tecton

Tecton Security & Compliance Whitepaper

> *" Tecton stands out as one of the most complete, enterprise-ready feature store platforms that can be incorporated into any ML infrastructure."*
>
> *– TheSequence Scope AI Newsletter*

As a service provider responsible for handling sensitive data, we understand that our security program, policies, and controls must meet or exceed our customers' standards. Data for machine learning (ML) is often subject to the most stringent legal, regulatory, privacy, compliance, and security requirements. Furthermore, operational ML systems typically power production features and business decisions representing huge amounts of value for our customers.

We believe that effective SaaS security requires a combination of powerful security controls with low operational overhead. After all, enterprises are employing the Tecton Feature Store because they want to quickly ramp up their operational ML efforts. To make sure that customers are always increasing their velocity with Tecton while maintaining the highest level of security, we have developed an innovative architecture and deployment model. Going beyond the industry-standard Bring Your Own Encryption approach, our deployment model gives customers complete control over their Tecton-managed data in AWS—without requiring that they manage a typical cloud platform installation.

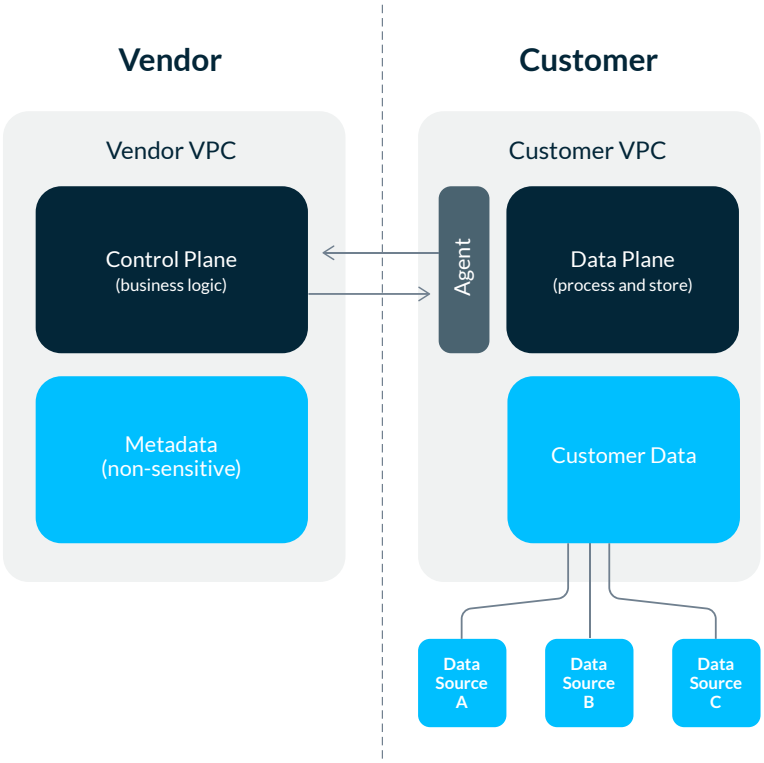
Data security is central to everything we build at Tecton. Our executive team has led ML infrastructure at some of the top software companies and understands the importance of security and compliance to our customers and to Tecton's mission. Our engineering team carefully considers the security implications of any changes made to the product, prioritizes transparency, and works hard to ensure that we are not only using the industry-leading techniques, but also constantly innovating to improve the user experience.

4 Pillars of Tecton Security

> *"Tecton has taken one of the most difficult services for CISOs and DPOs to get comfort around (ML) and built a solution that enables security, privacy, and compliance for all industries."*
>
> *– Josef Fukano, Managing Director at Hilltop GRCC, Fmr. Director of Compliance at Box*

1. Security designed to empower our customers

Most cloud solutions force you into a difficult trade-off: either trust a third party to manage your sensitive data, or keep the data in your control but take on expensive IT overhead. Tecton's innovative hybrid deployment model separates your data (the "data plane") from Tecton's managed software (the "control plane"), which gives you the agility of a SaaS product with the compliance and data ownership of an on-prem solution. In essence, this means quicker onboarding and time to value, fast and continuous software upgrades, and freedom from managing complex infrastructure—while keeping your data in your control at all times.



