smaRTE BY FLEX
SOLUTIONS DIGITAL

SMARTE SPLICE

HEALTHCARE

"REAL-TIME OPERATIONAL EXCELLENCE"

FLEX SMARTE SOLUTIONS

FLAWLESS EXECUTION THROUGH DIGITAL MASTERY

We will help you to maximise your organisation's Return on operational Assets (RooA). This means that we enable you to operate your assets as effectively and efficiently as possible, while also ensuring they are healthy and safe. In this way, you reduce your operational costs and risks, becoming far more profitable as a result.

We can achieve this through one or more of our six "smaRTE solutions" that have been built using a combination of our leading-edge, digital technologies and are focused around our "Real-Time Operational Excellence (RTE)" mantra.

OT CYBER SECURITY

BACKGROUND

Healthcare is a top target for cybersecurity threats

Healthcare organisations have experienced a massive spike in cyber attacks (an alarming 94% increase in just one year) due to their high propensity to pay ransoms, the value of patient records, and inadequate security measures to detect and prevent threats. Healthcare providers also cannot serve patients without access to their records and monitoring digital medical equipment connected to health networks.

Most organisations have Information Technology (IT) cybersecurity policies and systems in place believing that they are protected. Very few consider the vulnerabilities that are present in their Operational Technology (OT) environment. Savvy healthcare industry stakeholders, however, understand that IT Cybersecurity and OT Cybersecurity are vastly different fields. The traditional "Air Gap" is difficult to maintain in an ever-increasing connected world, where OT-IT networks are converging. IT Cybersecurity solutions are also not designed to secure OT networks and assets.

OT Cybersecurity is therefore critical in asset-intensive and highly regulated industries, like healthcare, that has a great dependency on continued operations. Healthcare systems and operational assets, such as medical devices, machines, monitors, operating theaters, air-conditioning systems, and generators are all crucial to ensure the effectiveness and efficiency of a healthcare facility and the safety and well-being of employees and patients. If any of these healthcare operational assets were to be exposed to cyber attacks, the entire medical facility could come to a halt, resulting in huge financial losses for the organisation and, health risks, serious injury, or even death.

It is therefore critical that an OT-focused cybersecurity intervention be employed that does not merely detect, but also prevents all connected OT equipment from becoming vulnerable to cyber-attacks. It must ensure the cyber-physical resilience of your healthcare environment and minimise the risk of downtime.

OT CYBER SECURITY

THE TYPICAL OPERATIONAL VULNERABILITIES:

The following are common operational vulnerabilities inherent in most healthcare environments:

- Digital transformation, growth of the Internet of Things (IoT), and interconnected technologies in the healthcare sector
- Innovations in medical technology and connecting them to health networks and the internet
- The large quantity of medical equipment and devices in the field makes managing security harder
- Insecure configurations aimed to ensure interoperability between different vendor equipment
- Security is unlikely to be factored into the design of most medical equipment and devices

THE RESULTANT IMPLICATIONS:

An adversary with a foothold on the network can leverage any of these inherent weaknesses to:

- Take over normal operations
- Disrupt normal operations (this can be achieved without a deep understanding of the healthcare environment)
- Holding the healthcare facility hostage and demanding exorbitant ransom amounts
- Steal confidential data, such as patients' medical records, personal data, and the healthcare facility's intellectual property and quickly sell it to their contacts.
- Cause damage, destruction, or unsafe working conditions by manipulating the state of the managed process and blinding operators to the real state of the process
- Cause health risks, serious injury, and even death to employees or patients

OT CYBER SECURITY

THE SMARTE SOLUTION - SPLICE:

smaRTE Splice actively prevents cyber-physical attacks through proactive vulnerability shielding inside an encrypted overlay network. It, therefore, embraces connection and convergence. It is the logical alternative to air gaps, firewalls, data diodes, and old-school thinking. The Splice solution comprises three layers with three operating modes as can be seen below:

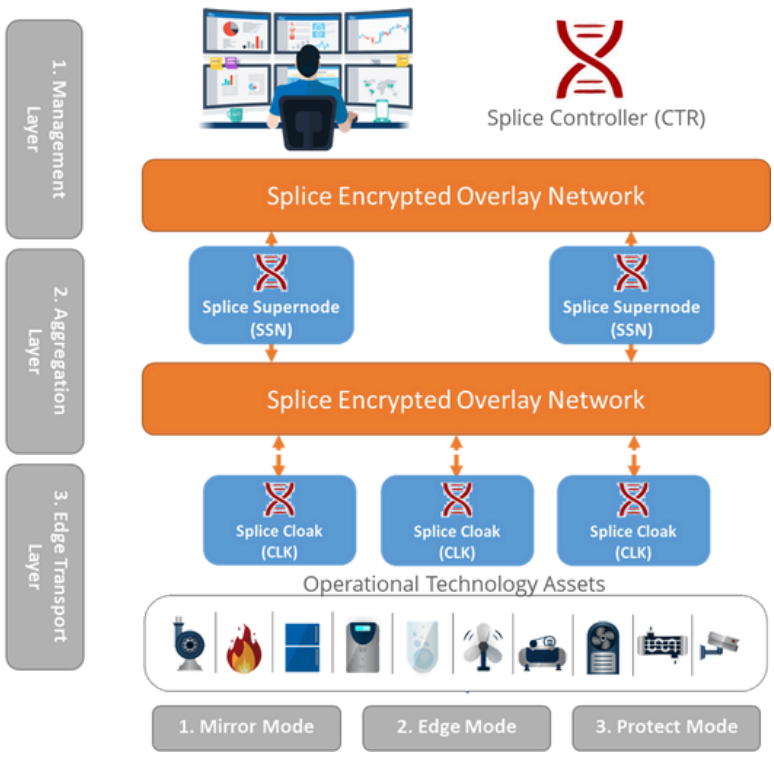
Simplicity & Flexibility!

