WIZ + CADO

The Challenge

Gaining access to cloud resources in a timely manner during an investigation often proves to be a significant obstacle faced by security teams. However, when it comes to incident response, speed is essential to efficiently managing risk, meeting SLAs, and reducing the potential impact of threats. Achieving rapid incident response requires solutions that work seamlessly together. The Cado Security and Wiz integration enables organizations to rapidly kick off forensic investigations of AWS EC2 instances, eliminating common access obstacles that can lead to delays in investigation and response.

Solution

Wiz and Cado Security's combined solution enables security teams to triage and fix risks that pose the most impactful threats to your cloud environment and have the context necessary to solve threats in the heat of an investigation. The integration with Wiz eliminates common cloud access obstacles while gaining a deeper understanding of the root cause, scope, and impact of cloud threats.

Joint Solution Benefits

- Respond to cloud threats faster
  - Automate forensics investigation of cloud resources using Wiz's one-click forensics capabilities to accelerate path to root cause and remediation and meet SLAs
- Better understand the impact of threats
  - Take advantage of deep forensics analysis capabilities, such as Cado's AI Investigator, to better understand the scope and impact of cloud-based threats.
- Simplify the IR process
  - Gain instant access to critical cloud resources without having to work through other teams or set up additional access

How it Works

Organizations already using Wiz to manage vulnerabilities and potential compromises can rapidly kick off forensic investigations within the Cado Security platform, accelerating the path to root cause and remediation of cloud-based threats. Leveraging Wiz's recently introduced Digital Forensics capabilities, security analysts can seamlessly copy captured EC2 volumes to a dedicated forensics account and apply specific tags. Based on these tags, the Cado Security platform will automatically discover and spin up a deeper forensic investigation, without analyst intervention.

Step 1: Snapshot & Copy Volume

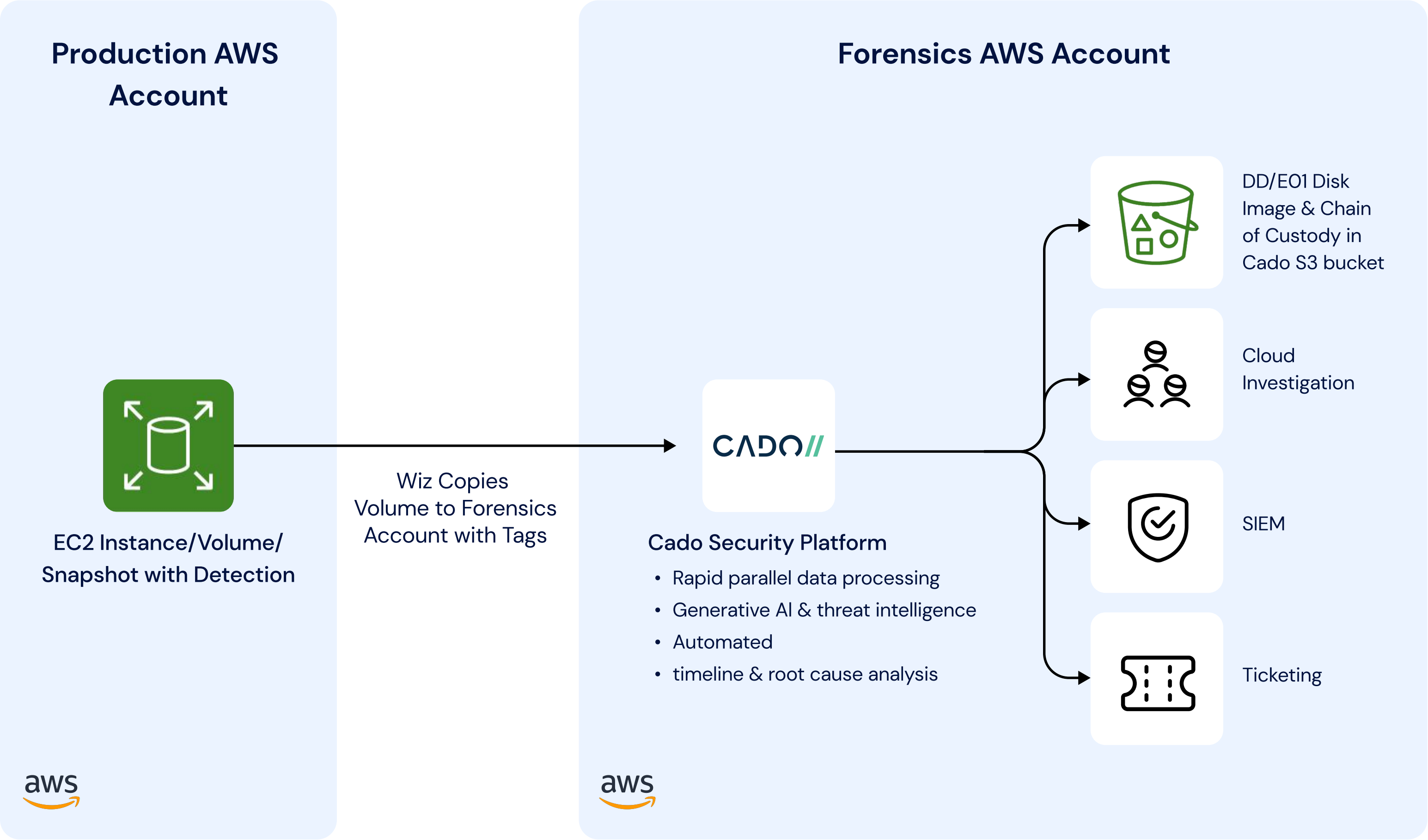
Using Wiz Digital Forensics capabilities, snapshot EC2 volume and copy the potentially compromised workload to a dedicated forensic account

