protiviti®
Global Business Consulting

Protect Your Cloud Environment With CNAPP

In 2023, a prominent global technology firm experienced a significant security breach when sensitive production data was inadvertently restored in a development environment. This misconfiguration led to the exposure of credentials and customer data, underscoring the persistent challenges even the most advanced tech companies face in securing cloud environments.

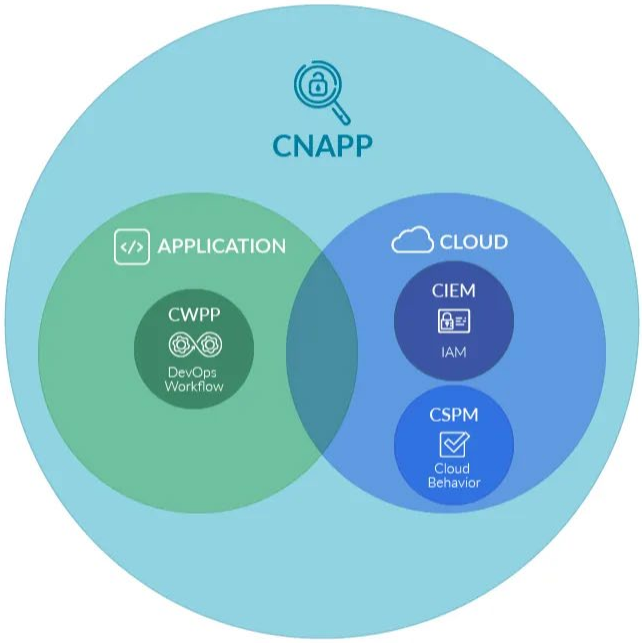
This incident is not isolated. According to Gartner, by 2023, 75% of cloud security failures were attributed to security misconfigurations. The primary causes of these failures include disconnected security tools, reactive security strategies and a lack of unified visibility across cloud environments. These issues highlight the critical need for comprehensive and proactive security measures.

Security teams frequently rely on security-information and event-management (SIEM) systems, such as Splunk, and endpoint detection and response (EDR) tools like CrowdStrike Falcon. While these solutions offer centralized log management and real-time threat detection, they often fall short in addressing the speed, scale and complexity inherent in cloud-native environments.

This is where cloud-native application-protection platforms (CNAPPs) come into play. CNAPPs provide an integrated, proactive approach to cloud security, unifying security and compliance into a single platform. Unlike traditional tools that operate in silos, CNAPPs offer continuous monitoring and governance, ensuring collabouration between development, operations and security teams to address risks throughout the lifecycle of modern applications.

Cyberattacks becoming more sophisticated

As cyberthreats and attacks grow in both frequency and sophistication in today's enterprise landscape, CNAPPs are not just a luxury — they are becoming a necessity. As cloud-native application development continues to grow and cyber threats become more sophisticated, CNAPPs provide the comprehensive, integrated security solutions that modern enterprises need to protect their valuable assets.



The evolution of cloud security leading to CNAPPs reflects the shift towards more dynamic and scalable security solutions, capable of keeping pace with the rapid development practices of cloud-native technologies. As organisations continue to adopt multi-cloud environments, the need for robust and integrated security platforms becomes increasingly critical. The future of enterprise security lies in the adoption of CNAPPs, ensuring that organisations can innovate and scale securely in the cloud.

> "With organisation cloud environment complexity increasing year-to-year, monitoring, detecting, and preventing threats and vulnerabilities in the cloud has also become an even greater challenge. Coupled with the proliferation and fragmentation of security tools, security teams are facing an increasingly intricate challenge when securing their cloud environments. It quickly becomes apparent why cloud-native application-protection platforms (CNAPPs), which provide a comprehensive, unified security across multiple cloud platforms, have quickly gained popularity in the industry."
>
> — *Hillary Baron, Senior Technical Director, Research, Cloud Security Alliance*

Understanding CNAPP's role

Traditional security solutions — including SIEMs, firewalls and endpoint detection — excel at monitoring logs and detecting threats post-incident. But they weren't built for cloud-native workloads, Kubernetes clusters, or dynamic, auto-scaling infrastructures.

