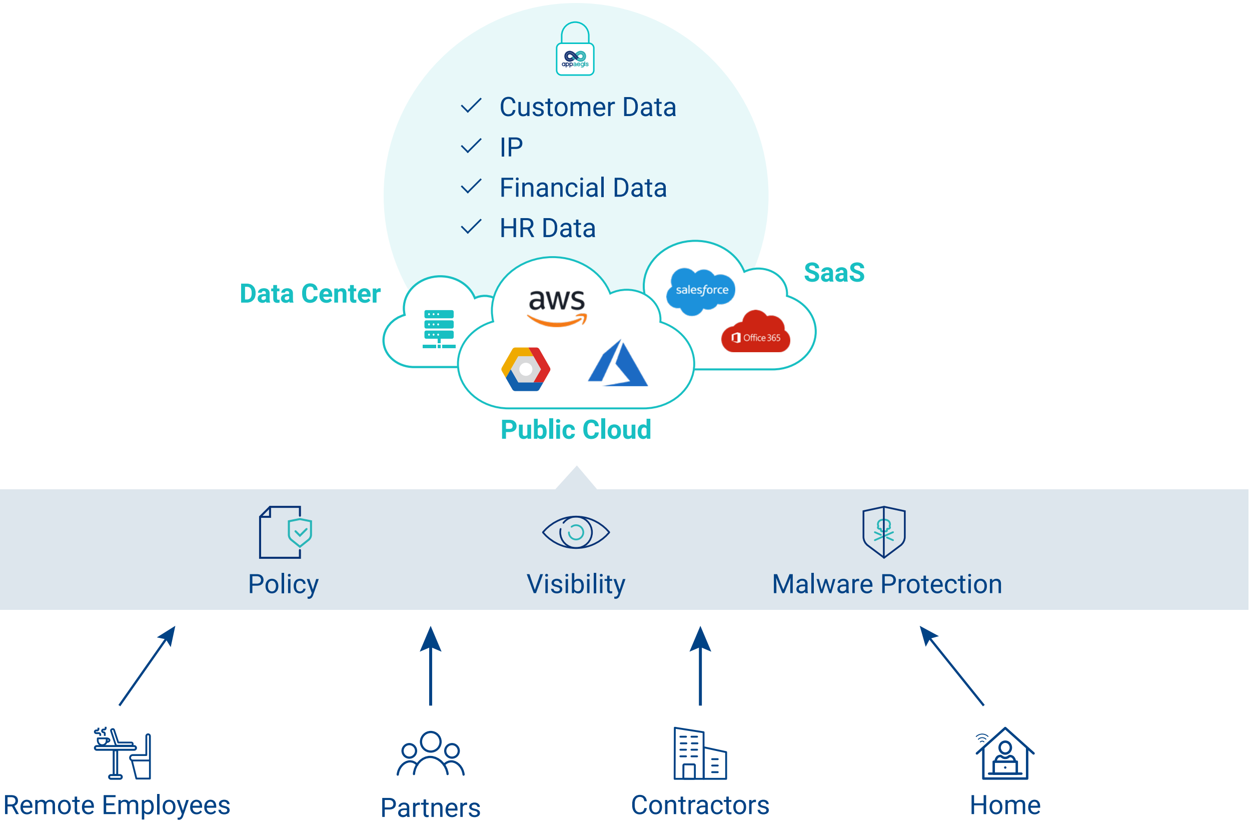
Appaegis Isolation Access Cloud For Data Safe Zero Trust

A decentralized workforce has become the new norm in today's organizations. Security teams are tasked with securing business applications and sensitive data those employees use every day. For security teams, every remote employee adds to the complexity of an already complex set of security requirements.

To meet stringent application and data access security requirements IT teams should look closely at remote access solutions. They must find solutions to manage application usage and more importantly for data access usage. These solutions must provide the ability to centrally enforce strict authentication and authorization, provide visibility, and a positive user experience.

Appaegis Isolation Access Cloud (IAC) was purposefully designed for today's environments where applications, data and employees have become decentralized. Appaegis IAC extends zero-trust principles for applications and data access, to the level which no other vendor provides. With Appaegis IAC, organizations can apply strong authentication and fine-grained access controls to data access, and actions users perform on data they need access to.

