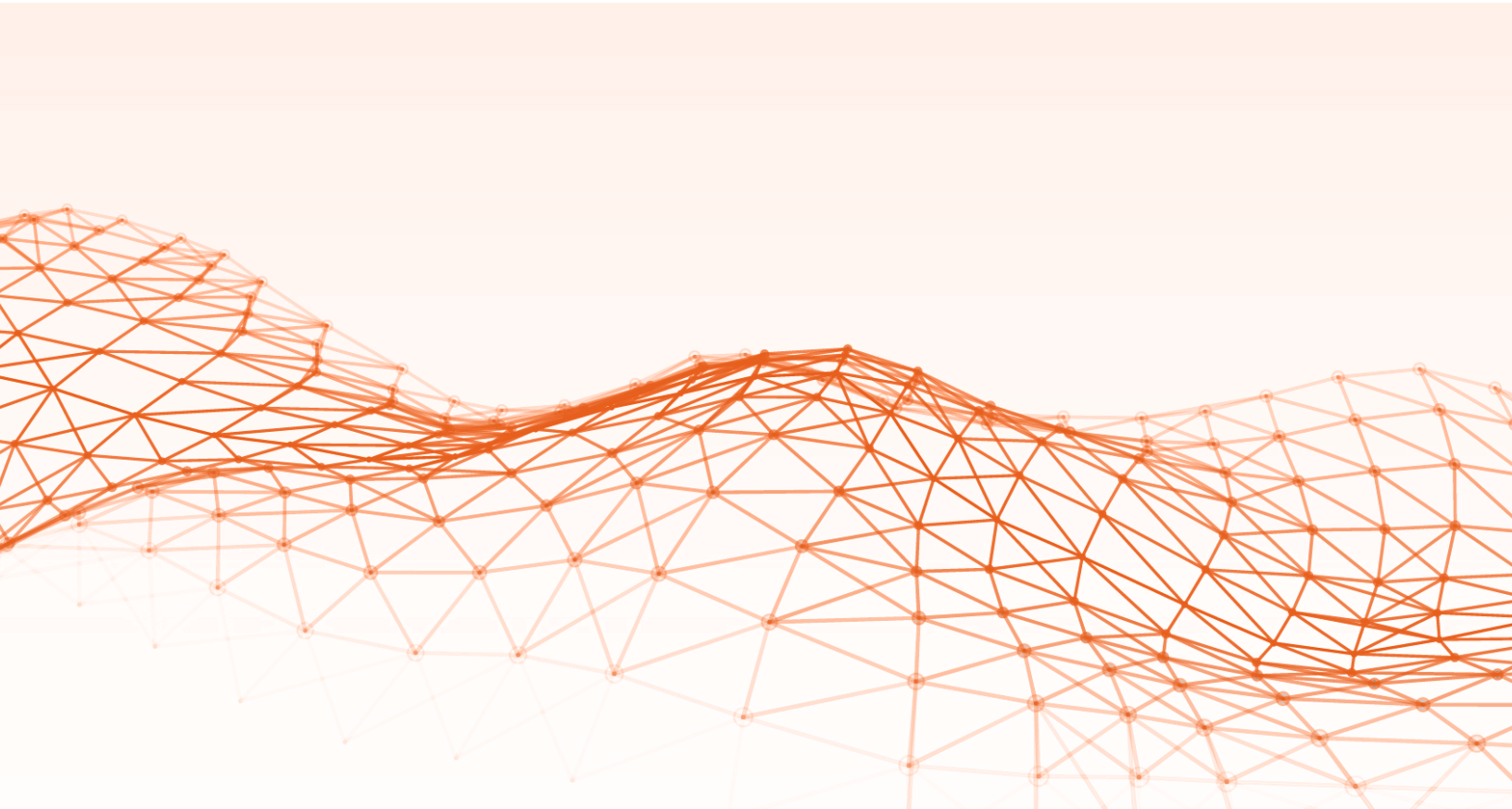
tetrate

TETRATE WHITE PAPER

PCI DSS 4.0

Meet the Latest PCI DSS Requirements for Modern, Cloud-Native Architectures



About Tetrate

Rooted in open source, Tetrate was founded to solve the application networking and security challenges created by modern computing so enterprises can innovate with speed and safety in hybrid and multi-cloud environments. As applications evolve into collections of decentralized microservices, monitoring and managing the network communications and security among those myriad services becomes challenging. This is why some of the largest financial institutions, governments and other enterprises rely on Tetrate to deliver modern application networking and security on a foundation of Zero Trust. http://www.tetrate.io.

Table of Contents

Background

The Payment Card Industry Data Security Standard (PCI DSS) establishes stringent requirements to protect cardholder data and ensure the integrity of payment systems. As businesses increasingly adopt cloud-native, distributed architectures, meeting PCI DSS compliance becomes more complex, particularly in managing the Cardholder Data Environment (CDE) across hybrid and multi-cloud infrastructures.

Modern architectures demand innovative solutions to address these challenges while maintaining robust security and operational efficiency. This is where Tetrate's enterprise-grade gateway and service mesh solutions—Tetrate Istio Subscription (TIS), Tetrate Enterprise Gateway (TEG), and Tetrate Service Bridge (TSB)—come into play. These products provide a unified platform for securing, managing, and observing application traffic, enabling organizations to implement PCI DSS requirements with precision and ease.

Tetrate's products empower businesses to achieve network segmentation, end-to-end encryption, fine-grained access control, and real-time observability—all essential components of PCI DSS compliance. By integrating seamlessly into existing infrastructure, Tetrate solutions reduce the scope of compliance efforts while enhancing the overall security posture of payment environments.

This white paper explores how Tetrate's solutions align with and support key PCI DSS requirements. It demonstrates how these tools simplify compliance, reduce operational complexity, and provide the flexibility to scale securely across modern, distributed systems. Whether you're securing a legacy environment, transitioning to the cloud, or managing a hybrid infrastructure, Tetrate enables you to meet the highest security standards while delivering consistent, compliant payment services.