Step 2: Apply Tags for Cado Discovery

Apply specific tags to enable the Cado Security platform to automatically discover and spin up a deeper-dive forensic investigation

Step 3: Automatically Process & Analyze

The Cado Security platform automatically processes and analyzes tagged EC2 volumes, delivering critical incident insights



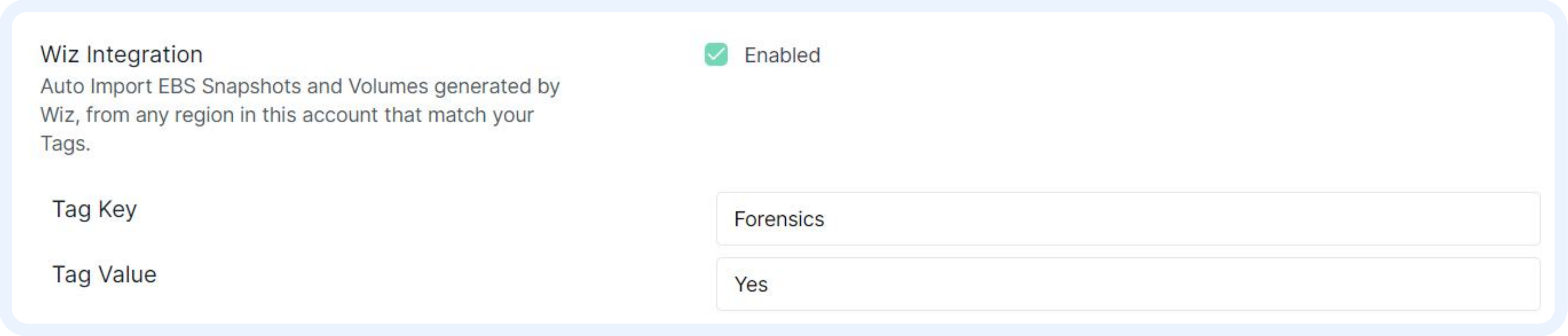
Production AWS Account
EC2 Instance/Volume/ Snapshot with Detection
aws
Wiz Copies Volume to Forensics Account with Tags
Forensics AWS Account
CADO//
Cado Security Platform
• Rapid parallel data processing
• Generative AI & threat intelligence
• Automated
• timeline & root cause analysis
DD/E01 Disk Image & Chain of Custody in Cado S3 bucket
Cloud Investigation
SIEM
Ticketing
aws

The Cado Security platform delivers an automated approach to forensics and incident response. As soon as the solution discovers the EC2 volume within the organizations dedicated forensic account that Wiz dropped in, it is rapidly processed at scale, powered by Cado's patented cloud-native architecture. Once the data is processed, the platform delivers key incident insights including an overview of key malicious and suspicious activity, a complete timeline of events, and more.

Key Forensic Capabilities

- Automation saves analysts precious time during investigations and enables forensics and incident response across disappearing resources such as auto scaling EC2 groups
- Patented cloud-native architecture delivers rapid, parallel data processing to drastically reduce time to investigation
- Data is enrichment using threat intelligence and YARA rules to automatically flag key malicious and suspicious events
- Cado AI Investigator (local LLM) provides a high-level summary of an incident and enables automatic analysis of potentially malicious files
- A complete timeline of events and advanced search capabilities allows security teams to easily pivot their investigation and identify root cause

The Wiz integration can be enabled within the Cado Platform, where administrators can also specify a tag for the purpose of automatic discovery.



Wiz Integration

Auto Import EBS Snapshots and Volumes generated by Wiz, from any region in this account that match your Tags.

☑ Enabled

Tag Key	Forensics
Tag Value	Yes

The Cado Security and Wiz integration empowers organizations to rapidly perform forensic investigations and minimize time to respond. When it comes to incident response, time is of the essence. Organizations already using Wiz can now more seamlessly take advantage of Cado Security's deep forensic capabilities to efficiently pinpoint incident root cause, impact, and scope, and respond faster.

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.