CONTROL UNDER PRESSURE

When something slips through, what can still be controlled?

Explore how the S10 operational containment platform helps organisations maintain governability under pressure.

THE FUTURE RESILIENCE CHALLENGE

The future resilience challenge is not whether organisations can see what is happening.

It is whether they can still govern what happens next.

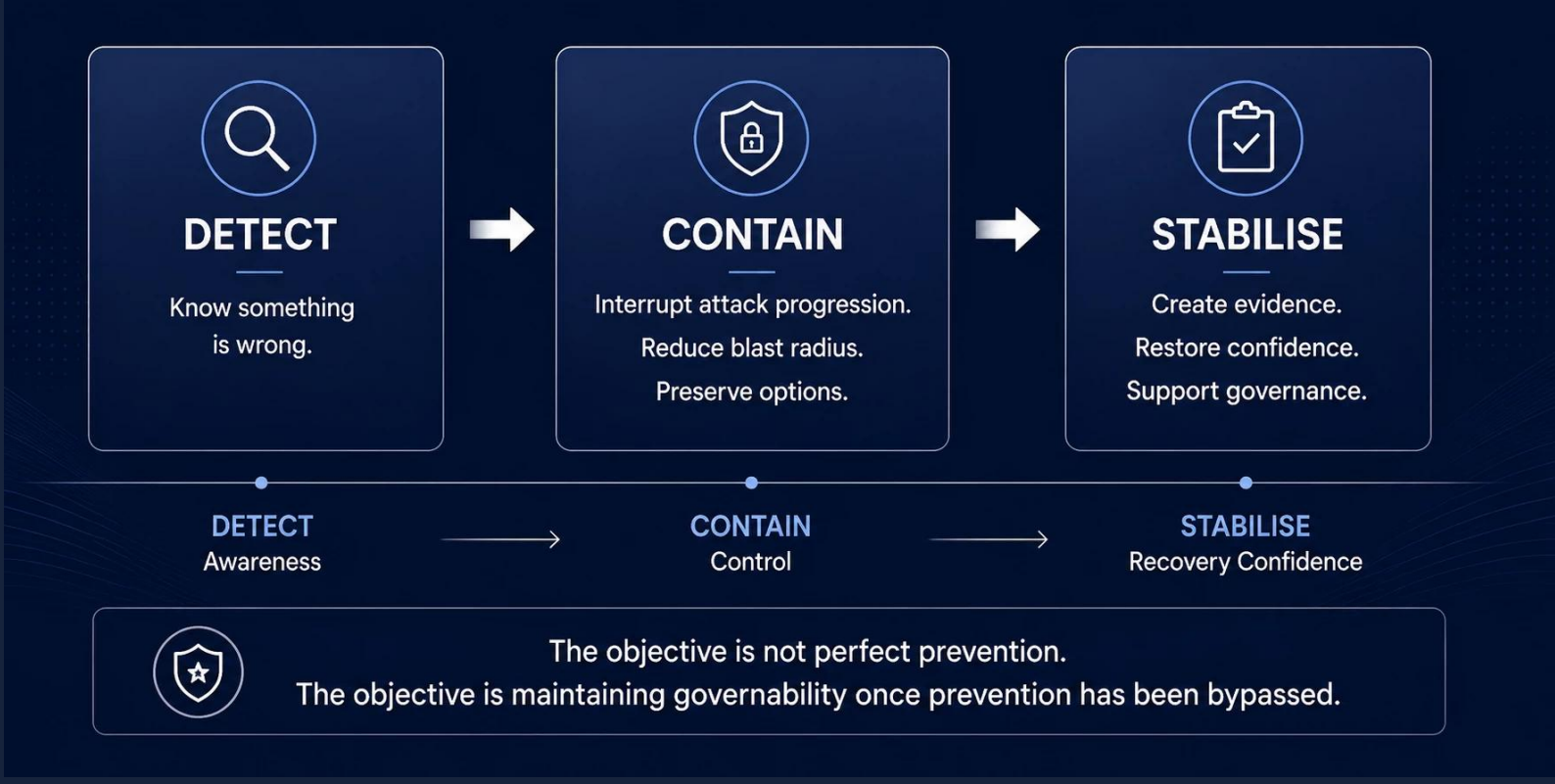
www.s10group.com

info@s10group.com

S10 Group

Control under pressure

Stop the cascade



THE S10 GROUP PLATFORM

S10 Group provides an operational containment platform designed to help organisations preserve governability once prevention has been bypassed.

