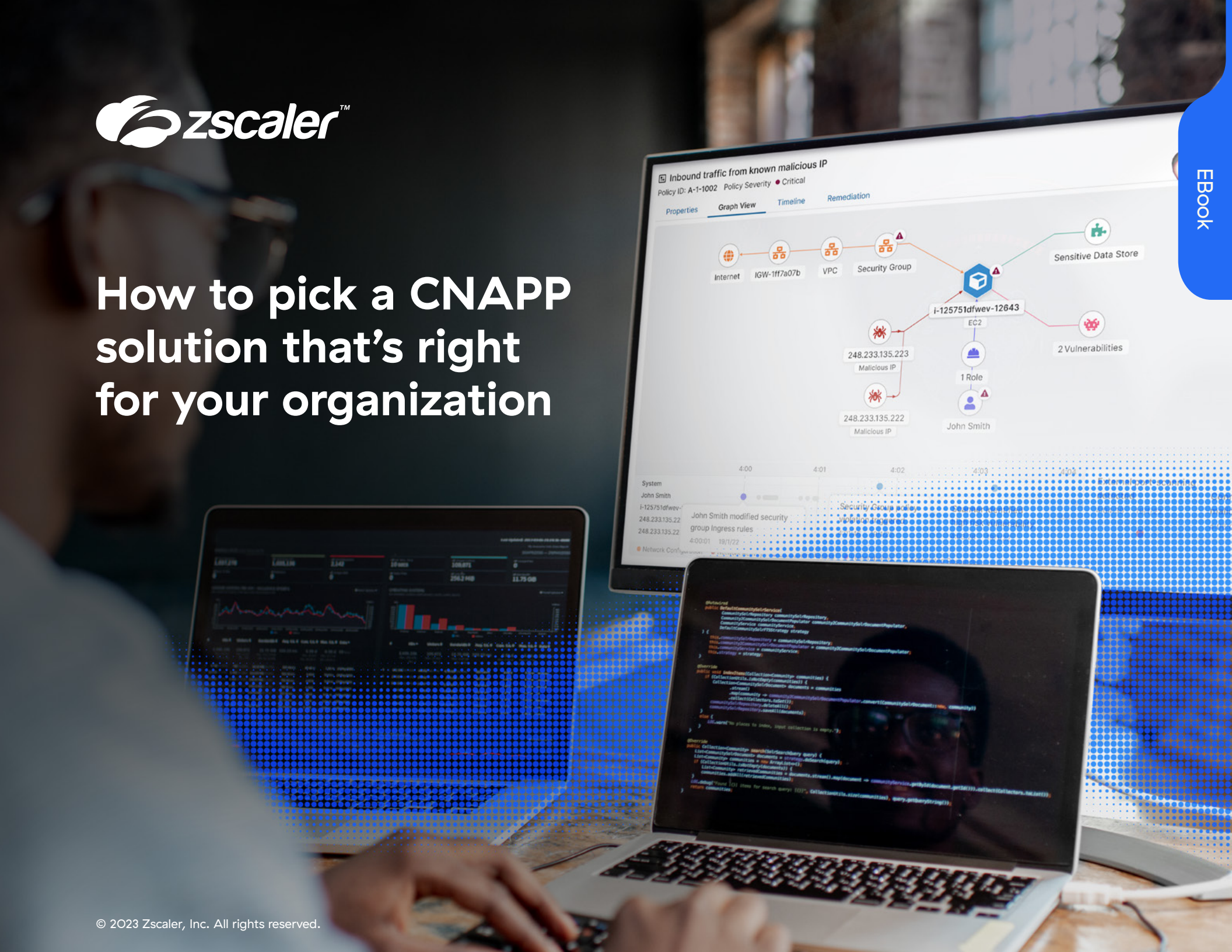
zscaler™

EBook

How to pick a CNAPP solution that's right for your organization



Contents

EBook

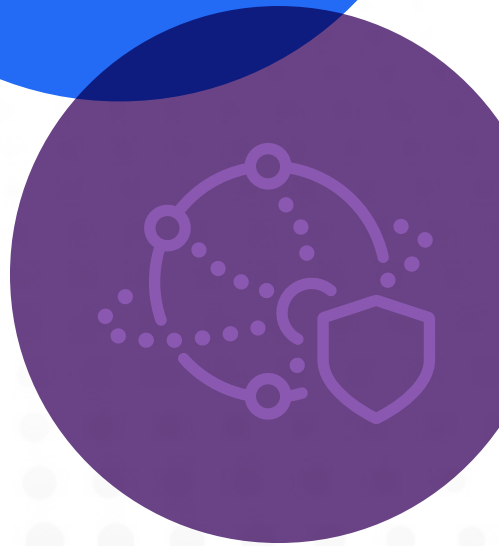
Intent

As organizations continue to migrate their resources to multicloud environments, attackers are right behind them, potentially about to make their next move to steal a business' crown jewels. Recently, headline-making security breaches are demonstrating that attackers can easily exploit cloud misconfigurations, mismanaged privileges, and vulnerabilities to penetrate an organization's public cloud infrastructure and reach its sensitive data. What's more, the dynamic and ephemeral nature of cloud resources dictates that they grow and shrink in a way that makes it almost impossible for security experts to identify, investigate, and understand compromised assets and data. Therefore, organizations are adopting different security tools to handle the scale of their cloud configurations, identities, sensitive data, and assets.

This has resulted in an increased demand for cloud security tools that can help InfoSec and DevOps pros boost productivity and identify software vulnerabilities, allowing organizations to remain agile in development while strengthening security. But maintaining a large inventory of security tools introduces its own set of challenges, such as increased complexity, new risks to mitigate, and reduced response times due to the need for cross-functional teams to gather the necessary context and wade through all types of alerts before they can understand an attack and take appropriate action.

An average enterprise uses 75 security tools to secure its infrastructure.

Source: CSO online



1. Source: CSO online

> “A CNAPP is an integrated set of security and compliance capabilities designed to help secure and protect cloud native applications across development and production.”
>
> **Source: Gartner, “Innovation Insight for Cloud Native Application Protection Platforms”, Neil MacDonald, Charlie Winckless, August 25, 2021**

Securing cloud native environments with CNAPP

Organizations are rapidly turning to cloud native application protection platforms (CNAPPs) to consolidate their security stacks while increasing both visibility over enterprise workloads and control over security and compliance risks in cloud environments. CNAPPs help organizations integrate security principles and standards across their development life cycles by implementing security controls at each stage—development, integration, deployment, and production operations. The overall idea is to identify security issues as early as possible, which helps save costs, avoids costly rework, and ensures that cloud workloads are born secure.

