Arc CyberShield

# Building a Secure Digital Tomorrow, Today

# CONTENTS

# The Ever-Evolving Threat of Cyber Attacks

You would not leave your office unlocked or unattended. So why would you do that to your digital networks? Your digital operations are just as vulnerable, if not more.

Our growing need for an always-on connectivity at work and in our daily lives via cloud technology has led to increased exposure to progressively sophisticated cybercrimes.

Without a solid cybersecurity system in place, you're leaving your organisation open to cyber attacks such as malware, phishing, identity theft, data breaches, and much more. These attacks can negatively impact a company's credibility and reputation, not to mention the financial cost associated with these attacks.

A 2022 study by Kaspersky reported that 88% of executives from companies previously victimised by ransomware said they would pay if attacked again.

Those threats are clearly demonstrated by cases such as the 2021 ransomware attack on JBS—the world's largest meat processing company, where the company paid the equivalent of US$11m to resolve the cyber-attack. In a separate incident, US-based Colonial Pipeline was forced to pay US$4.4m in ransom when fuel delivery in the southeast of the US was crippled for several days.

What would you do if you were locked out of your company's computer system and lost access to all your business and customer data? Most companies would give in and pay—often up to millions in ransom— to regain access to their data. It's a natural reaction under the circumstances.

So how do you protect your digital network?

# Cybersecurity Encryption

Arc CyberShield's state-of-the-art cybersecurity encryption solutions are developed in partnership with ST Engineering, providing businesses and organisations with the best of our combined technical experience and service excellence.

## Secure Network

Our encryptors secure the network and connect to multiple sites on public internet / private IP infrastructure. The customised encryption is ideal for different security requirements and applications.

### FEATURES

- Enhanced security with unique encryption keys with our Key Management System.
- Ability to configure as a layer-3 or layer-2 encryption tunneling device to fulfill the various infrastructure requirements desired
- Deployable as a security gateway for office corporate LANs, site-to-site VPNs, mobile vehicles, rugged deployment, or wireless inter-office connectivity.
- Customisable algorithm available to safeguard your data in transit.

## Netcrypt Series

### NetCrypt U1000

IP Layer Encryptor ideal for deployment as a security gateway in corporate LANs, site-to-site VPNs and wireless inter-office connectivity.

### NetCrypt S20

IP Layer Encryptor ideal for deployment as a security gateway of office corporate LANs, site to-site VPNs, mobile vehicles and wireless inter-office connectivity.

National IT Evaluation Scheme

CERTIFIED EAL4+

## Netcrypt Mini

Thumbdrive size IP encryptor is ideal for remote work and mobile users as a security gateway of office corporate LANs, WIFI and 5G/4G connectivity

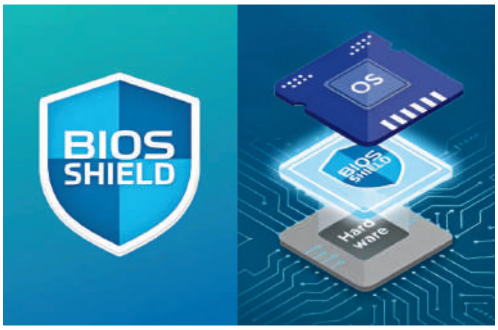
CES INNOVATION AWARDS 2022

# Secure Workspace

## BIOS-SHIELD® Series

BIOS-SHIELD® is a cutting-edge technology that simplifies users' experience in managing their endpoints in a safe and cyber-resilient environment. It provides security at your convenience for both users and organisations. It allows users to securely operate in both trusted (intranet) and untrusted (internet) environments without compromising productivity.

BIOS-SHIELD® will significantly enhance any existing endpoint security software in enterprise IT. With BIOS-SHIELD®, organisations will be empowered to have full control of their endpoints, and when needed, conduct swift responses to threats and execute prompt recovery actions.



Through its hardware-defined segregation technology, the system safely performs isolation in guarding against any exploitation, such as ransomware. BIOS-SHIELD® is the stealth cybersecurity solution that definitively eliminates endpoint vulnerabilities. This solution is virtually undetectable. It sits on the BIOS layer (located outside and below the OS), which is hard to detect and bypass, making it difficult for attackers to compromise the endpoint.

## FEATURES

### Shield Browser

- Enables access to all websites on the browser that operate separately from the OS, while preventing the risk of importing malware.

### Segmentation of User Clusters

- Allows grouping of users to prevent cross sharing of data via USB storage devices. For example, Finance Department computers can be segmented to prevent data transfer into Sales Department computers, which are enabled by BIOS-SHIELD®.

### Manage and Respond

- Centralised management system.
- Ease of deployment and recovery of endpoint.

### Time Machine Snapshot

- Quick recovery to the last saved snapshot in the hard drive.

