BLOCK

A compromised infusion pump shouldn't be able to take down a hospital's entire network.

FutureNow Networks give NHS organisations a self-defending campus fabric. One that identifies every device on the network, contains threats automatically, and turns cyber assessment principles into daily operational reality.



THE BUSINESS CASE

Evidence a finance director and network engineer can both sign off on

Independent analysis of large-enterprise deployments shows what a software-defined fabric returns in staff time, breach impact, and total cost.

67%
Savings in network provisioning time[1]

80%
Less time to issue resolution[1]

462%
within five years ROI[2]

48%
Reduced impact from a security breach[1]

45%
Reduced total cost of operation[1]

49%
More efficient network management staff[1]

[1] Internal TCO analysis with large-enterprise customer. Actual results may vary by site and estate size. [2] IDC business value study of Cisco Catalyst

THE ARCHITECTURE

Three components, one fabric across every site

FutureNow Networks unify wired and wireless, as well as acute and community sites, under a single automated policy model. This replaces manual VLAN changes and one-off firewall rules with intent that's defined once and enforced everywhere.

CONTROL

Catalyst Center

The SDN controller. Network and infrastructure teams design, provision, and apply policy from one console, with real-time assurance telemetry across every ward, site, and ICB location.

POLICY

Identity Services Engine (ISE)

Authenticates every clinician, device, and system, then applies Scalable Group Tags so access is granted by role and risk - not by which port or VLAN something is plugged into.

FABRIC

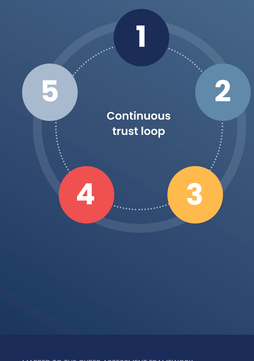
SDA Fabric

A programmable overlay across the physical estate. One infrastructure investment can host many logical networks: clinical, corporate, guest, IoMT. Each network is isolated from the others.

HOW IT OPERATES

A continuous Zero Trust cycle, not a one-off project

FutureNow Networks run a standing loop of identification, segmentation, verification and response, rather than a static configuration set once at go-live. This is the same loop that assessors expect to see evidenced under the Cyber Assessment Framework (CAF).



Identify and profile every endpoint
AI-driven and machine learning-based analytics fingerprint equipment such as blood-gas analysers for infusion pumps as well as BYOD the moment they connect.

Segment by policy, not by port
Group-based access separates clinical, corporate, guest, and IoMT traffic with macro- and micro-segmentation from a single design.

Verify trust continuously
Endpoint behaviour is continuously monitored for risky behaviours, with a scoring system that allows network policy to respond to events as they occur.

Steer suspect traffic to inspection
Traffic from high-risk sources is routed to firewalls for stateful inspection before it ever reaches the wider estate.

Contain and isolate automatically
Compromised or rogue endpoints are quarantined in place, shrinking the blast radius before a human needs to act.

MAPPED TO THE CYBER ASSESSMENT FRAMEWORK

Built for the evidence DSPT assessors actually ask for

The CAF-aligned Data Security and Protection Toolkit (DSPT) moved the NHS from checklist compliance to outcome-based principles. Intent-based networking gives you the live, technical evidence behind each objective, not a policy document describing intent.



OBJECTIVE A: Managing security risk

A live, accurate asset inventory

A3: Every IoMT device is discovered, profiled, and registered automatically. This closes the blind spots that legacy, flat networks leave around unmanaged clinical devices.

OBJECTIVE B: Protecting against cyber attack

Access that follows the clinician, not the port

B2/B3: Identity-based micro-segmentation grants a clinician access to the EPR system according to role and device posture, instead of static VLANs.

B5: Self-healing fabric reroutes clinical traffic around a failed switch or link in milliseconds, with no human intervention required.

OBJECTIVE C: Detecting cyber security events

Signal, not noise, from the network itself

C1/C2: AI-driven telemetry baselines normal traffic and flags lateral scanning or exfiltration attempts from a compromised legacy device immediately.

OBJECTIVE D: MINIMISING THE IMPACT OF INCIDENTS

Contain in seconds, not hours

D1/D2: A single command builds a digital quarantine zone around an affected network segment or site. This halts lateral movement while unaffected wards stay online.

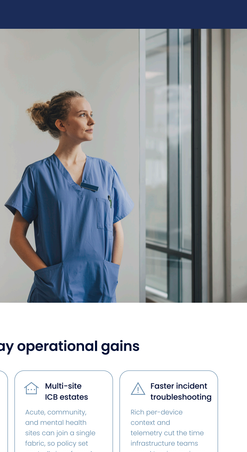
THE SCENARIO EVERY CIO PLANS FOR

When ransomware reaches a ward, only that ward goes dark.

In a flat network, one infected workstation can become a route to every site on the ICB. In a FutureNow Network, the same device sits inside a policy boundary that was already there before the attack started.

Network teams isolate the compromised assets with a single command or automated playbook instantly, without waiting for a firewall change request or a late-night bridge call.

The result is that your essential services (theatres, ICU, pharmacy dispensing) can keep running on within the affected segment while the incident is contained and investigated.



WHERE THIS SHOWS UP DAY-TO-DAY

Beyond the incident: everyday operational gains

IoMT device onboarding
New infusion pumps, monitors, and imaging kit are profiled and segmented automatically. No manual VLAN request per device.

Patient & visitor Wi-Fi
Guest access is policy-defined once, then applied consistently across every site, with no route into clinical systems.

Multi-site ICB estates
Acute, community, and mental health sites can join a single fabric, so policy set centrally is enforced identically everywhere.

Faster incident troubleshooting
Rich per-device context and telemetry cut the time infrastructure teams spend tracing an issue across sites.

Clinician mobility
Consistent identity and policy follow staff as they roam between wards, sites, and device types, wired or wireless.

Data centre & cloud policy
Identity federation extends the same access policy from the campus into data centre and multi-cloud clinical systems.

Regulatory evidence
Assurance analytics generate the live, defensible evidence that assessors expect under the CAF-aligned DSPT.

Reduced attack surface
Device segmentation by default limits what a compromised or rogue endpoint can reach, before any incident occurs.

Get in touch with our team to find out what a FutureNow Network could look like for your NHS Trust.

www.block.co.uk