WIZ for Gov

The cloud security workflow guide for government

A step-by-step guide to establishing a cloud security workflow that enables a secure foundation to support critical missions.

Practical guide to the cloud security workflow for government

Government agencies are adopting more cloud and realizing the benefits of scalability, flexibility, and cost-effectiveness. At the same time, the cloud has led to the largest transformation to security in our lifetimes. As public sector agencies often support critical missions, they must ensure the highest security standards in their cloud environment. Due to this transformation, public sector organizations are grappling with the new and unique security challenges to protecting their resources and data in the cloud.

Cloud security operations is a critical aspect of protecting an organization's cloud. It is essential for government agencies to have a clear understanding of the security risks and appropriate measures to protect their environment. In this practical guide, we will detail the journey that public sector organizations can take to achieve a cloud security operating model that enables visibility across a rapidly growing environment and appropriate measures to secure that environment efficiently. This guide will provide a series of simple steps for how to build a cloud security foundation and mature your practice over time. By following these best practices, public sector organizations can improve their overall cloud security posture and better protect their assets in the cloud.

Table of Contents:

The cloud has fundamentally transformed security 3

Principles of a modern cloud security workflow 4

Achieving the new workflow in four phases 5

Phase 1: Visibility 7

Phase 2: Critical risk reduction 9

Phase 3: Democratization for continuous improvement 12

Phase 4: Shift left for prevention 15

Appendix: 18

Cheat sheet for the new cloud security workflow 18

Cloud security platform RFP 18

The cloud has fundamentally transformed security

The cloud is the biggest transformation to security in three important ways:

The environment is completely different – Development teams are now building in the cloud faster and more decentralized than ever before. As a result, the environments are highly dynamic, with resources constantly being created, updated, and deleted. This dynamic nature of the cloud makes it more challenging to keep track of and secure all resources across clouds and architectures. Decentralized teams are also bringing in countless technologies that improve their efficiency. As a result, security teams must increasingly cover a multi-cloud, multi-architecture, and constantly changing surface area. 2021's Log4Shell crisis demonstrates the difficulty for teams to even identify where they may have exposure across an increasingly complex and dynamic environment.

The risks are completely different – Cloud environments are now shared and controlled by 3 rd party providers. With public cloud, these environments are by default on the internet or can be easily exposed to the internet with a single configuration. While exposure can happen simply, the underlying risk factors can be difficult to spot. Verizon's annual DBIR report routinely cites complex intrusion attacks that combine two or more risk factors as the most common attack vector for data breaches. This becomes even more difficult to monitor for and protect in today's landscape with the unprecedented velocity and scale of attacks and that an exposure can be exploited to become a breach in a matter of hours. Consistently, exposed databases are one of the top breaches that we read about in the news, underscoring the difficulty in securing an organization's crown jewels.

The ownership model is completely different - Development teams own their infrastructure and each team chooses and deploys their own technologies. Centralized architectural choices can quickly become obsolete if they are not approved or adopted by decentralized teams. The people, processes, and technology in an organization also face challenges in light of the new environment and new risks. Many organizations will need to adapt their security practices and redefine traditional security approaches and processes that are not well-suited for the cloud environment. There will need to be a concerted focus on education as an increasing number of cloud teams are building in the cloud oftentimes lack cloud security expertise. Security teams themselves need to learn the security risks of the cloud and implement new security processes and technologies to protect their resources. Many organizations find themselves in need of experts with deep domain expertise by cloud, architecture, or risk vector. Finally, teams will need to reconsider their tooling as many legacy technologies amplify overall cloud challenges with siloed views of the cloud environment and risk. For example, traditional tools may only look at a single architecture like containers or are only in use by security teams and not DevOps teams. This leads to organizational siloes that make it more difficult for security and development teams to identify and remediate security issues.