### Data Protection

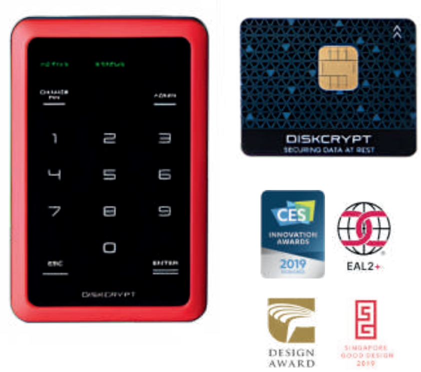
- Hard drive encryption protects data at rest from malicious insiders and hackers.
- USB port encryption which cannot be disabled by malware.

# Secure Storage

## Diskcrypt Series

### DiskCrypt M10

The world's first ultra-slim 2FA encrypted data storage helps users secure their information with enhanced cybersecurity capabilities. Coupled with its ultra-slim profile comparable to a credit card size, DiskCrypt M10 also comes in 6 vibrant colours. It offers unrivalled mobility and style to the modern workforce.



Colours :

## FEATURES

Enhanced Storage Security with two-factor authentication (2FA) smartcard (FIPS and CC certified) and AES-XTS 256 bits.

High performance with M.2 (SATA III) SSD and high-speed USB 3.1 and SATA III interfaces.

World's first ultra-slim encrypted data storage (Size of a credit card).

Ease of use with no software installation, upgrades or patches required.

# Cross Domain

Enjoy secure transfer of data between different security domains and isolated networks with our Data Diode. Besides being certified to Common Criteria cybersecurity standards for government use, our Data Diode features robust one-way physical controls to prevent leakage with file loss detection and a compact, interoperable design for secure connectivity across disparate systems.

## Data Diode

Data Diode is a unidirectional communication and data transfer gateway that enables organisations to transfer data securely across physically separated networks. Its security design prevents data leakage and eliminates cyber threats by enforcing the one-way data transfer at both the physical and protocol layers. The high-performance solution comes in a compact design that integrates seamlessly with users' operational environments.

Data Diode 300 Series

Data Diode 500 Series

COMMON CRITERIA CERTIFIED EAL4+

National IT Evaluation Scheme BY CYBER SECURITY AGENCY OF SINGAPORE

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

## FEATURES

### Information Assurance by Design

- Ensures no data leakage due to hardware-enforced one-way communication.
- Certified under Common Criteria (CC EAL4+) and NITES* by CSA.

### Enhanced Performance with Patented Technology

- Patented SFP+ ensures unidirectional communication with 99.99% high availability.
- Zero-loss files transfer with File Loss Detection capability.

### Ease of System Integration and Customisation

- Integrated Management Portal for ease of deployment, operation & maintenance.
- Stackable hardware for integration of 3rd party solution.