How CNAPP addresses these challenges, compared with traditional security tools:

Feature	Traditional Security (SIEMs, Firewalls, EDR)	CNAPP
Threat detection	Looks at past data logs to detect security breaches after they happen.	Monitors security in real-time, identifying risks before they become breaches.
Threat response	Sends security alerts that need manual investigation and fixing.	Automatically fixes security issues before they cause damage.
Threat protection	Protects computers, company networks, and traditional servers.	Protects cloud applications, containers, and serverless computing.
Modern app development	Security is added after software is built, meaning security issues are only caught later.	Built into the software development process, stopping security issues before deployment.
Compliance	Security teams do manual audits to check compliance with security rules.	Automatically checks compliance with security rules in real-time, reducing manual effort.

Figure 1: Traditional Security vs. CNAPP

Key takeaway: CNAPP doesn't replace SIEMs or EDR — it fills the security gaps that traditional tools miss in modern cloud environments.

How CNAPP Is Solving Real-World Cloud Security Challenges:

- **Stopping security threats before they happen (shift-left security):** A financial services company faced an issue with misconfigured storage buckets that left sensitive data exposed. The organisation's SIEM system alerted it, but only after the exposure had already occurred. By adopting CNAPP's shift-left approach, it integrated security checks before deployment, ensuring that misconfigurations were caught before they became vulnerabilities.
  Outcome: Proactive threat prevention and enhanced security posture.
- **Reducing tool sprawl and strengthening security Posture:** Security teams often manage over 10 tools to secure a multi-cloud environment, leading to blind spots, duplicated alerts and operational inefficiencies. A global enterprise consolidated its security stack using CNAPP, reducing its tool count by 60% while improving threat-detection accuracy.
  Outcome: Fewer alerts, better visibility and faster response times.

- **AI-driven threat detection — scaling security without scaling teams:** A client with a small security team struggled to keep up with misconfigurations and identity-related threats. By adopting CNAPP with AI-powered analytics, it automated misconfiguration detection and policy enforcement without needing additional analysts. **Outcome:** 40% faster threat detection and a reduced manual workload.

These examples illustrate how CNAPP is addressing critical cloud security challenges, providing organisations with a more efficient and effective approach to safeguarding their cloud environments.

IaC security: Looking beyond the code

When considering infrastructure-as-code (IaC) security, many organisations focus solely on scanning tools like Terraform or CloudFormation. However, true IaC security extends much further. CNAPP adopts a comprehensive approach, encompassing the following:

- **OS images and virtual machine (VM) templates:** This includes hardened Amazon Machine Images (AMIs) and Azure VM images.
- **Container configurations:** Covering Kubernetes YAML files and Helm charts.
- **IAM policies and access-control settings:** Addressing misconfigurations in Amazon Web Services (AWS) Identity and Access Management (IAM) and Azure Role-Based Access Control (RBAC).

A colleague from a large software-as-a-service provider shared an experience in which an insecure Kubernetes deployment YAML granted excessive permissions to application workloads. Though the organisation's SIEM failed to flag this issue, CNAPP detected and blocked the misconfiguration before deployment, showcasing its effectiveness in ensuring robust IaC security.

> "Security teams often rely on security-information and event-management systems (SIEM) like Splunk or endpoint detection and response tools (EDR), but these solutions weren't built for the speed, scale and complexity of cloud-native environments. This is where cloud-native application-protection platforms (CNAPPs) come in — offering an integrated, proactive approach to cloud security that traditional tools struggle to provide.
>
> — Stephen Sargon, Manager, Technology Consulting, Enterprise Cloud, Protiviti

Implementing CNAPP effectively

Adopting CNAPP is not merely about deploying a new security tool; it also represents a fundamental shift in how organisations approach cybersecurity in the cloud. This transition requires a proactive mindset, focusing on integrating security measures seamlessly into the cloud-native environment. Here's how organisations can implement CNAPP effectively:

- **Assess cloud-security posture**: Identify misconfigurations and risks by evaluating your current cloud infrastructure for vulnerabilities and compliance gaps.
- **Integrate with DevSecOps**: Embed security in development pipelines by incorporating measures into CI/CD processes to address issues early.
- **Leverage AI and automation**: Enhance threat detection using artificial intelligence and automation to reduce alert fatigue and expedite response times.
- **Continuously monitor compliance:** Automate security audits to adhere to standards like NIST, ISO 27001, CIS and regional regulations.
- **Implement IAM:** Enforce the principle of least privilege by regularly reviewing and adjusting access controls.
- **Utilize IaC security:** Secure configuration templates by scanning IaC templates for vulnerabilities before deployment.
- **Foster cross-functional collabouration:** Align teams by encouraging cooperation between development, operations and security teams to integrate security throughout the application lifecycle.

Take action now

In today's fast-paced digital landscape, relying on a reactive security model means you're already lagging behind. It's time to shift toward a proactive approach with CNAPP. Here's how you can prepare:

- **Stay ahead of threats:** Proactive security measures are essential to anticipate and mitigate threats before they materialize. CNAPP enables you to embed security into your development processes, ensuring that vulnerabilities are addressed early on.
- **Complement don't replace:** CNAPP doesn't replace your existing SIEM systems; it fills the security gaps that traditional tools miss. While SIEMs are excellent for monitoring and logging, CNAPP provides an integrated, end-to-end security solution tailored for cloud-native environments. This comprehensive approach ensures that no aspect of your cloud infrastructure is left unprotected.
- **Prevent costly breaches:** Cloud misconfigurations are a leading cause of security breaches. These errors can expose sensitive data and lead to significant financial and reputational damage. CNAPP prevents these misconfigurations before they happen by continuously monitoring and enforcing security policies across your cloud infrastructure.

The bottom line

As many organisations leverage a cloud-first enterprise landscape, delaying the adoption of CNAPP can leave organisations dangerously exposed. Traditional security tools, often siloed and reactive, struggle to keep pace with the speed and complexity of cloud-native environments.

CNAPP offers a unified, proactive approach that integrates security across the entire application lifecycle — from development to deployment — ensuring that vulnerabilities are identified and mitigated before they can be exploited. The benefits offered are numerous and include the following:

- **Enhanced security posture:** By adopting CNAPP, you ensure that your security measures are robust, proactive and capable of addressing the unique challenges of cloud-native environments.
- **Operational efficiency:** Integrating CNAPP reduces the complexity of managing multiple security tools, streamlining your operations and improving response times.
- **Futureproofing:** As cloud environments continue to evolve, having a comprehensive security platform like CNAPP ensures that your organisation is prepared to handle emerging threats and compliance requirements.

Finally, the reputational and financial risks of inaction are too great to ignore. Misconfigurations, data breaches and compliance failures can result in significant damage —in terms of both cost and customer trust. CNAPP helps prevent these outcomes by continuously monitoring cloud infrastructure and enforcing security policies at scale.

Don't wait until a breach occurs to take action. Embrace CNAPP today to secure your cloud infrastructure, protect your data and stay ahead in the ever-evolving cybersecurity landscape.

For additional information, examples and insights, visit Protiviti's Cybersecurity Page. Protiviti is not a law firm, and nothing within this paper should be relied on for legal purposes. Clients should always seek legal advice from inside or outside counsel.

About Protiviti Cybersecurity Consulting

Securing your future with trust and confidence

From the speed of innovation and digital transformation to economic expectations and evolving cybersecurity threats, the talent gap and a dynamic regulatory landscape, technology leaders are expected to effectively respond to and manage these competing priorities.

To grow securely while reducing risk, your cybersecurity posture needs to adapt and respond to your business changing. As technology rapidly evolves and digital adoption accelerates, Protiviti's cybersecurity and privacy team turns risk into an advantage, protecting every layer of an organisation to unlock new opportunities securely.

Our strategic and technical subject matter experts fully understand your cybersecurity needs. We set out to assess, develop, implement and manage end-to-end next-generation solutions tailored to your specific needs. We share your commitment to protecting your data and optimizing your business and cyber resiliency.