Centralized Egress Access Policies: Why They Matter in Hybrid Environments

The increasing adoption of hybrid cloud environments such as Amazon Web Services (AWS), the Google Cloud Platform (GCP), and Kubernetes clusters introduces significant security complexities, particularly regarding egress traffic control. Securing ingress traffic (traffic flowing from the internet into the enterprise's environment) often receives considerable attention. However, organizations must equally prioritize a robust egress access policy framework to secure traffic exiting the enterprise environment and moving to the internet. Centralization of policy management has emerged as a fundamental requirement for achieving effective egress controls in dynamic enterprise environments.

Egress Access

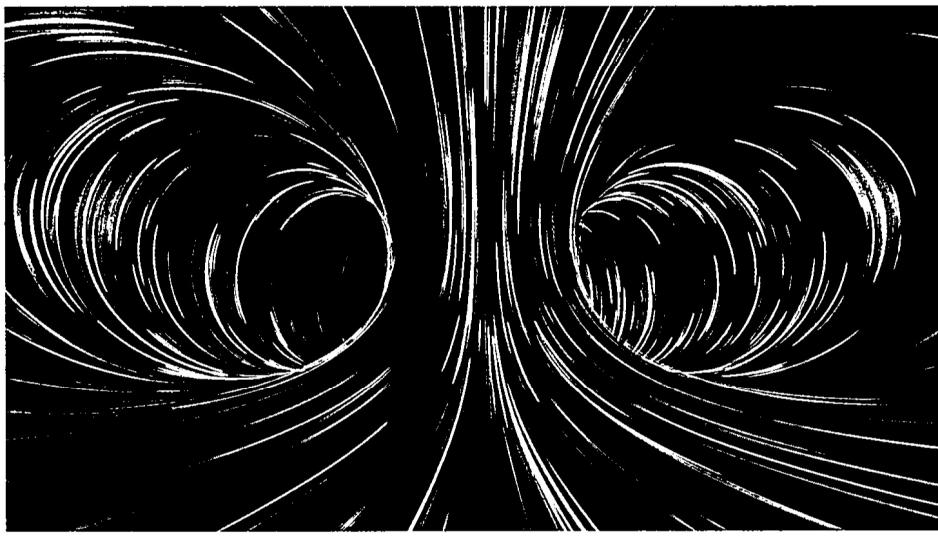
In the context of network security, egress access refers to the flow of data out of a network or system. It includes all the methods by which data can leave a controlled environment, such as:

- **Network traffic**—Data is transmitted over the internet or other networks.
- **Physical removal**—Data is copied to removable media such as USB drives or external hard drives.
- **Email and messaging**—Data is sent through email platforms or other messaging applications.
- **Cloud services**—Data is uploaded to cloud storage services or other cloud platforms.
- **API calls**—Data is accessed or transferred through application programming interfaces (APIs).

Egress access policies are simply rules that specify what data can be transmitted out of a network or system, including by whom and to whom. These policies can be implemented using various tools and technologies, including firewalls, data loss prevention (DLP) systems, identity and access management (IAM) policies, and intrusion detection and prevention systems (IDS/IPS).

Centralized egress access control is a specific approach to managing egress policies. It involves using a single system to define, manage, and enforce policies across all egress points.

Policy definition involves establishing clear guidelines: rules that govern which types of data can be transmitted, where data can be sent, and who is authorized to send it. For instance, an egress policy might prohibit sending sensitive customer data to specific countries to ensure compliance with data privacy laws, or it might block the upload of confidential files to unapproved cloud storage services to prevent unauthorized data exfiltration.



APARNA PATIL | CISA, ISO 27001 LA, ISO 22301 LI, PCI DSS IMPLEMENTER

Is an IS auditor with 10 years of experience in audit, risk management, compliance, and information technology. She is actively working to promote information security among students and professionals and has provided training in the domain. Patil can be reached at *https://www.linkedin.com/in/aparna-patil-a1302611/*.

