The Journey to Zero Trust Architecture for PCI DSS 4.0

Leveraging Microsegmentation, Workload Identities and Zero Trust Architecture to Limit PCI DSS Scope

PCI Security Standards Council

Kerry Steele

Principal, Payments and Cloud Advisory
Coalfire Systems, Inc.

COALFIRE

Agenda

Embracing Modern Network Architectures for Payment Systems

- Zero Trust Architecture (ZTA)
- ZTA Alignment with PCI DSS
- PCI DSS scope
- Service mesh
- Microsegmentation
- Workload Identities
- Identity-based microsegmentation with SPIFFE
- ZTA with Istio and Envoy

The Evolving Threat Landscape

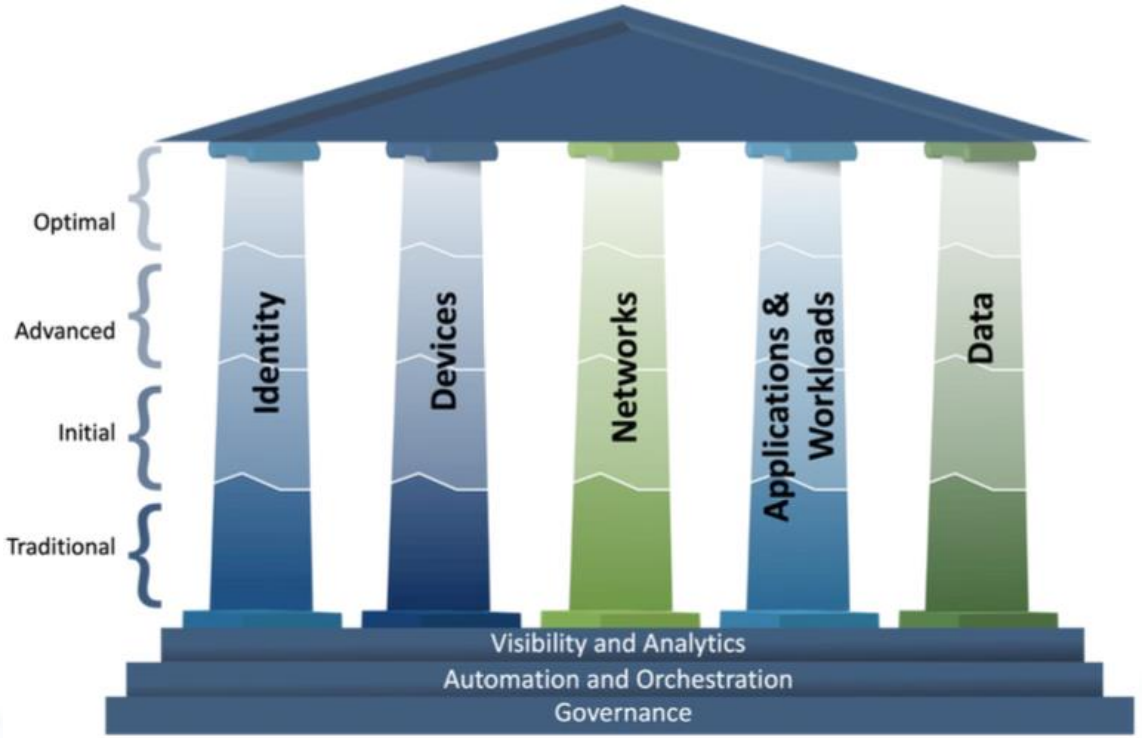
Why Traditional Security is No Longer Enough

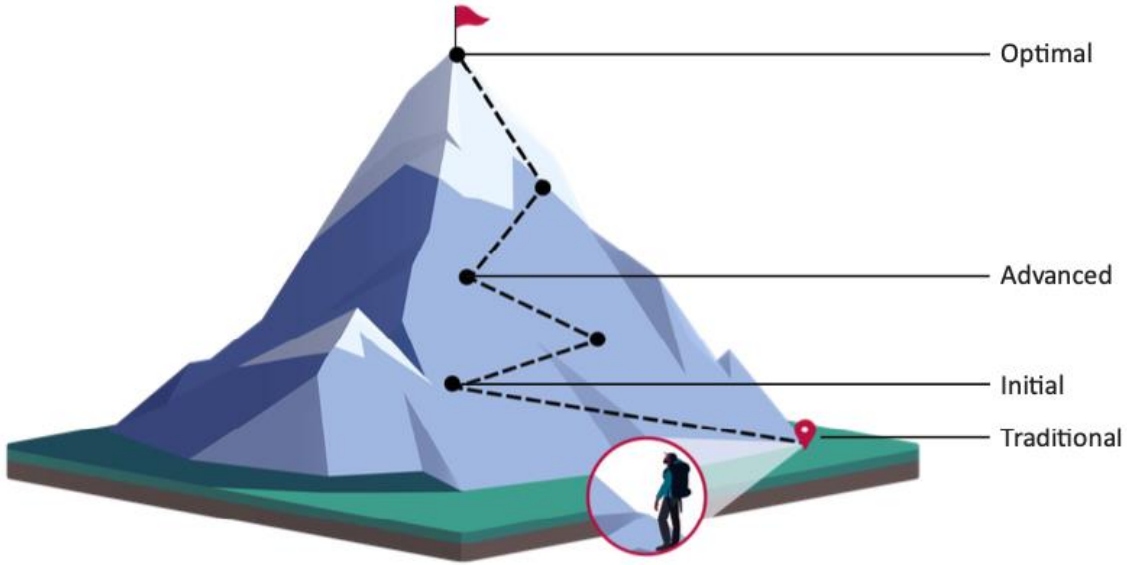
- Increased attack sophistication
- Expanding attack surface
- Insider threats
- Spearphishing / Vishing / Smishing
- Supply chain
- Artificial Intelligence