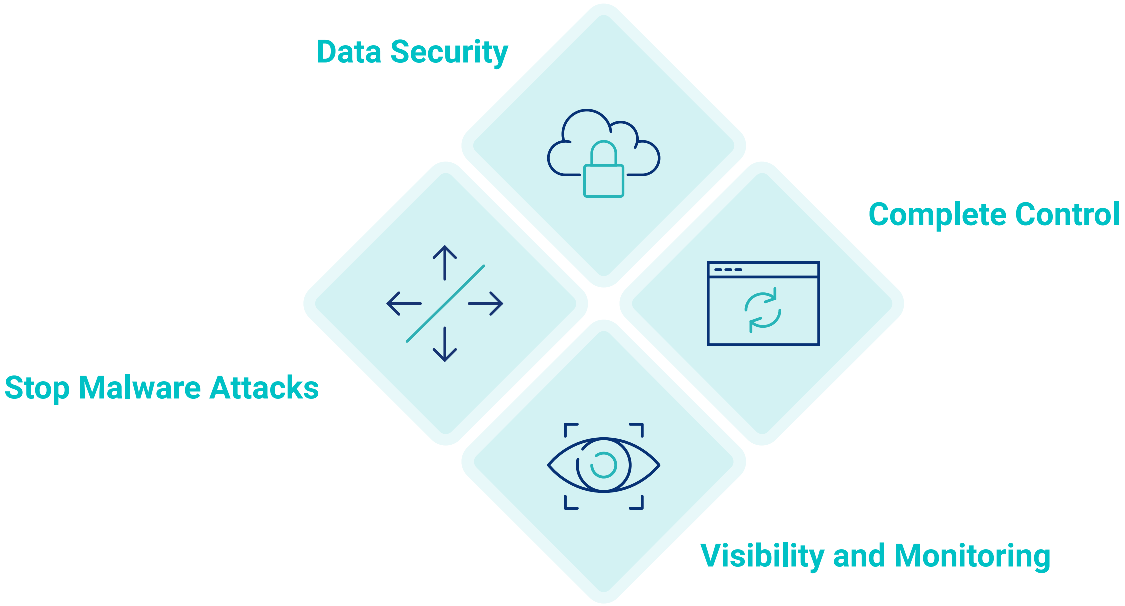
Data Safe Zero Trust



Appaegis IAC provides a solution that is effective for on premise and remote users. Appaegis Isolation Access Cloud (IAC) provides data security by only allowing authorized users to access data and applications. With Appaegis IAC, secure application access can be provided to users anytime, anywhere – in a matter of minutes! Users can be up and running without any installation on endpoints while maintaining visibility and control.

Appaegis IAC seamlessly integrates with web applications and security infrastructure. The integration is agnostic to the architecture or Infrastructure as a Service (IaaS) platform. Data and application access goes through an isolated cloud significantly reducing attack surface and risk.

Key Benefits



With Appaegis IAC organizations can protect their most critical assets – their data. Appaegis' Zero Trust approach combines data security with real-time continuous visibility into ever transaction. Appaegis provides context of each interaction, complete control over access to data, and prevents the lateral movement of malware.

Data Security

- **Appaegis IAC provides the ability to secure data anytime, anywhere, in any application, on any platform:** For applications deployed in traditional data centers, the cloud (public or private) or SaaS solutions, Appaegis provides control over data access.
- **Access based on context:** Access to applications is based on business rules and policy to ensure that least privilege access can be enforced.
- **Retain critical data at the source:** Appaegis IAC does not take control of data or make persistent copies. Therefore, there are no changes required to existing storage or methods of accessing data.

Complete Control

- **Agentless data access:** Appaegis IAC is device agnostic and does not require an agent. The agentless configuration makes deployment less complex, drives greater adoption and eliminates the need to retrain users.

- **Prevent unauthorized access in real-time:** Since Appaegis IAC works in-line, it can provide real-time enforcement of data access policies. This allows organizations to stop data exfiltration in-flight and simultaneously identify the root cause of malicious activity.

