WIZ for Gov

Driving Efficiency in Government Cloud Environments through Wiz

Adopting a Cloud-Native Application Protection Platform (CNAPP) has helped many organizations realize significant cost savings while strengthening their cloud security and accelerating their time to delivery for new products and features. After implementing Wiz, many private industry companies have reported experiencing a return on investment of over 100 percent, offsetting their initial licensing costs, optimizing cloud & security operations and monitoring cloud spend.

During discussions with the U.S. Navy and its business partners as part of the COSMOS project, Wiz found that software delivery times can exceed 18 months, and large expenditures for system-by-system authorization to operate (ATO) certifications are prime targets for efficiency gains through better technology and processes. The adoption of a CNAPP presents a significant opportunity for government agencies to consolidate their code and cloud security, while reducing operating costs.

A managing director supporting COSMOS at SBS recounted that his team "focused automating as many steps as we can across the security requirements. Being able to integrate Wiz's capabilities into COSMOS enabled us to take a process that typically requires three months down to 30 minutes."

Wiz Can Help Cloud Modernization Policy Become a Reality

Workloads, applications, and other IT systems continue to move into cloud, and, ever more commonly, multi-cloud environments. Alongside this growing shift is a demand for shorter timelines from code development to product deployment, a requirement to meet the demands for IT systems and services.

Forward-thinking government leaders have long recognized the potential efficiency of shifting to cloud, but a complex web of legal, budgetary, procurement, and regulatory factors have slowed this transition. The cloud security and risk management implications are evident, with many government agencies continuing to rely on disconnected, siloed network diagrams stored within static files in a Sisyphean effort to accurately map their resources.

By transitioning to a CNAPP, these agencies can reduce their cloud resource costs, decrease their human capital requirements for continuous deployment, and gain comprehensive real-time visibility into their cloud resources with prioritized risk context. This transition will help keep the U.S. Government on the technological edge, automate manually intensive processes and accelerate delivery timelines, all while reducing the cost to U.S. taxpayers.

Legacy Cloud Risk Management Solutions are Inefficient, and Costly

The Government frequently relies on a combination of IaaS native tools and adapted vulnerability/risk scanners designed for on-premises systems in an effort to secure their cloud environments. Best practice and the private sector have shifted away from this methodology due to:

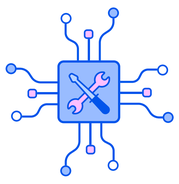
- ☑ Visibility gaps and duplication in risk findings
- ☑ Duplicative, siloed tools specific to each CSP (Azure, GCP, AWS, etc.)
- ☑ Competing alerts which lack prioritization for response
- ☑ Specialized knowledge to maintain, requiring larger IT teams and O&M budgets

- [x] Disconnected point solutions, slowing incident detection and response
- [x] Legacy agent-based scanners are inefficient for cloud deployments, lacking system-wide visibility, increase resource costs, and typically decrease system performance- leading to an increase in Shelfware.

These legacy tools are limited to operating system scanning and findings. Because they do not provide broader system visibility and context, additional tools and/or manual processes are required to relate the different systems together. Since most government systems require an ATO, these visibility gaps drive up the cost of internal and external system accreditations and audits, and prolong processes for swiftly adopting new, innovative technology.

Efficiency Advantages through CNAPP Adoption

Wiz is recognized as the market leading CNAPP solution. By adopting Wiz, organizations can have a quick impact on the functional security of their cloud environments with a positive impact on operational efficiency. This is due to several factors:



Tool Consolidation

> Wiz combines cloud security, vulnerability management, compliance, risk assessment, malware detection, exposed secrets detection, AI security posture management and other capabilities into a unified dashboard, reducing or eliminating the need for multiple cloud security solutions. Organizations leveraging Wiz reduce the number of unique security tools they license, while increasing visibility and context across their cloud environments.

Organizations could see more than $500k-$5MM in cost benefits from security tool and services consolidation after deploying Wiz.

Accelerated Time to Value

> Wiz increases time to value and decreases operational expenses by leveraging an agentless, cloud-native approach to security and automation. Wiz connects to multi-cloud environments in minutes, collapsing initial implementation time to an afternoon, conducted by a single administrator. Wiz also contains a robust API interface, allowing nearly every function to be scripted, further increasing automation and reducing administrative operational overhead.

Wiz customers see a faster time to value. One government agency reported making more progress in two weeks after deploying Wiz than what had previously been accomplished in two years with a competing, agent-based approach.

Faster Threat Detection & Remediation

> Wiz provides continuous security monitoring and real-time risk assessments, allowing teams to detect and respond to threats faster. Wiz differs from legacy solutions by having the context to quickly identify whether different events are connected. This reduces noise, and deduplicates alerts, resulting in faster, more efficient detection. By automating risk prioritization, Wiz helps agencies focus on the most critical vulnerabilities, reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Wiz customers could see efficiency increases by 20-40% within their cloud security teams. Overall, Wiz customers are less likely to experience a breach, and could reduce the impact of any breach that does occur by an average of 65%.

