OASIS DEFENDER

AI-DRIVEN SOFTWARE FOR UNIFIED VISUALIZATION AND CONFIGURATION OF NATIVE MULTI-CLOUD SECURITY

Our goal is to simplify and automate the process of configuring cloud security controls in their native environment to minimize the risks of misconfiguration and human errors
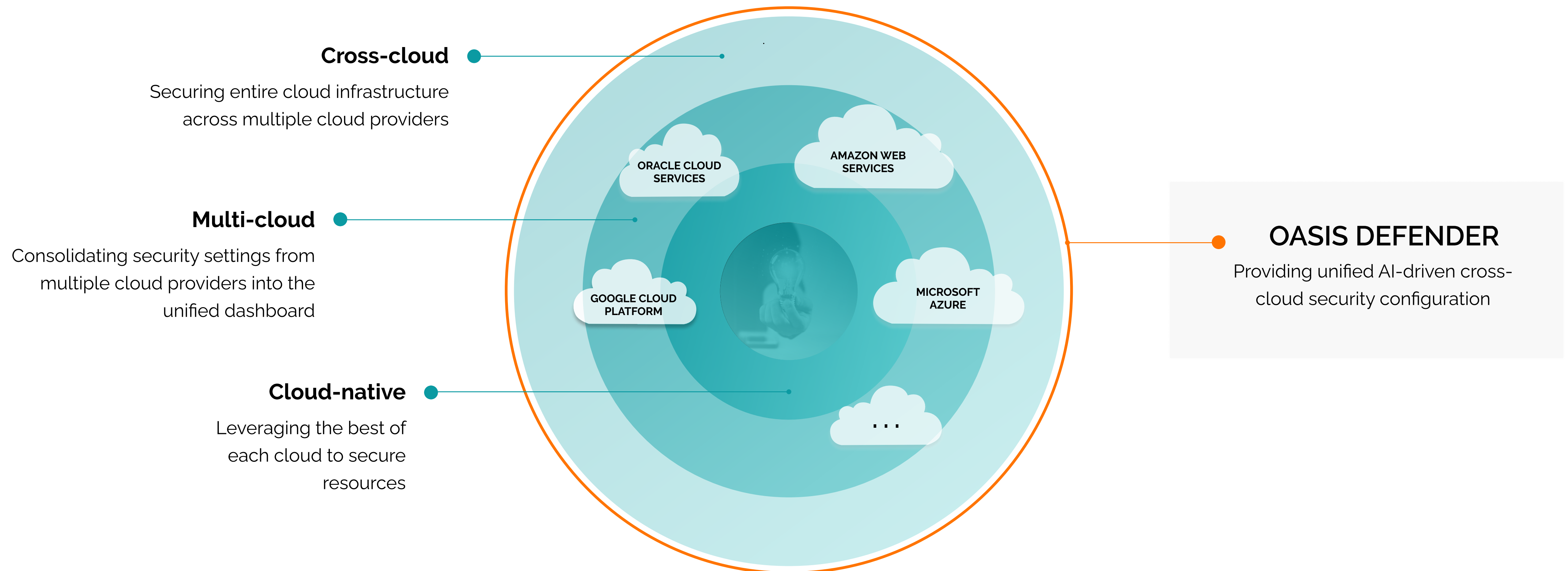
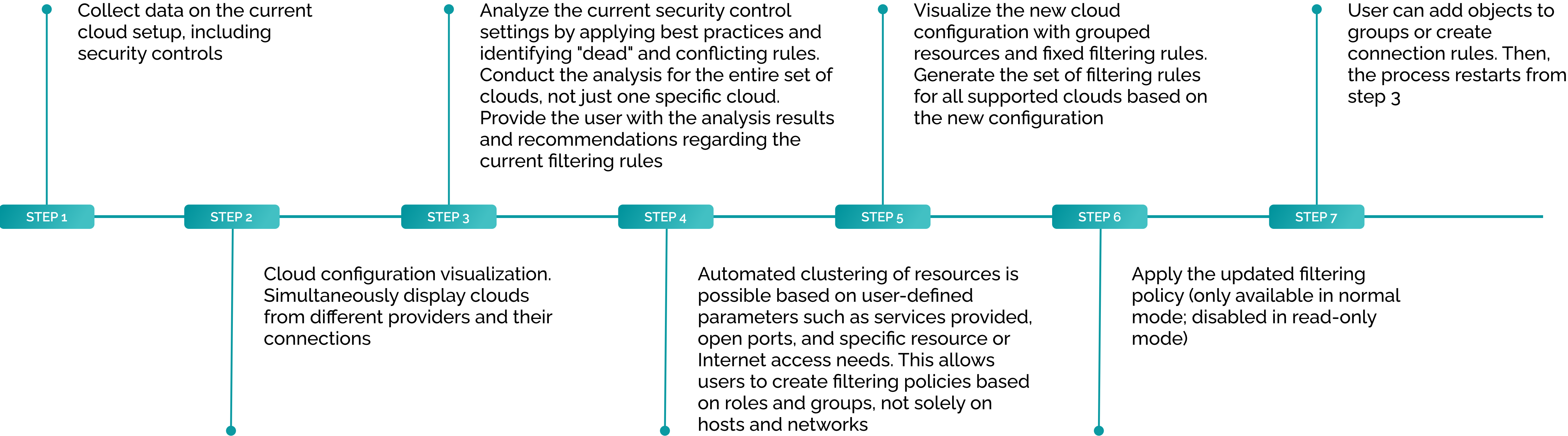**INDUSTRY:** INFORMATION TECHNOLOGY / CLOUD SECURITY   **TEAM SIZE:** 10 PEOPLE