3 Layers:

1. Management (Controller)
2. Aggregation (Supernode)
3. Edge Transport (Cloak)

3 Operating Modes:

1. Mirror - Observation
2. Edge – Manage access route to OT Equipment
3. Protect – All OT Equipment traffic via Splice



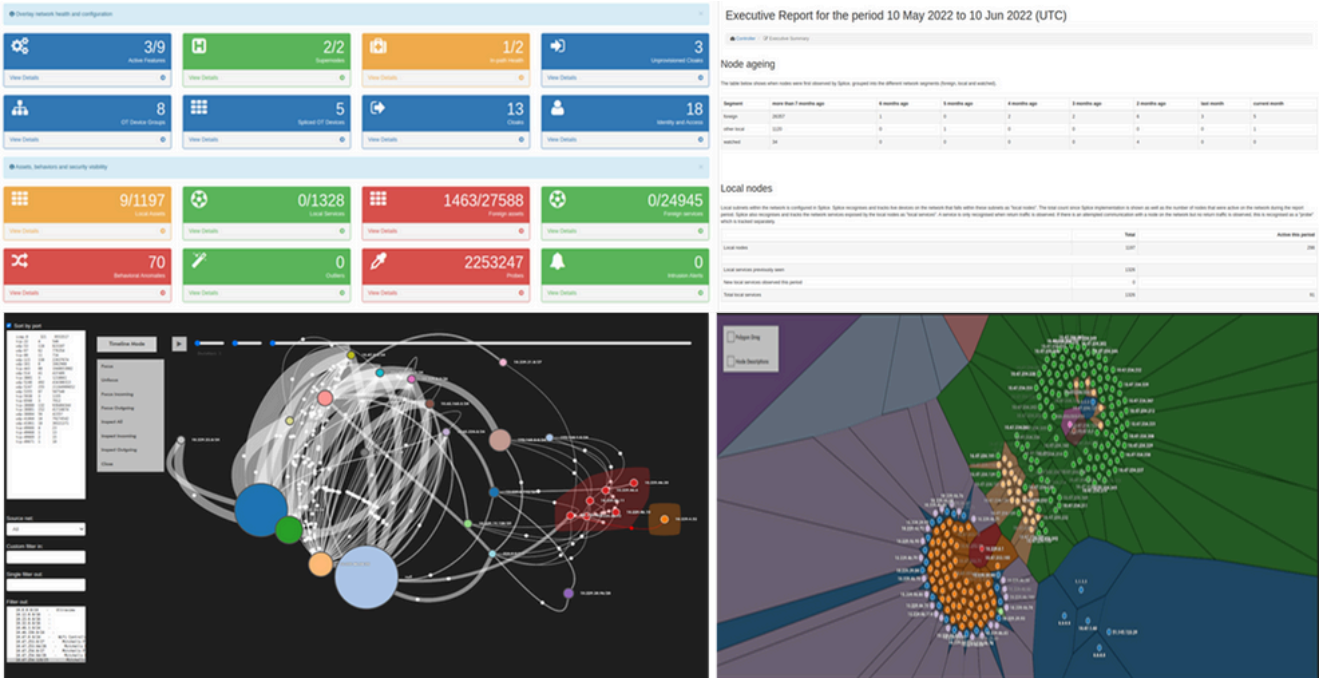
OT CYBER SECURITY

THE SMARTE SOLUTION - SPLICE:

smaRTE Splice actively prevents cyber-physical attacks by providing:

- Logical isolation within the control network core (rather than at the perimeter)
- Profiling of the entire control network traffic & full forensic audit trails (with visualisation of the “network universe”)
- Vulnerability shielding inside an encrypted overlay network
- Intrusion inspection
- Behavioural profiling & advanced machine learning-driven outlier & anomaly detection
- Passive node discovery & tracking
- Secure identity management
- Multi-factor authentication offloading
- Secure remote access for operators, engineers & support partners

Dashboard Examples:



OT CYBER SECURITY

THE BUSINESS BENEFITS:

- Actively reduces cyber exposure of all connected operational assets
- No rip-and-replace of existing network assets
- Continue operating with vulnerable equipment out in the field
- Enables passive asset management
- Increases asset uptime and production reliability

ROI < 1 YEAR!

INCREASE ROOA BY 10% OR MORE

CONTACT US TO FIND OUT MORE!

Website: www.flexdigitalsolutions.com

Email: info@flexdigitalsolutions.com

Phone: +27 (0)10 023 9044