



NO GUESSWORK, SAVE TIME & IMPROVE SECURITY

ARGOS - contextualised Cloud Security

<https://argos-security.io>

Problems

Companies need real time security insights of their cloud environments with real, actionable work items.

01

Cloud misconfigurations are a leading attack vector for malware and ransomware

Companies fall victim to simple, but common errors.

02

Cloud Security is a moving target

Without a dedicated cloud security person it is difficult to stay on top of things. Cloud Security is only one part of a company's overall security and with hundreds of changes being introduced by cloud providers, few can keep up.

03

Cloud Providers focus on "getting started" more than "be secure"

Companies following tutorials or "public advice" end up with insecure cloud environments.

04

Imprecise security alerts from existing products

Companies are overwhelmed by sheer flood of security-irrelevant alerts.

Solution

We're delivering even more precise and real-time cloud security alerts.

01

Never-before-seen visibility into cloud security posture.

At a glance customers can see how security issues relate to resources / applications in their business.

02

Focus on exploitable issues.

Customers are guided towards highly critical, exploitable security issues that require immediate attention.

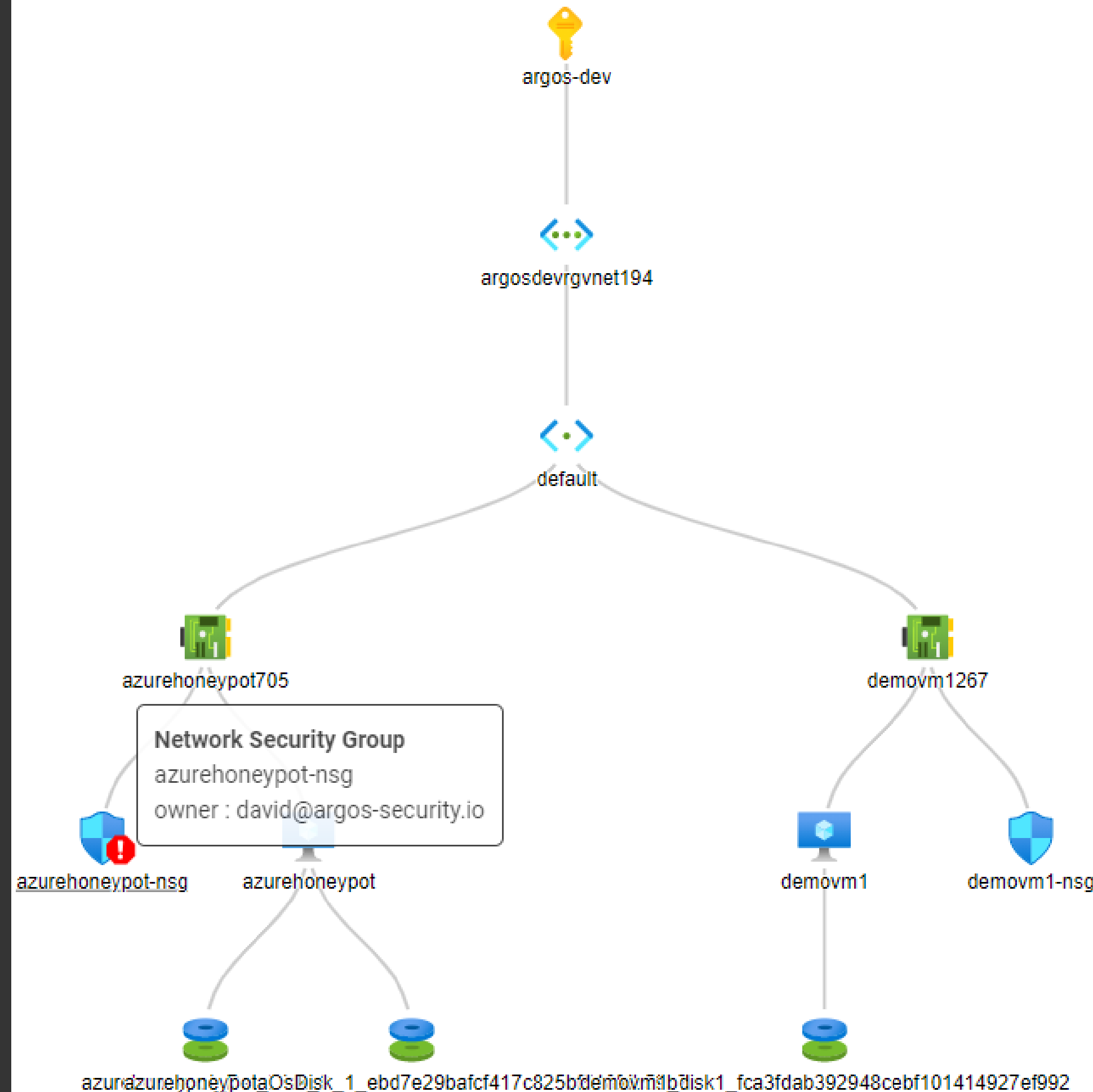
03

Real-time detection and fast remediation.

