5 Steps to establishing a Zero Trust foundation in the cloud with Wiz

In today's rapidly evolving digital landscape, government agencies are facing a multitude of cybersecurity threats as demonstrated by over 12,000 cyber incidents DOD has experienced since 2015 (GAO High Risk report). To effectively defend against these threats, agencies are required to adopt a Zero Trust strategy which is centered around the idea that organizations should never trust anything or anyone inside or outside their network by default. Instead, they should verify and validate the identity and security posture of every user, device, and application in their environment.

Wiz as your Zero Trust foundation

At the core of establishing a Zero Trust foundation in the cloud is the need for organizations to gain complete visibility into their environment in order to understand the risks within it. Agencies should focus on strengthening fundamental areas of cybersecurity capabilities across identity, devices, networks, applications, and data. Wiz helps organizations establish a Zero Trust foundation by providing visibility across these 5 fundamental areas, continuously assessing for risk, and enabling agencies to proactively prioritize and remove critical risk.

These are the 5 steps agencies should take on their journey to a Zero Trust foundation in the cloud:

Step 1

Identities: Agencies should work towards ensuring least privilege in their environment.

Users in your environment should only be able to access the right resources at the right time for the right purpose. Agencies should ensure that identities in their environment only have access to the resources they need, without granting excessive access. They also need to be able to detect identity misconfigurations and risks in real time.

Protect identities with Wiz

The first step in protecting identities and entitlements is gaining a centralized view of all your identities, across humans and services, and their permissions. Agencies can use Wiz's Cloud Infrastructure and Entitlement Management (CIEM) capabilities to gain complete visibility into identities and their permissions in their environment. The next step after gaining visibility, is understanding the effective permissions of each identity in your environment.

Wiz builds a map of effective access between all identities and resources, taking into account advanced cloud-native mitigating controls such as boundaries. This helps you answer questions such as “who has access and to what resources?”.

To help agencies enforce least privileges, Wiz automatically identifies and alerts of identities with high-privileges and admin permissions in your environment to ensure they are scoped properly. Wiz also detects identities with excessive permissions and IAM misconfigurations such as no MFA enabled and inactive users and generates granular recommendations to right-size permissions. Lastly, Wiz detects lateral movement paths in your environment, through permissions and exposed secrets, and to understand how they can allow an attacker to move laterally in your environment.

Step 2

Devices: Agencies should integrate device and vulnerability management across all agency environments, using automation as much as possible

When implementing device management, agencies need to gain visibility into the inventory of all assets in their environment including cloud resources, as well as every technology running on their workloads. For a Zero Trust foundation, agencies need to understand any misconfigurations and vulnerabilities related to their cloud resources and workloads.

Protect devices with Wiz

First, agencies need to gain full visibility into every resource in their cloud environment in order to be able to protect them. Wiz scans every resource in your cloud footprint across virtual machines, containers, and serverless functions, and provides agencies with 100% visibility into their environment. Next, Wiz runs deep risk assessment across different risk factors. Wiz CSPM capabilities identify misconfigurations in your cloud resources, with over 1,400 built-in Cloud Configuration rules, such as for data storage with no encryption enabled, and allow you to quickly remediate them. It also provides you with out-of-the-box compliance assessment against industry standards and regulations such as NIST SP 800-53 to ensure your environment stays compliant as your cloud footprint grows. Wiz’s agentless vulnerability scanning identifies vulnerabilities in your workloads, providing full coverage of every workload in your environment and eliminates blind spots. Wiz goes beyond conventional vulnerability management solutions by offering actionable context into risks present in the cloud environment. Wiz correlates vulnerabilities to all other risk factors including misconfigurations, network exposure, secrets, malware, data, and identities, to identify combinations of risks that can lead to an attack path in your environment. This allows agencies to focus on remediating the most critical risks in the environment, for example a virtual machine that is publicly exposed, has a vulnerability, and has an exposed secret that can lead to lateral movement in the environment.

Step 3

Networks: Agencies should segment their networks to reduce lateral movement, limit permissions, and control attack vectors, while gaining full network visibility.