PCI Security Standards Council

Adoption of Zero Trust Architecture

CISA Zero Trust Maturity Model





PCI Security Standards Council

	Identity	Devices	Networks	Applications and Workloads	Data
					
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

PCI DSS 4.0 and Zero Trust: Already Aligned

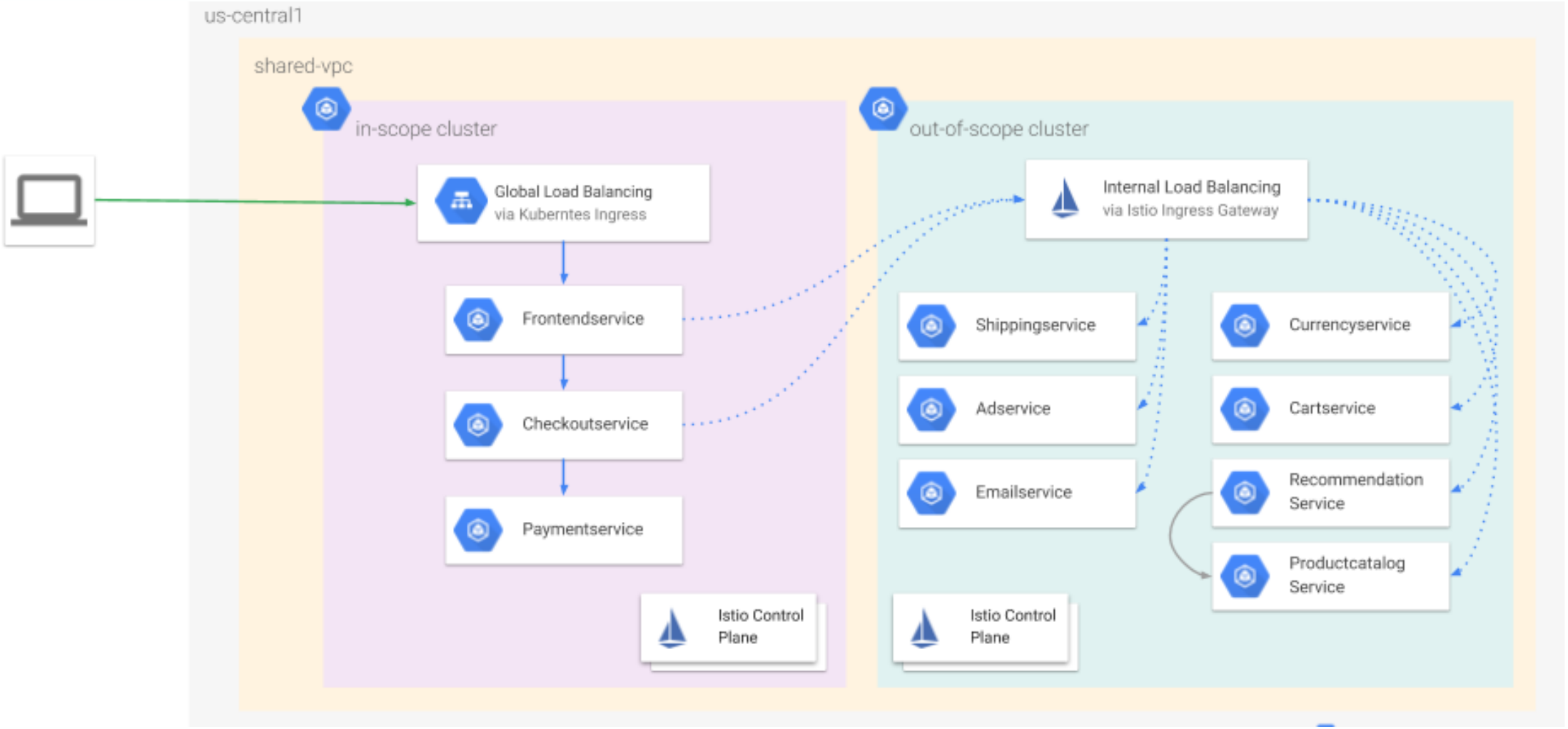
Strengthening Payment Security

- Zero Trust Architecture:
  - *Least privilege access*
  - *“Never trust, always verify”*
  - Assume breach
  - *Segmentation*
  - *Role-based access control (RBAC)*
  - *Multi Factor Authentication (MFA)*
  - *Strong Cryptography*
  - *Continuous Monitoring*
  - Attribute-based access control (ABAC)
  - Context-based access control (CBAC)
  - User and entity behavior analytics (UEBA)
- PCI DSS 4.0 Requirements:
  - *Least privilege access*
  - *Deny by Default*
  - Access reviews
  - *Segmentation*
  - *Role-based access control (RBAC)*
  - *Multi Factor Authentication (MFA)*
  - *Strong Cryptography*
  - *Continuous monitoring*
  - Software supply chain
  - Non-human identities
  - *Dynamic authorization*