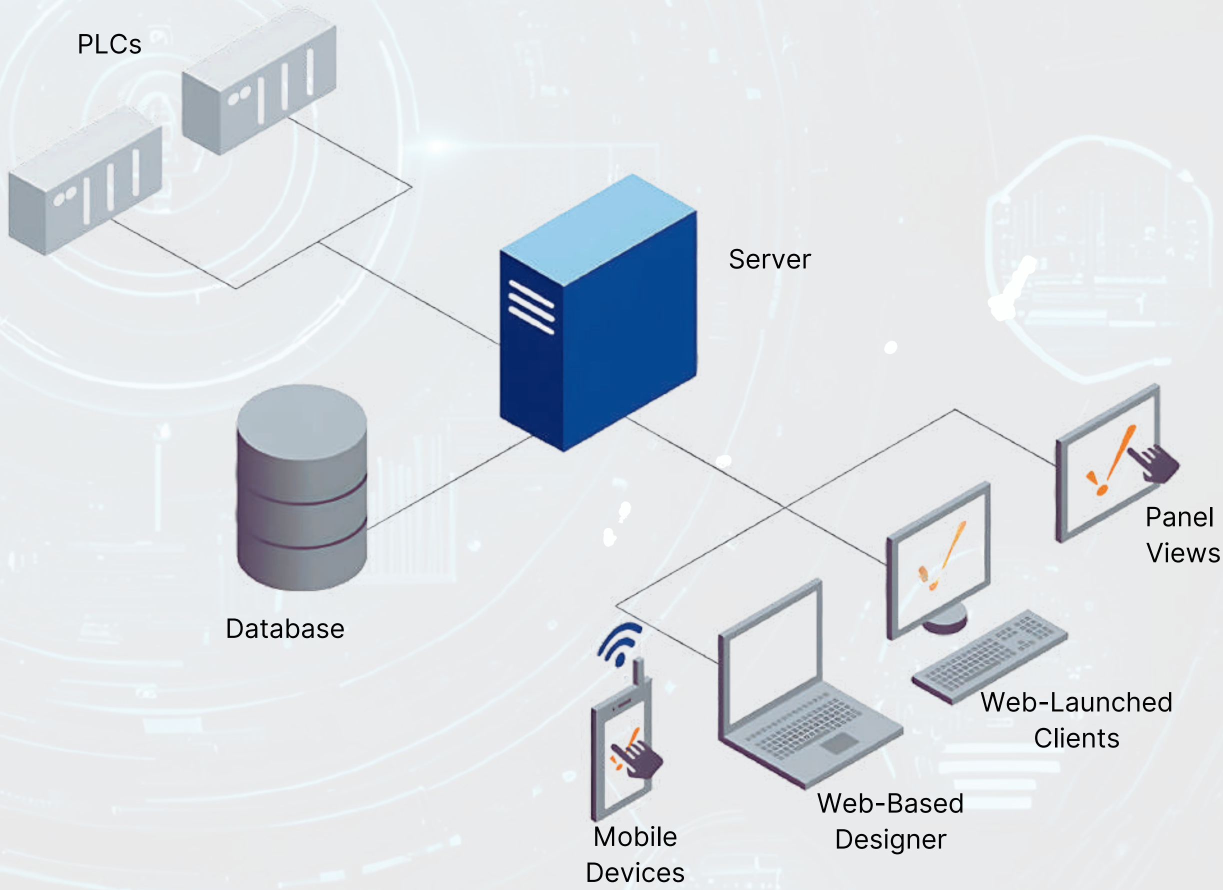
### Compact Design

- Allows all functionalities to be encapsulated within a compact footprint.

# Cybersecurity System

Designed for industrial operational technology (OT) environments like power plants, water treatment plants, and ports, our innovative cybersecurity solutions are integrated with IT security tools like Security Information and Event Management (SIEM) and sophisticated firewalls.

This allows you to monitor your ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition) systems for anomalies and cyber threats, besides enabling early detection of attacks against critical infrastructure to protect physical operations across converged IT/OT networks.



## OT Cybersecurity

### Product

Radiflow ISID,ISAP,ICEN,CIARA

- OT Network monitoring & anomaly detection
- Level 0 Monitoring

### Services

- Design & Implementation of secure architecture for OT networks
- OT Risk Assessments
- OT MSS