RAMESH RAMANI

Is a security engineer at Block Inc. He has more than 15 years of experience in the field of information technology with a focus on security. He has written several blog posts about Kubernetes security and holds three information security-related patents. Ramani can be reached at *https://www.linkedin.com/in/ramesh-ramani-08bb6b16/*.

Policy deployment can involve configuring firewalls to block specific types of outgoing traffic, configuring a DLP system to detect and prevent data leaks, or creating intrusion detection/prevention rules to monitor and block suspicious activities.

Consider, for example, how egress policy definition and deployment work in practice for an enterprise that wants to prevent its employees from sending confidential documents to personal email accounts.

- **Policy definition**—The enterprise first must define an egress access policy that explicitly prohibits sending files with specific extension types (e.g., .docx, .xlsx, .pdf) to email addresses outside of the enterprise domain. It might also define rules that block the upload of such files to unapproved cloud storage services.
- **Policy deployment**—To enforce this policy, the enterprise could implement a combination of egress endpoints:
  - **A network firewall**—Configured to block outgoing traffic to external email servers if it contains attachments with the prohibited file extensions
  - **IAM policies and resource policies**—Mandating that workloads in cloud environments will have identities (roles) with permissions that allow or deny the identity to make/transmit data via API calls
  - **A DLP system**—Deployed to scan outbound emails, for example, and block any messages that contain sensitive documents; could also be set up to monitor cloud storage uploads and prevent the transfer of confidential files to unauthorized services

Security Impact and Real-World Examples

Lack of proper egress control in hybrid environments can have severe security implications, as attackers increasingly target outbound traffic to enable communication with attacker command-and-control (C2) servers and allow data exfiltration.

The Uber data breach of 2022 is a good example of how a lack of egress access controls can lead to the exfiltration of customer data from production systems.[1] The attacker was able to access and bulk download data from Uber's finance tool. Blocking egress data transfer to attacker-controlled machines would have helped mitigate the attack.

The Equifax data breach of 2017 is another example of how a lack of egress access policies can lead to data exfiltration.[2] The attackers were able to access and exfiltrate sensitive data over an extended period (76 days) without detection. Robust and centralized egress access policies would have given the security and audit teams clear visibility into what each application needed access to. They could have maintained least-privilege access, minimizing opportunities for data exfiltration.

The Log4j vulnerability is another example. A well-crafted attack enabled Log4j to effectively run a Domain Name System (DNS) query to a malicious domain, exfiltrating access via DNS.[3] Strong egress access policies could have prevented the DNS exfiltration.

Why Centralized Egress Access Policy Management Is Essential

Principles of strict access control and least privilege are echoed in guidance including International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2022, the Cloud Security Alliance (CSA) Cloud Controls Matrix, and US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.[4] This translates directly to the importance of centralized egress policies in hybrid cloud environments for several reasons:

- **Enhanced visibility and control**—Hybrid cloud environments with data flowing across multiple platforms make it challenging to track and monitor egress traffic. Centralized egress policy management provides a unified view of outbound data flows, enabling security teams to identify anomalies, enforce consistent rules (e.g., firewall rules, DLP rules), and respond quickly to potential threats.
- **Consistent policy enforcement**—Managing egress policies in silos across diverse cloud platforms can lead to inconsistencies and gaps in security, often resulting in misalignments with the global enterprise security policies. A centralized approach ensures that the same policies are applied consistently, with context, across the entire hybrid cloud ecosystem, regardless of the underlying technology or location.
- **Reduced complexity and administrative overhead**—Centralized policy management simplifies the process of creating, deploying, and

LOOKING FOR MORE?

- Learn more about, discuss, and collaborate on cybersecurity and governance in ISACA's Online Forums. *https://engage.isaca.org/onlineforum*

updating egress rules. This mitigates the need to manage policies separately for each platform, simplifying administration and minimizing the potential for error.

