Vena Information Security Program (ISP)

Vena leverages the power of cloud computing to provide a scalable, flexible and secure enterprise-class planning and analysis solution. Keeping financial data confidential is vital, and Vena provides visibility into your sensitive information while controlling access across the platform. Comprehensive safeguards ensure security, stable costs and superior productivity in an always up-to-date environment.

Security Overview

Vena's security program begins with our culture—customer trust is a core value ingrained across all employees and the organization. Rigorous vetting, training and security policies cultivate robust employee awareness and compliance. A zero-trust architecture provides in-depth defense through cloud-based access controls, endpoint encryption and security, and network segmentation. Best-of-breed technologies and stringent operational processes follow security by design principles to keep customer data secure and ensure compliance with privacy and data protection obligations (e.g. PIPEDA, GDPR). Lastly, due diligence is conducted on all third parties to ensure end-to-end protections across the data, technology and security supply chain.

HIGHLIGHTS:

- **System And Organization Controls (SOC) 1 And SOC 2 Reports**
- **A Strong, Secure Software Development Lifecycle (SDLC)**
- **Zero-Trust Security Architecture**
- **AES 256-Bit Encryption Of All Customer Data In Vena, Including Backups**
- **Secure Data Transfers Transmitted Over HTTPS Using TLS1.2 Or Stronger Encryption**
- **Customer Data Isolation**
- **SAML 2.0 Single Sign-On And IP Restriction Functionality (Optional Customer Configuration)**
- **Multi-Factor Authentication (Optional Customer Configuration)**

Certifications

SOC AUDITS

Vena completes annual SOC 1 and SOC 2 audits conducted by Deloitte per American Institute of Certified Public Accountants (AICPA) standards.

- **SOC 1** validates controls relevant to financial reporting and is available upon customer request.
- **SOC 2** assesses security controls against AICPA's Trust Services Criteria (TSC) and is available upon customer request.
- **SOC 3** summarizes security controls for public trust.

- **Type I** assesses the design effectiveness of a system at a certain point in time.
- **Type II** assesses the design effectiveness of a system over a period of time.

** SOC 1 and 2 Type II reports are available for the Vena on AWS environment. SOC 1 and 2 Type I reports are available for the Vena on Azure environment, with SOC 1 and 2 Type II reports expected to become available in spring 2025.*

TRUSTED CLOUD PROVIDER

Vena is a **Trusted Cloud Provider Member** with the **Cloud Security Alliance (CSA),** the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. This strategic partnership aims to foster collaborative cybersecurity efforts, enhance data protection and promote a secure ecosystem—underscoring Vena's unwavering commitment to safeguarding its customers' data.

As a Trusted Cloud Provider with CSA, Vena reinforces its dedication to the security of its cloud-based corporate performance management software—which is trusted by leading organizations worldwide.

Vena Approach	Highlights	Benefits
RISK MANAGEMENT AND GOVERNANCE	Vena employs a three lines of defense model for risk management widely used across industries: • First-line business/process owners maintain security controls in daily operations per policies. • Second-line security team oversees compliance monitoring and control governance. • Third-line external auditors validate policies and controls to ensure they meet industry standards and regulations.	This organizational independence assures leadership that security controls are applied consistently across the business according to industry standards and regulatory and compliance laws.
DATA PROTECTION	Vena's data privacy, security and legal teams monitor and apply ongoing governance.	This allows Vena to meet evolving government and industry regulations related to data protection.

Vena Approach	Highlights	Benefits
ACCESS TO DATA	Vena restricts employee access to production and customer data via exclusive authorization on an as-needed basis.	Reinforces Vena's mature data security program around privacy, security, compliance, customer trust and risk management.
SEGREGATION OF DUTIES	Vena segregates product development from production infrastructure, enforcing peer code reviews before promotion to production environments.	This governs access between teams, limiting integration risks.
ACCESS TO PRODUCTION SYSTEMS	Vena grants least privilege access to production infrastructure through cloud provider SSO integrated with Vena's federated identity, MFA and VPN controls.	Strict access controls and audit logging prevent unauthorized access and secure customer data.
LOGICAL DATA SEPARATION	Vena logically isolates customer data, providing individual database instances not shared across clients.	Secure long-term storage with no mixing of customer data.
ENCRYPTION IN TRANSIT	All communications to Vena's cloud environment leverage TLS 1.2 encryption or higher.	Secure Excel, web and Extract Transform-Load (ETL) data transfers and workflows.
ENCRYPTION AT REST	All data is encrypted at rest using AES 256-bit or stronger encryption. Private keys are managed using the AWS Key Management Service (KMS) or Azure Key Vault.	Decryption uses short-term cryptographic leases, ensuring keys never leave protected memory.
ENDPOINT SECURITY	Vena secures the production environment with best practice hardening standards, vulnerability management and intelligent threat detection. Vena nodes run as a hardened cluster on default-deny host firewalls, refreshing weekly with the latest security patches and vulnerability scans blocking known risks. Tightly scoped TCP/UDP firewall rules communicate only between validated nodes. Anomalous threat detection services (AWS GuardDuty, MS Sentinel) leverage machine learning to analyze events and detect compromised credentials, privilege escalations, malware risks and unauthorized infrastructure changes.	Continuous monitoring and threat detection protects customer data at all times.

Vena Approach	Highlights	Benefits
DATA CENTER SECURITY	Vena operates only in AWS or Azure data centers that have been certified as ISO 27001 and PCI/DSS Service Provider Level 1.	State-of-the-art physical safeguards secure strategic global Vena Hubs in Canada, United States and EU cloud regions, including biometric access, 24/7 manned security and surveillance monitoring.
DATA BACKUP AND DISASTER RECOVERY	Vena performs nightly customer data backups across multiple cloud provider regions.	Customer data is stored redundantly and can be restored from the previous night's backups during disaster recovery.
DATA DELETION	At the end of the customer data retention period, customer data is securely deleted from all live systems, and backups are automatically purged either 12 months (Vena on AWS) or 180 days (Vena on Azure) from the last backup.	This facilitates compliance with data lifetime limits.
ADVANCED ENTERPRISE AUTHENTICATION MECHANISMS	Vena employs a secure session tracking mechanism that ensures only an authorized user is the initiator of any requests. Vena supports multiple authentication mechanisms (optional customer configuration): • Single Sign-On (SSO) via SAML 2.0 extends enterprise directory services. • IP restriction functionality restricts logins by location and can enforce VPN usage. • Multi-factor authentication adds a second form of identity verification.	Together, these mechanisms provide organizations with layered user authentication and authorization controls.
USER LEVEL DATA SECURITY	Vena restricts access through customizable Role-Based Access Controls (RBAC), enabling organizations to enforce least privilege and separation of duties policies.	Set per-user permissions for fine-grained access control to your sensitive information.
NATIVE USER AUDIT AND AUDIT TRAIL	Vena provides complete audit trails tracking all document, spreadsheet, budget, report, template and cell-level data changes with date, time and user stamps, version histories and rollbacks. User activity logs include account modifications, logins and permission changes and are filterable for reporting. Audit logs can be exported as CSV files for external analysis.	Comprehensive audit capabilities enable forensic investigations and internal accountability while addressing regulatory compliance mandates.