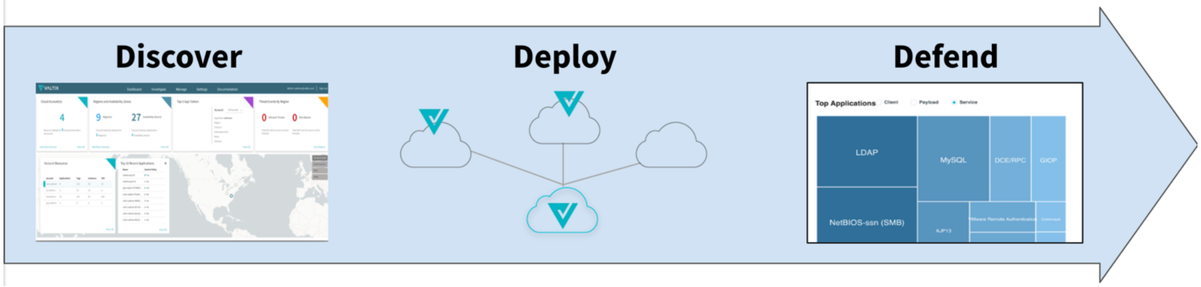
VALTIX

SOLUTION BRIEF

EGRESS SECURITY FOR PUBLIC CLOUD

In the 2020 Market Guide for Cloud Workload Protection Platforms (CWPP), **Gartner**[1] states: "**Protection requirements for cloud native applications are evolving** and span virtual machines, containers and serverless workloads in public and private clouds. Security and risk management **leaders must address the unique and dynamic security requirements of hybrid cloud workloads**." In addition, Enterprises are challenged with business requirements surrounding compliance, risk management and best practices while managing rising costs and the pressure to do more with less in today's complex economy.

Valtix's Cloud Security Service embraces this dynamic, unique and evolving environment of public cloud, and is delivering an architectural approach to cloud security that matches and enhances its very nature – our philosophy is security should match the agility of the applications it protects and provide value through simplicity. The solution utilizes the native cloud constructs offered by Cloud Service Providers (CSP's) without additional overlay and vendor lock-in, and is delivered through a Managed Service platform based on the following model:



Discover: Maintains an "evergreen" model of running cloud applications, auto-detecting changes, and providing the needed insights into security requirements. This allows for dynamic security policies that automatically protect dynamic and agile workloads.

Deploy: The deployment architecture is driven by the "discovery". Auto-scaled, provisioned and network-plumbed security (agent-less) with single-click deployment objectives. Support for AWS, Azure and GCP cloud deployments and network pathing with IaC automation - Terraform and API – without the need to build and manage a complex control plane.

Defend: Write custom security policies to protect your applications as you determine their need, and that may include some, or all, of the following defense functions:

- URL + FQDN Filtering: Custom + Domain Categories
- TLS decryption/re-encryption with single pass Deep Packet Inspection (DPI)
- Advanced Web Application Firewall (WAF)
- Network Protection (IDS/IPS) + Malicious Sources

Egress Security in public cloud comprises a significant portion of the total security posture toward protecting public cloud workloads handling or using: -

- PII** data that can be used to identify a specific individual. Technology has expanded the scope of PII considerably to include IP addresses, login IDs, social media posts, or digital images, in addition to traditional SSN's, credit card numbers, emails and phone numbers.
- Access to public internet resources for software updates, patches, public repositories, API calls, 3rd party interconnects and sensitive data logging toexternal sources.

Questions arise as to what is adequate, good, better and best when protecting the **applications requiring egress to public internet** and limiting the "blast radius" in the event of a security breach. Where am I vulnerable? Is FQDN, or URL, filtering better? Should I care about Data Loss Prevention (DLP)? Should I deploy a proxy? Maybe I need Malware detection also? How can I determine if my data is compromised? What are my workloads really accessing and why?

The answer is you should care about all of the above, and more. The Cloud Security Alliance (cloudsecurityalliance.org) and other bodies address "best practices" with specific types of sensitive data e.g. PCI, PCI, HIPPA, however, the Enterprise must determine their own security posture - what to deploy and where to acquire it. Valtix believe the decision should be made understanding both the Security Capabilities and the Automation/Management functions of a comprehensive Solution Architecture.