Tetrate Istio Subscription (TIS and TIS+)

A service mesh is a dedicated infrastructure layer that manages communication between services in modern, cloud-native, and microservices-based architectures. It provides security, observability, and traffic management capabilities, which directly help organizations comply with various PCI DSS requirements.

TIS is a FIPS-compliant and FIPS-verified distribution of Istio—the most widely-deployed service mesh—with the support required for enterprise applications operating in mission-critical and regulatory environments. [TODO: Add TIS+]

Tetrate Enterprise Gateway for Envoy (TEG)

Envoy Gateway, built on Envoy Proxy, is a high-performance edge and service proxy deployed as an application ingress gateway. It provides features like traffic management, encryption, monitoring, and access control, which align with the security, network, and data protection requirements of PCI DSS.

TEG is a FIPS-verified and CVE-protected distribution of Envoy Gateway built by Tetrate, with the compliance, support, and enablement required by applications running in highly secure regulatory environments.

Tetrate Service Bridge (TSB)

Tetrate Service Bridge is an application traffic management platform designed to provide robust security, reliability, and observability for applications running in modern cloud-native and hybrid environments. It directly helps organizations comply with PCI DSS by offering features that address key security, network segmentation, and monitoring requirements.

What Is PCI DSS?

PCI DSS is an abbreviation for the Payment Card Industry Data Security Standard, a compliance framework originally developed by the PCI Security Standards Council in 2004. The PCI DSS requires organizations interfacing with credit card data to adopt a robust set of security controls.

The framework is organized into six objectives and includes twelve requirements:

Build and Maintain a Secure Network and Systems

- **Requirement 1:** Install and maintain network security controls.
- **Requirement 2:** Apply secure configurations to all system components.

Protect Account Data

- **Requirement 3:** Protect stored account data.
- **Requirement 4:** Protect cardholder data (CHD) with strong cryptography during transmission over open, public networks.

