CANOPUS

SOLUTION BRIEF
HIGHER EDUCATION



Protecting the integrity of online exams

Network observability and AI agents give universities a clearer, evidence-led view of exam-period activity.

The challenge

Online assessment has expanded access and flexibility, but it has also changed how misconduct can happen. Students may use virtual machines, remote desktops, generative AI tools, communication services, or auxiliary devices during an exam.

Some activity is difficult to see from the exam platform or a webcam alone, especially when students use their own devices and familiar network services. Universities need to protect academic standards while preserving a fair and workable exam experience. A single control rarely provides the full picture: platform logs show activity inside the assessment, while invigilation tools observe only parts of the physical or digital environment.

One view across the exam session
Correlate exam activity with network-observed applications.

Any exam platform
Designed to work alongside Inspera, Proctorio, Respondus and others.

Evidence plus live response
Support review during and after the exam.

The Canopus solution

Canopus monitors network activity associated with exam sessions on a university's wired or Wi-Fi network. It identifies exam takers through activity on supported assessment platforms, then examines other applications active on the same device using a library of more than 30,000 applications. AI agents continuously assess this activity and flag configurable categories of concern, including generative AI, remote desktop and communications tools.

1. **Identify exam takers**
Detect exam sessions on supported assessment platforms.

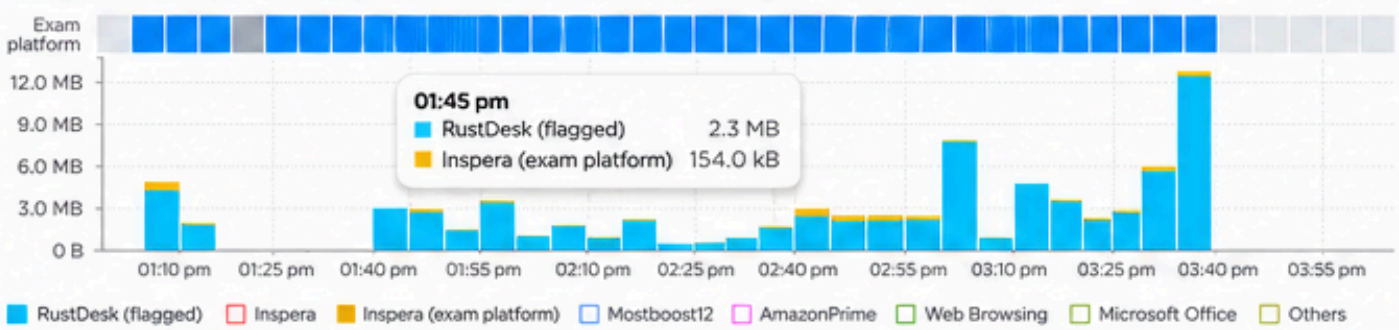
2. **Analyse device activity**
Examine other applications active on the same device using a library of 30,000+ applications.

3. **Detect and flag suspicious activity**
AI agents continuously assess activity and flag configurable categories, including generative AI, remote desktop and communications tools.

4. **Support investigation**
Provide network-level evidence to inform review, policy and response.

One exam taker, one session timeline

Exam-platform activity is shown alongside other observed applications, including flagged remote-desktop traffic.



CANOPUS

SOLUTION BRIEF
HIGHER EDUCATION

From visibility to action

Canopus turns exam-period network observations into three practical outputs:

1

Activity evidence that is irrefutable

For each exam period, identify exam sessions and the other applications active on each device. AI agents flag suspicious services for review, helping investigators understand what was accessed and when. The platform exports irrefutable evidence to support a misconduct process.

2

Real-time remediation

Live session information can help invigilators focus attention on a student or session. Where university policy and operational controls permit, IT teams can respond during the exam, for example by blocking access to identified remote desktop services at the network firewall.

3

Post-exam reporting

A cohort-level report summarizes exam takers and sessions, the number of sessions with high-confidence suspicious activity, and the prohibited services identified. This supports consistent review, audit and follow-up after the assessment.

Network insight for stronger exam controls

The approach adds a network-level perspective to existing exam controls. It is designed to work across exam platforms and identify known techniques such as virtual machines, remote access and use of AI tools. Findings are surfaced for human review; universities can determine the appropriate policy, investigation and response.



Potential outcomes

With a consistent view of exam-period activity, universities can strengthen the evidence available for case review, focus investigation and decision-making resources, and make timely operational decisions when suspicious access is detected. Cohort reports also help institutions understand patterns across assessments and refine exam controls over time.

- Stronger evidence for case review
- More focused investigation and operational decisions
- Cohort insights to refine exam controls over time



A university-built platform

Canopus was incorporated in 2018, drawing on 12 years of networking and AI research at UNSW Sydney. The company holds 20+ patents related to AI models for encrypted network traffic analysis, and has raised over US$12 million in venture investment. Its platform is developed in Australia and has been deployed in several large-scale networks. The broader platform also supports campus network, cyber, and governance operations.

See what is happening during your exams

Let's talk

Start with a three-month paid pilot to establish a baseline of online exam activity and assess how network visibility can support your university's integrity processes.

Want to discuss a pilot?
Reach out to **Vijay Sivaraman**
Professor, UNSW
CEO/Co-Founder, Canopus
vijay@unsw.edu.au | vijay@canopusnet.com
Visit: www.canopusai.com

CANOPUS