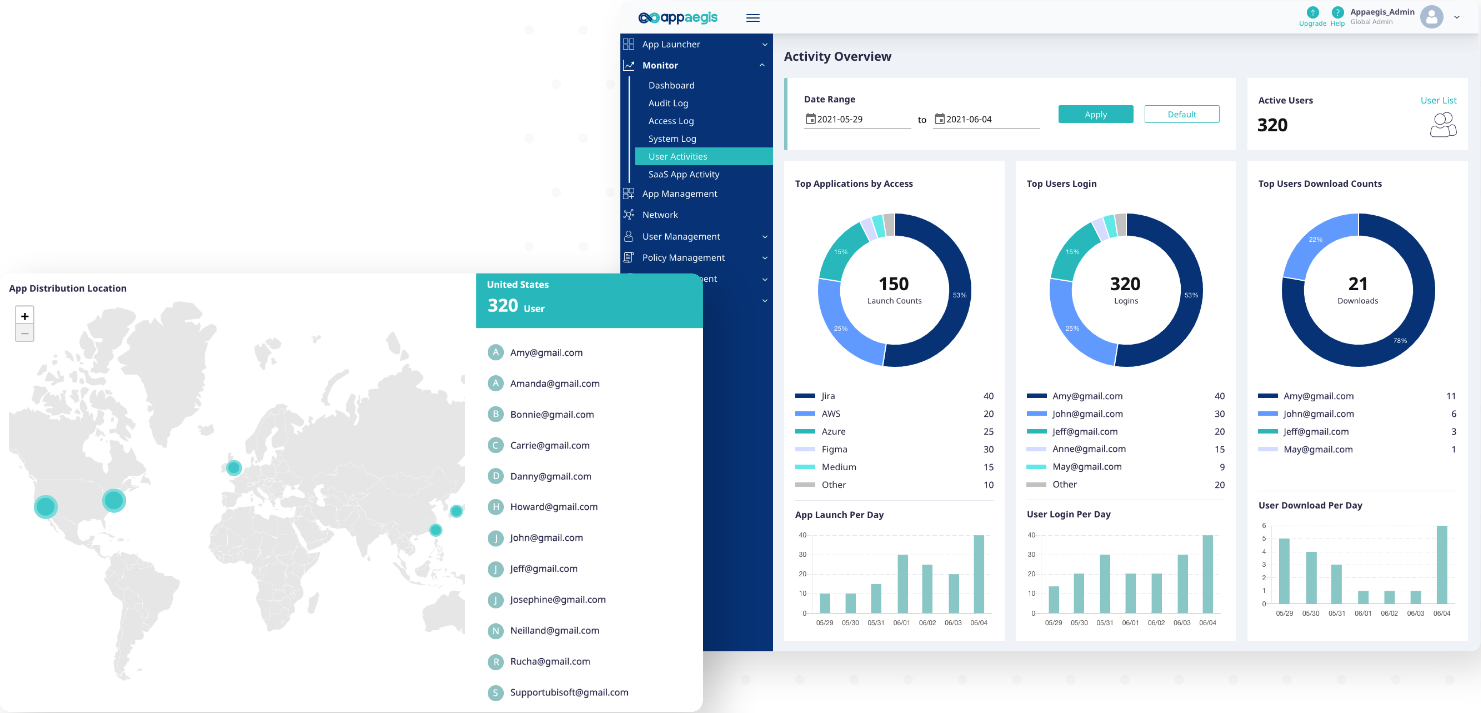
- **Application and platform agnostic approach:** Appaegis' isolation technology is agnostic to the underlying platform, applications, and resources endpoints are trying to access.

Visibility and Monitoring

- **Continuous monitoring of data & application access:** Appaegis IAC logs every interaction between end points and applications, and data access within applications. Information essential for root cause analysis and identification of patterns of access. To ensure compliance information about access is encrypted, and the actual data is neither replicated nor stored. This approach ensures compliance with privacy policies of the native application.

