Integrity360

your **security** in mind

Managed CNAPP Service

Your end-to-end solution for uncompromised cloud security

Introduction

By 2025, 95% of new digital workloads will be deployed on cloud-native platforms, marking a pivotal shift in digital infrastructure. This creates unprecedented challenges and opportunities, necessitating a robust approach to cloud security. Integrity360 is at the forefront, guiding enterprises through the complexities of cloud security with unmatched expertise and solutions.

The challenges at a glance:

- **Lack of visibility:** Maintaining a comprehensive view of dynamic workloads, user activities, data movements, and cloud configuration changes becomes a huge challenge. These gaps prevent the management from realising the context behind what is running in their cloud environments? What are the risks? How to detect and prevent human error or suspicious behaviour? This lack of meaningful context makes it harder to prioritise cloud risk or required remediations.
- **Inadequate protection:** Traditional endpoint protection falls short in cloud environments, especially with ephemeral workloads. The nature of cloud assets demands innovative security solutions that are built for purpose, rather than solutions built for legacy architectures.
- **Dispersed solutions:** With organisations leveraging multiple cloud platforms, relying on the security capabilities of the public cloud provider alone usually doesn't deliver the required level of security, causing disjointed and siloed security controls that in many cases fall short in comparison with the leading cloud security vendors. This fragmentation complicates the task of painting a unified picture of threats and exposures, making it difficult to manage risks and detect threats effectively.

Nearly 95% of cloud breaches trace back to user misconfiguration, coupled with an alarming 75% stemming from insufficient permission management.

Secure your cloud journey with Integrity360:

Integrity360's managed CNAPP service offers a seamless, integrated approach to protect your organisation against the multifaceted threats of the cloud.

"We ensure that every asset in your cloud is visible, evaluated, analysed, every risk captured, prioritised, with remediation guidance and actionable insights to improve your cloud risk posture, improve operational efficiency and collaboration between teams, detect and mitigate threats, and keep your cloud estate compliant to regulatory frameworks and best-practice standards"

The cloud security challenges

Organisations are increasingly leveraging the cloud's power for its flexibility, scalability, and efficiency. However, this transition introduces a range of security challenges that can jeopardise your operations, data, and compliance posture.

1. Visibility gaps in dynamic cloud environments

The nature of cloud assets, coupled with the vast volume of data and the accelerated pace of changes, creates significant visibility challenges. Organisations often find it difficult to keep track of dynamic workloads, user activities, data transactions, and configuration alterations in real-time. This lack of comprehensive visibility is a fundamental obstacle to securing the cloud ecosystem against threats and vulnerabilities.

2. The limitations of traditional endpoint protection

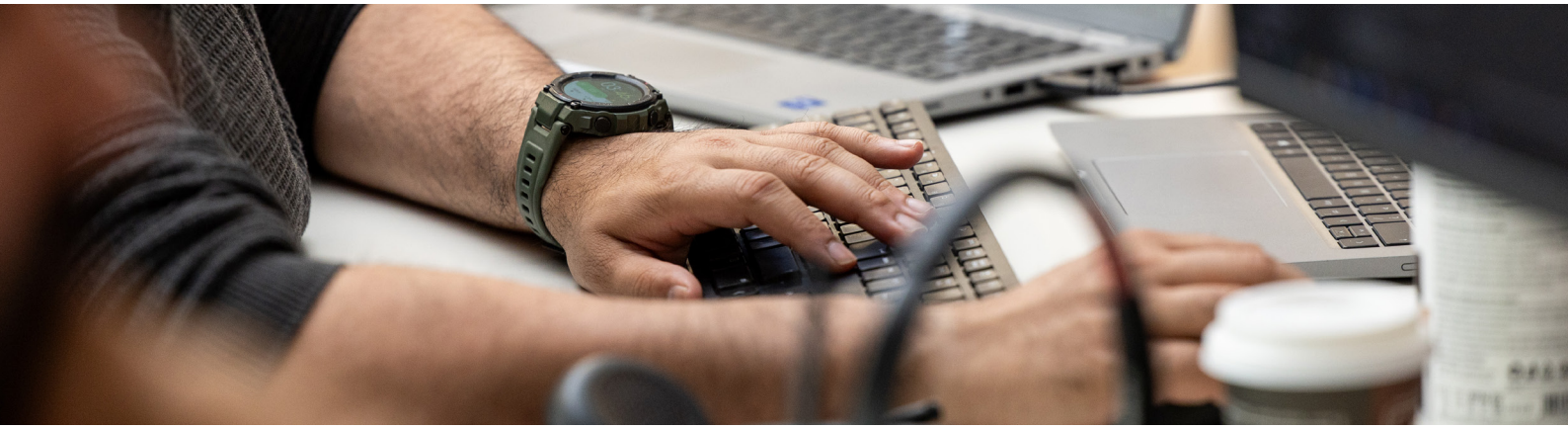
Traditional endpoint security solutions fall short in the cloud domain. The transitory existence of cloud resources demands a security approach that is as dynamic and flexible as the cloud itself. Adapting to this requirement means moving beyond conventional methods to embrace cloud-native security solutions designed to safeguard ephemeral cloud assets effectively.

