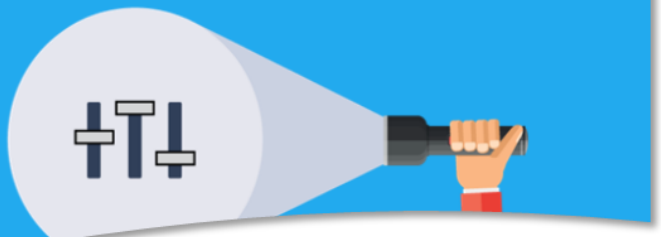
Device Visibility & Control

You can't effectively manage what you can't effectively see or control



Device Visibility and Control, why now?

- Cyber Resilience is a key priority on all boardroom agendas
- Billions of devices connected to organisations' networks worldwide
- The average CIO will be responsible for securing more than 3 times the number of endpoints in 2023 compared to 2018
- The biggest growth of devices is in IoT and IIoT, which cannot have agent monitoring software installed
- The merging of IT and OT due to digital transformation
- 100% device visibility in real time to support the 'new way of working'

CounterACT combined with C-STEM's expertise *"blew the competition out of the water."*

Systems Engineer
Education

The Challenge

Designing and modernising architecture to enhance interoperability between individuals, business units and ecosystems, as required to achieve targeted business outcomes. Maintaining and evidencing the secure and consistent delivery of an effective user experience pre, during and after change.

Area of Focus - Cyber Resilience

C-STEM SMART device security services offer consultancy, design, engineering and the complementary phased introduction of best of breed technology, which is proven to impact business outcomes in digital transformation. Whether there is a need to overcome challenges in 1 or multiple areas, C-STEM can provide the right solution designed to complement existing systems and tools, reduce time & effort and cost effectively bridge the gaps.
Five real world scenarios are:

Asset Management	An accurate picture of connected endpoints, infrastructure components and BYOD/ IoT devices.
Device Compliance	Detect and take action against suspicious/rogue endpoints the instant they access the network. Achieve device compliance without the administrative burden software agents.
Network Access Control	Control access to confidential data based on device and user profiles. Prevent infected or noncompliant devices from spreading malware. Automatically enforce actions.
Network Segmentation	Gain visibility and control of what and how devices are communicating. Dynamically assign segments as the network and/or devices change.
Incident Response	Remediate mis-configured, vulnerable & non-compliant virtual & physical devices. Hunt for vulnerabilities, IOCs & other attributes provided by leading threat detection, VA & SIEM vendors.

Hassle Free Engagement

To assist with qualifying a complementary fit, C-STEM has evolved a 3 stage collaborative process to empower business leaders and heads of IT with a minimum to no disruption risk free efficient evaluation. This includes:

Qualifying existing technologies & services; Accurately scoping and defining success criteria; Assessment, testing & evidence based reporting.

The Solution powered by

SMART Services

- ✓ Comprehensive continuous monitoring
- ✓ Agentless deployment
- ✓ Fragmentation reduction
- ✓ Automated response and re-mediation
- ✓ Rapid installation
- ✓ No need to replace existing systems
- ✓ Complementary professional services
- ✓ Reduced demands on time and resource

Kick start the acceleration of your digital transformation journey with our hassle free assessment, gap analysis and risk report