The cloud environment is completely different from traditional environments. The expanding cloud footprint, increasing complexity of risks, growing number of development teams, and unrelenting pace of innovation creates exponential demand on security teams. These teams are tasked with a broad set of responsibilities to understand these new risks and take appropriate measures to mitigate them. This includes implementing robust security measures, training employees, and adapting security processes and technologies to the cloud environment. Unfortunately, the reality is that many organizations have limited security capacity, much of which is bogged down and burnt out from manually investigating baseline security issues and alerts and chasing down developers to remediate those issues. This creates a gap between actual capacity and what is needed to properly secure the cloud environment. As a result, organizations face blind spots in coverage, an inability to identify the most critical risks to their crown jewels, and a growing feeling of distrust between security and development teams -- all resulting in a slowing of the cloud journey. This widening gap can't be solved only by hiring more security experts, especially considering the global shortage of security personnel. As a result, organizations need to rethink how they scale security to meet their requirements.

Cloud security needs a new workflow

Key to this new approach is recognizing that cloud security needs to evolve to become a team sport. To effectively scale security, each cloud development team will need to understand and control risks together with security across the development pipeline. This means that tools and processes will need to evolve so that they can easily be incorporated into the development process. It needs to be self-service for simple access on demand, simple to use without requiring deep security domain expertise, and focused as developers won't have time to parse through long lists security issues.

In order to extend cloud security responsibilities to the development teams, a modern cloud security workflow will need to incorporate three important principles.

Full-stack visibility: You must start with a foundation of visibility across your entire cloud environment for everyone involved in building and security the cloud. This visibility needs to always be up-to-date without disruption to the business or relying on developers to deploy agents. It must also be very easy to understand without requiring deep domain expertise. This visibility allows every team to understand their entire cloud environment, identify risks, and take appropriate measures to mitigate them.

Proactive security: Security must be proactive to eliminate risks before they become breaches. This requires pinpoint accuracy to reduce noise and to focus teams on the highest priority issues. By prioritizing the most critical issues, security can build trust with development teams and ensure that developer's time is spent wisely in streamlining security as part of the development process.

Enable business agility: Lastly, in order to scale and operate efficiently across teams, cloud security must be tightly integrated into the technology stack, organizational structure, and development pipeline. This enables organizations to route issues directly to the teams that own them using the automation tools that their teams are already familiar with. This enables self-service to rapidly understand and remediate issues.

A modern cloud security operating model is essential for organizations to address the new challenges of cloud and to effectively protect their environment. It requires treating cloud security as a team sport and making security self-service in the development process. This requires enabling collaboration and cooperation across teams through a foundation of visibility, a proactive approach to security, and tight integration into the overall business process. By following these principles, organizations can improve their overall cloud security posture and better protect their cloud assets.

Achieving the new workflow in four phases

The modern cloud security operating model is not a destination but rather a journey of continuously improving an organization's cloud security posture. It is a journey that involves gaining visibility into an organization's cloud environment, identifying and remediating critical risks, adopting best practices to continuously improve overall security posture, and shifting left to focus on preventing issues from even entering the production environment. In the next section, we provide key goals for each phase as well as the core capabilities that organizations should strive to achieve. While this guide frames the journey in 4 discrete steps, organizations should not focus on each step solely in sequential order. For example, we recommend that customers begin the process of critical risk reduction outlined in phase 2 even if they have not achieved the full visibility א in phase 1.

1. Visibility	100% visibility into any cloud, any architecture Normalization across clouds to simplify security for any engineer Ability to segment visibility by team based on infrastructure ownership
2. Critical risk reduction	Comprehensive understanding of workload and cloud risks Identification of attack paths and critical combinations of risk Clear prioritization, context, and evidence for remediation down to 0 critical risks
3. Democratization	Proactive reduction of the attack surface and blast radius for continuous improvement Ingrain security into the development process through self-service Enterprise readiness for the next threat or business shift
4. Prevention	Secure from source to production including container registries, VM images, and IaC Prioritize policy enforcement in the pipeline to prevent introduction of issues into production Implement hardened baselines to reduce drift

Phase 1: Visibility

The first phase in the journey is to build your cloud security foundation so that security becomes the default in your strategy, processes, and culture across teams. Achieving this starts with full-stack visibility across all clouds and architectures for all your teams that build and secure your cloud environment. This allows organizations to have a holistic view of their cloud environment, including all resources, configurations, and vulnerabilities, regardless of where they are located. As the old saying goes, you can't secure what you can't see.