Limiting Systems in Scope for PCI DSS

Reducing Compliance Burden with Microsegmentation and ZTA

- PCI DSS Scope:
  - System components that store, process, or transmit cardholder data (CHD)
  - Connected-to and *Security-impacting system components*
- Zero Trust Architecture:
  - Fine-grained real-time dynamic access to in scope resources
  - Can reduce PCI DSS scope
- Microsegmentation with Service Mesh:
  - *Implementations can enforce a ZTA for payment systems*
  - Isolate systems not in scope of CHD environments
  - Reduce the number of systems requiring compliance



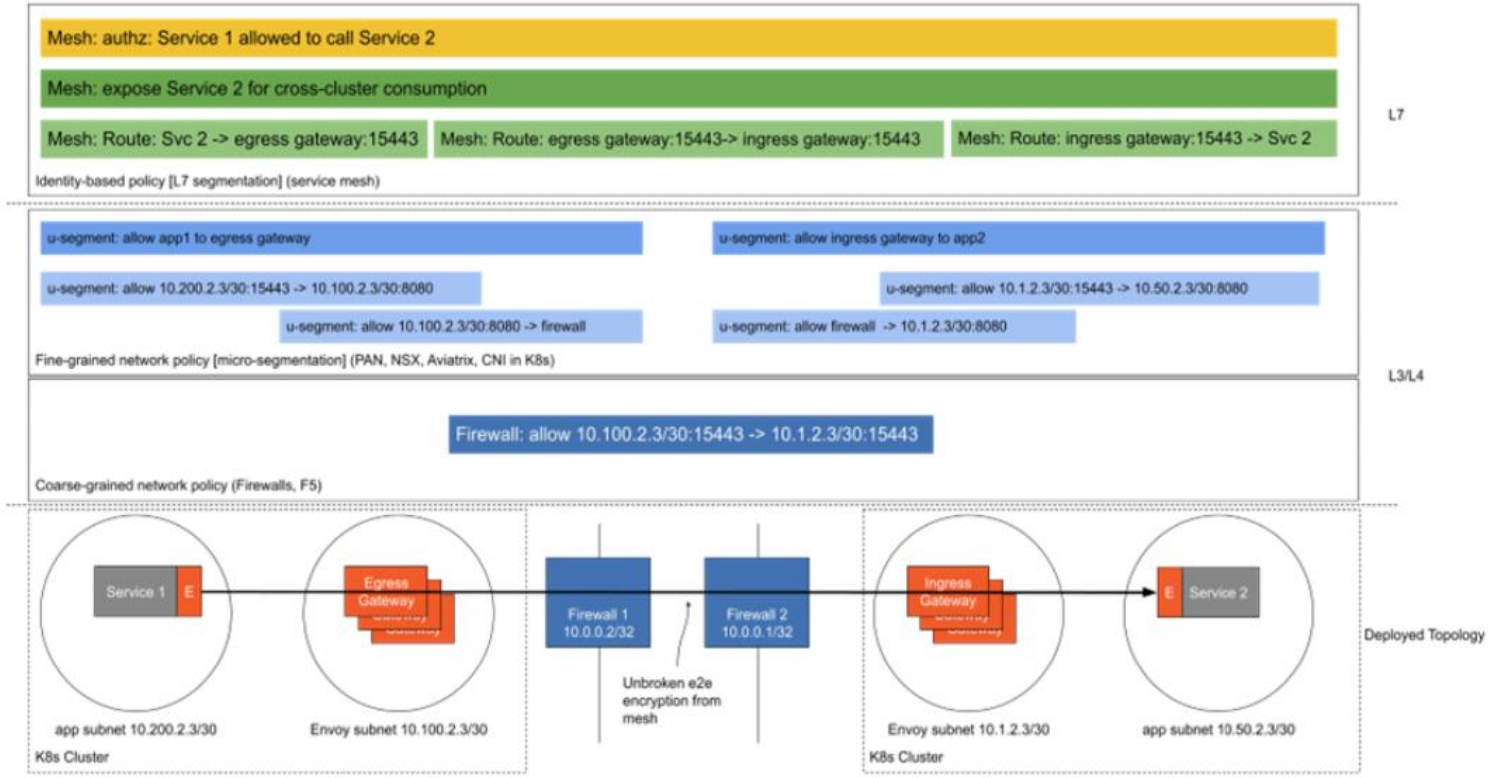
Limit PCI DSS Scope with Microsegmentation

PCI Security Standards Council

Service Mesh for Mutual Authentication and Authorization

Enhancing Security in Microservices

- Service Mesh:
  - Dedicated infrastructure layer
  - Facilitates service-to-service communication
  - Provides security, observability, and reliability
- Mutual TLS (mTLS):
  - Authenticates both client and server
  - Encrypts traffic between services
- Authorization Policies:
  - Fine-grained access control
  - Least privilege enforcement