3. Fragmented security solutions across cloud platforms

With the adoption of multi-cloud environments, organisations face the challenge of managing disparate security solutions. This fragmentation leads to silos of information and users, complicating the task of obtaining a unified risk perspective. Ensuring comprehensive protection across various cloud environments, workloads, user and access management, and development cycles is a complex endeavour that requires a strategic and integrated approach.

4. The skills shortage in cloud security

As cloud architectures become increasingly sophisticated, finding suitable security solutions and the expertise to implement and manage them effectively is a growing concern. Organisations must adopt modern solutions to protect the move to cloud-native application architecture, to ensure their security posture is robust and resilient.



5. Mitigating risks of cloud misconfiguration

Misconfigurations in cloud pose a significant risk, often leading to data breaches and compliance violations. The challenge lies in securing cloud configurations and enforcing remediation measures without impeding productivity. Organisations must strike a delicate balance between security and operational efficiency.

6. Implementing robust access controls

Enforcing the right level of Role-Based Access Control (RBAC), adhering to the principle of least privilege, and managing access controls is critical. Ensuring appropriate permission levels for both human and non-human identities, including APIs, scripts, microservices, and other cloud workloads, is paramount for safeguarding cloud environments against unauthorised access and potential breaches.

7. Threat detection gaps

In cloud environments, it's a common use case where workloads (or even entire tenants) are left without adequate security controls – usually used as testing or preproduction environments. However, this can lead to breach scenarios where such environments are used as attack initial entry points for attackers to establish foothold then leveraging various tactics such as lateral movement or credential access.

8. Collaboration between security, cloud and development teams

Security teams, cloud architects and application developers don't necessarily have visibility into each other's side of the organisation. For example, a security analyst can see a security alert on a container but doesn't know the impact or the best way to address it, so they probably need to go to the application development teams, who may also miss the big picture, and address this issue without considering the context or the other factors that led to these alerts at first place.

CNAPP technology overview

Cloud Native Application Protection Platform (CNAPP) is a unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production. CNAPP consolidates a large number of previously siloed capabilities and tools:

Cloud Security Posture Management (CSPM): CNAPP centralises the monitoring of cloud configurations, identifying misconfigurations and vulnerabilities across multi-cloud environments, enhancing compliance while removing the need for standalone CSPM solutions.

Cloud Infrastructure Entitlement Management (CIEM): With embedded identity and access management capabilities, CNAPP manages permissions across cloud services, reducing excessive entitlements and potential attack vectors, replacing traditional CIEM tools.

Kubernetes Security Posture Management (KSPM): CNAPP includes in-depth Kubernetes security, managing configurations and policies specific to Kubernetes environments.

Cloud Workload Protection (CWP): CNAPP secures workloads at development and runtime, ensuring applications are safeguarded without relying on disparate workload protection tools.

Data Security Posture Management (DSPM): CNAPP provides visibility into where sensitive data resides, who has access, and how it is used or moved across cloud environments. By incorporating DSPM, CNAPP enhances data governance and helps prevent data exposure due to misconfigurations, while ensuring compliance with privacy regulations.

Attack Path Management: CNAPP enables visualisation and management of potential attack paths within the cloud environment. By identifying and blocking attack vectors, CNAPP allows security teams to proactively mitigate exposures, enhancing overall threat prevention.

Vulnerability Scanning: Integrated vulnerability scanning detects vulnerabilities across workloads, images, and infrastructure in real time. This feature supports DevSecOps by providing security feedback throughout development, securing both the development process and production environments, and reducing reliance on separate scanning tools.