For this first stage of the journey, organizations should aim to achieve three key goals:

1. 100% visibility into any cloud and any architecture that their business chooses today and in the future. For example, if development teams choose to adopt serverless containers or if the business acquires another organization that uses Oracle Cloud in the future, the cloud security team needs to gain seamless visibility without needing to deploy new technology or hire dedicated experts.
2. Normalization across clouds and technologies to simplify security for any security or engineering team. For example, identities are treated completely differently from AWS to Azure to Google Cloud. For most organizations, it is unreasonable to ask a developer to understand how identities and entitlements are modeled across each. As part of this goal, can you make it easy for developers to quickly understand who has access to what?
3. Segmentation of visibility for development teams based on their ownership of the infrastructure. While it is useful and necessary for security to have full visibility into the environment, it becomes noisy for a developer that may own only a portion of the infrastructure. For this goal, can you show the developer only what they care about to further simplify and streamline their security responsibilities?

As part of achieving full-stack visibility, organizations should look for the following capabilities:

Full cloud inventory of your cloud resources:

Cloud coverage – Your organization may be all in on a single cloud service provider or leveraging multiple clouds. Ensure that your cloud security foundation provides you consistent visibility into your cloud resources across all your environments regardless of if they are in AWS, Azure, Google Cloud, Oracle Cloud, Alibaba, or hybrid cloud with VMware vSphere. You should also consider Kubernetes and OpenShift as a cloud within a cloud and similarly gain visibility into those resources.

Architecture coverage – Your cloud teams will have likely chosen a broad mix of architectures across the IaaS and PaaS services. Gaining full-stack visibility means understanding all your cloud workloads including virtual machines, containers, serverless functions, serverless containers, and buckets.

Technology coverage – In addition to your cloud workloads, your security team needs visibility into all the cloud services utilized in your environment (eg: Amazon OpenSearch Serverless) and technologies deployed on your workloads, including operating systems, applications, API endpoints, databases, code libraries, etc as well as their status to control for shadow IT.

Automatic and continuous detection – Cloud environments are always changing. If you only evaluate your cloud inventory on an infrequent basis, you are nearly guaranteeing that your inventory is always out-of-date. It is therefore very important that you have the ability to discover new resources automatically as they are deployed and to monitor your existing resources for changes in realtime. Traditional security approaches have leveraged agents for visibility but this approach is flawed as it relies on developers deploying agents proactively on every workload. Consider using an agentless approach to remove the neverending burden of agent enforcement and management.

Configuration visibility – There are a broad variety of configurations that affect the way that your cloud operates. Identity and Access Management (IAM) configurations define who can view, modify, and run cloud workloads. Network settings control which other resources a workload can interact with over the network. Platform-specific configurations, such as environment settings defined inside container images or RBAC policies in Kubernetes, add yet more layers to cloud workload configurations. Visibility into your cloud needs to extend to these different configuration options across your cloud, application, and OS layers.

Role-based access control:

In order to streamline cloud security into the development process for development teams, it is important that the full cloud inventory created for full-stack visibility can also be simplified and focused for each cloud team. These teams each own different parts of the infrastructure whether by cloud provider, by business unit, by application, or other organizational structure. One key capability you need to develop to ensure effective collaboration and efficiency across teams, is the ability to have granular environment segmentation to align with development separation. This means having the ability to group cloud resources according to their users or purposes with role-based access controls to give developers visibility over the resources related to their projects. Any technology that you leverage to populate and update your cloud inventory must therefore be made available to your development teams.

Gaining comprehensive visibility into a cloud environment is crucial for organizations to effectively protect their resources and data in the cloud. One key metric that organizations should be cognizant of in this stage is what percentage of their environment does the security team have automated, continuous visibility over? By implementing a modern approach to cloud security that provides visibility across all cloud architectures, organizations can improve their overall cloud security posture and better protect their assets in the cloud.