Selecting a CNAPP can be challenging as the cloud security market provides hundreds of standalone and consolidated tools. Each solution comes with its own set of features and technologies and the differences often aren’t easily discernible. With that in mind, this buyer’s guide is intended to help security leaders and practitioners gain a deeper understanding of core cloud security challenges, requirements, key architectural considerations, and questions to consider before purchasing a comprehensive CNAPP.

2. Source: Gartner, “Innovation Insight for Cloud Native Application Protection Platforms”, Neil MacDonald, Charlie Winckless, August 25, 2021

The key components of a CNAPP

- **Cloud security posture management (CSPM)** helps with the continuous assessment and monitoring of cloud security and compliance. At its core, CSPM detects cloud misconfigurations that put an organization at risk of security breaches or compliance violations. It generally uses cloud provider APIs to gather configuration data to check against the desired security posture.
- **Cloud infrastructure entitlement management (CIEM)** solutions address challenges related to human and non-human identities, permissions, and access by improving visibility and identifying and remediating IAM misconfigurations to establish least-privileged access throughout multicloud environments.
- **Infrastructure as code security (IaC)** is a form of automation that minimizes cloud misconfiguration risks. IaC scanning tools scan configuration files (e.g., HCL files for Terraform) to find vulnerabilities and misconfigurations. They can detect issues like vulnerable exposures, compliance violations, and the principle of least-privilege infringements.
- **Advanced threat and risk correlation** aggregates and transforms security data into meaningful insights to uncover hidden risks or attack vectors that could lead to a compromise or breach.
- **Compliance and governance** help to automate continuous compliance and remediate configuration drift and policy violations across multicloud environments.
- **Data protection** monitors, classifies, and inspects data to prevent its exfiltration resulting from exposure, vulnerabilities, malicious insiders, or other cyber threats.
- **Cloud workload protection platforms (CWPPs)** provide visibility and control for physical machines, VMs, containers, and serverless workloads in multicloud, and data center environments.