Issues are detected in near-real-time allowing them to be fixed in minutes, not days, weeks or even months. ARGOS can optionally auto-remediate the most critical issues.






ARGOS Resource Graph

Customers can now understand how security issues relate to other cloud resources and the potential impact on other parts of the business. Impossible with cloud native tools.



Not all alerts are equal

Customers save hours to days with ARGOS's exploitability check that tests if a security issue actually represents a real threat and warrants immediate attention.

Rule	Total Detections	Exploitable
 Storage Account - Default network access denied	22	22
 Remote Admin Ports should not be accessible from Everywhere	17	6
 Unrestricted SSH Access from Internet	14	4
 ELB should use at least TLS 1.2	3	3
 Unrestricted RDP Access from Internet	1002	2

ARGOS is the easiest way to secure the cloud.

ARGOS is your full-time Cloud Security Expert

Little time needed to get started, ARGOS will hit the ground running and is the 24/7/365 Cloud Security Expert that does not need constant check-in by a team member.

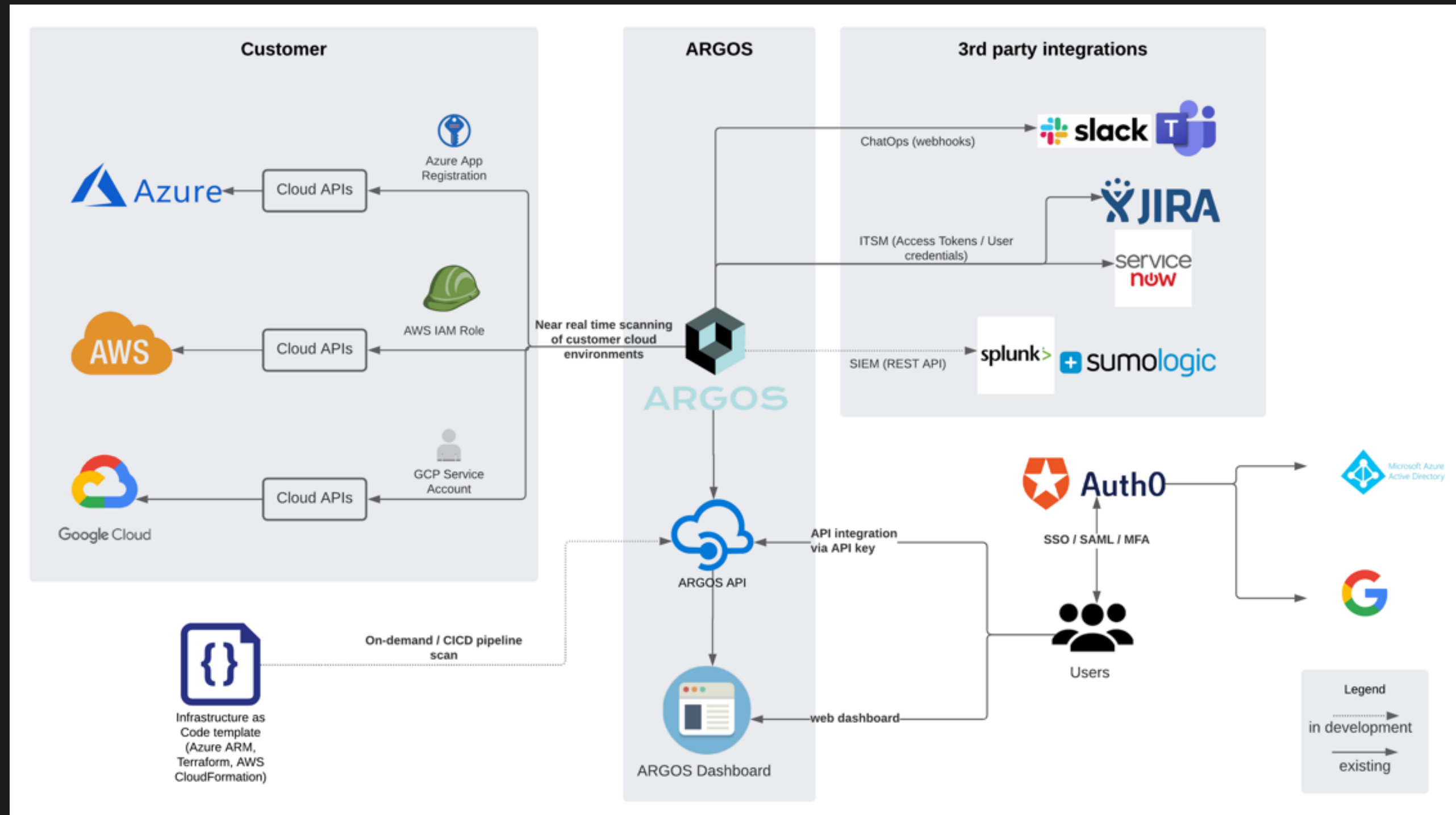
It's time to reduce the customer's effort.