Agencies should deploy tools to monitor and provide network visibility into their cloud resources, to be able to detect misconfigured network segmentations, publicly exposed resources, and ensure encryption in transit. Controls should be implemented on different layers from application to the data to improve defense-in-depth.

Protect against unintentional network exposures with Wiz

Proper segmentation between environments is essential to security in the cloud, as segregation can be a significant obstacle to an attacker moving laterally and prevent human error from affecting critical infrastructure. Wiz helps agencies monitor and enforce environment segregation with full network analysis for both containers and cloud platforms. Wiz's cloud-native network analysis calculates the effective exposure for every cloud object by analyzing the combination of network rules in network management services such as load balancers, firewalls, network interfaces, gateways, VPCs, subnets, etc. Based on this analysis, Wiz identifies all cloud resources that can be accessed from external VPCs or accounts and shows cross-account network paths. Wiz also detects resources in your environment that have network reachability and identifies on which ports, protocols, and IP addresses. For each exposed resource, Wiz provides you with the full path of the exposure, and lets you further investigate this exposure. This allows agencies to stay ahead of public exposure risks and quickly remediate them.

Step 4

Applications: Agencies should perform continuous and dynamic application health and security monitoring for all applications and services deployed in the cloud.

Agencies need to gain full visibility and continuously monitor all applications and workloads in their environment, understand risks related to them, and detect threats in real-time. Best practice for a Zero Trust foundation is to adopt a shift-left strategy of identifying risks early in the CI/CD pipeline.

Protect applications and workloads with Wiz

Agencies can use Wiz for a unified approach to workload protection from prevention to real-time detection and response. First, Wiz's agentless scanning capabilities discover all the workloads and applications running in your cloud. Next, Wiz analyses every cloud workload including virtual machines, containers, and serverless functions to detect risk across misconfigurations, vulnerabilities, secrets, identities, data, and malware. Agencies can quickly detect misconfigurations of their hosts against built-in CIS Benchmarks and application misconfigurations with built-in rules created by the Wiz Threat Research team. To enable your agency to shift left, Wiz integrates with CI/CD pipelines to detect misconfigurations, vulnerabilities, and exposed secrets early in the development cycle. All of this allows agencies proactively remove risks in their cloud before they become threats. For the last line of defense, Wiz detects known and unknown threats and suspicious activity across your cloud environments, including remote code execution, malware, crypto-mining, lateral movement, privilege escalation, container escape, and more. Wiz automatically correlates threats across real-time signals, cloud activity, and audit logs, to uncover attacker movement in your cloud so you can respond rapidly to limit the impact of a potential incident.

Step 5

Data: Agencies should always protect data at rest in the cloud and in transit to, from, and within the cloud environment

Agency data should be protected no matter where it is in the cloud, on devices, in applications and on networks. They need visibility into where their sensitive data is in the cloud, enforce protection of the data at rest and in transit, and understand paths to data exfiltration.

Protect data in the cloud with Wiz

As cloud environments can grow rapidly and become complex, the first step to protecting your data is detecting where it resides in your cloud. Wiz provides agencies with full visibility into where their data stores are, and continuously monitors for sensitive data across buckets, data and OS volumes, managed and hosted databases, with pre-defined and custom classifiers. This allows agencies to easily answer the question of what data is located where. Wiz automatically correlates sensitive data with underlying cloud context, including public exposure, identities and entitlements, and vulnerabilities to understand who can access what data, how data assets are configured and used, and how data moves within environments. Wiz alerts you when toxic combinations of risks create attack paths to your sensitive data so your teams can focus on remediating the exposure before it becomes a breach. Wiz also identifies where you have encrypted data in your environment so you can quickly remediate.

Build a secure foundation from the start

As agencies are moving to a Zero Trust strategy, Wiz helps them establish a secure foundation from the start that aligns with the Zero Trust model. Wiz provides government agencies with complete visibility into their environment, its risks, and the context around them so they can remove the most critical risk and enable Zero Trust.

Wiz for Government provides coverage for aws