The growing challenge of securing cloud migration

Gartner predicts[3] that by 2023, more than 99% of cloud breaches will have a root cause of customer misconfiguration or mistakes, stating, "The reality is that securely configuring the cloud will remain a daunting task due to the sheer size, scale and continuous changes in workloads and infrastructure."

Some of the key challenges for secure cloud adoption are outlined:

DevOps speed and agility

DevOps is an area that deserves particular attention. Its rise derives from the need for increased visibility resulting from the thousands of resource and permission changes per day, and tens of millions overall. With developers having access to hundreds of services in the public cloud, it's extremely important that these services are used securely, least risk posed to the organization.

Complex, distributed multicloud environments

To achieve business goals, technology leaders are choosing to work with multiple cloud providers and embracing different clouds optimized for various services. Major cloud platforms are rapidly evolving to boot, regularly adding new services and features. More clouds mean more accounts, more access control policies, services, and so on. All of this adds up to a broader, easier-to-reach attack surface. To have a successful cloud security and compliance program that can grow with the organization and still be easily operationalized, security leaders need to identify, evaluate, and validate a solution that has the right security and automation capabilities and can support multicloud security operations smoothly.

Shared responsibility model

Many organizations believe the cloud is secure by default and that cloud native security tools will protect them against security breaches by themselves, but moving to a multicloud environment doesn't mean outsourcing security to cloud vendors. Though most vendors have controls and tools in place, security ultimately remains an organization's responsibility. Securing the cloud depends on a shared responsibility model. By understanding the proper responsibilities, organizations can better avoid security gaps.

3. Source: https://blogs.gartner.com/andrew-lerner/2020/11/10/four-cloudy-predictions/

Scattered sensitive data

Data in a multicloud environment is spread across multiple clouds. It's also increasing in volume, constantly changing, and being accessed by both internal and external sources. As data and control become increasingly distributed, the risk of inadvertent exposure rises, too, and maintaining visibility over data and compliance with legacy offerings becomes difficult, if not impossible.

Threats and vulnerabilities

One of the biggest challenges security teams face with cloud vulnerability management is a lack of visibility into and control of multicloud environments. Cloud environments are highly dynamic and ephemeral, with the average lifespan of a container being just hours. Without understanding exactly where vulnerabilities are, an organization can leave itself exposed to the latest attacks by cybercriminals.

Securing such an environment using a conventional approach and agent-based tools is difficult and sometimes impossible as it requires tedious deployments and management for each workload, elevating cost, complexity, cross-team friction, and performance issues. To stay ahead of attacks, security and risk leaders need sophisticated insights into vulnerabilities that are high-risk with remediation options for all assets.

Tool sprawls and siloed teams

Multiple, non-integrated traditional security tools create complexities that lead to security gaps and increased overhead. Moreover, securing cloud native environments requires strong collaboration between security, development, infrastructure, and operations teams. Unifying these teams and their processes with traditional security tools can be challenging, as undefined roles and policies can lead to gaps in security and add to cost and management complexities.

The most significant benefit of a CNAPP approach is better visibility and control of cloud native application risk.

Source: Gartner, Innovation Insight for Cloud-Native Application Protection Platforms

What to look for in a CNAPP

Deep visibility with risk context, analytics, and impact

The first step to a strong security posture is deep contextual visibility that allows you and your team to gain insight into all cloud resources, entities, and data, and see how their relationships affect your organization's overall security posture.