### People

OT Certifications – GICSP, GRID & ISA/IEC 62443

### KEY CUSTOMER

Defence

Security & Emergency

Banking & Finance

Vehicle

Healthcare

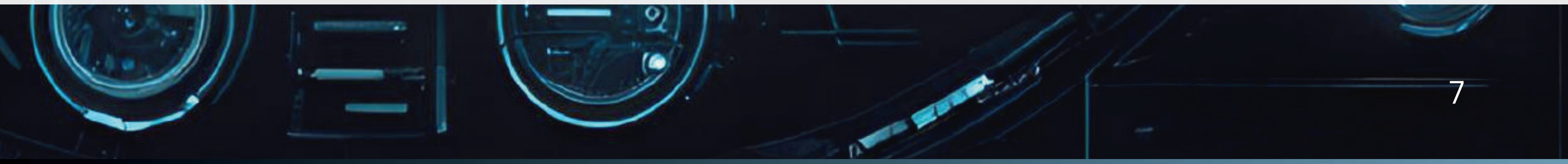
Government

Aviation

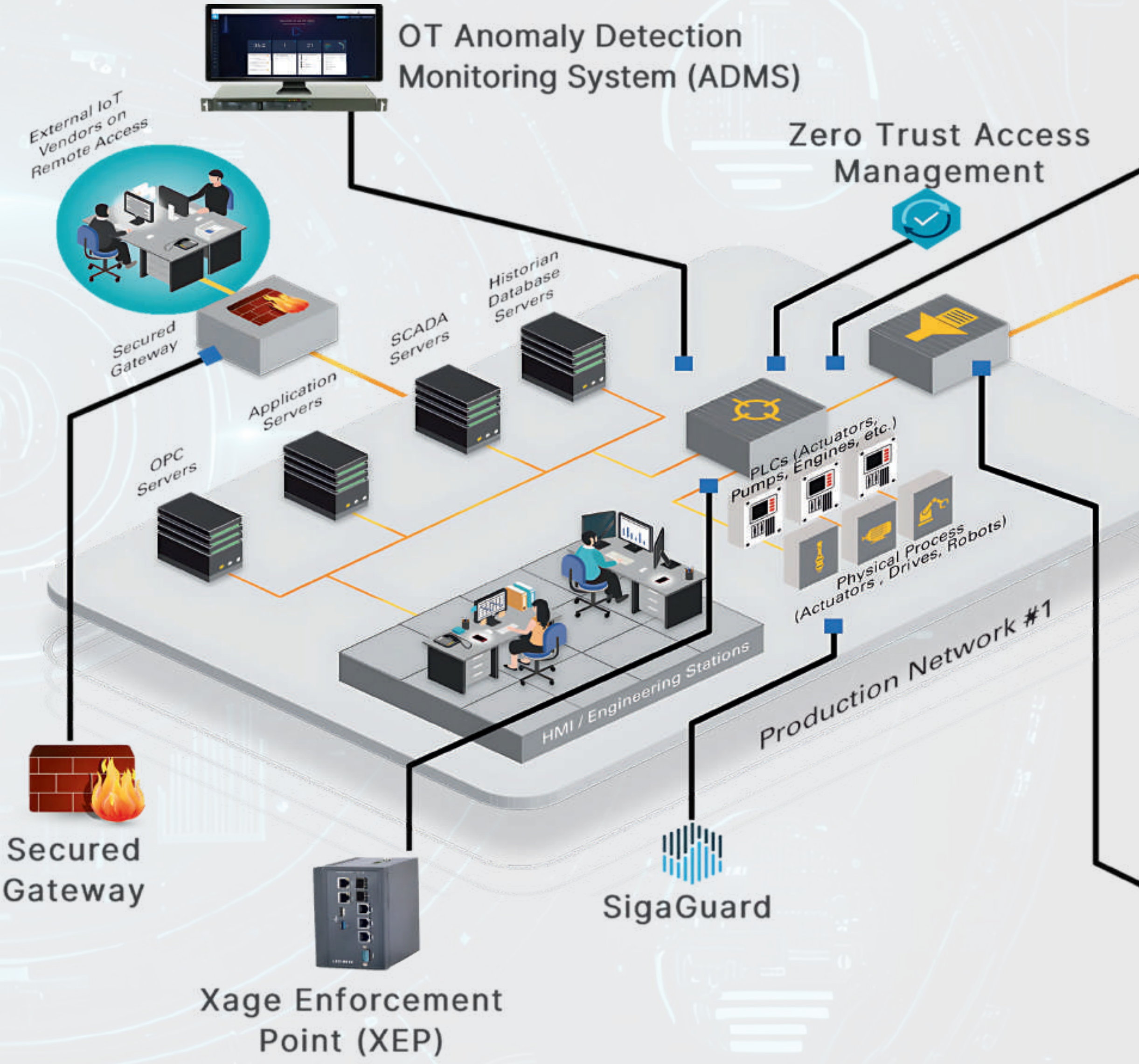
Maritime

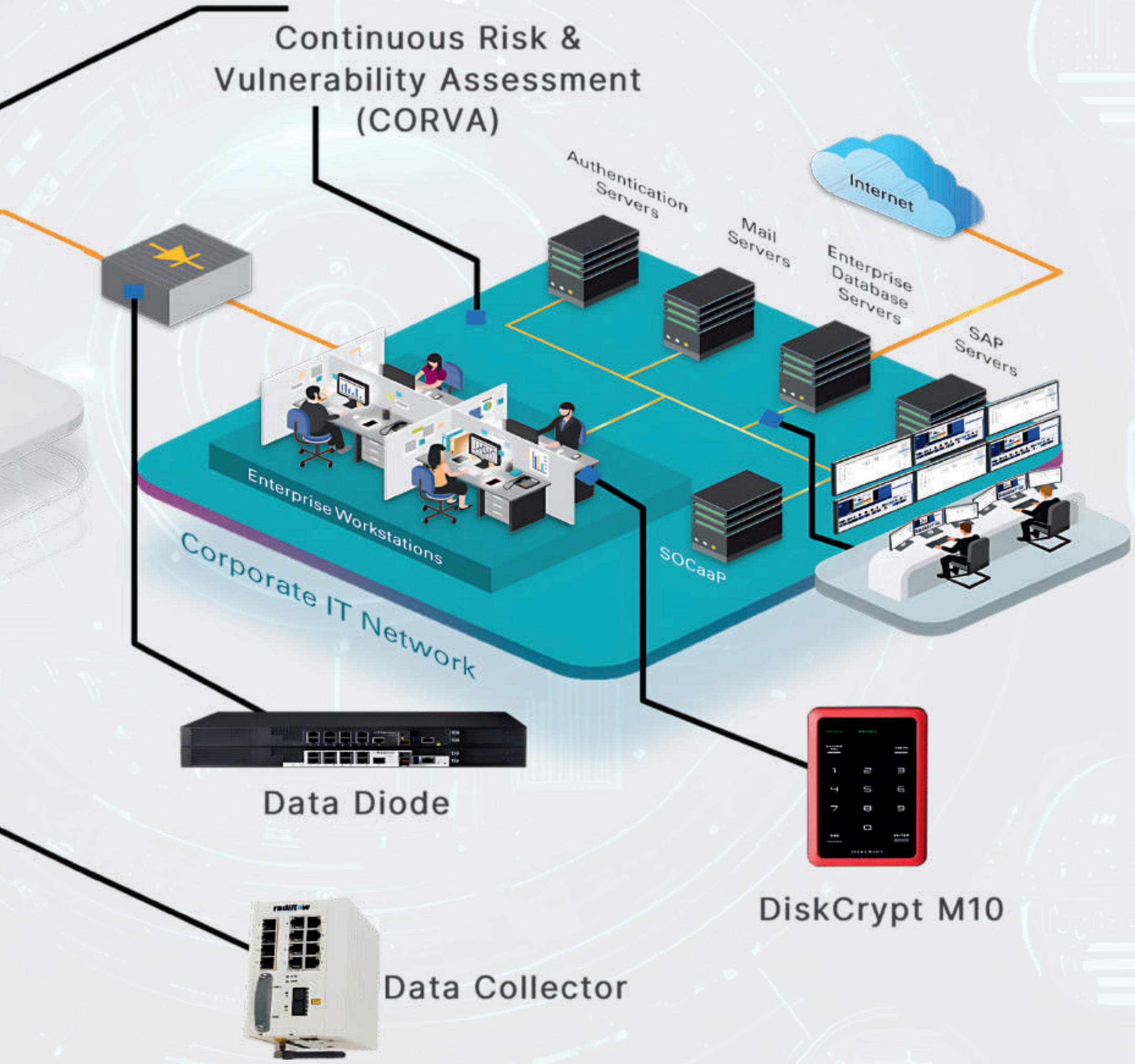
Water & Energy

Infocom



# Our Holistic Solution For OT & IT Networks


OT Anomaly Detection Monitoring System (ADMS)
Zero Trust Access Management
External IoT Vendors on Remote Access
Secured Gateway
Historian Database Servers
SCADA Servers
Application Servers
OPC Servers
PLCs (Actuators, Pumps, Engines, etc.)
Physical Process (Actuators, Drives, Robots)
HMI / Engineering Stations
Production Network #1
Secured Gateway
Xage Enforcement Point (XEP)
SigaGuard


Continuous Risk &
Vulnerability Assessment
(CORVA)
Authentication Servers
Mail Servers
Internet
Enterprise Database Servers
SAP Servers
Enterprise Workstations
Corporate IT Network
SOCaaP
Data Diode
DiskCrypt M10
Data Collector

# Digital Twin - Cybersecurity Simulator

In the Oil & Gas, Petrochemical, Power industries for building & infrastructures, Arc Technologies can create a training environment for the IT engineers and operators. A Digital Twin of the Cyber Security ecosystem of an actual 'live' plant is replicated and can be incorporated to provide an even more realistic training experience.