2. Commitment to innovation

Tecton provides a "built in the cloud, for the cloud" solution, which enables fast iteration and allows us to remain ahead of the curve in a rapidly changing industry. Tecton's unique architecture and deployment model just is one example of how we are always looking to find the best solution for our customers. Our team is composed of veterans who built operational ML systems at companies such as Uber, Google, Facebook, Lyft, and Airbnb. This expertise has led to state-of-the-art security and privacy controls across our product—and we're determined to push the state-of-the-art even further.

3. Zero trust infrastructure

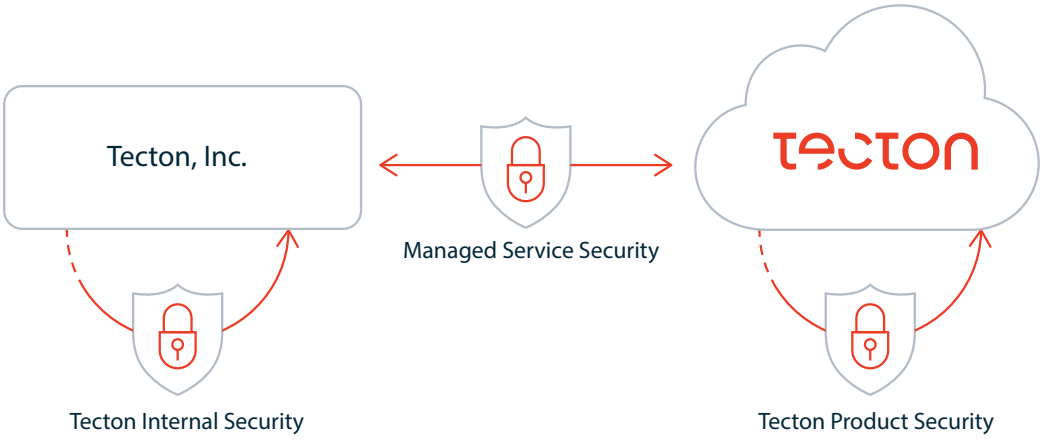
> *"Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."*
>
> *– National Institute of Standards and Technology (NIST)*

Tecton is built on the Zero Trust Infrastructure principle to keep customer data secure and protected. Secure authentication is required to access all components of Tecton's product. This is enforced for both user-level access to the product as well support-level access to the infrastructure.

4. Trust through transparency

As a fast-growing company, we're committed to gaining our customers' trust through transparency and ownership of data. Tecton's architecture is designed to maximize your control over your data, logging, and monitoring and give you visibility into Tecton's infrastructure. In addition, we invest in tooling and features that provide up-to-date information on our product, architecture, and security controls. Customer questions and concerns are handled immediately by our expert security and support team.

Security Overview



Security at Tecton falls into three key areas:

- **Tecton Internal Security:** Security policies and controls that Tecton Inc. has in place internally.
- **Service Management and Support Security:** Security policies and controls to govern Tecton Inc.'s access to the customer's environment and the Tecton product.
- **Tecton Product Security:** Security capabilities made available to the customer within the Tecton product.

Tecton Product Security

Tecton's product is designed to provide best-in-class security and access controls that fit seamlessly into customers' workflows. Access can be granted to users, teams, or services using Access Control Lists (ACLs). Data is encrypted at rest and in public transit using industry-standard AES-256 encryption. Tecton's secure APIs, CLI, and web UI allow for an integrated management and auditing environment.

Tecton Access Controls

Customers always manage their own data in their own AWS account with Tecton. The product protects data access by providing three main interfaces where customers can configure security controls:

» **Serving Access:** Security governing read access to feature data computed and managed by Tecton for training or serving.

» **Config Access:** Security governing permissions to update feature definitions managed by Tecton.