Improved Developer & Security Collaboration

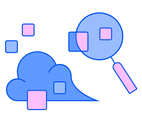
> Wiz integrates security directly into DevOps workflows, ensuring security is addressed earlier in the software development lifecycle. Wiz provides developers with contextual insights into vulnerabilities, misconfigurations, and other security risks directly within their CI/CD pipelines, enabling faster remediation. This reduces the time DevOps projects need to be in development, reduces risks to be addressed by the production cloud security team, and decreases overall time to code commit into production, which increases productivity.

Wiz customers could see efficiency increases by 20-40% within their cloud security teams. Overall, Wiz customers are less likely to experience a breach, and could reduce the impact of any breach that does occur by an average of 65%.

Automation & Reduced Manual Effort

> Conducting automated security scanning, compliance checks, and policy enforcement through Wiz reduces or eliminates many manual processes. Wiz automations reduce administrative burden and decrease the level of effort required for generating routine security reports. For example, Wiz can automate the discovery and reporting of CVEs within cloud environments, as required by Binding Operational Directive (BOD) 23-01, which requires agencies to perform asset discovery every 7 days, and report vulnerabilities every 14 days. Wiz can fully automate these tasks, generating a daily report for all cloud environments, without requiring any repetitive administrative action or impact on system performance. This ensures our nation's cyber defenders are able to spend their capacity on eliminating threats rather than completing routine compliance exercises.

Wiz allows customers to eliminate many manual tasks that their highly compensated resources are undertaking today. This allows them to drive productivity and better scale their teams. Some Wiz customers have claimed labor hour savings equivalent to 3-4 full-time highly compensated administrators.



Scalability & Consistency through Agentless Connectivity

> Wiz provides consistent security policies across multi-cloud environments, ensuring scalable, uniform protection without adding additional complexity. Since Wiz leverages agentless, cloud-native APIs, there is a lower resource cost within the operational cloud environment, and a greater adaptability to growing cloud workloads. This approach ensures security remains efficient even as cloud environments expand. Agent-based security solutions struggle to keep pace with rapid development, as agents must be continuously added to the newer workloads to ensure complete coverage. Agent-based cloud security software often results in an increase in shadow IT and visibility gaps, at the increased cost in production resources.

Wiz allows customers to identify orphaned resources in their cloud environments which are effectively cloud waste. Some Wiz customers could see as much as a $40k-$450k reduction in their cloud costs.

Wiz has helped many organizations with driving up their operational efficiency. This table outlines some specific areas where large enterprises reported significant savings by consolidating existing tools:

Wiz Feature	Security Function	Business Value	Savings
Cloud Security Posture Management (CSPM)	Continuously detect & remediate misconfigurations from build time to runtime across multi-cloud environments	Replaces multiple cloud-specific security tools & reduces alerts based on prioritized risk	40-100%
Kubernetes / Container Security Posture Management (KSPM)	Identifies vulnerabilities, misconfigurations, & other risks across containers, hosts, and other Kubernetes and serverless setups	Provides single-pane-of-glass view of security risks to reduce complexity, deduplicate alerts, & eliminate redundant scanning tools	40-100%
Cloud Infrastructure Entitlement Management (CIEM)	Detects identity risks including excessive admin privileges, identity misconfigurations, lack of MFA, & inactive users	Eliminates standalone CIEM tools and consolidates identity risk with workload security & compliance	40-100%
Cloud Workload Protection Platform (CWPP)	Complete monitoring from inside the workload for threats & malicious behavior and enables remediation within the SDLC	Agentless CWPP functionality reduces cloud resource cost & complexity	40-100%
Vulnerability Management	Discovers CVEs & KVEs across clouds and workloads, from code to runtime	Prioritizes remediation based on toxic risk- reducing alert fatigue w/o separate scanners	20-100%
Secrets and Code Scanning	Reduces risks spanning code & pipeline configs, and traces risks in cloud back to source code	Unifies security scanning between code & cloud, and consolidates separate secrets scanners	40-100%
Attack Path Analysis	Visualizes the blast radius & potential attack pathway for combinations of risk	Reduces time for root cause & impact analysis w/o the need for deploying agents	25-75%
Compliance & Governance	Enables automated compliance assessments against industry & government benchmarks and standards	100+ built-in frameworks with granular & flexible report generation	40-80%
Cloud Detection & Response (CDR)	Real-time visibility reducing time to detect, investigate, and contain cloud attacks	Prioritizes security-relevant data & filters out unnecessary logs- reducing data sent to SIEM	30-70%