White Paper

# Building Australia's Critical Infrastructure Resilience

Containment as a strategy

Akamai Security

# Executive summary

Australia's evolving Security of Critical Infrastructure (SOCI) framework has shifted the focus from security controls towards codifying operational resilience.

**Horizon 2** of the 2023–2030 Australian Cyber Security Strategy and the June 2026 Enhanced Critical Infrastructure Risk Management Program (CIRMP) announcements are pushing critical infrastructure organisations to assess artificial intelligence-related risks, manage legacy systems, segregate critical systems, address supply chain dependencies, and mitigate insider threats.

The focus is increasingly shifting from preventing every breach to the management and mitigation of their subsequent operational impacts.

Artificial intelligence (AI) technologies are significantly accelerating the transition from the discovery of vulnerabilities to their subsequent exploitation and operationalisation.

At the same time, critical infrastructure systems are becoming increasingly connected, and nation-state actors are actively targeting essential services around the world. This makes rapid containment increasingly important. A breach in the water utility systems, for example, may bring down other critical services such as manufacturing, transport, and healthcare at the same time.

When the traditional security approach — preventing breaches — is no longer sufficient, organisations cannot only ask if attackers are able to get in. The question has become *what happens when they do?* Can critical infrastructure continue to operate when compromise occurs?

Prevention alone is not sufficient these days. Resilience matters more.

This paper explores why resilience, containment, and architectural defensibility are becoming defining characteristics of critical infrastructure security in Australia.

# Blueprint for modern critical infrastructure security

Cybersecurity strategies have previously focused on preventing attackers from gaining access, but the real problem is not initial access.

The Australian regulators' view of critical infrastructure security is evolving, given the wide-ranging national consequences in the event of a breach.

Whether due to supply chain interruptions, water treatment outages, energy disruption, hospital service degradation, or telecommunications failures, any breach on critical infrastructure operators can create wide-ranging operational, regulatory, and business risks.

However, for many critical infrastructure organisations, asset visibility and operational complexity are among the top challenges. In addition, distributed applications, APIs, cloud workloads, and hybrid infrastructure expand the attack surface beyond what traditional inventories can capture.

## Challenges faced by critical infrastructure

| | |
|---|---|
| **No visibility** | "We don't know what talks to what" |
| **Fear of breaking applications** | "If we block traffic, production stops" |
| **Operational complexity** | "We don't have enough people" |
| **Legacy OT and IoT systems** | "We can't patch or replace them" |

The Enhanced CIRMP announcements unveiled by Australia's Cyber and Infrastructure Security Centre (CISC) signal where critical infrastructure regulation is heading:

1. Segregation of critical and noncritical systems
2. AI risk assessment
3. Legacy technology management
4. Supply chain resilience
5. Insider risk management
6. Stronger logging, monitoring, and cyber maturity requirements
7. API and application visibility
8. Continuity of essential services during disruption

SOCI marks a transition in focus from *prevention* to *impact management and containing the damage*. Critical infrastructure organisations are increasingly expected to demonstrate this resilience by implementing advanced logging and rigorous risk management for emerging technologies, including AI, API, and MCP (Model Context Protocol) services, to ensure they can contain compromise and maintain essential services.

Australian regulators have shifted their focus from asking "can you stop every breach?" to "can you survive one?"

## Critical infrastructure resilience maturity

**Stage 1: Visibility**
"We know and understand our assets"

**Stage 2: Compliance**
"We monitor and manage our assets"

**Stage 3: Containment**
"We can isolate compromise"

**Stage 4: Resilience**
"We maintain operations under attack"

Such resilience needs to be engineered by minimising the blast radius, identifying critical systems, and maintaining continued operations in the event of a breach.

# CIRMP amendments and the soft middle

Critical infrastructure organisations have invested heavily in firewalls, security operations centres (SOCs), and identity management.

As a result, cybercriminals find it increasingly tough to breach organisations that have strong perimeter controls, strict authentication, and strong endpoint protection.

However, many organisations continue to operate with over-permissive internal access; limited visibility of application dependencies, APIs, AI services, and other digital assets; as well as excessive trust between systems. This creates a “soft middle” where attackers are free to move laterally, escalate privileges, discover dependencies, and reach critical systems.

This hidden attack surface increasingly includes shadow APIs, zombie APIs, unmanaged AI services, MCP servers, and exposed application interfaces that can provide attackers with alternative pathways to critical systems.

Most major breaches follow the same pattern of initial access, privilege escalation, lateral movement, and operational impact. The greatest damage rarely occurs at initial compromise but is more likely to occur after attackers begin moving through the environment.

The enhanced CIRMP proposals increasingly emphasise architectural resilience through stronger segregation, visibility, and proactive governance. This requires a rigorous approach to AI and emerging technologies — including APIs and MCP — that extends beyond basic inventory to include continuous risk assessment. Effective governance must now incorporate detailed API/MCP asset inventories with contextual risk scoring, alongside proactive testing using synthetic attack traffic to identify business logic vulnerabilities, shadow assets, and authenticated abuse before they are exploited.