» **Raw Data Access:** Security governing access to raw data sources such as data warehouses, data lakes, and streams.

Tecton's Access Controls are Workspace Centric

Customers configure access controls and secrets in Tecton's product on a per-workspace basis. A workspace is a fully isolated environment in Tecton used by teams and individuals to manage features. Every raw data source and feature is associated with exactly one workspace. Workspaces have many benefits, enabling teams to run experiments or separate staging and production features. From a security perspective, workspaces let you isolate your sensitive data from your non-sensitive data, and make it possible to implement the least access principle.

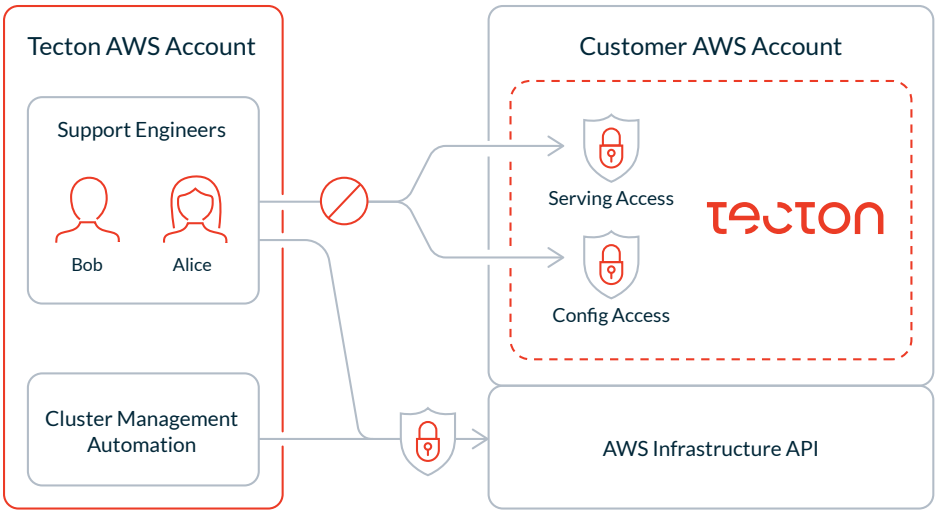
Serving Access and Config Access

Every workspace is associated with an Access Control List (ACL). The ACL defines serving and config access for individual users, services (e.g. API keys), and groups. ACLs can be configured in the UI or via Tecton's API. User authentication is SSO-ready.

Raw Data Access

Besides features, a workspace configures raw data sources used for feature transformation pipelines. Tecton supports both IAM-role protected (e.g. Kinesis, S3) as well as password-protected data sources (e.g. Snowflake). Secrets and IAM roles can be managed securely via Tecton's Web UI, CLI, and API. As a result, workspaces can be configured following the least-access principle.

Service Management and Support Security



The above diagram showcases our deployment model, where your Tecton cluster is split between an AWS account managed by Tecton and an AWS account managed by your company. Tecton's core services and metadata live in Tecton's account, but all the data processing and feature data at rest are stored in your AWS account. This unique setup keeps your data within the bounds of your AWS account while reducing the work and permissions required from your IT organization (for example, version-controlled software upgrades happen automatically).

Data Access and Protection

All AWS account access is logged including any operations that assume cross-account roles, S3 access, and DynamoDB access. Logging is enabled by default and accessible to the customer.

Tecton's deployment model makes it possible for customers with the flexibility they need to meet their internal requirements. For example, from their AWS account customers can configure IAM permissions and IAM policy restrictions and set network configuration restrictions as long as they are compatible with Tecton's requirements. Customers can also perform ad hoc and scheduled operations such as security scans.

Employee Observability

Tecton subscribes to a least-privilege methodology for user access, meaning we limit our support teams to the access they need to ensure the reliability of our infrastructure and services. All production environ-

ment access is always considered untrusted. Support engineers must authenticate using a unique ID, strong password, and MFA when connecting to Tecton infrastructure.