## KEY CUSTOMER

Defence

Building

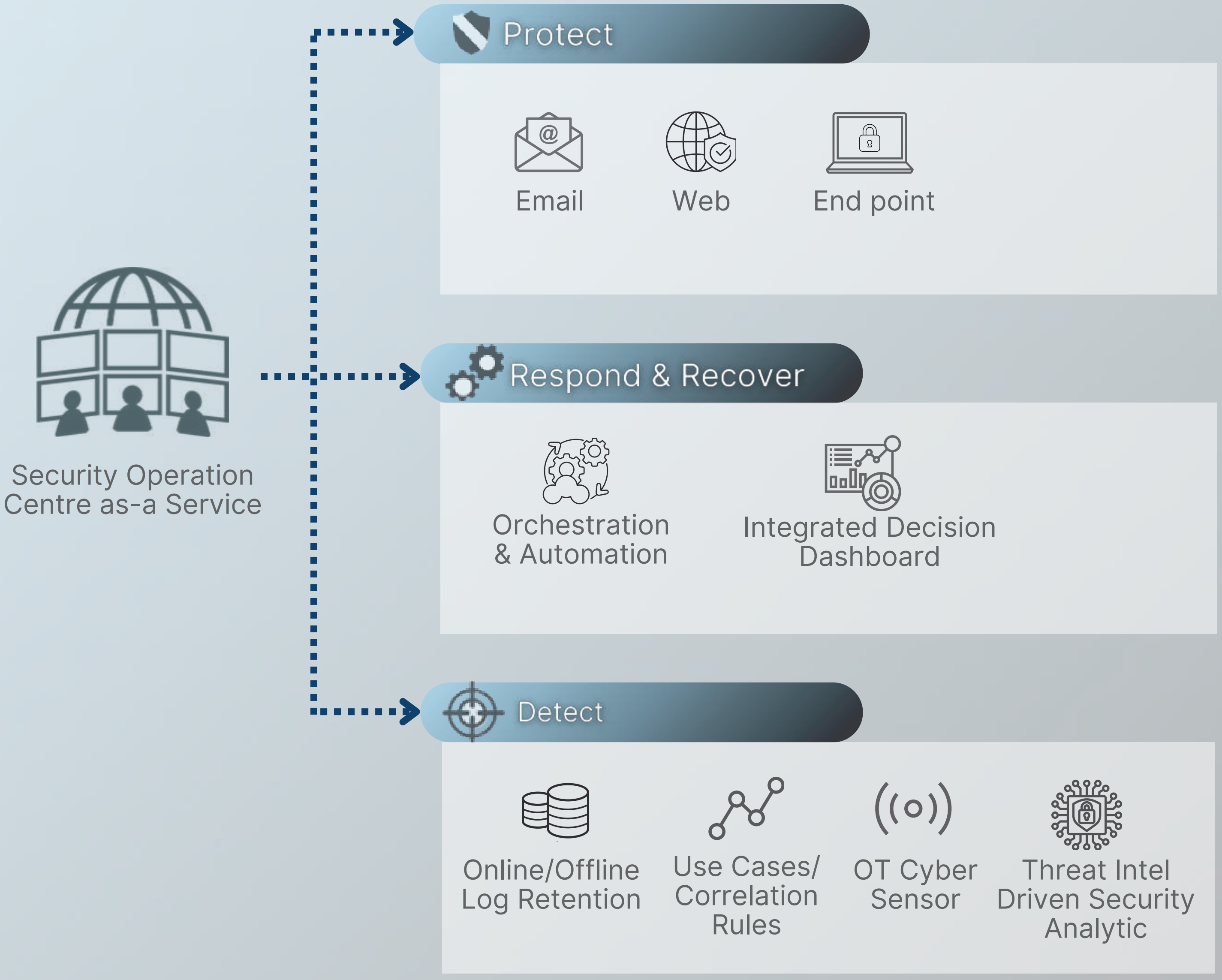
Infrastructure

Marine

# Cybersecurity Operation Centre

## 24/7 SOC-as-a-service

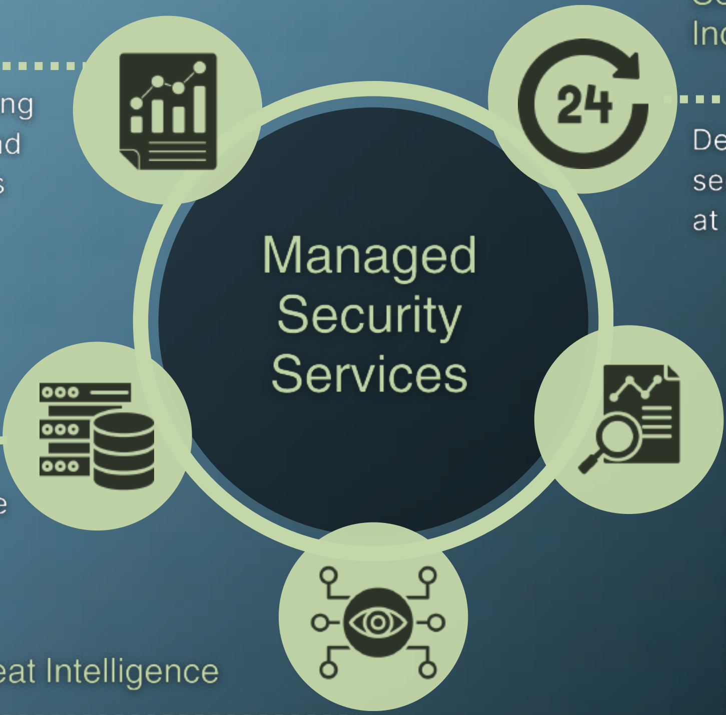
From design, build and operating more than 20 SOCs across nations, with our technology partner, ST Engineering, we bring to you this unified solution that combines machine-based analytics, contextualized threat intelligence and security orchestration, automation and response (SOAR). Allow Arc Technologies to manage your security operations centre with our highly skilled cybersecurity personnels.


Security Operation Centre as-a Service
Protect
Email
Web
End point
Respond & Recover
Orchestration & Automation
Integrated Decision Dashboard
Detect
Online/Offline Log Retention
Use Cases/ Correlation Rules
OT Cyber Sensor
Threat Intel Driven Security Analytic

# Managed Security Services

## Managed Security Services

Our comprehensive managed security services (MSS) provide your organisation's security team with the required expertise and services cost-effectively.  It is designed to adapt to specific enterprise requirements and built to provide a cyber-secure and resilient environment to grow your business with confidence. We provide organisations with intelligence-driven, proactive and managed real-time cybersecurity monitoring and alerts through our managed security services. Powered by our Cybersecurity Operation Centre, we provide state-of-the-art monitoring of your IT & OT infrastructure against cyber-attacks, making security monitoring and detection work for you.



