewalls, Pulse Policy Secure provisions user session information and gives additional perimeter-based security. Pulse Secure Access solutions are managed centrally through Pulse One.

Pulse Secure®