Maintain a Vulnerability Management Program

- **Requirement 5:** Protect all systems and networks from malicious software.
- **Requirement 6:** Develop and maintain secure systems and software.

Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to system components and cardholder data by business need to know
- **Requirement 8:** Identify users and authenticate access to system components.
- **Requirement 9:** Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

- **Requirement 10:** Log and monitor all access to system components and cardholder data.
- **Requirement 11:** Test security of systems and networks regularly.

Maintain an Information Security Policy

- **Requirement 12:** Support information security with organizational policies and programs.

What's New in PCI DSS 4.0

Customized Approach for Security Requirements

A major update in PCI DSS 4.0 is the introduction of a "Customized Approach" as an alternative to the "Defined Approach." This provides flexibility for organizations with unique environments or modern architectures (e.g., cloud-native or serverless infrastructures).

- Defined Approach: Follows traditional, prescriptive controls to meet compliance requirements.
- Customized Approach: Allows organizations to use alternative methods or controls to achieve the same security objectives, provided they demonstrate effectiveness through risk analysis, testing, and documentation.

For example, where earlier versions of PCI DSS prescribed controls in terms of firewall, router, and switch configuration, the latest guidance focuses on broader network security controls to allow for the use of newer techniques like service meshes and software defined networking that help segment environments in ways not previously available (Kandyce Young, PCI Security Standards Council, 2024).

Other notable updates include:

- Expanded and enhanced multi-factor authentication (MFA)
- Enhanced password management, enforcing stronger password complexity and retention requirements
- Improved logging and monitoring to capture all critical events and ensures centralized logging capabilities plus an enhanced focus on detecting and responding to anomalies in real time
- Risk-based authentication and access controls
- Improved encryption standards, including migration away from outdated protocols such as TLS 1.0/1.1
- Greater focus on continuous risk management rather than periodic assessments.
- Strengthened vendor management

How Tetrate Helps Meet PCI DSS Requirements

Security Kernel for Modern, Distributed Applications

Tetrate provides a unified and centralized security layer to enforce policies, manage communications, and ensure compliance for modern, distributed applications across hybrid and multi-cloud environments. Acting as a security kernel, Tetrate's service mesh and gateway products simplify and strengthen compliance with PCI DSS requirements by embedding security into the core infrastructure of distributed applications. This ensures consistent, automated enforcement of security controls and visibility across all services.

Here's how Tetrate helps organizations meet the new PCI DSS objectives and requirements.

Objective: Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Requirement	**How Tetrate Helps**
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Provides centralized management of security policies and automated application and enforcement of security rules.
1.2 Network security controls (NSCs) are configured and maintained.	Ensures secure default configurations, such as encrypted traffic and restricted access.

Requirement	How Tetrate Helps
1.3 Network access to and from the cardholder data environment is restricted.	Implements segmentation and traffic filtering at ingress, egress and between application components to limit communication to authorized systems.
1.4. Network connections between trusted and untrusted networks are controlled.	Enforces encrypted, authenticated, and authorized connections between trusted and untrusted networks.

Tetrate provides advanced tools for network segmentation, traffic management, and policy enforcement that simplify the implementation and management of network security controls in modern, distributed environments.

Microsegmentation. Tetrate enforces fine-grained segmentation at the service level, isolating the cardholder data environment from non-CDE systems. This minimizes attack surface and ensures only explicitly allowed traffic can communicate with systems in the CDE.

Deny-by-Default Policies. Tetrate automatically blocks unauthorized traffic by enforcing default deny rules, allowing only traffic that meets defined business requirements.

End-to-End Encryption. Enforces encryption for all application traffic using TLS and mutual TLS (mTLS), ensuring that traffic is secure both within and outside the CDE. This prevents unauthorized interception or tampering with cardholder data in transit.