- **Context who, what, where, how, and when:** In addition to keeping track of transactions, Appaegis IAC tracks the context of each interaction. The enriched context allows easier root cause analysis that can prevent future malicious attempts.

- **Insight into anomalies & malicious activities:** Appaegis IAC uses visibility into application and data access to detect anomalies based on baselines and policy. Appaegis IAC applies machine learning, to quickly identify zero data attacks that violate access policies. Appaegis IAC also applies machine learning to identify malicious activity.



Activity Overview

Date Range 2021-05-29 to 2021-06-04

Active Users 320

Top Applications by Access — 150 Launch Counts

Jira	40
AWS	20
Azure	25
Figma	30
Medium	15
Other	10

Top Users Login — 320 Logins

Amy@gmail.com	40
John@gmail.com	30
Jeff@gmail.com	20
Anne@gmail.com	15
May@gmail.com	9
Other	20

Top Users Download Counts — 21 Downloads

Amy@gmail.com	11
John@gmail.com	6
Jeff@gmail.com	3
May@gmail.com	1

App Launch Per Day

User Login Per Day

User Download Per Day

App Distribution Location

United States
320 User

A Amy@gmail.com
A Amanda@gmail.com
B Bonnie@gmail.com
C Carrie@gmail.com
D Danny@gmail.com
H Howard@gmail.com
J John@gmail.com
J Jeff@gmail.com
J Josephine@gmail.com
N Neilland@gmail.com
R Rucha@gmail.com
S Supportubisoft@gmail.com

Stop Malware Attacks

- **Prevent the spread of malicious software:** Appaegis' isolation technology ensures that malware that has infected the end host cannot move laterally to servers or the cloud.

- **Reduce attack surface:** By blocking malware at the source, Appaegis IAC prevents it from migrating from one host to another. This limits the number of infected end points reducing the attack surface.

- **Protect against unpatched hosts:** Appaegis IAC prevents malware migration from endpoints to servers, limiting the ability of malware to exploit vulnerabilities on unpatched servers. By reducing the need for direct access, Appaegis IAC makes it harder for malicious actors to introduce malware directly on hosts.

Appaegis Isolation Access Cloud (IAC) has the following Key Capabilities

Authentication & Authorization

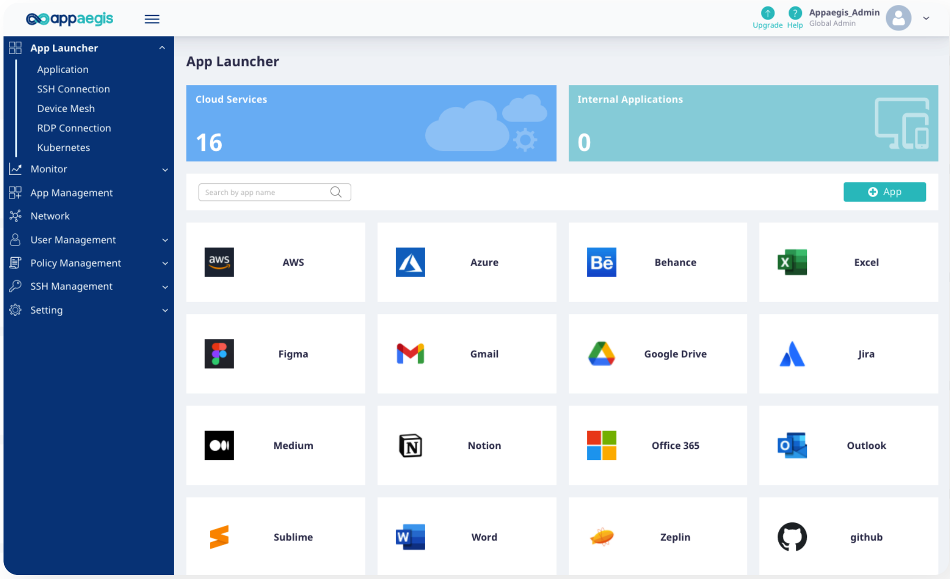
Appaegis IAC provides the capabilities for seamless integration into existing identity and authentication methods. If the user passes authorization and authentication challenges, only then, are they allowed access to the requested resources.