Together, these capabilities support limiting lateral movement, reducing the blast radius, and maintaining operational continuity instead of relying on perimeter controls.

This development demands a fundamental change towards a defensible architecture model — the next evolution beyond Zero Trust.

## Security architecture maturity

| Stage 1 | Stage 2 | Stage 3 |
|---|---|---|
| Perimeter security | Zero Trust | Defensible architecture |
| **Focus** | **Focus** | **Focus** |
| Keep attackers out | Verify users | Limit blast radius |

As part of a defensible architecture, resilience should be engineered across the entire stack — from infrastructure communications and workloads to identities, applications and APIs, and data/machine interactions.

By limiting the blast radius, the organisation can continue operating even while parts of its environment are compromised.

## Defensible architecture

| Resilient organisation | Resilience metrics |
|---|---|
| • Identification of critical systems | • Critical system isolation |
| • Monitoring of communication paths | • Blast radius reduction |
| • Maintenance of essential operations | • Operational continuity |
| • Rapid containment | • Recovery readiness |
| • Operational independence | |

# API visibility is essential to API security

Although visibility is the foundation of resilience, few critical infrastructure organisations understand what APIs do, what data they expose, and how they support critical services. This comprises:

1. **Infrastructure visibility.** Understanding of systems, workloads, application dependencies, communication paths, internet exposure, and attack pathways.
2. **Digital visibility.** Continuous real-time change monitoring to discover shadow (AI, API, MCP, and domains) and neglected zombie APIs. Including discovering API from code, provides a complete digital asset visibility and correlation between both documented design vs. runtime reality.
3. **Posture visibility.** Inspection of every API runtime transaction to identify vulnerabilities like misconfiguration, missing authentication, weak auth, and rate-limiting gaps.
4. **Data visibility.** Continuous deep API payload monitoring and analysis for sensitive PII/PCI data classification and data in transit tracking for protection against exfiltration vectors.
5. **Advanced technology visibility (AI governance).** Automatic AI agent discovery and tagging of GenAI, LLM, and MCP servers and tools, preventing shadow AI adoption without proper governance control.
6. **Behavioural visibility.** API security using AI/ML to detect business logic abuse and anomaly threat against learnt normal baseline per API endpoints that is missed by static policy and signature-based security control.

Modern critical infrastructure increasingly depends on APIs to facilitate machine-to-machine communication, digital service delivery, OT integrations and critical workflows.

As organisations modernise services and adopt AI workflows, APIs increasingly become the pathways through which critical systems exchange data.

This creates a second layer of exposure.

Many organisations believe they have API visibility, but far fewer understand sensitive data exposure, critical business dependencies, and API risks.

Exploitable runtime flaws in API such as broken authorisation and misconfigured endpoints are the exact vulnerabilities attackers target to silently exfiltrate data, making proactive API vulnerability penetration testing a foundational defence.

Performing penetration runtime testing of multilayered security controls early and frequently is vital; fixing exploitable vulnerabilities during the CI/CD pipeline phase is up to 100 times less expensive than remediating them in production,[1] providing security and development teams with a significant operational and financial advantage.

## API visibility: You can't defend what you don't understand

- Can you see which APIs exist?
- Which APIs expose sensitive data?
- Which APIs support critical operations?
- Which APIs support AI workloads?

According to **Akamai's 2025 API Security Impact Study**, Australia had the highest frequency of API security incidents (96% in 12 months). At the same time, Australia had the highest percentage of respondents who claim to have complete API inventory (81%) but only 30% know which APIs expose sensitive data. As for root causes of API incidents, leaders most frequently pointed to API misconfigurations.

When it comes to spotting API vulnerabilities early in the lifecycle, Australian respondents had the lowest rate of real-time API testing among the countries surveyed (6%), with about a third testing daily (34%) or weekly (35%). None of the respondents in financial services, healthcare, or manufacturing industries reported that they test in real time. This lack of real-time testing is concerning.

[1] Source: **NIST Planning Report 02-3**, Table 1-5: Relative Costs to Repair Defects When Found at Different Stages of the Life-Cycle.

In fact, AI security starts with API security — as every AI workload depends on APIs, data pipelines, and integration.

Unprotected APIs create AI data exposure and model manipulation risks. In addition, if the pathways are poorly understood or poorly protected, AI initiatives will inherit those weaknesses.

With less than a third of Australian respondents saying that they know which of their APIs return sensitive data, the growing threat to GenAI applications should be a high priority for both IT and security leaders.

## AI rewrites the rules

*AI does not change the attacker's objectives; it increases the attack speed.*

Now that AI-assisted attackers have automation, speed, and scale, organisations require a dual strategy:

1. **Shift left.** Denying exploitability at the source: CI/CD integrated API vulnerability testing discovers and remediates issues before they become exploitable vulnerabilities in production.
2. **Shield right.** Containing compromise at machine speed: AI-driven behavioural detection and instant isolation uses real-time runtime monitoring and automated workflow to detect anomalous activity and immediately contain zero-day attacks and business-logic abuse, while preserving operational resiliency and business continuity.