Phase 2: Critical risk reduction

Reducing critical risk in a cloud environment is crucial for organizations to effectively protect their resources and data in the cloud. First, you need to understand risks holistically. This involves a comprehensive view of all cloud risks impacting your resources. This allows organizations to identify and understand the risks associated with their cloud environment. In the cloud, there are risks everywhere and it is not possible nor reasonable to expect your teams to remediate all of them. You can never patch everything or always ensure correct configurations across every resource. Log4Shell was just one example of how the old playbook has expired. Simply creating lists of findings is obsolete and further erodes trust between security teams and developers. The key question is how quickly can you patch and correct the most critical risks?

For this second phase of the journey, organizations should aim to achieve three key goals:

1. Comprehensive, continuous evaluation of workload and cloud risks. Your security program should analyze all of the potential risk vectors into your cloud including external exposure, cloud entitlements, configurations, use of secrets, sensitive data detection, vulnerabilities, patch management, malware, and threat detection across your architectures and clouds.
2. Identification of attack paths and toxic combinations of risk. Verizon's DBIR report indicates that complex attacks are routinely amongst the most common source of data breaches for organizations. Your security program needs to effectively correlate the risks uncovered in goal #1 to uncover the complex chains of exposures and lateral movement paths that lead to high-value assets such as admin identities or crown jewel data stores. These attack paths that represent the highest probability of breach with the largest potential blast radius are sophisticated and oftentimes hidden but are the most critical for your teams to discover and address quickly.
3. Clear prioritization, context, and guidance for remediation down to 0 critical risks. Once you've discovered these attack paths, the most important goal is to work effectively across teams to rapidly remediate them. This is where the granular environment segmentation goal described in phase 1 of this journey is critical. You need to know exactly which team owns the part of your infrastructure that a critical risk impacts and route this issue, along with all of the evidence for it to the right team so they understand the importance of taking rapid action. Intelligent remediation guidance is also critical to taking the guesswork out of moving rapidly.

As part of eliminating critical risks from your cloud environment, organizations should look for the following capabilities:

Exposure analysis and validation: Identify public exposure of your resources by conducting a thorough network analysis to determine exactly which resources are exposed and how. This involves understanding effective exposure by analyzing your network management services such as load balancers, firewalls, network interfaces, gateways, VPCs, subnets, etc and your network rules.

Go a step further by validating the status of ports and IP addresses of externally exposed resources.

Misconfiguration analysis: Identify misconfigurations by evaluating your current configurations against best practice policies for each layer of your cloud environment including your cloud, application, and host layers. Assess against industry standard benchmarks such as CIS, NIST, and ISO to evaluate regulatory compliance and risk.

Vulnerability management: Understand how each compute instance in your environment is vulnerable using up-to-date vulnerability databases that keep pace with the ever-changing world of patch and vulnerability assessment. Enrich your assessment by including version information such as whether the version in use is end-of-life or the latest version.

Secure use of secrets: Secrets are one of the most common lateral movement paths used by attackers. Detect leaked secrets or credentials that are exposed on your workloads. Correlate secrets with identity entitlements to understand the full blast radius if a secret is compromised.

Malware detection: Continuously scan for potentially malicious software on all your compute resources to prevent the spread of malicious code in your environment.

Sensitive data detection: Identify where sensitive data such as Personally Identifiable Information (PII), Payment Card Industry (PCI) data, or Protected Health Information (PHI) about your employees, partners, and customers resides to uncover possible data leaks.

Kubernetes security posture management: Continuously monitor Kubernetes clusters to identify misconfigurations and assess them against CIS benchmarks for Kubernetes, EKS, AKS, and GKE.

Identity analysis: Analyze effective permissions across all your identities and policies and normalize them across your cloud security providers to understand who can access which resources and what actions they can perform on them. Use this analysis to flag excessive permissions and lateral movement potential.

Attack path analysis: Contextualize your risk factors together by correlating them to uncover toxic combinations of risk that create attack paths into your environment. These attack paths can include lateral movement that can lead to compromised highvalue assets.