Customers don't want nor do they need another product that adds more workload. ARGOS reduces effort to find, analyse and remediate cloud security issues.

It's time to provide end to end security.

Customers want end to end assurance that their cloud is secure, from the developer to production. ARGOS checks infrastructure code (upcoming release) and all running infrastructure to production.

ARGOS Solution Architecture



What do our customers say?

Engineering Lead - IDS

"Knowing that ARGOS has our back lets us sleep easy at night."

.....

Head of Cloud Security - Large Australian Retailer

"Twenty-two exploitable and High-Risk vulnerabilities have been mitigated since May 2021."

Security Architect - Metricon Homes

"What I like about ARGOS is that I got accurate results of our security posture within minutes, the ROI was less than 20 minutes."

.....

Cloud Security Architect - ISV / SaaS

"ARGOS assisted to detect and decommission an unused Azure FTP resource that was highly vulnerable and present in our environment for quite a while."

A person is sitting cross-legged on a dark carpet, holding a tablet and a pen. They are wearing a grey t-shirt and brown pants. A plaid blanket is visible to their left. The text "Competitive Advantages" is overlaid on the image.

Competitive Advantages

Laser-focused on cloud security

We used to be in our customers' shoes. We had this problem, we were the best to solve it. So we did.

We answer the hard questions - the ones others ignore

Our exploitability checks go beyond the simple "here's a misconfiguration" detections of other products. That way we save security and operations teams hours of effort and reduce the dreaded alert fatigue.

Easy to use

Go from sign-up to actionable information in under 20 minutes. Clear instructions on issues and course of action including one-click remediation.

Development to Security to Operations

ARGOS is designed for busy developers, security and operations teams with our infrastructure as code and runtime scanner.

Vendor Partnerships

We are part of the Microsoft for Startups and Amazon Activate Startups programmes.

Comparison to Cloud Native Services

	PRICE	CONTEXT AWARENESS	EXPLOITABILITY CHECKS	RESOURCE GRAPH VISUALISATION	REMEDICATION
ARGOS Cloud Security	Free (monitoring only) or per cloud connection (unlimited resources)	✓	✓	✓	out of the box for most detections
Azure Security Center / Defender	Free (very limited) or charged per resource ¹	✗	✗	✗	very limited / custom code
AWS Security Hub / Config	Charged per check ²	✗	✗	✗	very limited / custom code

¹ <https://azure.microsoft.com/en-us/pricing/details/azure-defender/>

² <https://aws.amazon.com/config/pricing/> and <https://aws.amazon.com/security-hub/pricing/>

Comparison to Cloud Native Services

	INTEGRATION	EASE OF SETUP	MULTICLOUD	REAL-TIME
ARGOS Cloud Security	Slack / MS Teams / Jira / ServiceNow	Little tuning required	✓	✓ ¹
Azure Security Center / Defender	custom	High customisation required	Partially	✗ ²
AWS Security Hub / Config	custom	High customisation required	✗	✗ ³

¹ max delay of 10 minutes

² max delay of 24hrs

³ depends on configuration

Our Business Model

These are the tier plans we offer our customers.

FREE

For customers who only need to scan a single cloud environment and don't need any integration or remediation capabilities.

Common path for conversion to paid customer.

STANDARD

For customers who have fewer than 25 cloud environments, that want integration to Slack / MS Teams and remediation capabilities.

\$200 / month for each cloud environment.

PREMIUM

For customers who have more than 25 cloud environments, that want above features and integration into JIRA / ServiceNow and direct ARGOS API access.

\$180 / month for each cloud environment.

PREMIUM MSP

For Managed (Security) Services Providers and resellers.

Next Steps

Sign up for 30 day free trial at <https://argos-security.io>

or

Contact us for guided Proof Of Value

Contact Us



david@argos-security.io



ARGOS



<https://argos-security.io>