- **Improved compliance and auditability**—Regulations such as the EU General Data Protection Regulation (GDPR) or industry-specific standards often mandate strict control of data leaving the organization.[5] Centralized egress policies simplify compliance audits by providing a clear and auditable record of outbound data flows and enforced security rules.

Key Opportunities With Centralized Egress

One of the most complex challenges in network security for large-scale hybrid environments is ensuring that organizations send data only to approved partners. Organizations may have a database of approved partners, but ensuring that data leaving their environment goes only to approved partners is not easy. With centralized egress access control, security teams can bridge the gap between approved vendors and approved egress domains (fully qualified domain names) or IP addresses. It allows security teams to create policies that ensure that data leaving the organization via the internet goes only to approved partners.

With centralized egress access control, security teams can bridge the gap between approved vendors and approved egress domains (fully qualified domain names) or IP addresses.

Another opportunity this creates is that organizations can classify what type of data their data processors can receive. With this information, security teams can add policies that not only restrict data access to approved partners, but also directly control what type of data can be sent to partners. This further enhances data security governance.

There are some minimum requirements to be met before an enterprise can implement a centralized egress access policy life cycle:

- Understanding the enterprise infrastructure
- Understanding the enterprise's applications
- Identifying the data processors

Understanding the Enterprise Infrastructure

An enterprise must have a comprehensive understanding of its infrastructure, including:

- Architectural diagrams
- Asset inventory
  - API endpoints
  - Physical devices
  - Virtual devices
- Asset owners
- Data owners

Understanding Enterprise Applications

Similar to understanding its infrastructure, an enterprise should understand its applications. This may entail:

- Understanding what fully qualified domain names, IP addresses, ports, and protocols an application requires access to
- Understanding what other applications within or outside (e.g., software as a service [SaaS]) the enterprise an internal application/user needs access to
- Understanding the sensitivity of the data that the application could be sharing with the external entity
- Understanding the compliance requirements for the application

Identifying the Data Processors

Identifying the partners an enterprise connects with is important to understand what policies are required to allow its applications to interact with those partners/data processors.

Apart from this, it is important to understand what types of data can be shared with each data processor. Permissions could be based on business requirements, security assessments of the partner, regulatory requirements, or internal security policies. It is also important to identify the services provided by the data processor to facilitate the design of controls that can enforce purpose limitation, an important principle of privacy laws and regulations.

Maintaining a catalog of approved data processors that specifies what type of data, based on

Centralized policy management enables a simplified approach to developing and deploying security controls, leading to a more secure and compliant architecture across platforms.

classification, can be shared with them allows an organization to clearly define what applications or clients can interact with the data processors and how those communications should be handled.

Developing an Egress Policy Management Strategy

To effectively manage egress policies across hybrid environments, organizations should focus on eight key deliverables:

1. **Application–data processor mapping**
   - **Goal**—Maintain a central database that links each application to approved data processors. This can be updated by users with infosec approval, or the infosec team can update this database with information via automation.
   - **Actions**—Capture key information, such as application name and egress rules. Use the vetting process to validate whether the internal application requires access to the mapped data processor. Ensure that this follows an approval process.
2. **Data processor catalog**
   - **Goal**—Create a catalog that outlines all the partner data processors for an organization and documents the types of data and permissions for each data processor. Use the vendor management process to verify whether the data processor is an approved vendor.
   - **Actions**—Capture key information, such as data classification and allowed data types for each data processor.
3. **Centralized policy framework**
   - **Goal**—Establish a central system to manage applications and data processor mapping inputs and deploy this mapping as rules on egress endpoints.
   - **Actions**—Create a central user interface (UI) to define applications and data processor mapping. Establish a system to enforce this mapping as egress rules across platforms such as AWS, GCP, Kubernetes, etc., from one central interface.
4. **Dynamic policy access**
   - **Goal**—Ensure that systems can retrieve the latest policies as they are updated.
   - **Actions**—Implement a system to pull policies from the central database in real time, with alerts for retrieval issues.
5. **Identified enforcement points/egress endpoints**
   - **Goal**—Know where policies are enforced (e.g., firewalls, IPS) for each application–data processor connection.
   - **Actions**—Map enforcement points to support effective policy deployment.
6. **Automated policy deployment**
   - **Goal**—Automate policy deployment to reduce manual work and improve consistency.
   - **Actions**—Use automation tools to deploy policies across environments and integrate testing to verify deployments.
7. **Continuous monitoring and audits**
   - **Goal**—Maintain visibility into egress data flows and ensure compliance.
   - **Actions**—Monitor logs for policy violations and conduct regular audits to refine policies and address any emerging security needs.
8. **Feedback loop for policy improvement**
   - **Goal**—Continuously improve egress policies based on system performance and security insights.
   - **Actions**—Regularly review feedback from monitoring and compliance audits to adjust policies as necessary.