Tecton support engineers cannot access raw data, as they are subject to the same access controls as customer-internal users. Access to Tecton-managed feature data will never be accessed unless directly required and permitted. Any such access would also be mandatorily logged and trigger an investigation alert.

Tecton Internal Security

In addition to product and infrastructure security, Tecton maintains a strict security, policy, and control framework internally to ensure customer data is always safe and protected.

Compliance and Reporting

- Industry-standard policy framework based on ISO 27001 and AICPA SOC 2 (SSAE 18) guidance. The Tecton information security and privacy policy framework is continually improved and formally reviewed, approved, and published at least annually.
- SOC 2 Type 1 (Type 2 In Process): Tecton has implemented a control framework based on the American Institute of Certified Public Accountants (AICPA) SSAE 16 (SOC 2) guidance. An external auditor has reviewed the design of these controls and confirmed implementation. A Type 2 report is scheduled for Q4 of the 2021 calendar year.
- Public Privacy Policy: Tecton complies with relevant privacy laws and regulations.
- Data Processing Agreements: Tecton uses Standard Contractual Clauses (SCCs) and Data Processing Agreements (DPAs) to ensure legal transfer and processing of data when applicable.
- GDPR and CCPA compliance: Enterprises can maintain GDPR and CCPA compliance while using the Tecton Feature store.
- Tecton performs external penetration testing at least annually. High-priority issues are resolved in a timely manner according to internal SLAs.

Logging and Monitoring

Tecton has implemented extensive logging and monitoring to identify, escalate, and resolve suspicious activity. Logging includes security and availability monitoring, and messages are sent directly to an immutable security channel aggregated to a secure location where they cannot be tampered with.

Disaster Recovery and Business Continuity

At Tecton we've adopted a risk-based Disaster Recovery approach. We conduct formal Business Impact Analysis (BIAs) to identify critical and high-risk processes and systems; these are used to create and refresh our business continuity plan annually. We also perform annual testing of both technical disaster recovery controls and the business continuity plan, to ensure that metadata created can be restored with a 24-hour recovery point objective (RPO) and a 24-hour recovery time objective (RTO).

Third-Party / Vendor Compliance

Modern SaaS providers must treat key subservice providers as part of their infrastructure. Tecton performs risk-based security and privacy procedures on all new vendors, followed by annual reviews of sub-processors to ensure they are compliant with industry-standard control and policy frameworks as they are relevant for the services provided. These procedures include reviews of external reports and certifications (ISO 27001, SOC 2, etc.) as well as external penetration tests.

Employee Training

All Tecton employees must complete security and privacy training upon hire and annually to ensure they understand their responsibilities for securing your data. Training includes an overview of security policy, phishing, spear phishing, secure configuration, secure coding, and secure release management, among many other topics. In addition, engineers must complete Open Web Application Security Project (OWASP) Top 10 training on secure coding practices.

Human Resources

Tecton has standard HR processes in place to ensure that new employees receive background checks, sign appropriate confidentiality/security agreements, and receive access commensurate with their job function. Processes also ensure that access is removed or is limited to least privilege upon termination or transfer.

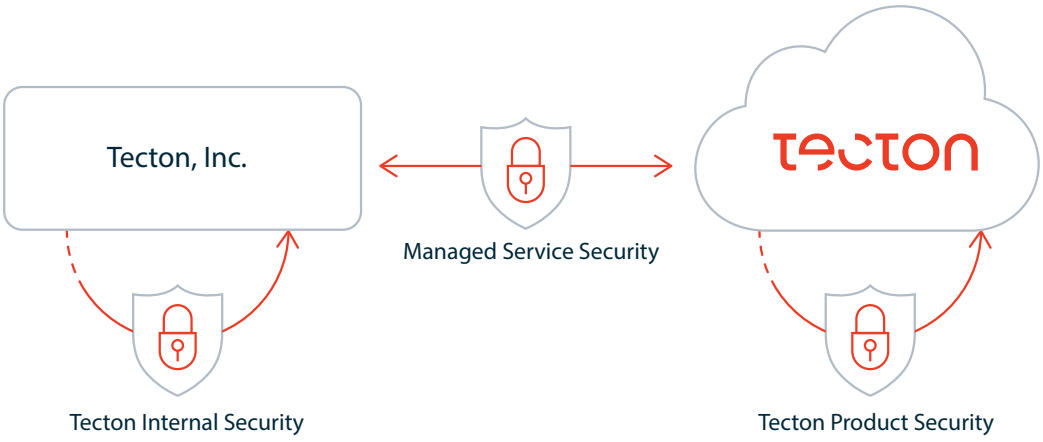
Defined and Secure Development Lifecycle (SDLC) Process