Customizable policy frameworks: Build organizational controls to surface the security risks that are most relevant for your business. For example, risks that impact your production environments should be assigned higher severity than risks in your development or test environments.

- **Automated workflows:** Build automation workflows and leverage cloud-native playbooks to intelligently alert the teams responsible for the infrastructure and risks with all the context of your risk analysis and remediation guidance to ensure rapid action is taken on critical risks. Your workflows need to be tightly integrated into your cloud infrastructure ownership model with RBAC and into your development team's technology stack by leveraging the automation and ticketing systems that they are already comfortable with.

By understanding risks holistically, stopping attack paths into the cloud, and driving the total number of critical issues down to zero, organizations can rapidly improve their overall cloud security posture and build tighter relationships between security and development teams. The most critical metrics for organizations to measure for this phase is the number of critical issues open in their environment and overall reduction in critical issues over time..

Phase 3: Democratization for continuous improvement

The next step of the journey is to democratize security across the organization in order continuously improve security posture. It involves ingraining security into the development process through self-service. Organizations should enable all cloud teams to work together on assessing the current state of an organization's cloud security against best practices, identifying areas for improvement, implementing measures to improve the overall cloud security posture, continuously monitoring and evaluating the effectiveness of the security controls and processes in place, and maintaining a high level of security maturity. This process must be automated and continuous to successfully respond to a rapidly changing and dynamic environment. This enables organizations to stay ahead of the relentless pace and scale of attacks and to prevent unintentional exposures from becoming breaches by reducing the time it takes teams to detect and respond to new combinations of risks and threats

For this third phase of the journey, organizations should aim to achieve three key goals:

1. Proactive reduction of the attack surface and potential impact of a successful attack for continuous improvement. While phase 2 focused on critical risk reduction, phase 3 should focus on the reduction of lower, but still high-priority risks. Organizations should approach this with an intentional program that focuses on both reducing the attack surface and the potential blast radius of a successful attack. We recommend that organizations take a programmatic approach with projects to address each risk area (eg: this month our team will patch all Linux machines with high issues, rotate all keys all that allow high privileges, or enforce least privilege in our Azure environment).
2. Democratization of security across teams with security a seamless part of the development process. Organizations should ingrain security into the development process. This means implementing development team specific measures and processes to continuously improve security posture and ensure adoption of best practices. This enables security teams to get out of tactical firefighting and into strategic planning and decision-making. This requires continuous monitoring and evaluation of the controls and processes in place and ensuring that developers have the tooling and education for them to effectively self-serve security in their development processes.
3. Enterprise readiness for the next threat or business shift. Cloud security is one of the fastest evolving areas of InfoSec. Organizations need to ensure they are ready for the next threat (eg: Log4Shell) so that they can easily provide answers to leadership and the board on how they are impacted and the time required to address issues. Additionally, businesses shift constantly, including through mergers and acquisitions. Security teams must be ready to repeat the steps laid out in this practical guide as they assess, acquire, and integrate new businesses that may come with an entirely different cloud and technology stack.

As part of continuous security improvement of your cloud environment, organizations should look to establish the following capabilities:

Self-service access for development and operations: Organizations need to provide direct visibility into risks and their evidence to all their teams that build in the cloud. These teams don't want noise so give them visibility into only the parts of the infrastructure that they own through role-based access control. This approach must simplify security for any engineer and focused with clear priority, context, and evidence for efficient remediation.

Segment cloud security and remediation by risk factor: Organizations need intuitive, visual summaries of their risks and how to fix them sorted by risk factor. Whether you have one security team or dedicated teams for identity, vulnerability management, or other risks, this enables organizations to programmatically create projects and roadmaps for addressing high and medium level risks.

Continuous monitoring and incident response management: Ensure sufficient logging for your environment across tools and that you've connected your cloud tools to a SIEM solution. Integrate these solutions together so that you gain more context to make better prioritization decisions in your organization. Integrate with cloud-native playbooks to automate response at scale.

Policy management, enforcement, and alerting: Centralize your security policies so that you have consistent approaches across your clouds, architectures, and teams. Apply business specific rules (eg: unapproved cloud services may not be used in production or customer databases cannot be exposed without proper authentication) to provide visibility to security with alerting when thresholds are violated or critical risks are detected.