Rather than adding another detection layer, the platform focuses on operational interruption.

It enables organisations to:

- Stop ransomware encryption instantly
- Prevent data theft
- Interrupt malicious lateral movement
- Terminate compromised identities
- Protect virtual infrastructure
- Preserve operational continuity
- Generate evidence and incident reporting for leadership, regulators and stakeholders
- Support defensible leadership decisions

The objective is to preserve governability once prevention has been bypassed.

VALIDATE YOUR RESILIENCE

Most organisations have invested heavily in prevention and detection. But do you know for sure how your stack responds when those controls fail?

S10 Group offers a Free Ransomware Containment Validation. In a controlled, zero-risk simulation, we benchmark your actual capability to stop the cascade.

- Can the attack be interrupted instantly?
- Can the infected user or device be isolated?
- Can recovery be limited to a few files instead of entire systems?
- Can leadership act with absolute certainty?

Our free validation scan maps your containment gaps and proves what remains controllable afterwards.

REQUEST YOUR FREE RESILIENCE ASSESSMENT.

www.s10group.com

info@s10group.com

S10 Group

Control under pressure

Stop the cascade

THE ASSUMPTION THAT CHANGED

For years, cybersecurity was built around a simple objective: keep attackers out.

Organisations invested in prevention, detection, monitoring, segmentation, identity management, backups, threat intelligence, and increasingly AI-assisted defence.

Those investments remain essential. But something changed.

AI is accelerating both defence and attack.

The time between vulnerability discovery, exploitation and operational consequence continues to shrink.

At the same time, legal and regulatory obligations increasingly require organisations to explain and report incidents while certainty is still incomplete.

Modern organisations now operate through hundreds of trusted relationships:

- cloud services
- suppliers
- SaaS platforms
- remote access
- APIs
- operational technology
- AI-assisted workflows
- virtual infrastructure

The question is no longer:
“How do we prevent every compromise?”

The question increasingly becomes:
“What happens when one trusted path is compromised anyway?”

THE CONTROLLABILITY GAP

Many organisations can see an incident.

Fewer organisations can interrupt it.

Detection continues to improve.
Visibility continues to improve.
AI will improve both even further.

Yet many incidents still become difficult because leadership discovers a different problem:

The organisation knows something is wrong—but nobody knows what can safely be interrupted.

www.s10group.com

info@s10group.com

S10 Group

Control under pressure

Stop the cascade

WHEN CONTROL IS LOST

Control is rarely lost in a single moment.

It is usually lost through a sequence of events:

- reconnaissance remains unnoticed
- trusted credentials are abused
- lateral movement expands
- dependencies become uncertain
- containment decisions are delayed
- recovery scope becomes unclear

Operations may still appear normal.
The data may already be outside the organisation.

TRUST BREAKS BEFORE SYSTEMS FAIL

Operations may continue.
The backup may still exist.
The systems may still be running.
Trust may already be compromised.

INCIDENT PROGRESSION

1. INITIAL COMPROMISE

Attackers gain a foothold through a trusted pathway, vulnerability, misconfiguration, compromised identity or third-party connection.

2. ENVIRONMENT DISCOVERY

Attackers identify systems, dependencies, backup structures and valuable data.

3. LATERAL MOVEMENT

Attackers expand access and increase control across systems and accounts.

4. DATA THEFT

Sensitive data is collected, extracted or prepared for exfiltration.

5. OPERATIONAL IMPACT

Operations become disrupted, visibility decreases and the risk of wider impact increases.

6. CRISIS GOVERNANCE

Decisions must be made with incomplete information, under pressure and with high stakes.

The earlier you interrupt, the less damage uncertainty can cause.

www.s10group.com

info@s10group.com

S10 Group

Control under pressure

Stop the cascade