- **Integration with MFA and SSO:** Out of the box integration with Okta and other SSO providers.

- **Agentless identity-aware access:** Integration with popular identity providers, including Okta and Azure Active Directory.

- **Support Identity brokerage for internal and SaaS applications:** Appaegis IAC provides integrated password vaulting to manage identity across SaaS, custom built or off-the-shelf self-hosted web-based applications.

- **Authorize resources and data access.** Appaegis IAC has built in integration with networking and application services including HashiCorp Vault.



Elastic SD-Edge

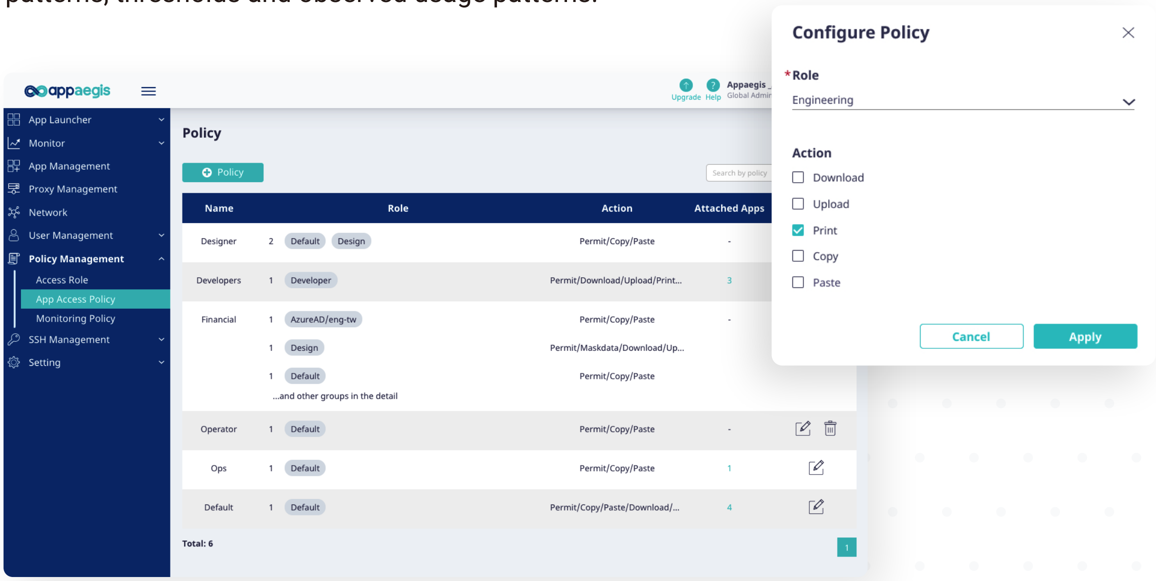
An elastic edge that can be easily deployed in any infrastructure (private, public, hybrid cloud) provides superior performance and lower latency. Appaegis IAC can scale to support the exponential growth in applications and optimize last mile connectivity . It’s container-based architecture can be scaled to support growth in applications and any transaction load.

- **Identity-based forwarding with a containerized service edge based on the location of users and applications to reduces latency.**
- **Adaptive security functions depending on applications and security requirements:** This includes the ability to incorporate various security functions like software web gateways, URL filtering as needed by the organization.
- **Expansive point of presence (PoP) that support edges deployed in customer’s cloud:** Appaegis IAC supports distributed public cloud applications, those deployed in a private cloud and SaaS solutions. A lightweight container deployed close to the application ensures efficient communication and an optimal user experience.

Real Time Policy Enforcement

Appaegis IAC provides a robust framework to define policy that governs access to data and applications. Policy definition is agnostic to applications architecture and platform. Policies can be applied across a wide range of applications and a broad range of data types or

- **Context-based Policy (identity, networking, location, and application-based parameters):** Policies definition includes a wide range of parameters that incorporate location, role, IP address, geography and more. The policies can be applied to applications or data within applications.
- **Consolidated identity across platforms and applications with RBAC:** By providing the ability to organize privileges into groups, policies can applied based on role or group.
- **Dataplane integrated with analytics for real time enforcement:** In addition to policy based control, Appaegis leverages analytics to determine if certain types of access is suspicious. Risk is determined based on behavioral patterns, thresholds and observed usage patterns.