Organizations should consider a CNAPP that streamlines visibility into assets, accounts, data, and areas of exposure in one platform. Cross-functional teams should be able to visually explore and analyze the business impact of exposure, prioritize risk remediation, and trace the likelihood of security incidents. As a result, security teams can more effectively enforce policies and procedures and monitor for continuous governance and security.

Integrated data security

As the value of data continues to grow, a greater percentage of cyberattacks become financially motivated, leading bad actors to focus harder on data breaches.

The shared responsibility model dictates that customers are partially responsible for securing sensitive data. This is where a comprehensive CNAPP comes in, as it delivers the granular data protection organizations need. It allows scanning storage services to automatically identify and classify sensitive content and apply cloud data loss prevention (DLP) policies to prevent unauthorized activity. The solution you choose should be able to compare storage configurations against industry benchmarks and compliance

frameworks to report violations, quickly remediate them, and ensure public cloud applications are configured to prevent data exposure and maintain compliance.

Automated compliance

The ever-expanding use of the cloud makes it much more difficult, complex, and time-consuming to meet and keep up with industry standard regulations. As organizations adopt and move to cloud platforms, compliance standards and rules evolve in tandem.

An ideal CNAPP should help cross-functional teams to meet the needs of ever-changing compliance standards and keep up with evolving cloud infrastructure. It should provide a complete picture of compliance posture with deep visibility, enable auto-check against cloud service configurations across major CSPs, run scans against hundreds of industry best practices and compliance frameworks like HIPAA, GDPR, NIST, etc., and remediate compliance violations. It should have the flexibility to create custom policies for improving compliance according to an organization's unique security and regulatory needs.

Vulnerability management

An ideal CNAPP solution should continuously monitor an environment for unexpected changes and provide full-stack visibility through a single pane of glass covering VMs, containers, and serverless and cloud infrastructure resources. It should identify vulnerabilities and prioritize remediation with rich context supported by comprehensive data analysis, correlation, and a background reporting engine. It should empower users and cross-functional stakeholders to proactively address potential risks with seamless third-party ticketing or existing security ecosystem integration to configure near-to-real-time alerts reducing mean time to remediation (MTTR).

Infrastructure as Code (IaC) security integration

It's crucial to identify and resolve misconfigurations in infrastructure as code during the earlier development phases to maintain a secure posture in runtime. This helps in establishing a secure baseline and ensures that cloud infrastructure can be provisioned without risk or hindering a developer's workflow and agility.

CNAPP should support IaC and other key technologies and be able to review code through development. It should also offer a robust policy library and the flexibility to create custom policies. It should also be able to detect, prioritize, and remediate risk or policy violations and enforce guardrails so security can keep pace with development.

Gartner recommends:

- Implementing an integrated security approach that covers the entire cloud native application life cycle, starting in development and extending into production
- Scan development artifacts and cloud configuration comprehensively, and combine this with runtime visibility and configuration awareness to prioritize risk remediation
- Evaluate emerging CNAPP offerings as contracts for CSPM and CWPP expire and use this opportunity to reduce complexity and consolidate vendors

Source: Gartner, Innovation Insight for Cloud-Native Application Protection Platforms

A CNAPP should empower cross functional teams to:

Developers

- Gain critical insights to detect, track, and fix issues as part of a normal workflow
- Easily collaborate and address security concerns to save cost and time
- Enable security teams to implement specific controls with full visibility and approval

Operations

- Ensure secure deployment while reducing costs and complexity
- Accelerate secure release cycles with strong collaboration and communication
- Automate workflows

Security

- Gain visibility and control over the attack surface
- Enforce consistent baseline security policies and guardrails
- Reduce alert fatigue while receiving real-time alerts to high risk security incidents
- Reduce MTTR with guided remediation for cross-functional teams
- Validate compliance with standards

Application life cycle security

Most organizations leverage CI/CD pipelines to continuously build and deploy infrastructure. CNAPP can help detect misconfigurations, vulnerabilities, and violations during the development phase to help maintain security posture during runtime. An ideal CNAPP needs to integrate with CI/CD tools and ensure security is woven into the development cycle to act as a guardrail. This ensures continuous security and blocks misconfigured or non-compliant resources from being deployed, so that the SecOps and DevOps teams receive a single source of truth. When selecting a CNAPP solution, organizations need to explore the breadth of CI/CD integrations to be sure that their solution of choice supports the tools they use.