### Quarterly Reviews

Agreed upon monitoring metrics, conditions and service improvements

### 24/7 Real-time Security Monitoring & Incident Management

Dedicated 24/7 team of security professionals at our SOC

### Enterprise Grade Log Storage

Software defined storage solutions with build-in redundancy

### Incident Analysis & Reporting

When events are alerted, the SOC team will perform their triage. An actionable insights will be presented to you with the appropriate remediation measures. An incident management portal gives you real-time visibility to address the incidents with the SOC and retrieve incident reports.

### Threat Intelligence

Applies ongoing knowledge of threat intelligence to continuously assess monitored conditions and intelligence that are contextualised to your environment

# Compromise Assessment

Arc provides compromise assessment service through evaluation of a client's environment to determine if they have been compromised and to identify the extent of the breach. The following explains the steps involved in a compromise assessment service:

## 1 INITIAL CONSULTATION AND SCOPING

- Meet with the client to understand their concerns and the extent of the suspected compromise.
- Gather information about the client's infrastructure, including network diagrams, asset inventories, and access controls.
- Define the scope of the assessment, including systems, networks, and data repositories to be examined.

## 2 PREPARATION AND PLANNING

- Develop a detailed plan and timeline for the assessment, including objectives, milestones, and deliverables.
- Assemble a team of skilled professionals with experience in incident response, digital forensics, and threat hunting.
- Obtain the necessary access credentials, permissions, and tools required for the assessment.

## 3 DATA COLLECTION AND ANALYSIS

- Collect and analyze relevant data, including system logs, network traffic, and endpoint artifacts.
- Arc installs ThreatSonar* agent to all the workstations and servers to scan and search for artifacts, threats, or hacking tools.
- Use advanced threat hunting techniques to search for signs of compromise, such as suspicious processes, network connections, and file activities.
- Analyze the collected data to identify indicators of compromise (IOCs), unusual patterns, and potential attack vectors.

## 4 INCIDENT VALIDATION AND CONTAINMENT

- Validate identified incidents by correlating them with known IOCs, threat intelligence, and historical data.
- If a compromise is confirmed, work with the client to contain the incident and prevent further damage.
- Implement short-term remediation measures, such as isolating affected systems, blocking malicious IP addresses, and resetting compromised credentials.

## 5 ROOT CAUSE ANALYSIS AND REMEDIATION

- Collect and analyze relevant data, including system logs, network traffic, and endpoint artifacts.
- Arc installs ThreatSonar* agent to all the workstations and servers to scan and search for artifacts, threats, or hacking tools.
- Use advanced threat hunting techniques to search for signs of compromise, such as suspicious processes, network connections, and file activities.
- Analyze the collected data to identify indicators of compromise (IOCs), unusual patterns, and potential attack vectors.

## 6 REPORTING AND DOCUMENTATION

- Validate identified incidents by correlating them with known IOCs,threat intelligence, andhistorical data.
- If a compromise is confirmed, work with the client to contain the incident andprevent further damage.
- Implement short-term remediation measures, suchas isolating affected systems, blocking malicious IPaddresses, andresetting compromised credentials.

ThreatSonar

An Engine to Hunt down Intruders

## Threat Forensic Analysis Platform

An easy-to-use & automated deployed threat hunting tool in a breached environment

### Easy To Understand

The threat forensic reports are easy to understand

### Easy To Deploy

It can be deployed to endpoints through the dispatch mechanism of corporate software. The deployment process only takes a little bit of network bandwidth, system resource, and detection time.

### Execute Digital Forensic Efficiently & Accurately

It can be deployed to endpoints through the dispatch mechanism of corporate software. The deployment process only takes a little bit of network bandwidth, system resource, and detection time.

### On-Premise & Cloud Modde

Incident response function can be activated remotely or offline in order to grasp the status of each endpoint.

## Main Features of ThreatSonar

### Smart Forensics

- APT risk models trained with real cases.
- Identify hundreds of abnormal dynamic behaviors automatically e.g. memory, files, network connections, system login files, event logs, work schedules, boot sectors, WMI, and startup processes, etc.

### Intelligence Driven

- Carry third-party intelligence to each endpoint.
- Thousands of APT backdoor signatures are built-in.
- Able to compare intelligence through the cloud or offline.
- Allow importing external intelligence, including hash, IP, domain, Yara Rule, and IoC, etc.