Name		Role	Action	Attached Apps
Designer	2	Default Design	Permit/Copy/Paste	-
Developers	1	Developer	Permit/Download/Upload/Print...	3
Financial	1	AzureAD/eng-tw	Permit/Copy/Paste	-
	1	Design	Permit/Maskdata/Download/Up...	
	1	Default	Permit/Copy/Paste	
	...and other groups in the detail			
Operator	1	Default	Permit/Copy/Paste	-
Ops	1	Default	Permit/Copy/Paste	1
Default	1	Default	Permit/Copy/Paste/Download/...	4

Total: 6

Configure Policy

*Role

Engineering

Action

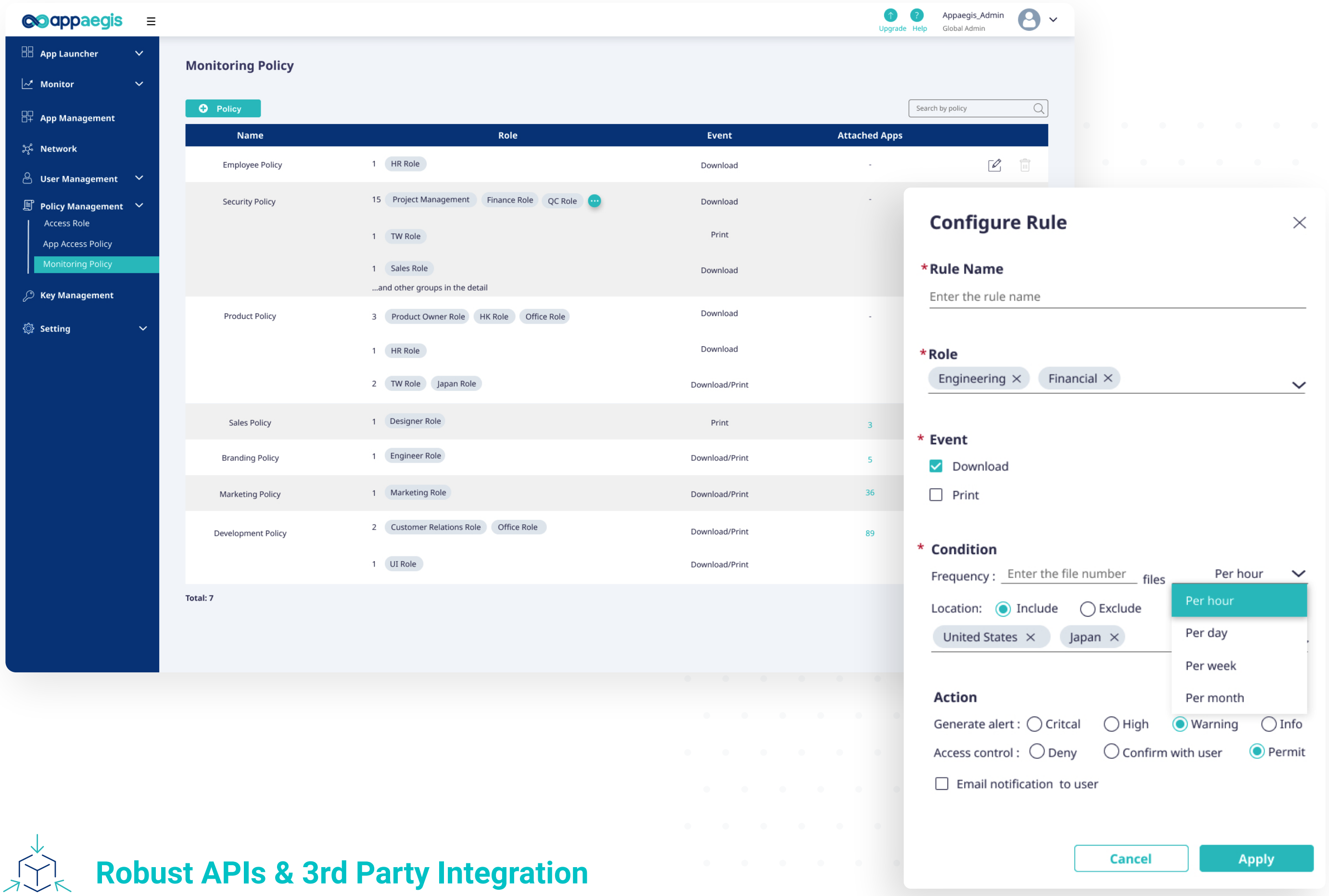
☐ Download
☐ Upload
☑ Print
☐ Copy
☐ Paste