Shift-left Security: CNAPP provides comprehensive security and compliance checks across the full software development lifecycle (SDLC), offering capabilities such as code security that includes software composition analysis (SCA), secrets detection, IaC security, container image scanning, and more. Helping to secure the SDLC early in the development stage, and track findings in production environments back to the original development artifacts.

Our methodology

Integrity360's Managed CNAPP Service is designed to offer businesses a holistic security management solution purposefully built for the challenges of the cloud. We follow a structured approach to cloud security, covering both exposures and threats across every layer of your cloud estate.

Here's how our services transform your cloud security play:

Everything that happens across your organisation's cloud environment is captured, analysed, and categorised based on the different assets, artifacts, configurations and data.

All the data captured is analysed and evaluated against 100+ threat models, security policies, frameworks, vulnerabilities DB and threat-intel feeds.

The outcome of this process consists of 3 categories: Exposures, Threats, and Compliance findings.

Exposures (such as misconfigurations, data-at-risk, neglected assets, vulnerable workloads, etc) are summarised and prioritised based on severity and affected assets and mapped to an attack path. Then we apply our standard exposure alerts handling process to them, which includes reporting, notification, remediation support, and other customisable actions and automations.

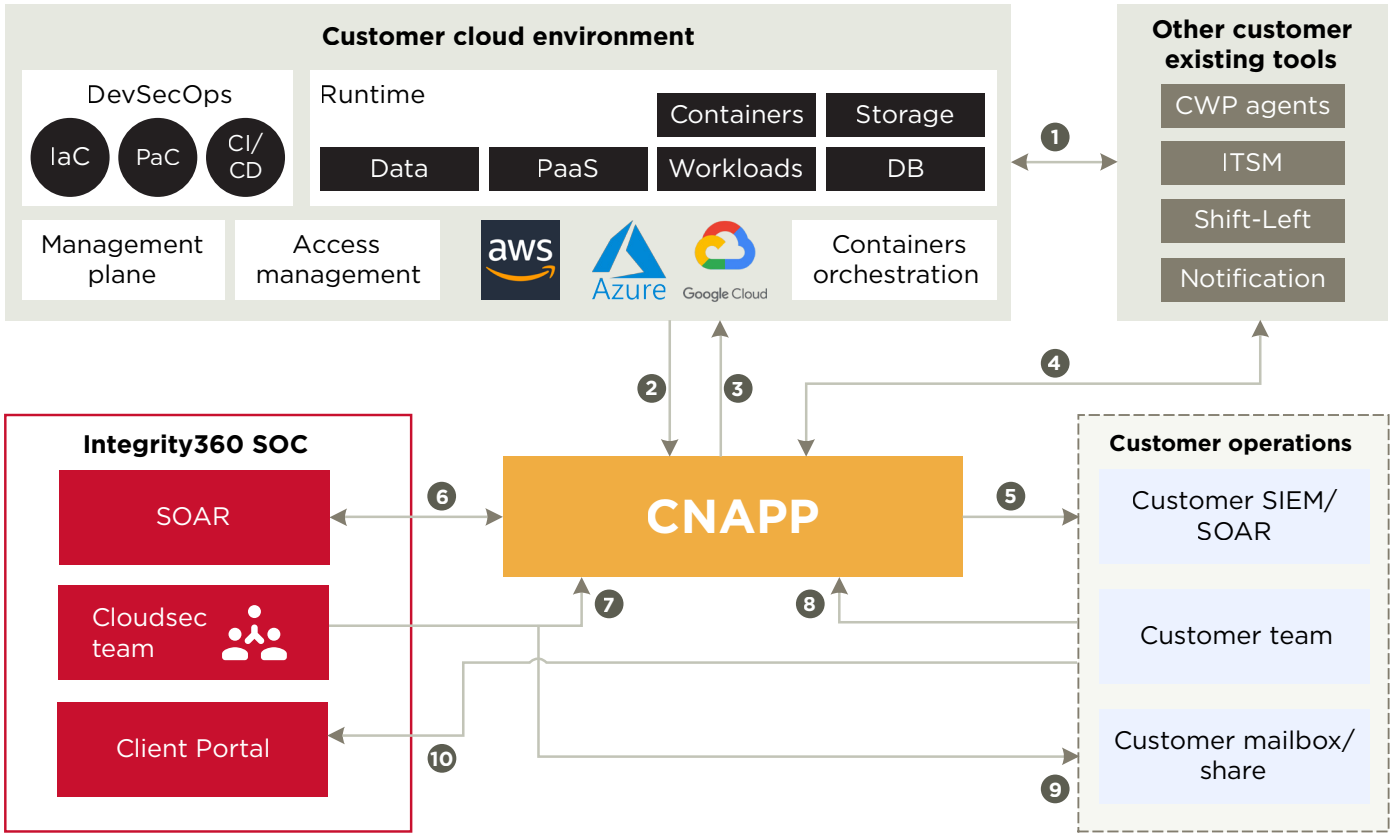
Threats (such as malware and malicious or suspicious behaviours) are handled with a different process, due to their criticality and the urgent requirement for a response action. Threat alerts are prioritised and raised immediately to the security operations team.