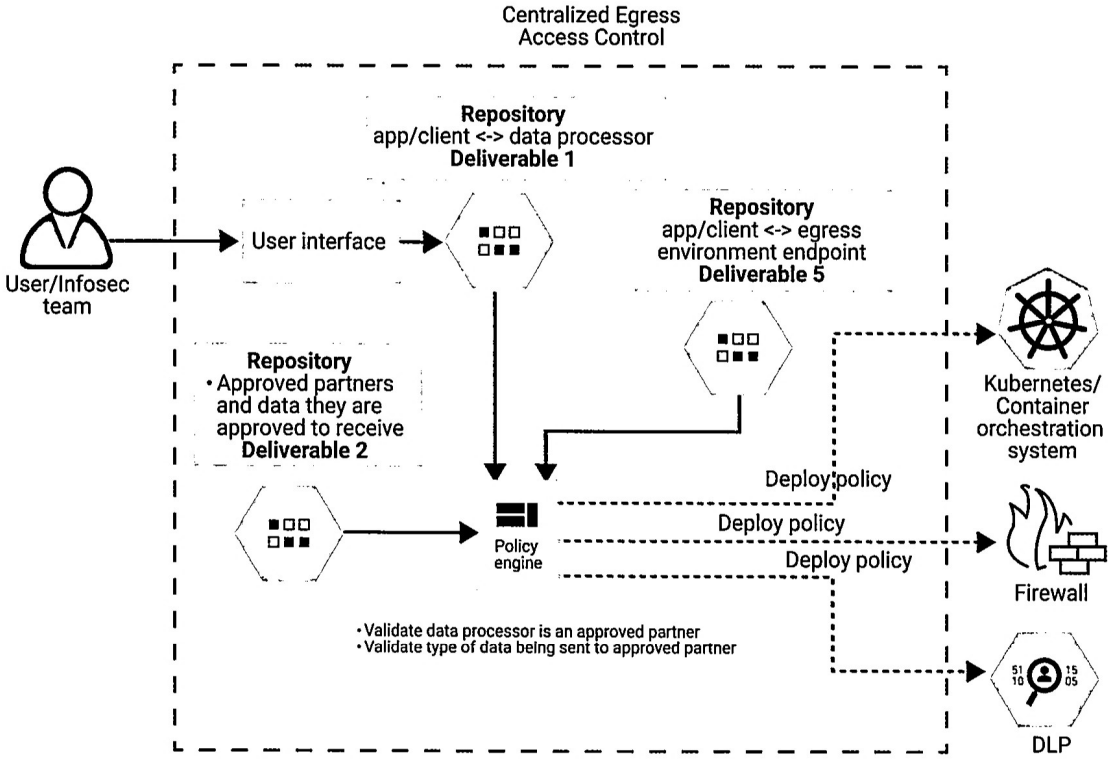
Workflow and Automation

To effectively manage workflow and automation, organizations should focus on 10 steps (**figure 1**):

1. **Define application-to-data processor mapping.** User or Infosec enters the intended egress destination via a central UI along with other metadata such as fully qualified domain name, IP address, etc. (Deliverables: 1, 3)