PCI Security Standards Council

Microsegmentation with Service Mesh

Limiting Lateral Movement

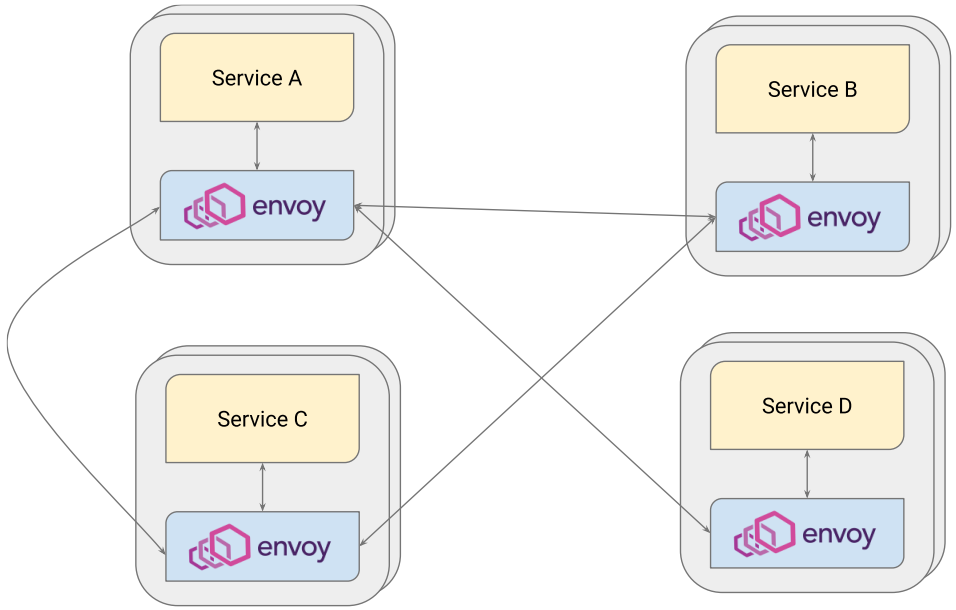
- Traditional Network Segmentation:
  - Traditional approach: VLANs, subnets
  - Limitations: Static, inflexible
- Microsegmentation with Service Mesh:
  - *Fine-grained isolation at the service level*
  - *Dynamic policy enforcement*
  - Reduced attack surface
- Identity-Based Microsegmentation:
  - *Uses workload identities*
  - Granular access control policies
  - Dynamic policy enforcement
- Benefits:
  - Enhanced security through granular access controls.
  - Improved agility and scalability in dynamic environments.
  - Reduced attack surface and minimizes lateral movement.