Compliance assessment findings are evaluated based on the frameworks selected by the customer, from a selection of 180+ frameworks that covers regulations (such as PCI DSS, GDPR, DORA, etc), AWS and Azure best practices, CIS controls, or a custom policy that captures specific requirements per customer environment.

Furthermore, the service provides management and support for all the CNAPP features, including shift-left security, integrations with the wider cloud and security technology stack, enabling your wider teams to utilise the full capabilities of CNAPP with solid support and guidance from our cloud security team.

Monthly proactive cloud risk workshop that ensures continuous optimisation of the platform, to increase operational efficiency and ensure value realisation of your cloud security investment.

Managed CNAPP Service Architecture



1. Integrations between customer cloud and other 3rd party tools
2. API read-access
3. (Optional) API write-access for auto-remediation
4. Integration between CNAPP and 3rd party tools such as agent-based CWP, Jira, GitHub, and others
5. Forwarding of selected alerts
6. Integration for alerts forwarding/polling and alerts modification
7. Secure management access
8. Secure access (custom dashboards and self-service)
9. Custom reports and communications
10. Self-service (change requests, service overview, and other features)

Our Managed CNAPP Service Tiers

Feature	Cloud Risk Management	Managed CNAPP	Managed CNAPP+
Platform administration	✓	✓	✓
Platform access management	✓	✓	✓
Platform integration with 3rd party solutions	✓	✓	✓
Remediation policy management	✓	✓	✓
Risk remediation support	✓	✓	✓
Custom compliance policy	✓	✓	✓
Prioritised risk reporting	✓	✓	✓
Custom dashboards and reporting	✓	✓	✓
Monthly cloud risk review sessions	✓	✓	✓
Platform incident management	✓	✓	✓
Risk alerts optimisation	✓	✓	✓
Threat alerts optimisation	✓	✓	✓
Cloud Workload Protection	-	✓	✓
CWP policy management	-	✓	✓
Agentless CWP as a standard	-	✓	✓
Agent-based CWP (platform dependent)	-	✓	✓
24x7 threat alerts monitoring	-	-	✓
Threat alerts triage and investigation	-	-	✓
Monthly threat intel report	-	-	✓
Ability to integrate with the wider MDR service	-	-	✓

Our Managed CNAPP Service Features

End-to-end cloud risk management

Our managed service provides complete management of the CNAPP solution, whether your organisation operates in AWS, Azure, Google Cloud, or a multi-cloud environment, our service ensures thorough coverage, safeguarding your digital assets across any cloud infrastructure.

Agentless and agent-based Cloud Workload Protection

Our service can mix both agentless and agent-based approaches for cloud workload protection, combining the benefits of both approaches in one. Our service covers all your cloud workloads with agentless CWP as standard without the need to wait for an agent's rollout plan that can take weeks and may leave gapped workloads unprotected, with the addition of agents where required, for example for critical containers and Virtual machines, or across a specific tenant or account.

Real-time threat monitoring

With continuous monitoring, we identify cloud threats in real-time, carry out the triage and investigation with industry leading SLAs, shielding your security operations from false positive and unnecessary noise, only responding to the real threats.