FIGURE 1

Automated Workflow Illustration



2. **Specify data type to be sent.** User, via a central UI, provides the type/classification of data for validation. (Deliverables: 2, 3)
3. **Validate processor against approved partner list.** The system verifies whether the destination is an approved data processor. (Deliverable: 2)
4. **Validate data type for the processor.** The system verifies whether the data type is allowed for that partner. (Deliverable: 2)
5. **Justify the business need for access.** If validation is successful, the request is reviewed to ensure that there is a valid use case. (Deliverables: 1, 8)
6. **Retrieve the enforcement point and mapping.** The system fetches the right enforcement system for the application. (Deliverables: 1, 4, 5)
7. **Convert mapping into policy rule.** The policy engine renders the rule for the target enforcement system. (Deliverable: 6)
8. **Validate rule and endpoint readiness.** The system checks for policy conflicts and endpoint health. (Deliverables: 6, 7)
9. **Deploy the egress rule.** The system pushes the validated rule to the enforcement point. (Deliverables: 4, 6)
10. **Monitor and refine policies continuously.** Violations and logs feed back into policy improvements. (Deliverables: 7, 8)

Key Benefits

There are numerous benefits of centralizing egress access policies that enterprises can take advantage of to streamline operations and increase efficiency.

Enhanced Visibility

A centralized egress policy provides the chief information security officer (CISO) with enhanced visibility into the organization's security posture, especially regarding outbound data flows. This insight allows the CISO to strategically plan both short- and long-term security roadmaps, justify budget needs, and efficiently allocate resources. With a unified view of egress traffic control, the CISO can proactively address emerging threats and compliance needs that directly impact teams under the CISO's jurisdiction.

Centralized egress policy management can ensure better governance while decreasing staff workload and reducing the potential for human negligence and error.

Simplified IAM

Centralized egress policies simplify IAM by clearly defining which users and applications can access external entities. Identity-based policies with egress rules ensure that only authorized users and systems have data transfer permissions, which strengthens access control and reduces exposure.

Optimized Security

The security operations center (SOC) directly benefits from centralized egress monitoring, making it easier to detect and respond to abnormal outbound data flows. With consistent egress rules, the SOC can quickly identify and act on potential data exfiltration, minimizing response times and improving incident detection accuracy.

Centralized policies also streamline incident management by providing guidelines on acceptable data transfers. During incidents, security teams can quickly assess compliance with egress policies, enabling quicker investigation, root-cause analysis, and containment of potential breaches.

Similarly, security engineers can integrate egress control requirements into system designs from scratch, reducing the need for retroactive security patches. Centralized policy management enables a simplified approach to developing and deploying security controls, leading to a more secure and compliant architecture across platforms. For example, the cloud security and network security teams will have a better understanding of their data perimeters, which will enable them to fine-tune controls and tools for developers to securely interact with the internet.

Ease of Compliance and Governance

Compliance teams can effectively influence data handling standards across cloud environments, making audits smoother and reducing regulatory risk. Centralized egress control allows these teams to take a standardized approach to outbound data management. This is crucial for meeting EU GDPR, US Health Insurance Portability and Accountability Act (HIPAA), and other regulations' requirements. Furthermore, this drastically improves the efficiency and the ease with which evidence can be gathered in response to audit, compliance, and regulatory queries.

Red Team Advantages

Red teams gain a structured framework to test for egress control weaknesses. By knowing the established egress policies, they can better simulate potential data exfiltration techniques, helping identify gaps in the policy framework and improving overall defenses.

Enhancing AI Data Security and Compliance Through Centralized Egress Control

Artificial intelligence (AI) and machine learning (ML) are evolving rapidly. Ensuring data security and compliance has become paramount, especially as organizations increasingly rely on third-party environments, such as Databricks and Snowflake, for storing models, training data, and operational data.[6] A centralized egress control system offers a solution by regulating data flows between enterprise infrastructures and AI processing platforms. Centralized egress control not only safeguards data in transit but also serves as a critical DLP mechanism, especially for mapping applications to specific egress domains along with validating both data types and recipient identities.