Continuous Monitoring & Alerting

- **Single pane of glass view of access across applications:** Appaegis provides a single pane of glass view into activity across all applications connected to Appaegis. Appaegis IAC provides granular visibility into every interaction with all the applications and attempts to access data.

- **Integrate inline inspection with machine learning analytics to self-tune risk and enforcement:** In addition to anomaly detection, Appaegis IAC applies machine learning to detect suspicious activity and prevent zero day attacks. Appaegis IAC blocks events or generates actionable alerts based on high-quality context-based analytics.

- **Granular logging of all data and application access, easy reporting and data export:** In addition to identifying malicious activity in real time, Appaegis IAC logs access transaction meta-data for analysis, audits or export.



Monitoring Policy

Name	Role	Event	Attached Apps
Employee Policy	1 HR Role	Download	-
Security Policy	15 Project Management, Finance Role, QC Role	Download	-
	1 TW Role	Print	
	1 Sales Role ...and other groups in the detail	Download	
Product Policy	3 Product Owner Role, HK Role, Office Role	Download	-
	1 HR Role	Download	
	2 TW Role, Japan Role	Download/Print	
Sales Policy	1 Designer Role	Print	3
Branding Policy	1 Engineer Role	Download/Print	5
Marketing Policy	1 Marketing Role	Download/Print	36
Development Policy	2 Customer Relations Role, Office Role	Download/Print	89
	1 UI Role	Download/Print	

Total: 7

Configure Rule

*Rule Name

Enter the rule name

*Role

Engineering × Financial ×

* Event

☑ Download

☐ Print

* Condition

Frequency : Enter the file number files Per hour

Per hour
Per day
Per week
Per month

Location: ● Include ○ Exclude

United States × Japan ×

Action

Generate alert : ○ Critcal ○ High ● Warning ○ Info

Access control : ○ Deny ○ Confirm with user ● Permit

☐ Email notification to user

Cancel Apply

Robust APIs & 3rd Party Integration

- **API driven configuration:** A robust set of APIs allow integration into workflow, infrastructure management and security solution. Appaegis IAC provides the ability to automate workflow and automate response to security events.

- **Easy integration with DevOps and orchestration systems for efficient user on and off-boarding.**