Authentication and Authorization. Tetrate enforces strong authentication mechanisms, ensuring only trusted services and users can access CDE systems. Role-Based Access Control (RBAC) and Next-Generation Access Control (NGAC) ensure that security configuration is accessible only to authorized personnel, reducing the risk of accidental or malicious changes.

- **Service-to-Service Authentication**: Tetrate uses mutual TLS (mTLS) to authenticate and encrypt communication between services, preventing unauthorized traffic.
- **Policy-Based Access Control**: Fine-grained authorization policies allow traffic only between explicitly permitted services based on business needs, adhering to a "deny-by-default" model.
- **Identity-Based Access Control**: Tetrate integrates with identity providers (e.g., OAuth2, OpenID Connect) to enforce authentication for all access points.
- **Gateway-Level Protection**: Tetrate's Enterprise Gateway provides an additional layer of authentication and authorization at the edge, blocking unauthorized requests before they reach sensitive systems.
- **Protocol Enforcement**. Tetrate blocks outdated or insecure protocols, such as TLS 1.0 or SSL, ensuring compliance with modern cryptographic standards.

Requirement 2: Apply Secure Configurations to All System Components

Requirement	How Tetrate Helps
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Tetrate provides tools to define baseline security configurations for all application traffic, including encryption, protocols, and access policies. Centralized policy management allows organizations to standardize security settings across environments, ensuring consistency and reducing the risk of misconfigurations.
2.2 System components are configured and managed securely.	Tetrate provides centralized configuration management, automation of secure settings, and continuous monitoring. Tetrate ensures that application communication adheres to secure configuration baselines and remains compliant throughout their lifecycle, even in complex, distributed environments.

Centralized Policy Management. Tetrate enables organizations to define and enforce uniform security configurations across all services, ensuring consistency in applying secure defaults, such as:

- Enabling TLS and mutual TLS (mTLS) for encrypted communication.
- Restricting insecure protocols, such as outdated versions of TLS, SSH, or HTTP.
- Configuring allowed ports and protocols to minimize attack surfaces.

Automated Policy Enforcement. Tetrate ensures secure configurations are applied consistently across environments, including hybrid and multi-cloud deployments. Automated deployment of security policies ensures consistent policy enforcement and reduces the likelihood of human error in configuration.

Dynamic Updates. Tetrate automates the propagation of changes to configurations in real-time, ensuring that all systems remain compliant as security standards evolve.

Global Visibility. Tetrate provides centralized visibility, real-time monitoring, and post-facto audit capabilities across distributed environments, enabling organizations to ensure that all application communication adheres to secure configuration baselines and that any deviations are quickly identified and addressed.

Objective: Protect Account Data

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Requirement	How Tetrate Helps
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.	• Allows organizations to define policies to enforce strong cryptographic mechanisms for data in transit and ensures encryption requirements are consistently applied to application traffic, regardless of environment. • Continuously monitors encrypted traffic flows and logs compliance-related activities, simplifying auditing and validation processes.
4.2 Primary account number (PAN) is protected with strong cryptography during transmission.	• Automates the use of TLS and mutual TLS for application communication, ensuring data is authenticated, authorized, and encrypted during transmission. • Encrypts traffic entering and exiting the network, ensuring cardholder data remains protected during transit over public networks. • Securely routes data between services while maintaining encryption throughout. • Enforces modern, secure cryptographic protocols (e.g., TLS 1.3) and disables insecure or deprecated protocols. • Automates the lifecycle of cryptographic keys and certificates, ensuring strong encryption and reducing the risk of key compromise.

Objective: Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications.

Requirement	How Tetrate Helps
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	• Enables organizations to define standardized security policies for application communication • Provides a unified platform for managing and enforcing security mechanisms such as encryption, authentication, and access control. • Automates the application of secure configurations to ensure consistency and prevent drift. • Continuously monitors systems and software for vulnerabilities or deviations from secure configurations.
6.3 Security vulnerabilities are identified and addressed.	• Provides and integrates with scanning tools to identify and address vulnerabilities during development and in production. • Enables automatic updates and patching to address identified vulnerabilities promptly.
6.4 Public-facing web applications are protected against attacks.	• Deploys WAF solutions to protect against common web application vulnerabilities. • Detects and blocks unapproved service connections or misconfigured endpoints. • Ensures secure application communication and enforces zero-trust principles in application environments.