### Automatic Investigation and Analysis

- Discover the sources and processes of attack incidents.
- Actively discover hidden TTPs threats often used by hacker groups.
- Track intranet movement footprints and data outflow paths.
- Incident timelines are used to present the sequence.
- Graphical and visual methods are used to display threat incidents.

### Threat Hunting

- Statistical association analysis is used to identify unknown attack techniques.
- Establish baselines to lock on abnormal behaviors.
- Tag hidden unknown threats e.g. abuse of rare programs, folders, or legal system tools in the organization; malware with digital signature, etc.

### Automatic Defense

- Open API integrates existing protection equipment.
- Automatic transmission of alarms and intelligence updates.
- Send CEF warning to SIEM to set rules for blocking. Restful API downloads reports and samples.
- Programmatic intelligence update and adjustment of detection rules.

# ABOUT US

## What We Do?

Arc CyberShield provides world-class cybersecurity solutions for Malaysian businesses and government agencies. Developed in partnership with world-leading cybersecurity experts ECQ and
ST Engineering, Arc CyberShield offers a powerful suite of cutting-edge digital security services customised to your specific business needs and goals.

Arc CyberShield is the cybersecurity arm of Arc Technologies—an innovative tech solutions provider specialising in advanced cybersecurity and intelligent systems.

## A Forward-Thinking Approach

We don't just sell cybersecurity solutions. Our focus is on futureproofing your business operations as you embark on your digital transformation. This means ensuring a solid cybersecurity framework for your digital operations from the very beginning, designed to scale in tandem as your business grows.

# MISSION & VALUES

Arc Technologies is on a mission to create progressive, secure, and sustainable intelligent cities in Malaysia using state-of-the-art technological solutions.

Our services and solutions are designed with the following values as our guiding principles:

## Innovative

We believe in continuously developing new and improved software solutions that utilise the latest cutting-edge technologies in cybersecurity and intelligent systems, to keep your organisation ahead of the curve.

## Secure

With cybercrime on the rise and growing more sophisticated by the day, cybersecurity is no longer optional but a prerequisite for all digital environments. We're committed to ensuring the highest standards of cybersecurity for all our customers and projects.

## Sustainable

As we continue to experience the harsh effects of climate change, Arc Technologies is committed to creating sustainable, intelligent cities in Malaysia that will help curb our collective environmental impact and allow Earth to regenerate.

# WHY PARTNER WITH US

## We Care About Your Long-Term Growth

We believe in continuously developing new and improved software solutions that utilise the latest cutting-edge technologies in cybersecurity and intelligent systems, to keep your organisation ahead of the curve.

## Innovative Solutions Tailored to Your Needs

By partnering with established international cybersecurity experts with specialised know-how and real-world experience, we're able to offer state-of-the-art cybersecurity solutions customised to your unique business needs.

## Robust Cyber Protection From Day 1

Our solutions are designed to scale with your digital transformation, customised to offer the appropriate protection levels at different stages of your digital expansion. This ensures ironclad cybersecurity for your organisation from day 1.

## In-House Security Operations Centre (SOC)

We believe in continuously developing new and improved software solutions that utilise the latest cutting-edge technologies in cybersecurity and intelligent systems, to keep your organisation ahead of the curve.

## Vast Industry Experience

Arc Technologies is founded by a management team with a combined 50 years of experience in the technology and software industry, with deep expertise in innovative IT solutions.

# OUR PARTNERS

ecq

ECQ is a network security company specialising in offensive security services and solutions, established in Thailand, Vietnam and Singapore. They have a proven track record in providing superior consultancy services for clients in the financial and infrastructure sectors, as well as service providers and government agencies. Arc CyberShield partners with ECQ in offering our Cybersecurity Awareness Training Programmes and Vulnerability Assessments & Penetration Testing services.

OFFENSIVE security OSCE
OFFENSIVE security OSWE
OFFENSIVE security OSCP
OFFENSIVE security OSWP
GXPN
GWAPT
GREM
GRID
GPEN
GSEC
CREST
CISSP

ST Engineering

ST Engineering is a renowned Singaporean multinational technology and engineering group with a global network of subsidiaries and associated companies across Asia, Europe, the Middle East, and the U.S. The company's diverse security portfolio spans aerospace, smart city, digital solutions, defence, and public security segments. Arc CyberShield's software and hardware cybersecurity solutions are offered in partnership with ST Engineering.

ISA/IEC 62443 CYBERSECURITY EXPERT
GRID
GICSP
CREST
CDPSE
GSEC
GCCC
CISA
CISM
CRISC
OFFENSIVE security OSCP
CISSP

Arc Technologies

Lot 304, 3rd Floor,
The Spring Shopping Mall,
Persiaran Spring, 93300
Kuching, Sarawak

+6010-961 1515
info@arctechnologies.io
arctechnologies.io