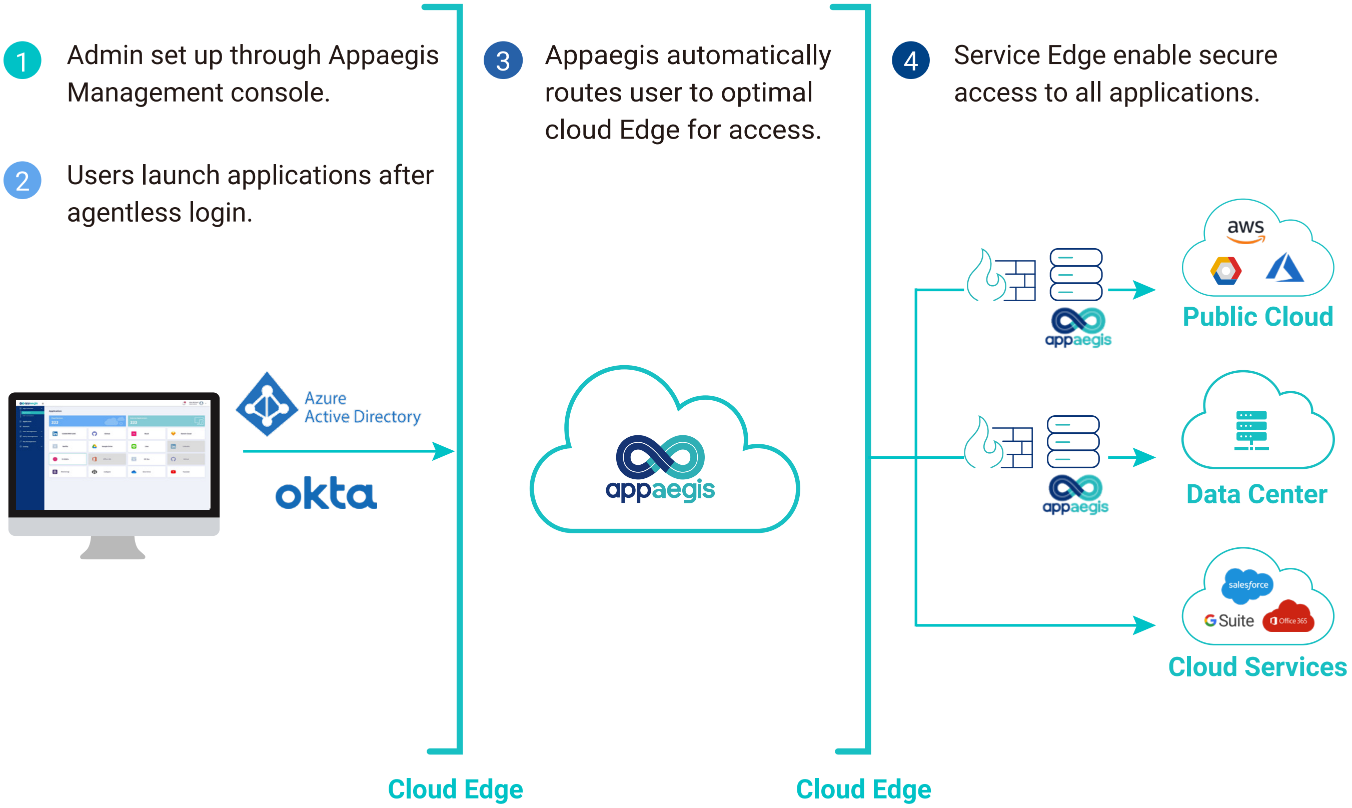
- **Simplified data export to SIEMs or other analytics engines:** All log data can be exported to external systems, like a SIEM, for further analysis, analytics or reporting.

Rapid Deployment and Configuration

Deployment and configuration of the Appaegis Isolation Access Cloud is simple. An intuitive user interface allows users to configure connectivity to applications in a matter of minutes. Adding users can be done through the application portal by simply entering a users' email address. Once the application is configured and users are added the user can start taking advantage of Appaegis IAC immediately.

Users log into the Appaegis IAC portal and are presented with a tile for every application to which they have access. When the user clicks on the desired application, they are automatically logged in and can use native functionality of the application. Since the user is presented with the experience of the native application no retraining is required. This reduces or eliminates the need for any retraining of the entire user base.

Appaegis IAC brings Zero Trust to data security. Typical use cases include securing DevOps access by enabling Zero Trust with SSH, providing a Zero Trust VPN replacement, enabling secure easy access to data and applications for remote employees or partners, and securing access to applications.



1 Admin set up through Appaegis Management console.

2 Users launch applications after agentless login.

3 Appaegis automatically routes user to optimal cloud Edge for access.

4 Service Edge enable secure access to all applications.

Appaegis provides secure, agentless, zero trust access connecting users and devices to applications with minimal investment. Appaegis reduces the attack surface with visibility into interactions with applications, allowing access control and identifying anomalies. Appaegis integrates with existing workflows, security infrastructure and is agnostic to the type of applications or endpoints.

Appaegis HQ | 555 Bryant St. Suite 220 Palo Alto, CA 94301
+1(669)699-1122 | www.appaegis.com | info@appaegis.com