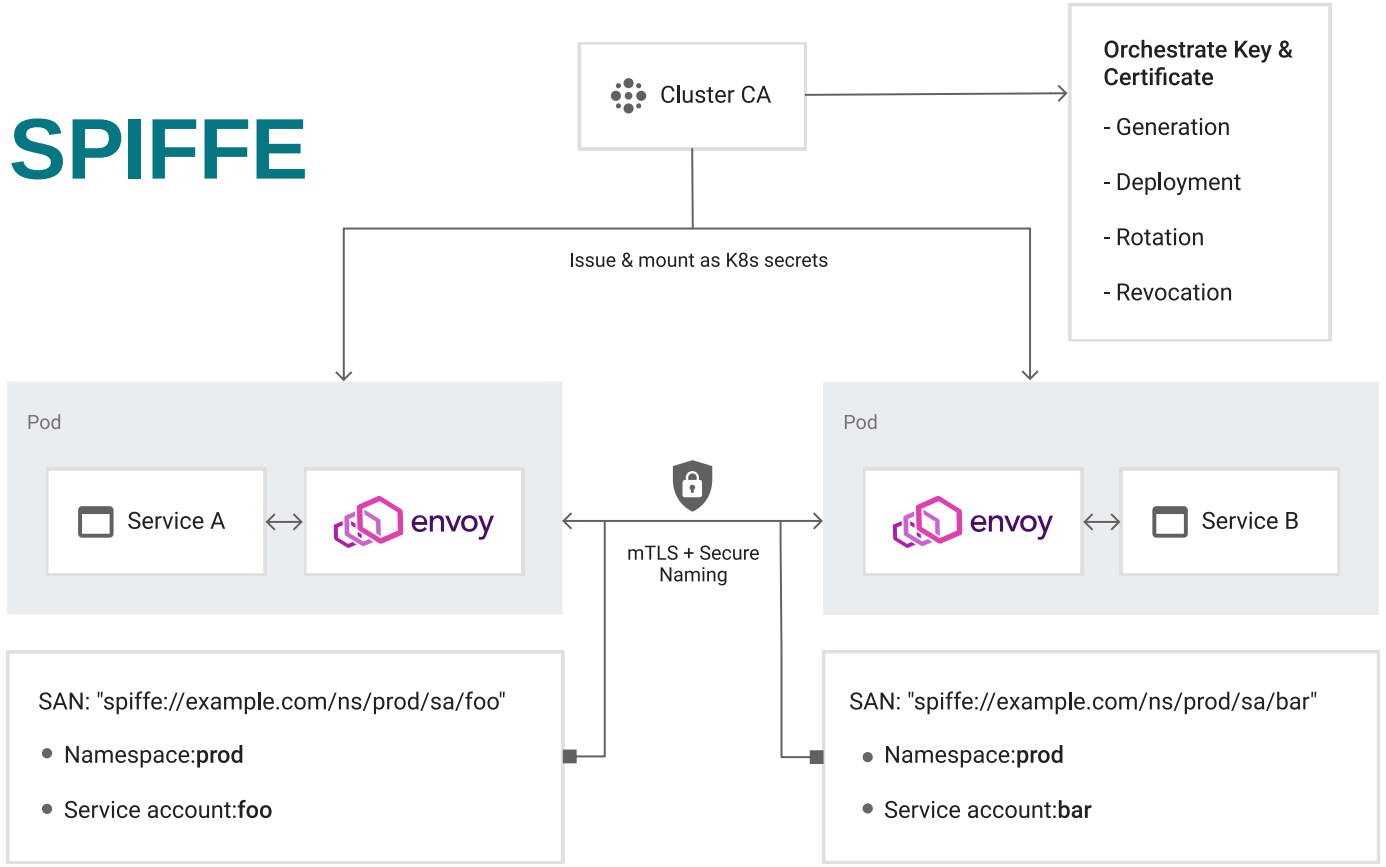
Workload Identities

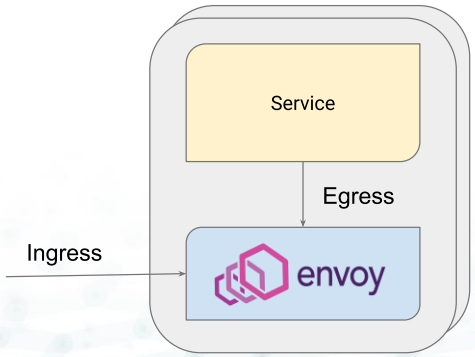
Establishing Trust in Dynamic Environments

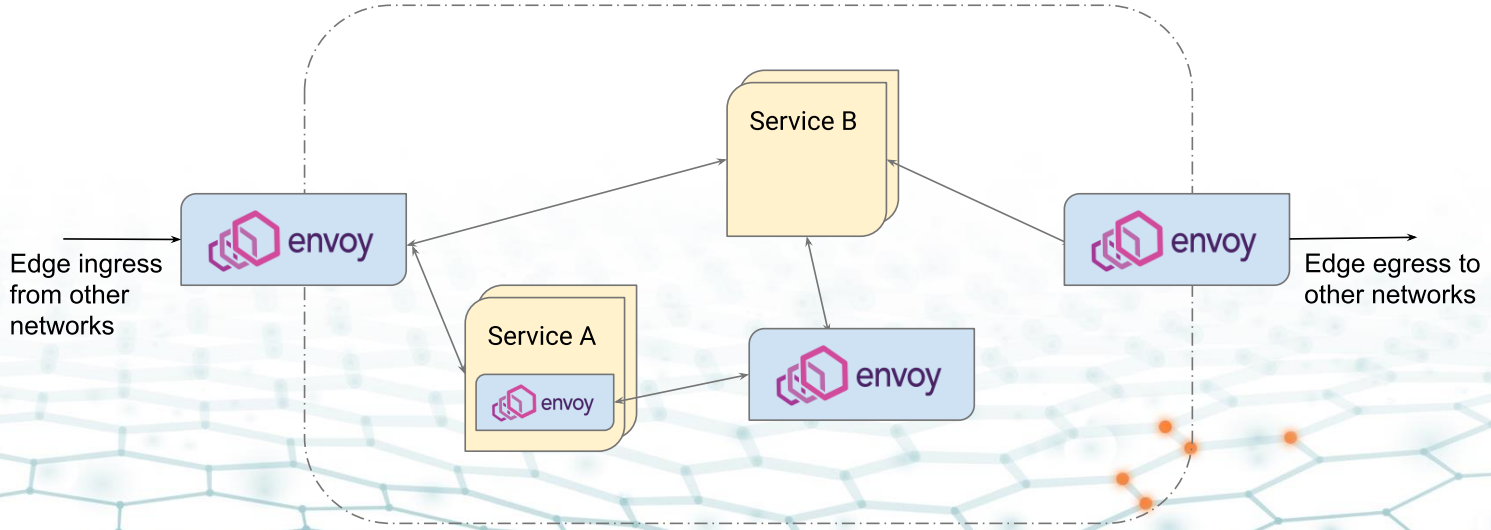
- SPIFFE (Secure Production Identity Framework for Everyone):
  - Open-source framework for creating and managing platform-agnostic, cryptographic identities for software workloads.
- SVID (SPIFFE Verifiable Identity Document):
  - Cryptographically verifiable document that carries a workload's identity.
  - Typically implemented as an X.509 certificate.
- Benefits:
  - *Enables secure communication between workloads with Non-human Identities (NHI).*
  - *Facilitates authentication and authorization in zero trust environments.*
  - *Can be assigned to any software program, not just microservices.*