Requirement	How Tetrate Helps
6.5 Changes to all system components are managed securely.	• Workspace-based isolation and role-based access control (RBAC) ensure only authorized personnel can initiate or approve changes. • Automated policy updates enable secure and consistent updates to system configurations and policies without manual intervention. • Dynamic configuration management updates configurations in real time, ensuring no downtime or exposure during changes. • Change tracking logs all configuration changes, providing an auditable trail for compliance validation. • Integrates with CI/CD pipelines to test configuration changes in staging environments before deployment. • Maintains strict access controls and segmentation during changes, ensuring that the CDE remains protected.

Tetrate helps organizations develop and maintain secure systems and applications by:

Defining Secure Configurations: Security teams use Tetrate to create baseline security policies that enforce mutual TLS (mTLS), RBAC, and encrypted communication.

Integrating with Development Pipelines: Developers integrate Tetrate into their CI/CD pipelines, ensuring secure configurations and policies are validated during development.

Applying and Maintaining Policy Configuration: Tetrate consistently applies and updates application control and data plane configuration to eliminate drift, protect against known vulnerabilities, or deviations from established policy, automatically alerting teams for remediation.

Objective: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Tetrate's provides an identity and access management (IAM) architecture based on three core object classes:

- Tenants: any logical grouping that matches a corporate structure.
- Workspaces: a strictly partitioned zone where teams manage their exclusively owned resources.
- Groups: named collection of users, service accounts, and other teams that may be assigned access permissions on various resources.

Organization control permissions through RBAC mapped to users and groups from the organization's identity provider. These roles and permissions limit the data users have access to for all logical groups of system components managed by Tetrate, including those with CHD.

Requirement	**How Tetrate Helps**
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	• Role-based access control (RBAC) allows organizations to define and enforce access policies based on user roles and responsibilities. • Identity and role mapping integrates with identity providers to map users and services to predefined roles for access control.
7.2 Access to system components and data is appropriately defined and assigned.	• Centralized management provides a unified platform for defining, managing, and monitoring access controls. • Policy visualization displays active access policies and their enforcement status to ensure clarity and understanding of access mechanisms.

Requirement	How Tetrate Helps
7.3 Access to system components and data is managed via an access control system(s).	• Fine-grained access control enforces access at the service and API level, ensuring that users and services can access only what is required. • Applies the principle of least privilege by default, allowing access only to explicitly permitted resources. • Real-time visibility tracks all access attempts and provides insights into who accessed what systems or data. • Comprehensive logging captures all access events, including granted and denied requests, for auditing and compliance validation.

Requirement 8: Identify Users and Authenticate Access to System Components

Tetrate aligns with an organization's structure by synchronizing with users and groups from an organization's identity provider and using NGAC to internally map them to the access control policies defined in Tetrate's management plane. This ensures comprehensive and up-to-date authentication and authorization of user access to system components.

Requirement	How Tetrate Helps
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Tetrate regularly syncs with an organization's identity provider, automatically reflecting the addition, deletion, and modifications of user IDs and credentials.

Requirement	How Tetrate Helps
8.3 Strong authentication for users and administrators is established and managed.	Tetrate stores passwords using Vault or Kubernetes secrets. The credentials entered by users are stored in memory and transferred only via secure https connection.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	Implementation of multi-factor authentication (MFA) may be configured through a preferred provider. Tetrate is not tied to a specific MFA vendor.

Objective: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Tetrate provides global, detailed telemetry (e.g., logs, metrics, and traces) for all gateway-to-service and service-to-service communications plus audit logs of policy, configuration and other system change events, enabling tracking and monitoring access to CHD environments. This can integrate with SIEM tools for real-time monitoring, anomaly detection, and forensic analysis.