Capabilities that we believe are required in any Public Cloud Egress Security solution are: -

Functions	NAT Gateway	Squid Proxy[1]	Aviatrix FQDN	Valtix Egress
Security Capabilities				
URL Filtering*	No	No	No	Yes
FQDN Filtering**	No	Yes	Yes	Yes
Forward/Reverse Proxy (as needed)	No	No	No	Yes
Custom Lists for Domain Category	No	No	No	Yes
Auto-Scaling	Yes	No	No	Yes
Auto Discovery (App-Tag-based)	No	No	No	Yes
Auto Malware Detection	No	No	No	Yes
Data Loss Prevention (DLP)	No	No	No	Yes
Application Tagging	No	No	No	Yes
Flow Log Visibility	No	No	No	Yes
Multi AZ High Availability	Yes	No	Yes	Yes
Allowed/Denied Session Logs	No	No	Yes	Yes
Automation and Management				
Terraform Support	Yes	No	Yes	Yes
API Support	Yes	No	Yes	Yes
Managed Service (SaaS)	No	No	No	Yes
Enterprise Support	Yes	No	Yes	Yes

Valtix can assist you, and your cloud teams, understand the complexities of each capability. For example – what is the real difference between URL vs FQDN filtering when limiting access to a specific GitHub repository? e.g. “stevevaltix/app” should be permitted.

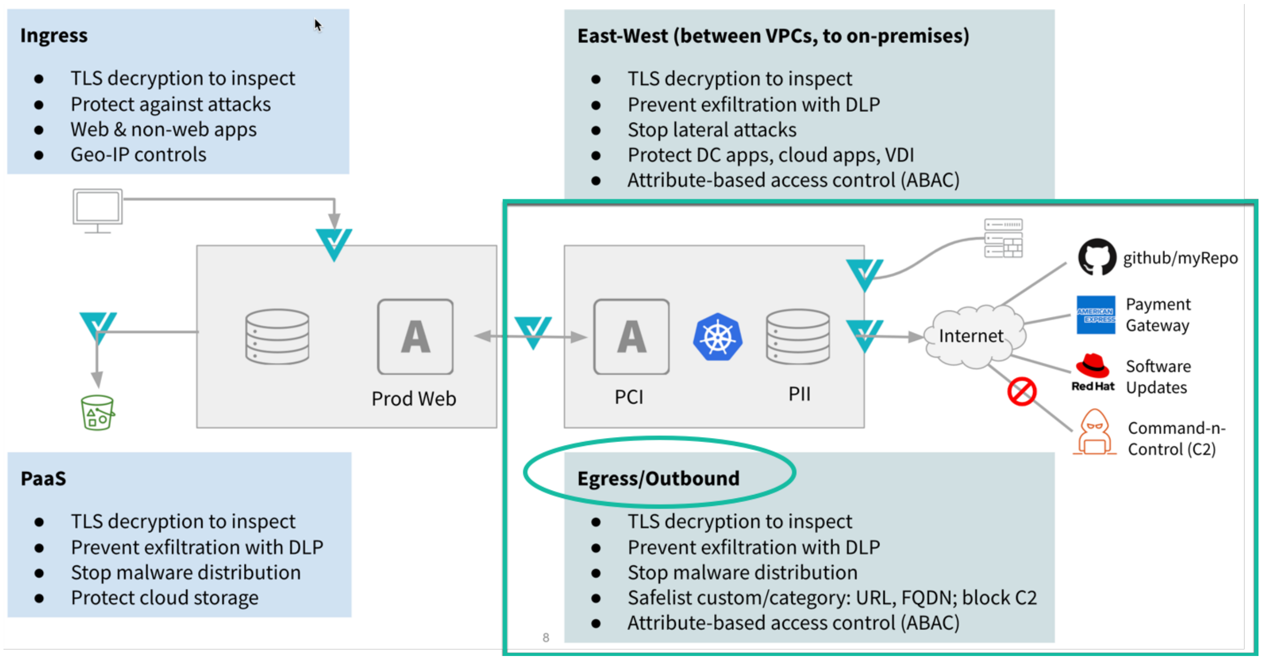
* URL filtering is more prescriptive in filtering entire URL and path permitted for access: https://github.com/stevevaltix/app **Allow** ** FQDN filtering operates on tLD and sub-domains only and would handle this with an FQDN rule: *.github.com **Allow**

FQDN filtering alone is inadequate since it allows access to all public GitHub repositories, some of which are known to contain malware and data loss mechanisms.

In addition, URL filtering combined with tags, Valtix’s attribute-based access control and use of custom lists for Domain categories (80+), makes this highly manageable at scale.

Egress Security Architecture

Valtix is architected using software defined principles of a decoupled Control and Data Plane, offering a SaaS-delivered Control Plane and a PaaS-delivered Data Plane residing in the Enterprise’s cloud accounts. This includes all Certificate, Key, and Data stores – your data and security constructs never leave your boundaries. Deployment models include both Centralized, Distributed or both, and based on your specific architecture security posture.



