ACT Against Cyber Risk: The Mid-Market Security Reset

A Practical Guide for UK CISOs

NODE4

Executive Summary

UK mid-market security has reached a critical point. Security environments have grown in size and complexity, yet teams have not grown or integrated at the same pace. There are more cloud services, more identities, more third-party integrations, and too many tools working in isolation that are operated in silos. This fragmentation creates blind spots, policy drift, and operational drag, while lean teams are under constant pressure to deliver business as usual.

Investment in cyber security may be rising year on year, but measurable confidence in posture is not. Many organisations feel less certain about their ability to prevent or recover from a serious incident than they did several years ago. The gap is not simply technical, it is operational.

Our ACT approach is a framework developed specifically for the UK mid-market to help close this gap. It is designed to help CISOs simplify the operating environment, align security to business priorities, and build measurable resilience.

This guide takes our ACT approach and turns it into a practical operating model that UK CISOs can adopt immediately. It offers pragmatic actions to strengthen posture, reduce complexity, and bring risk under control without adding more complexity or resource strain.

Why Now?

The security landscape for the UK mid market is shifting quickly. The risks you face are not just evolving, they are becoming faster, more frequent, and more disruptive. The way security is managed must adapt to keep pace.

Threats are accelerating:

Phishing remains the most common attack vector in the UK mid market, while ransomware continues to evolve. Attacker automation and human operated campaigns are compressing the time from entry to impact.

Complexity is creating risk:

Many organisations are managing overlapping and disparate toolsets, fragmented policy enforcement, operational silos and integration gaps. This leads to poor visibility and inconsistent control.

Incidents are more disruptive:

The impact of recent high profile UK incidents shows that operational downtime and recovery costs can easily reach hundreds of millions of pounds, even for established brands.

Confidence is not matching reality:

Research from our UK Mid Market Report 2025* highlights a confidence–action gap, with many leaders confident in their defences but few actively addressing the most significant risks.

Our ACT Approach: An Operating System for Resilience

Our ACT approach is designed to work as a continuous cycle, giving you a simple, clear way to reduce complexity and risk without overwhelming your team.

Assess

Know your risks before the attackers do

Consolidate

Simplify and strengthen your environment

Triage

Detect, prioritise and respond confidently

Assess

Gain Clarity on Risk

Start by getting absolute clarity on your risk. You need to know exactly what assets, identities, and data flows you are protecting, and where your vulnerabilities lie. This is not about a long audit that gathers dust, it is about building a live picture you and your board can act on.

Objectives

- Build an accurate inventory of assets, identities, and data flows
- Map critical business services and dependencies
- Benchmark controls against recognised frameworks
- Validate assumptions with technical testing and exercises

What Good Looks Like

- A live risk register tied to business services
- Measurable posture metrics and ownership
- Practised incident runbooks for high-impact threats

Consolidate

Reduce Complexity and Strengthen Control

You are probably running more security tools than you need, and they are likely not working together as well as they could. Consolidation is about simplifying the estate, integrating controls, and making the platforms you keep work harder for you. The result is less operational drag and more consistent control.

Objectives

- Rationalise toolsets around trusted, integrated platforms
- Standardise identity and access controls
- Centralise telemetry and detection into a unified SIEM/XDR
- Simplify network and edge security with identity-aware architecture

What Good Looks Like

- A clear consolidation roadmap with legacy retirements
- Automated enforcement of core policies
- A single source of truth for monitoring, detection, and investigation

Triage

Rapid Response Around the Clock

Incidents will happen, and when they do, speed matters. Triage is about being ready to respond with confidence. With rapid detection, clear playbooks, effective monitoring, and tested recovery processes, you can contain threats quickly, reduce impact, and keep operating.

Objectives

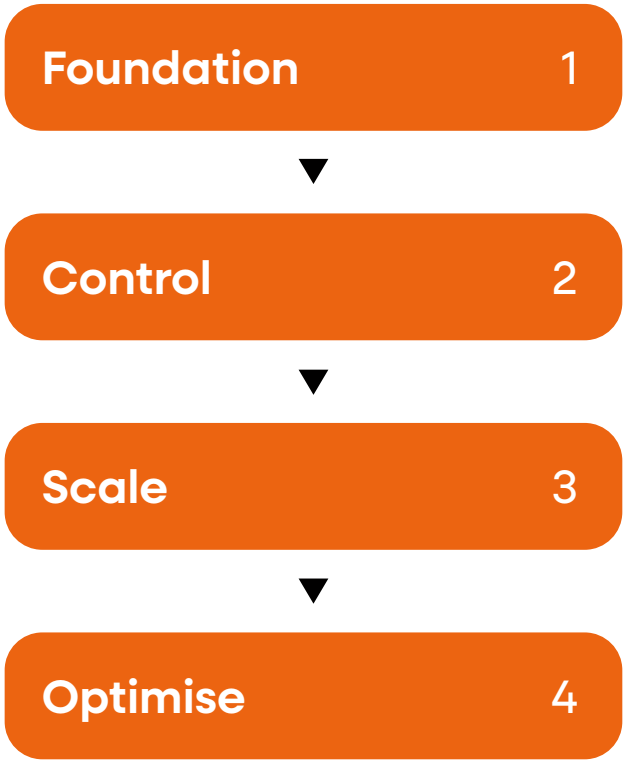
- Maintain round-the-clock visibility across key attack surfaces
- Operate prepared playbooks for high-priority threats
- Ensure tested recovery processes and validated backups