Policy enforcement and compliance assurance

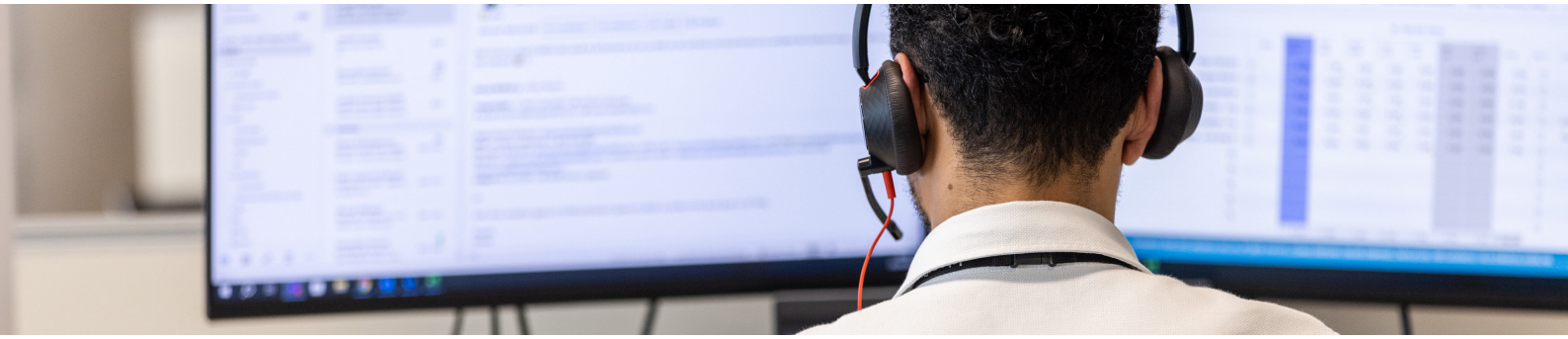
Our service allows you to enforce strict security policies across your entire cloud estate, facilitating compliance with industry regulations and standards. Through detailed audit trails, we offer transparency and accountability, making compliance an integrated aspect of your operations.

Automated risk prioritisation and remediation

Our sophisticated tools automatically detect potential security risks, prioritising them to provide actionable insights for rapid remediation. This pre-emptive approach to risk management keeps your cloud environment secure and resilient. Aligning your cloud operations with industry best practices and significantly reducing human error, providing detailed remediation steps. This proactive stance ensures that your cloud environment remains robust against misconfiguration threats.

Customisable security policies

Understanding that each organisation has unique security needs, we offer customisable security policies. Tailored to align with your specific requirements and evolving business objectives, our policies ensure you stay ahead of the security curve and industry standards.



Multi-cloud support

Our expertise extends across multi-cloud environments, enabling a unified and consistent security posture regardless of the cloud providers you leverage. This cohesive approach eliminates visibility gaps and provides a single source of truth.

Support for SOC automations

Enhance your Security Operations Centre (SOC) with our support for seamless integration. Our automated workflows facilitate efficient incident response, ensuring swift identification, containment, and resolution of security incidents.

Custom dashboard and reporting

Gain real-time insights into your cloud security status with our intuitive dashboards. Accompanied by comprehensive reports, our platform empowers informed decision-making, offering a clear view of your security landscape.

Expert support and guidance

Leverage the expertise of our seasoned security professionals, who provide proactive guidance, valuable industry insights, and unwavering support. Our team is dedicated to ensuring the effectiveness of your cloud security strategy, helping you achieve and maintain an optimal security posture.

Your cloud security, our priority

With Integrity360's Managed Cloud Security Services, safeguarding your cloud environment becomes a seamless and integrated process. Secure your cloud assets with us and focus on what you do best: driving your business forward.

Why choose Integrity360?

Choosing a cyber security provider is a critical decision for any business. Here are just a few reasons why you should choose Integrity360:

- **Passion and commitment:** We are passionate about cyber security and committed to delivering the best possible protection for our clients' businesses.
- **Certifications:** Greatest level of technical certifications and capability.
- **Partnerships:** Strongest vendor partnerships and support arrangements.
- **Recognition:** Recognised by Gartner in multiple market guides.
- **Five Security Operation Centres (SOC)** located in Ireland, Italy, Sweden, Bulgaria and South Africa.
- **Experience:** With over 400 security consultants, engineers, and analysts, we have the global experience and expertise to safeguard your business from even the most complex and evolving threats.
- **Reputation:** We have earned the trust of over 2500 global companies and have a strong reputation in the industry, built upon by exceptional technical expertise, a client first attitude, and a proven track record on complex security projects.
- **Customised solutions:** We take a personalised approach to cyber security, partnering closely with each client to understand their unique needs and recommend the most effective security solutions.