Ingress

- TLS decryption to inspect
- Protect against attacks
- Web & non-web apps
- Geo-IP controls

East-West (between VPCs, to on-premises)

- TLS decryption to inspect
- Prevent exfiltration with DLP
- Stop lateral attacks
- Protect DC apps, cloud apps, VDI
- Attribute-based access control (ABAC)

PaaS

- TLS decryption to inspect
- Prevent exfiltration with DLP
- Stop malware distribution
- Protect cloud storage

Egress/Outbound

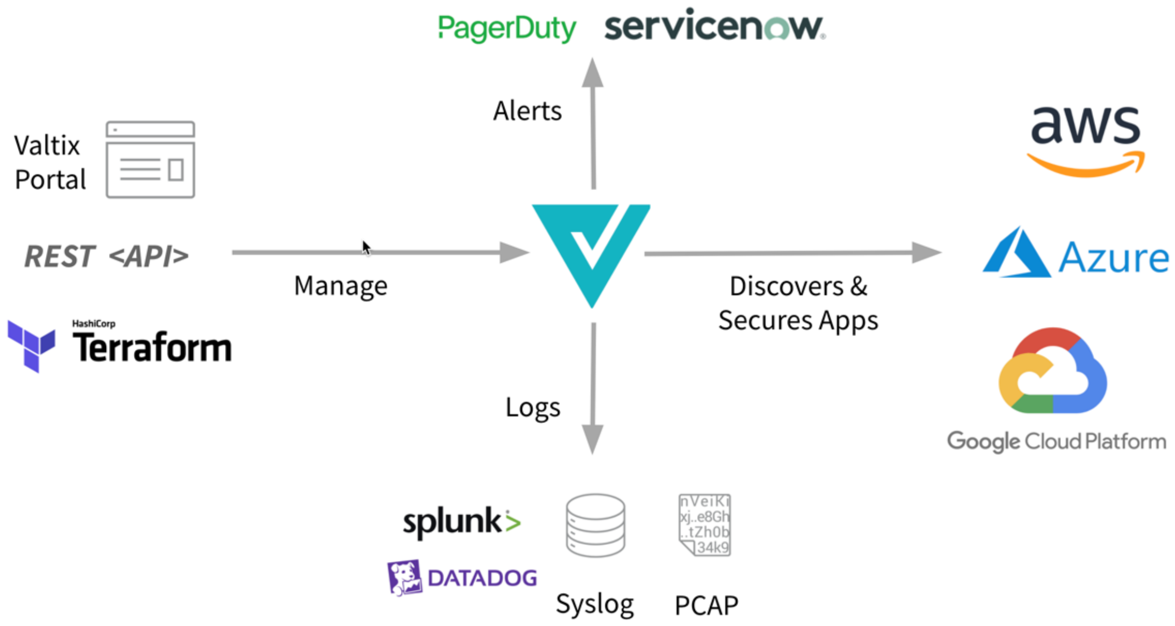
- TLS decryption to inspect
- Prevent exfiltration with DLP
- Stop malware distribution
- Safelist custom/category: URL, FQDN; block C2
- Attribute-based access control (ABAC)

** Personally identifiable information (PII) is any data that can be used to identify a specific individual. SSN’s, mailing or email address, phone numbers, IP address, login IDs, social media posts, digital images, geolocation, biometric, and behavioral data.

Automation and Integrations

Valtix provides native support in the three (3) major Cloud Service Providers (CSP's) – AWS[4], Azure[5] and GCP[6], while abstracting the complexities and nuances involved with deploying and configuring network and security constructs for each individual CSP. The solution is fully supported via Terraform[7], RESTful API and the Valtix Portal GUI.

Additionally, Valtix is integrated into popular SIEM's and Alerting solutions, while PCAP's can be optionally pushed to your CSP data store.



Engage with Valtix

Want to discover more? Observe a demonstration? Discuss a challenging project, or your Cloud Security posture generally? Contact your Account Team today:

Email info@valtix.com or Phone 650.420.6014
Valtix Corporate Website
Valtix Documentation Site

[1] Gartner is a registered trademark and service mark of Gartner, Inc. a research and advisory firm.
[2] Aviatrix is a registered trademark and service mark of Aviatrix Systems, Inc.
[3] Squid is currently being developed by a handful of individuals donating their time and effort to building current and next generation content caching and delivery technologies Source: squid-cache.
[4] AWS is a trademark of Amazon.com, Inc. or its affiliates in the United States and/or other countries.
[5] Azure is a registered trademark of Microsoft Corporation or its affiliates in the United States and/or other countries.
[6] GCP is a registered trademark of Google LLC or its affiliates in the United States and/or other countries.
[7] Terraform is a register trademark of HashiCorp, Inc. or its affiliates in the United States and/or other countries.