What Good Looks Like

- Measurable MTTD (< 15 minutes) and MTTR (< 1 hour) targets
- Consistent human-validated triage within minutes of detection
- Smooth escalation into incident response and business continuity processes

Pragmatic ACT Delivery Plan

Our ACT approach is designed to be practical, not theoretical. This plan gives you a clear sequence of actions to follow over the first year, so you can build momentum, demonstrate progress, and embed improvements without overwhelming your team.



First 30 Days – Foundation

- Commission assessments and baseline posture
- Build inventories and map dependencies
- Agree success metrics with the board

Days 31 to 90 – Control

- Enforce strong identity controls such as MFA and conditional access
- Migrate priority protections to integrated platforms
- Implement round-the-clock monitoring for high-risk threats

Days 91 to 180 – Scale

- Extend least privilege and secure admin practices
- Standardise network controls and pilot modern architectures
- Automate tier one incident responses

Days 181 to 365 – Optimise

- Retire overlapping tools and reinvest savings
- Mature data protection and insider risk controls
- Establish quarterly testing and continuous improvement cycles

By following these steps, you will have the core foundations in place. The next step is to keep our ACT approach working for you as the threat landscape changes.

Applying our ACT Approach to Emerging Risks

The threats you will face in a year's time may not be the same as today. Our ACT approach is built to adapt so that new risks fit into the same cycle without creating extra programmes or disruption.

Key Principles

- Start with visibility by defining the service, the owner, and the minimum telemetry required
- Use what is already in place by applying existing access platforms, controls, detection pipelines, and playbooks
- Integrate feedback quickly by adjusting one detection, one policy, and one platform decision per cycle
- Maintain a regular cadence by reviewing quarterly and delivering incremental improvements while keeping board oversight

By using our ACT approach to manage new risks, you avoid constant resets and keep security improvements on track. The final step is to embed ACT into everyday operations, so it becomes part of how your organisation runs, not just a one-off initiative.

Turning Strategy into Operations

To make ACT effective in the long term, it must be embedded into day-to-day operations. This means board alignment, clear ownership, and operational discipline.

Board Engagement

- Present a concise ACT roadmap with measurable outcomes
- Provide a clear consolidation business case
- Report current and target detection and response metrics

Operating in a Skills Short Market

- Pair internal knowledge with external round-the-clock monitoring capabilities
- Document clear roles and responsibilities
- Prioritise analyst time for proactive improvement over reactive workload

Compliance without the Theatre

- Use frameworks as a structure for sustainable improvement
- Automate evidence collection through existing platforms
- Align audit outputs to business risk narratives

Once ACT is part of day-to-day operations, it becomes a living system that adapts as your organisation grows, and threats evolve.

Why Node4?

Our ACT approach provides a pragmatic and repeatable structure for CISOs to manage complexity and risk in the UK mid-market

By adopting ACT, you can:

- Gain clarity on risk by building a live, business-aligned understanding of your security posture
- Reduce complexity by consolidating tools and integrating platforms, making security operations leaner and more effective
- Respond with confidence through tested playbooks and 24/7 readiness that reduce the impact of incidents
- Demonstrate progress with measurable outcomes that can be clearly communicated to boards and stakeholders
- Sustain improvement through a cycle that absorbs new risks without adding unnecessary programmes or disruption

Security posture strengthens, complexity reduces, and risk becomes a managed and transparent part of business governance. With ACT in place, you have a clear operating system for resilience that grows with your organisation and keeps you ready for whatever comes next.

CISO Takeaway

Our ACT approach is not a one-off project. It is a way to run security with focus, speed, and confidence so you can stay ahead of risk while supporting the business to move forward.

At Node4, we combine people, platforms and the proven ACT framework to help UK mid-market organisations move from complexity to control – fast. Our UK SOC, Microsoft Security expertise, Fortinet Fabric engineering, and other supporting cyber solutions are designed to work as one service, with measurable outcomes and a pragmatic approach to change.

Next Steps

1	Find out why Cybersecurity confidence is taking a hit in the mid-market	Find out now
2	Speak to a Node4 cyber expert about consolidation and 24/7 triage.	Lets chat
3	Book your Security Doctor assessment to baseline risk and build your roadmap.	Book now