Enterprise integration

A CNAPP should be able to prioritize critical security incident notifications and alerts. It should integrate with an existing SecOps ecosystem to automatically generate and assign tickets to the appropriate Cloud Operations (CloudOps) team members. These tickets must contain vital information about non-compliant resources that helps teams to understand and undertake the immediate corrective steps necessary to rectify any identified risks in cloud environment while supporting data protection, compliance reporting, and auditing.

While selecting a CNAPP solution, businesses must ensure that the platform they choose properly integrates with SecOps and DevOps tools and that technical infrastructure teams can benefit from a unified approach to reporting as well as real-time dashboards.

CNAPP checklist and considerations

Requirements vary between organizations, but the following checklist and considerations can help security teams comprehensively evaluate a CNAPP solution.

Operations

- Agentless coverage/broader coverage
- Risk-based prioritization
- Security best practice enforcement
- Compliance framework and number of auto-checks
- Dedicated dashboards for assets, inventory, compliance, identities, etc.
- Security alerts and notifications across multiple channels
- Context-based reports for resources, assets, and identities
- ITSM integration
- Complete cloud insights using simple query language
- Custom policies in private benchmarks
- Backend integrations with BI tools
- Utilization dashboard
- License scalability as an enterprise requirement grows
- Auto-upgrades and the addition of new capabilities

CSP Support

- Support across all leading public cloud service providers such as AWS, GCP, and Azure

Visibility

- Asset inventory
- Risk posture
- Compliance posture
- Vulnerability
- IaC violations
- Investigation
- Advanced threat and risk topography visualization

Security automation

- Automated security monitoring, evaluation, analysis, risk prioritization, reporting, and remediation (manual, guided, and automated)

Compliance assurance

- Compliance assurance across security standards and regulations
- Custom compliance standards and regulations
- Auditor reports and dashboard visibility

IAM and permissions management

- Dashboard and risk scorecard
- Enforcement of security and least-privileged access
- Entitlements network topology visualization
- Cross-cloud entitlements correlation
- Permission right-sizing
- Over-permission detection and remediation

IaC

- Types of IaC supported
- Compliance and security standards supported
- Integration with CI/CD tools
- Capability to remediate and resolve issues in runtime

Summary

Organizations want to unleash benefits of multicloud environments and realize their developers' true potential so they can create compelling, compliant applications that enable strategic business outcomes. Hence, security now needs to evolve and be integrated into every stage of development, breaking the traditional silos between cross-functional teams and, at the same time, reducing the complexity and cost of innovation. Organizations need a more straightforward way to mitigate risk and reduce complexity without compromising on the speed of innovation and security. CNAPP can be a one stop solution for organizational security requirements. That being said, when evaluating CNAPP, it's critical to look for a platform that can provide continuous visibility and proactive risk prevention for infrastructure, workloads, data and applications covering build, deployment, and runtime protection.