Automated compliance assessments: Implement processes that evaluate your compliance against industry standard and custom benchmarks automatically. Segment compliance reports using your role-based access control mechanism so you have a clear understanding of performance across infrastructure, business units, and applications to focus teams on gaps.

Rapid threat detection and response: <24 hour detection of the presence of emerging threats in your environment. Prioritize the most critical risks with immediate next steps using the context of other cloud risks to reduce downtime and urgent triage. Automatically route or enable self-service for development teams to remediate issues in their portion of the infrastructure.

Readiness for M&A: Enable M&A or integration teams to rapidly assess the security posture of target organizations using agentless capabilities that provide full visibility into new cloud environments and identification of critical risks.

Democratizing security and continuously improving security posture helps organizations to protect unintentional exposures from becoming breaches, thus further reducing the risk of a security incident. These efforts will ultimately help organizations to protect their assets and maintain the trust of their customers and stakeholders. Key metrics include active usage of your security platform across all teams, reducing the time it takes to detect and respond to risk, increasing the adoption of security best practices, and reducing downtime associated with unexpected security issues. By measuring and monitoring these KPIs, organizations can ensure that they are effectively identifying and mitigating risks, improving incident response times, and proactively preventing security breaches across all their cloud teams.

Phase 4: Shift left for prevention

The final step of the journey is to shift left to create security guardrails that unleash developer productivity. As organizations increasingly adopt cloud-based infrastructure and shift to a DevOps model, it is becoming increasingly important to integrate security into the development pipeline with a prevention-first approach. This approach can help to ensure that security is built into the development process from the beginning, rather than being an afterthought, and can help to reduce the number of risks introduced into the production environment. By focusing on prevention, security teams can proactively identify and eliminate risks against their security policies before they are deployed. This approach can also enable development teams to take greater ownership of security, which can lead to a more efficient and effective security posture overall. By shifting left and creating security guardrails with a prevention-first approach, security teams can help to ensure that the organization's resources and data are protected while also enabling development teams to be more efficient and productive.

For this final phase of the journey, organizations should aim to achieve three key goals:

1. Secure their development pipeline from source to production. Comprehensive coverage from build to deploy to production across container registries, virtual machine images, and infrastructure-as-code templates helps organizations to identify and mitigate risks across the CI/CD pipeline. This enables organizations to proactively prevent breaches and ensure that their applications and data are protected throughout the development process.
2. Prioritize policy enforcement in the pipeline to prevent introduction of issues into production. Failing builds based on knowledge of the production environment with a unified policy framework across the entire pipeline allows organizations to enforce security without burdening developers with becoming security experts. This approach can help to ensure that security is built into the development process from the beginning while saving valuable developer time.
3. Implement hardened baselines that reduce drift. VM golden images provide a secure and consistent starting point for virtual machines, while Kubernetes admission controllers provide a way to enforce security policies on pods and services in a Kubernetes cluster. By hardening these baselines, organizations can prevent vulnerabilities and compliance violations from ever reaching the production environment to ensure security by design.

As part of shifting left for prevention, organizations should look to establish the following capabilities:

Full cloud configuration lifecycle coverage: Detect misconfigurations and secrets in IaC templates across your developer's preferred tooling including Terraform, CloudFormation, ARM, Kubernetes, Helm, and Docker.

Full container security lifecycle coverage: Scan container images at build-time from the developer's sandbox for vulnerabilities and secrets, preventing non-compliant images from being pushed to the registry. Scan images continuously before deployment and at runtime to ensure compliance across the lifecycle. Block security risks using Kubernetes admission controllers during the deploy phase.

Unified policy framework across the CI/CD pipeline and production: Learn from production and shift left by automatically assessing and enforcing policies and compliance frameworks across production environments and IaC code.

Golden VM images: Implement a golden VM image pipeline, hardening images before distribution to ensure all teams create instances from hardened VM images. Assess all running VMs in your environment against the same baseline to identify drift or VMs instantiated from old or non-hardened images. Create processes for updating these baselines.