Envoy Sidecar Proxies + SPIFFE



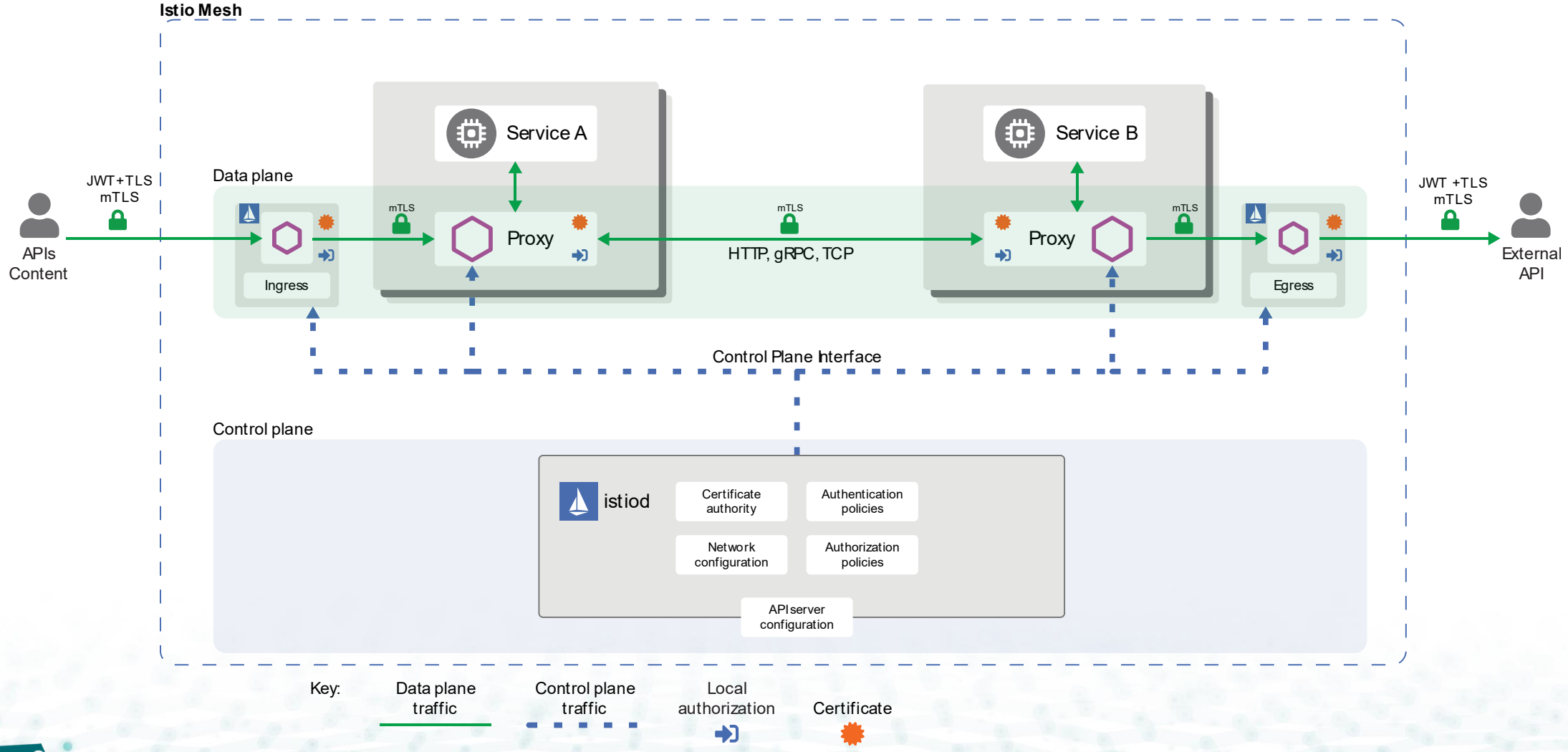






PCI Security Standards Council

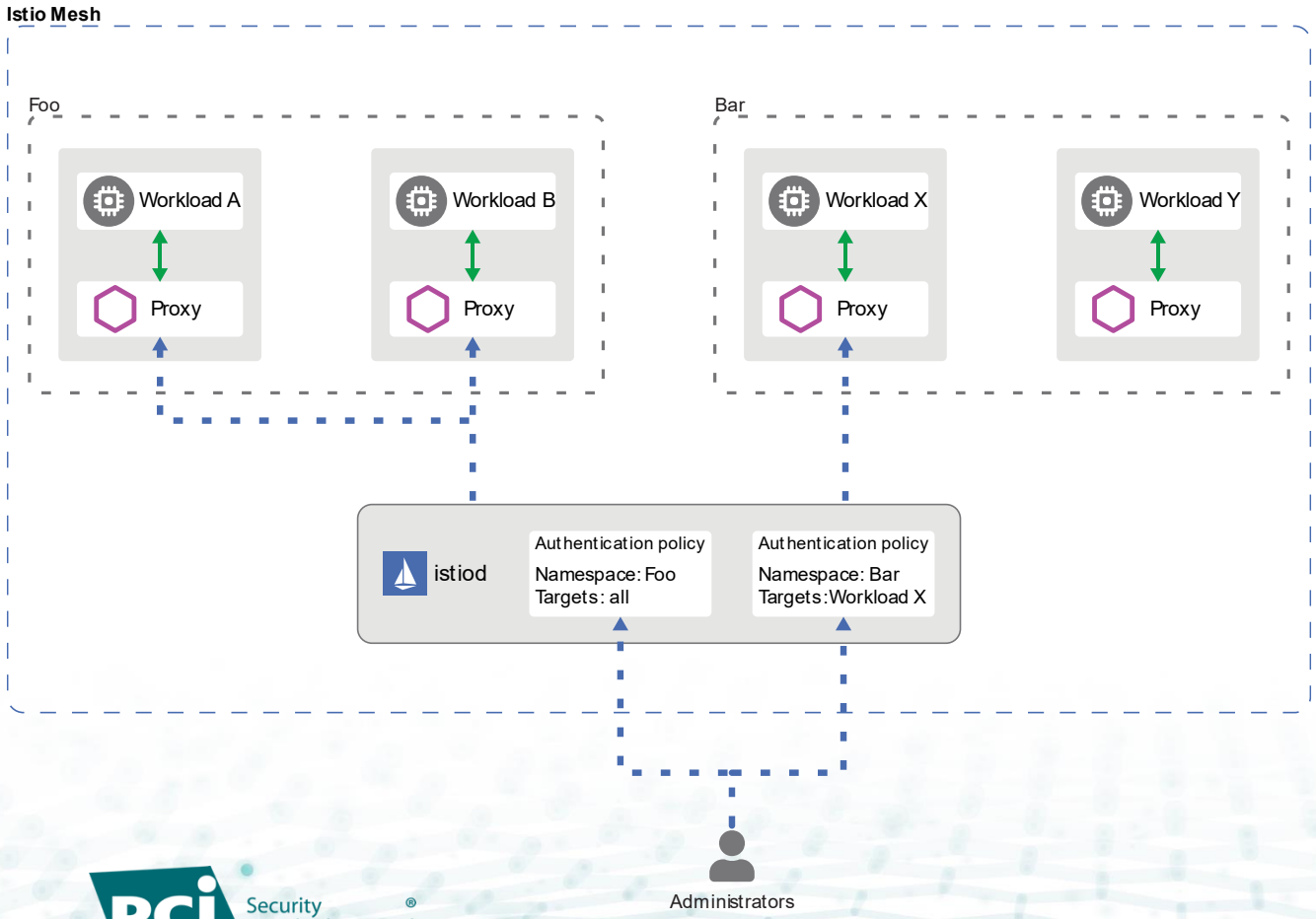
Implement ZTA with Istio and Envoy



PCI Security Standards Council

Istio Authentication

Istio enforces peer authentication policies that define mTLS authentication modes on target workloads



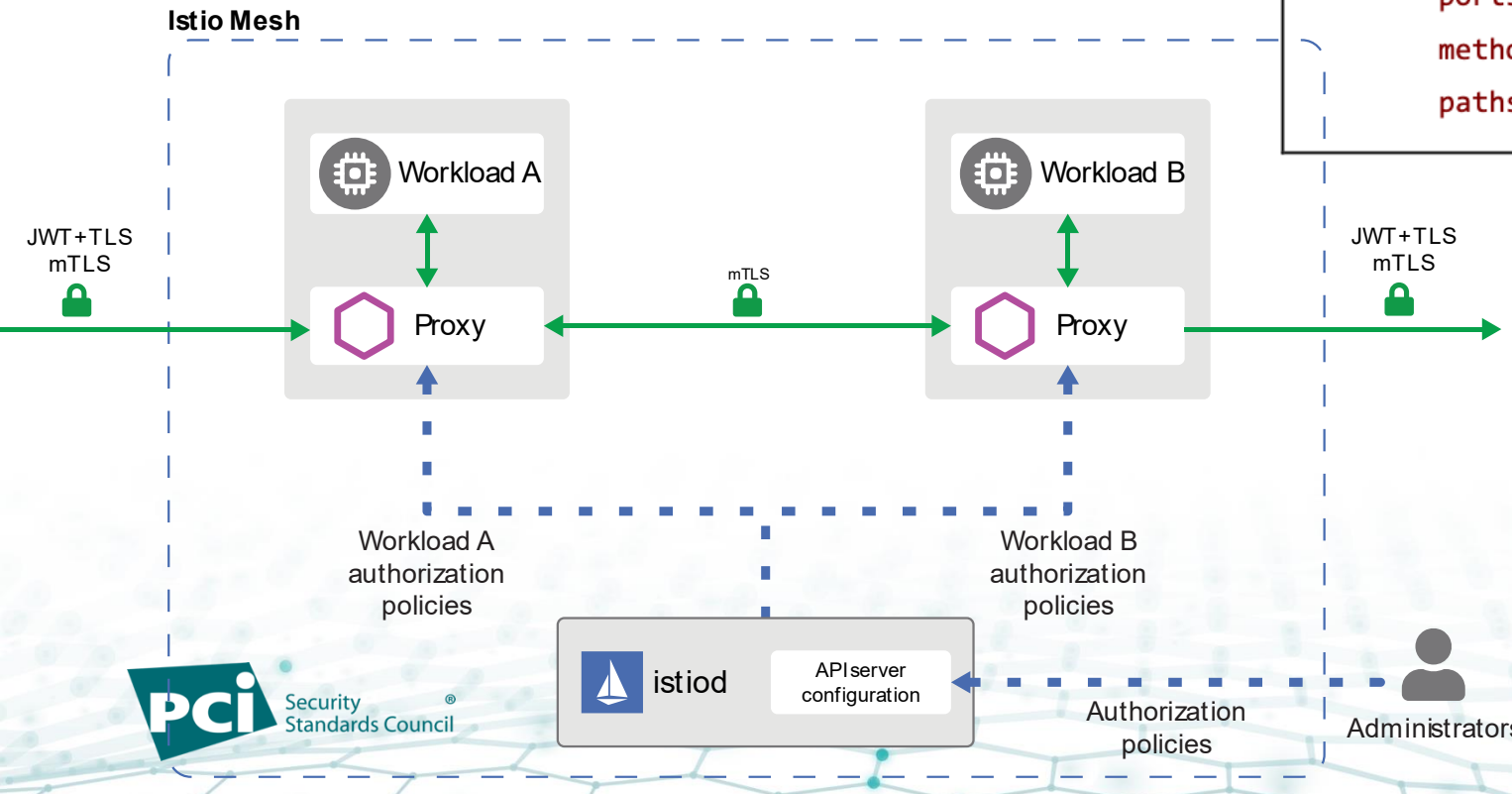
- PERMISSIVE *(Default setting)*: Workloads accept both mutual TLS and plain text traffic. This mode is most useful during migrations when workloads without sidecar cannot use mutual TLS. Once workloads are migrated with sidecar injection switch the mode to STRICT.
- STRICT: Workloads only accept mutual TLS traffic.
- DISABLE: Mutual TLS is disabled. This mode should not be used for payment systems or ZTA environments.