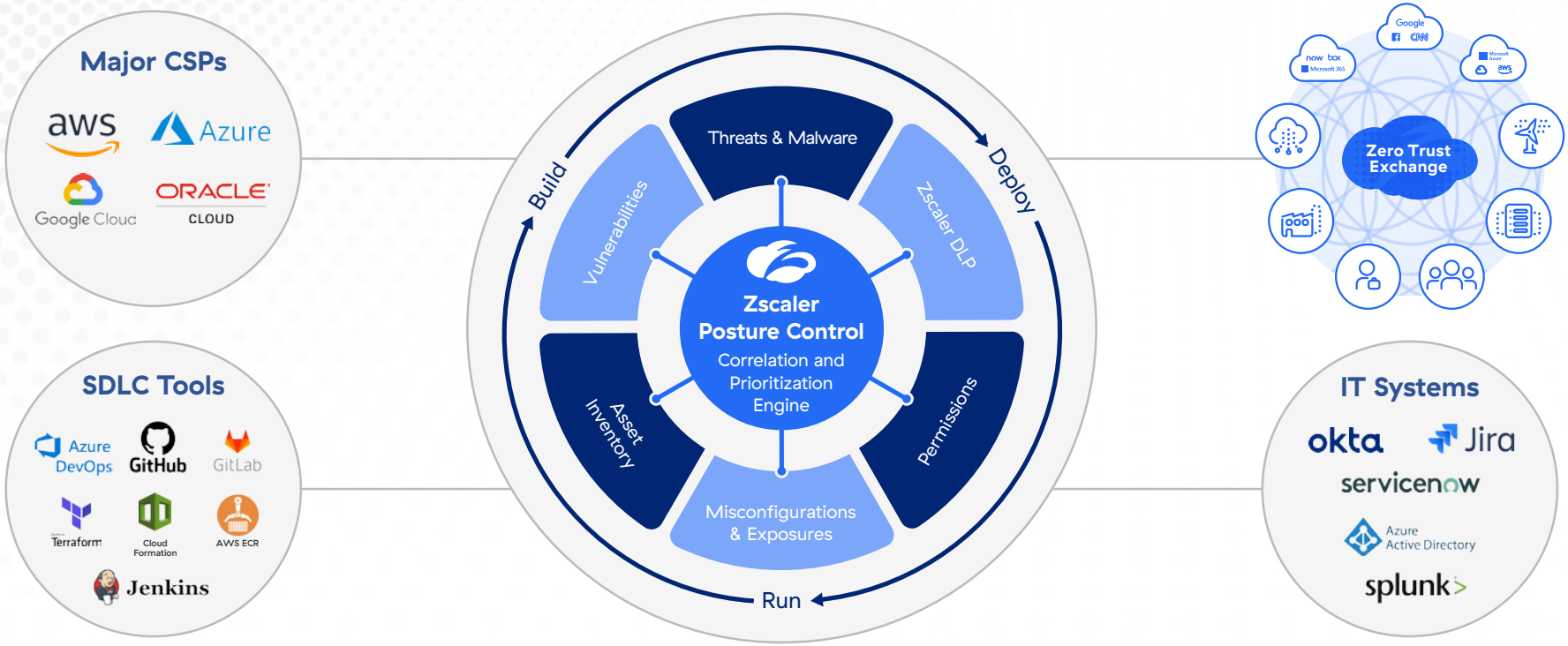
Transforming cloud native security with Posture Control by Zscaler

A CNAPP that suits your security needs

Posture Control by Zscaler is a cloud native application protection platform (CNAPP) purpose-built from the ground up to solve the above use cases and more.

At the heart of Posture Control is a robust graph- and database-based correlation and prioritization engine that takes signals from various data sources to identify, classify, and prioritize true cloud risk. The platform looks for a wide range of risk indicators and identifies combinations of weaknesses that can be exploited by bad actors and alerts security teams so they can focus on the right resources and aspects.

Zscaler Posture Control: Build, Deploy, and Run Secure Cloud Apps



Faster cloud migration via up to 80% reduction in security & compliance delays

40–60% cloud security **program cost reductions**

Prioritize risk to maximize infosec effectiveness and dev/DevOps collaboration

Continuous compliance saves 4–6 months vs manual audit

Input signals for Posture Control include an agentless/API–based scanning mechanism for a complete, robust asset inventory from public cloud environments (AWS, Azure, Google Cloud and others) which includes but is not limited to elements such as compute resources, databases, identities, and entitlements. Through these capabilities, Posture Control is able to consolidate several point solutions including CSPM, CIEM, vulnerability scanning, and more.

Posture Control also provides a broad range of integrations that help your team operationalize findings and fully integrate them into your teams' workflows. Posture Control has native integrations into the most commonly requested IT systems, including IAM, SIEM, and ITSM platforms.

Improve productivity and increase agility without compromising security

Tell us your use case and our experts can show you how Posture Control can address your security needs, or schedule a personalized demo today to experience Posture Control.

Discover more at:

zscaler.com/cloud-security-assessment

zscaler.com/products/posture-control

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com