We conduct manual and automated code reviews and have implemented a defined, secure, and automated release management process to prevent unauthorized changes to code. Our release pipeline is configured such that all changes must be tested, approved manually, and released through our automated and secure code review. In addition, logging and alerting is in place to notify Tecton's security team in the event of any changes that are not authorized by the aforementioned process.

Formal Risk Management Procedures

The Tecton Risk team performs an annual risk assessment to identify risks related to the industry and those specific to Tecton. The risk areas in the assessment are ranked by likelihood and impact and ranked (high, medium, or low). Formal risk-treatment plans are created for any identified risks and are tracked throughout the year to continuously drive down risk at the organization.

Security Checklist at-a-glance:



Tecton Product Security

- Authentication: Self-serve API keys, SAML/SSO
- Authorization: Access limited through Access Control Lists (ACLs)
- Data encrypted at rest and in public transit using industry-standard AES-256 encryption
- Role and secret-based raw data access
- Secure APIs/GUI/CLI
- Audit logs track every access attempt
- Least privileged access
- Full isolation between teams' workspaces is supported
- Fully isolated individual experimentation workspaces are supported
- Sensitive data can be securely kept out of non-sensitive workspaces
- Zero Trust Infrastructure

Service Management and Support Security

» Hybrid deployment model separating your data in your AWS account from Tecton's managed software in Tecton's AWS account
» Flexibility to meet customer requirements, e.g. IAM permissions and IAM policy restrictions, network configuration restrictions, custom resource tagging
» Software upgrades happen automatically
» All AWS account access logging is enabled by default and accessible by the customer
» Cross-account access is protected using an IAM role (AWS Best Practice)
» Tecton support engineers cannot access data as they are subject to the same access controls as customer-internal users
» All support engineers and processes follow SOC2 compliant security protocols, including:
  - Action logging for auditing purposes
  - All patches and software upgrades deployed to customers require mandatory code reviews. Upgrades are version-controlled, fully reproducible, and logged for auditing purposes.
  - Support engineers must authenticate using a unique ID, strong password, and MFA when connecting to Tecton infrastructure

Tecton Internal Security

» SOC 2 Certification
  - Type 1 completed (2020)
  - Type 2 in progress (active evaluation period)
» SOC 2 Type 1 report available upon request including
  - Complementary subservice organization controls (CSOCs)
  - Complementary User-Entity Controls (CUECs)
  - Controls Related to the Security, Availability, and Confidentiality Trust Services Criteria
  - & more
» Information Security Policy based on ISO 27001 and AICPA SOC 2 (SSAE 18) guidance
» Public Privacy Policy
» Records Retention Policy
» Standard Contractual Clauses (SCCs) and Data Processing Agreements (DPAs)
» GDPR and CCPA ready
» Formal Business Continuity & Disaster Recovery Planning and Testing
» Incident Response & Communication

- Vulnerability Management
- Formal Risk Management Procedures
- Defined and Secure Development Lifecycle (SDLC) Process
  - Secure Coding Practices
  - OWASP top 10 training
  - Security Advisory for major changes to infrastructure and new products
- Security and availability monitoring and logging
- Required background checks and security & privacy training for all employees
- Comprehensive vendor onboarding and review policy