Together, these capabilities reduce exploitable risk before deployment while limiting operational impact after compromise.

# Segmentation: Foundational, not optional

Segmentation is now recognised as a foundational component of a mature Zero Trust strategy.

As Australian regulators increasingly require the "greatest practical level of segregation", organisations are accelerating the adoption of microsegmentation to strengthen cyber resilience.

Historically, the challenge with segmentation has not been recognising its value but making it operationally practical at enterprise scale. Organisations have often faced significant effort to discover application dependencies, develop accurate policies, and maintain them as environments evolve. AI is fundamentally changing this by automating many of the tasks that have traditionally limited the speed, scalability, and long-term success of segmentation initiatives.

Modern segmentation is increasingly supported by AI-assisted discovery, application dependency mapping, policy recommendation, exposure analysis, and automated enforcement.

Organisations are now able to deploy microsegmentation at the enterprise level while adapting to changing environments:

- Asset discovery/labelling automatically identifies workloads, applications, dependencies, and critical systems.
- Dependency mapping understands application relationships, communication paths, and hidden dependencies.
- Policy recommendations generate segmentation policies, least-privilege recommendations, and risk-reduction pathways.
- Exposure analysis identifies lateral movement opportunities, high-risk pathways, and critical attack routes.

*The **Akamai Guardicore Segmentation** generative policy engine combines segmentation, detection, and response to include exposure analysis, threat detection, incident visibility, threat intelligence, deception technology, and collective intelligence initiatives.*

AI is transforming both sides of the cyber battlefield. Attackers are using AI to automate vulnerability discovery, privilege escalation, and lateral movement at unprecedented speed and scale. Defenders are responding by using AI to simplify and operationalise microsegmentation — automating asset discovery, dependency analysis, and policy recommendations while rapidly identifying malicious behaviour, containing lateral movement, and accelerating incident response.

# Defensible architecture

Security strategies are now shifting away from absolute prevention towards resilience, continuity, containment, and operational stability during active attacks.

The organisations that succeed move beyond compliance exercises and have already begun building defensible architectures designed for containment, resilience, operational continuity, and rapid recovery.

## Defensible architecture for critical infrastructure

### Current challenges

- Limited infrastructure visibility
- Shadow APIs and AI services
- Unknown application dependencies
- Legacy OT and IoT
- Operational complexity

### Outcomes

- See what attackers can see
- Break attack paths
- Reduce blast radius
- Validate critical system isolation
- Maintain operational continuity

### Capabilities

- Discover application dependencies
- Identify shadow APIs and AI assets
- Monitor north-south and east-west communications
- Detect overprivileged connections
- Govern application and API communications

In an era where AI is accelerating both attackers and defenders, the objective is not to stop every breach but to ensure that no breach becomes a national infrastructure crisis.

How prepared is your organisation? Use the checklist below to assess your organisational readiness.

## Defensible architecture for critical infrastructure

| | | |
|---|---|---|
| **Attack path reduction** | Can we prove risk reduction to regulators? | How many lateral movement paths have been eliminated? |
| **Critical system isolation** | Can we identify our critical systems? | What is the percentage of critical systems that can be isolated independently? |
| **Blast radius reduction** | Can we isolate them quickly? | What is the percentage of potential systems reachable after a breach? |
| **API and AI governance** | Can we continuously discover APIs, AI services, and shadow assets? | What is the percentage of conformance for APIs discovered from runtime versus known API documentations? |
| **Monitoring and detection** | Can we detect API posture vulnerabilities and anomalous API behaviour in real time? | What is the mean time to mitigate detected API posture vulnerabilities and business logic abuse? |
| **Recovery readiness** | Can we rebuild if compromised? | How much time is needed to isolate critical systems? |
| **Operational resilience** | Can we operate while isolated? | What percentage of the organisation can maintain service during containment? |

# Plan for continuity and survivability

The challenge is no longer simply that of cybersecurity, but it is the continuity of essential services regardless of breach.

Now, the future of critical infrastructure security will not be defined by organisations that prevent every breach. It will be defined by organisations that engineer operational continuity and survivability.

Building cyber resilience requires visibility and governance across identity, network and application and API layers.

Organisations need continuous understanding of infrastructure, application dependencies, and digital assets while validating authorisation, maintaining strict zone microsegmentation, discovering app-layer vulnerabilities, detecting business-logic behavioural abuse, and executing automated containment of breaches at machine speed.

Australia's enhanced CIRMP requirements increasingly position operational resilience as a measurable capability rather than an aspirational objective.

Organisations that invest in comprehensive visibility, governance, and containment today will be better positioned to ensure that future compromises remain as contained security incidents and not national crises.

## Ready to build your defensible architecture?

**Visit our website to learn more or contact our sales team to discuss your business needs.**

---

Akamai

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence. Learn more at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 09/26.