DESCRIPTION OF OUR SOLUTION

Cross-cloud

Securing entire cloud infrastructure across multiple cloud providers

Multi-cloud

Consolidating security settings from multiple cloud providers into the unified dashboard

Cloud-native

Leveraging the best of each cloud to secure resources

ORACLE CLOUD SERVICES

AMAZON WEB SERVICES

GOOGLE CLOUD PLATFORM

MICROSOFT AZURE

. . .

OASIS DEFENDER
Providing unified AI-driven cross-cloud security configuration

PRODUCT WORK-FLOW

Support for multiple cloud providers (currently Amazon AWS and Microsoft Azure, with Google and Oracle to be added) is offered in two modes of operation: read-only and normal. In read-only mode, the user can seek advice from the system and attempt to generate a new configuration, but cannot apply changes to the clouds.

Collect data on the current cloud setup, including security controls

Analyze the current security control settings by applying best practices and identifying "dead" and conflicting rules. Conduct the analysis for the entire set of clouds, not just one specific cloud. Provide the user with the analysis results and recommendations regarding the current filtering rules

Visualize the new cloud configuration with grouped resources and fixed filtering rules. Generate the set of filtering rules for all supported clouds based on the new configuration

User can add objects to groups or create connection rules. Then, the process restarts from step 3

STEP 1   STEP 2   STEP 3   STEP 4   STEP 5   STEP 6   STEP 7

Cloud configuration visualization. Simultaneously display clouds from different providers and their connections

Automated clustering of resources is possible based on user-defined parameters such as services provided, open ports, and specific resource or Internet access needs. This allows users to create filtering policies based on roles and groups, not solely on hosts and networks

Apply the updated filtering policy (only available in normal mode; disabled in read-only mode)

VALUE PROPOSITION

Use of native secirity controls

Solutions like Valtix's require significant changes to cloud configurations and can introduce new potential points of failure. However, in most cases, a user-friendly graphical tool for customizing existing security controls is sufficient. Our product provides this opportunity with minimal modifications to current cloud setups

Open Source distribution model

Reduced costs, quicker time-to-market, customization, improved quality, increased innovation, broader market reach, brand credibility, talent attraction, ecosystem benefits, and decreased dependence on vendors

Visualized security

Existing cloud infrastructure management solutions such as Calico Enterprise, Istio, and Kong Gateway are capable of configuring built-in security controls. However, they do not provide a visual interface that offers a complete overview of the security posture. This limitation increases the likelihood of potential errors

Cross-cloud approach

Among other things, our product offers two key features. First, it allows you to visualize the network structure created by multiple clouds, which lets you create groups and apply traffic filtering rules that affect multiple cloud providers. This generates a consolidated set of filtering rules for each provider. Second, the product enables you to analyze existing or new connection rules in terms of best practices and consistency

OASIS DEFENDER

AI-DRIVEN SOFTWARE FOR UNIFIED VISUALIZATION AND
CONFIGURATION OF NATIVE MULTI-CLOUD SECURITY

CONTACT US

JOIN US IN REVOLUTIONIZING NETWORK SECURITY FOR A MULTI-CLOUD WORLD

E-MAIL: CONTACT@OASISDEFENDER.COM

SITE: OASISDEFENDER.COM

FOLLOW US:

Linkedin   **Twitter**   **Github**