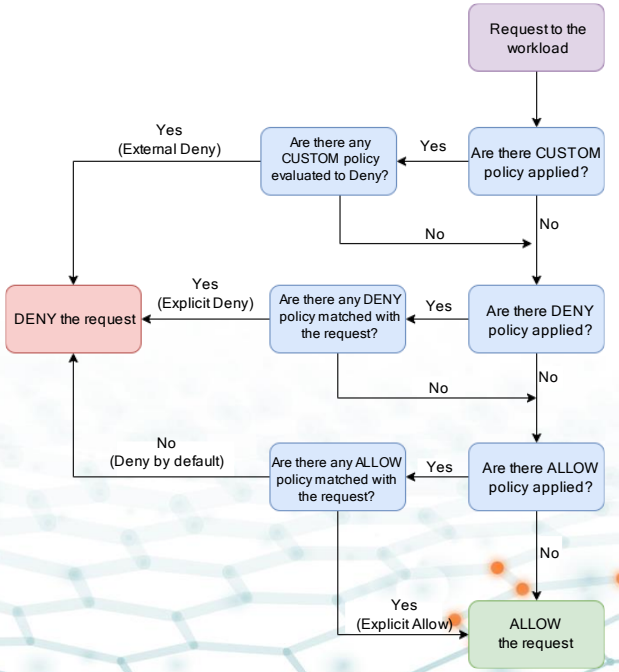
PCI Security Standards Council

Istio Authorization

Policy Defined in Infrastructure as Code

```
    selector:
  matchLabels:
    app: service-2
action: ALLOW
rules:
- from:
  - source:
      principals: ["cluster.local/ns/service-1/sa/service-1"]
  to:
  - operation:
      ports: ["443"]
      methods: ["GET"]
      paths: ["/public"]
```





Conclusion

Embracing Modern Network Architectures for a Secure Payment Future

- Zero Trust Architecture is a powerful framework for strengthening payment security and aligns closely with the requirements of PCI DSS 4.0.
- The path to zero trust is a journey, but the benefits are significant.
- By adopting Zero Trust Architecture for payment systems with modern network security controls like service mesh with microsegmentation, and identity-based microsegmentation, organizations can enhance security, limit PCI DSS scope, reduce risk, and streamline their compliance efforts.

References

- CISA Zero Trust Maturity Model v2.0
- PCI on GKE Blueprint
- PCI DSS compliance on GKE
- NIST SP 800-204, Security Strategies for Microservices-based Application Systems
- NIST SP 800-207, Zero Trust Architecture
- NIST SP 800-207A, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments
- NIST SP 1800-35, Implementing a Zero Trust Architecture
- NIST SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture
- NIST SP 800-204B, Attribute-based Access Control for Microservices-based Applications using a Service Mesh
- NIST SP 800-204C, Implementation of DevSecOps for a Microservices-based Application with Service Mesh
- NIST SP 800-204D, Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines
- NIST SP 800-233, Service Mesh Proxy Models for Cloud-Native Applications


PCi
Security
Standards Council
®