The centralized system approach is critical in meeting stringent AI governance and compliance requirements. It addresses the EU AI Act's mandate for ensuring data quality, integrity, and cybersecurity in high-risk AI systems, particularly in preventing data poisoning and adversarial attacks.[7] The granular controls align with NIST's AI Risk Management Framework, supporting the Map and Govern functions by providing clear data lineage and enforcing access controls.[8] Furthermore, with features such as a data processor catalog, it enables compliance with the EU GDPR's principles of data minimization and purpose limitation and supports adherence to the US State of California Privacy Rights Act (CPRA) requirements for limited data collection and secure processing.[9]

Consider a healthcare organization developing an AI model to predict patient outcomes using sensitive medical records on an AI processing platform. A centralized egress system ensures that only approved types of de-identified patient data are transmitted to the approved AI processing platform. It enforces data minimization and maintains a detailed audit trail. This approach not only mitigates risk associated with unauthorized access or data misuse but also establishes a baseline for ethical and responsible AI development. By implementing these controls, organizations can leverage the power of third-party AI platforms while maintaining detailed visibility of the data and models leaving their environment, thereby improving trust and compliance in their AI initiatives and partners.

Multinational organizations with diverse service and product offerings often must abide by multiple regulations. This could be because they are regulated entities (REs) that are required to do so by vendor contracts, because they want to avoid lawsuits, or because they want to follow industry best practices to safeguard their data. Regardless of the reason, meeting requirements for multiple endpoints in a hybrid infrastructure, while actively managing the life cycle of each control, is a herculean task. Centralized egress policy management can ensure better governance while decreasing staff workload and reducing the potential for human negligence and error.

Conclusion

Centralizing egress access policies is not merely an option but a fundamental necessity for organizations operating in large hybrid cloud environments. By focusing on policy management and governance of egress data, organizations can improve visibility, enforce consistent security controls, and mitigate the risk of data breaches. This proactive approach ensures compliance with relevant standards, enhances operational efficiency, and strengthens the overall security posture of organizations in dynamic and distributed hybrid cloud environments.

Endnotes

1 Egress, "Uber Breach Proves Power of Social Engineering," 26 September 2022, *https://www.egress.com/blog/phishing/uber-breach-social-engineering*

2 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach*, USA, 2018, *https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf*

3 Weems, A.; "Log4j 2.15.0 Stills Allows for Exfiltration of Sensitive Data," Praetorian, 15 December 2021, https://www.praetorian.com/blog/log4j-2-15-0-stills-allows-for-exfiltration-of-sensitive-data/

4 International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection—information security management systems—requirements*, 2022, *https://www.iso.org/standard/27001*; Cloud Security Alliance, "Cloud Controls Matrix (CCM)," *https://cloudsecurityalliance.org/research/cloud-controls-matrix*; National Institute of Standards and Technology (NIST), *NIST SP 800-53 Rev. 5—Security and Privacy Controls for Information Systems and Organizations*, USA, September 2020, *https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final*

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [GDPR])

6 Databricks, "Deploy Models Using Mosaic AI Model Serving," *https://docs.databricks.com/aws/en/machine-learning/model-serving*; Snowflake, "Snowflake Model Registry," *https://docs.snowflake.com/developer-guide/snowflake-ml/model-registry/overview*

7 European Parliament, "EU AI Act: First Regulation on Artificial Intelligence," European Union, 14 June 2023, *https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence*

8 National Institute of Standards and Technology (NIST), NIST AI-600-1 *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, USA, 2024, *https://doi.org/10.6028/NIST.AI.600-1*

9 IAPP, "CCPA and CPRA Topic Page," *https://iapp.org/resources/topics/ccpa-and-cpra/*