Streamlined responsibilities and processes across teams: Define the shared responsibility model across security, DevOps, and development teams. Create automation works that are tightly integrated into your organization's team structure, technology stack, and development pipeline. Consider creating a DevSecOps function, if one does not already exist, and guidelines for a) who is responsible for what and b) implementing security design principles while building secure applications.

Shifting left for prevention is vital for organizations to protect their cloud with the greatest efficiency for security and development teams. By implementing security guardrails in the development pipeline, organizations can proactively identify and mitigate risks, preventing security breaches before they occur. By doing this, organizations not only improve their security posture but also increase operational efficiency, reduce costs, and increase business agility. A key metric of this approach is the saving of developer time and reducing the number of risks in production. This approach can also help to reduce the number of vulnerabilities and compliance violations in the production environment. By shifting left, organizations can empower their development teams to focus on delivering value to the business, rather than being bogged down by security concerns, ultimately unleashing developer efficiency.

Are you ready to take the first step?

A modern cloud security workflow can bring significant business value to an organization. It can help to improve the overall security posture by proactively identifying and mitigating risks, reducing the number of security incidents, and increasing the speed of incident response. This can lead to an increase in operational efficiency and cost savings by automating security assessments and reducing the number of vulnerabilities and compliance violations. Additionally, it can increase business agility by integrating security into the development pipeline and enabling teams to move quickly and efficiently. This approach can also transform the operating model by shifting security left and empowering development teams to take ownership of security. Overall, organizations gain rapid time-to-value by improving overall security posture, increasing operational efficiency and reducing costs, increasing business agility, and transforming the operating model.

If you're ready to take the first step, we've included a cheat sheet for the four steps for achieving the new cloud security workflow that summarizes the key goals and capabilities that you will need in each. If you're ready to go further and evaluate a new platform that enables the new workflow, please leverage the Request for Proposal template which outlines all the capabilities that your teams should evaluate.

About Wiz

Wiz transforms cloud security for customers – including 40% of the Fortune 100 – by enabling a new operating model. With Wiz, organizations can democratize security across the development lifecycle, empowering them to build fast and securely. Its Cloud Native Application Protection Platform (CNAPP) drives visibility, risk prioritization, and business agility, and is #1 based on customer reviews.

Appendix:

A cheat sheet for the new cloud security workflow

Phase 1: Visibility	Phase 2: Critical Risk Reduction	Phase 3: Democratization	Phase 4: Shift left for Prevention
Key Goals			
100% visibility into any cloud and architecture today and in the future Normalization across clouds to simplify security for any team Segmentation of visibility for development teams based on infrastructure ownership	Comprehensive evaluation of workload and cloud risks Identification of attack paths and toxic combinations of risk Clear prioritization, context, and guidance for remediation down to 0 critical risks	Proactive reduction of the attack surface and blast radius for continuous improvement Ingrain security into the development process through self-service Enterprise readiness for the next threat or business shift	Secure the development pipeline from source to production Prioritize policy enforcement in the pipeline Implement hardened baselines that reduce drift
Key Capabilities			
Full cloud inventory Complete cloud coverage Complete architecture coverage Complete technology coverage Automatic and continuous detection of new resources (requires agentless approach) Full configuration visibility (IAM, network, PaaS) Role-based access control for segmented visibility for dev teams	Misconfiguration analysis (includes Kubernetes) Vulnerability and patch management Secure use of secrets Malware detection Sensitive data detection Identity and entitlements analysis Attack path and toxic combination analysis Automated workflows for selfservice for dev teams	Self-service visibility into infrastructure, risks, and evidence for development and operations teams Segment cloud security and remediation by risk factor Policy management, enforcement, and alerting Automated compliance assessments Rapid threat detection and response Readiness for M&A	Full cloud configuration lifecycle coverage Full container lifecycle coverage Unified policy framework across CI/CD and production Golden VM images Streamlined responsibilities and processes across teams

Request for Proposal (RFP) template :
Cloud security platform RFP