Requirement	How Tetrate Helps
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	• Tetrate collects logs from all services and system components, ensuring a unified view of access events. • Tracks every service-to-service and user-to-service interaction, identifying who accessed which system and when. • Comprehensive audit trails are logged for all user activities, including logins, access attempts, and changes to configurations or data.

Requirement	How Tetrate Helps
10.3 Audit logs are protected from destruction and unauthorized modifications.	Each user may only view logs relevant to the tenant, workspace, and group objects to which they belong. No user can make changes, additions, or deletions to Tetrate-managed audit trails.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	Audit logs are readily available to authorized users via Tetrate's administration user interface as well as via Tetrate's secure management API to facilitate regular review.
10.5 Audit log history is retained and available for analysis.	Audit trails are stored in the PostgreSQL database specified during initial setup. The database should be hardened according to PostgreSQL and reputable outside security sources. Organizations should forward logs generated by Tetrate to a security information and event management (SIEM) solution with capabilities for log protection.

Conclusion

Achieving and maintaining compliance with the Payment Card Industry Data Security Standard is a critical requirement for organizations handling cardholder data. The evolving threat landscape, coupled with the adoption of cloud-native and microservices architectures, has introduced new challenges in securing the cardholder data environment. Tetrate's products—Tetrate Istio Subscription (TIS), Tetrate Enterprise Gateway for Envoy (TEG), and Tetrate Service Bridge (TSB)—offer comprehensive solutions to address these challenges and enable organizations to meet PCI DSS requirements effectively.

By leveraging Tetrate's offerings, organizations can implement robust network security controls, enforce end-to-end encryption, and achieve fine-grained access control to protect cardholder data. The advanced visibility, logging, and monitoring capabilities provided by these tools empower organizations to meet the stringent requirements of PCI DSS while maintaining a scalable and resilient infrastructure. Tetrate's support for multi-cloud and hybrid environments ensures that compliance and security controls remain consistent, visible, and auditable regardless of where services are deployed.

With features like dynamic traffic segmentation, mutual TLS (mTLS), role-based access control (RBAC), and automated policy enforcement, Tetrate enables organizations to isolate their CDE, protect sensitive data in transit, and reduce compliance scope—all while simplifying operations and reducing costs. These capabilities align directly with PCI DSS requirements for securing cardholder data, protecting networks, managing access, and responding to incidents.

Tetrate provides organizations with the tools and capabilities to seamlessly integrate PCI DSS compliance into their modern, distributed architectures. By bridging security, compliance, and operational efficiency, Tetrate empowers organizations to focus on delivering secure, reliable, and compliant payment services in an ever-changing digital landscape.

###

If you're new to service mesh, Tetrate has a bunch of free online courses available at Tetrate Academy that will quickly get you up to speed with Istio and Envoy.

Are you using Kubernetes? Tetrate Enterprise Gateway for Envoy (TEG) is the easiest way to get started with Envoy Gateway for production use cases. Get the power of Envoy Proxy in an easy-to-consume package managed by the Kubernetes Gateway API. Learn more ›

Getting started with Istio? If you're looking for the surest way to get to production with Istio, check out Tetrate Istio Subscription (TIS+). Tetrate Istio Subscription has everything you need to run Istio and Envoy in highly regulated and mission-critical production environments. It includes Tetrate Istio Distro, a 100% upstream distribution of Istio and Envoy that is FIPS-verified and FedRAMP ready. For teams requiring open source Istio and Envoy without proprietary vendor dependencies, Tetrate offers the ONLY 100% upstream Istio enterprise support offering.

Need global visibility for Istio? TIS+ is a hosted Day 2 operations solution for Istio designed to simplify and enhance the workflows of platform and support teams. Key features include: a global service dashboard, multi-cluster visibility, service topology visualization, and workspace-based access control.