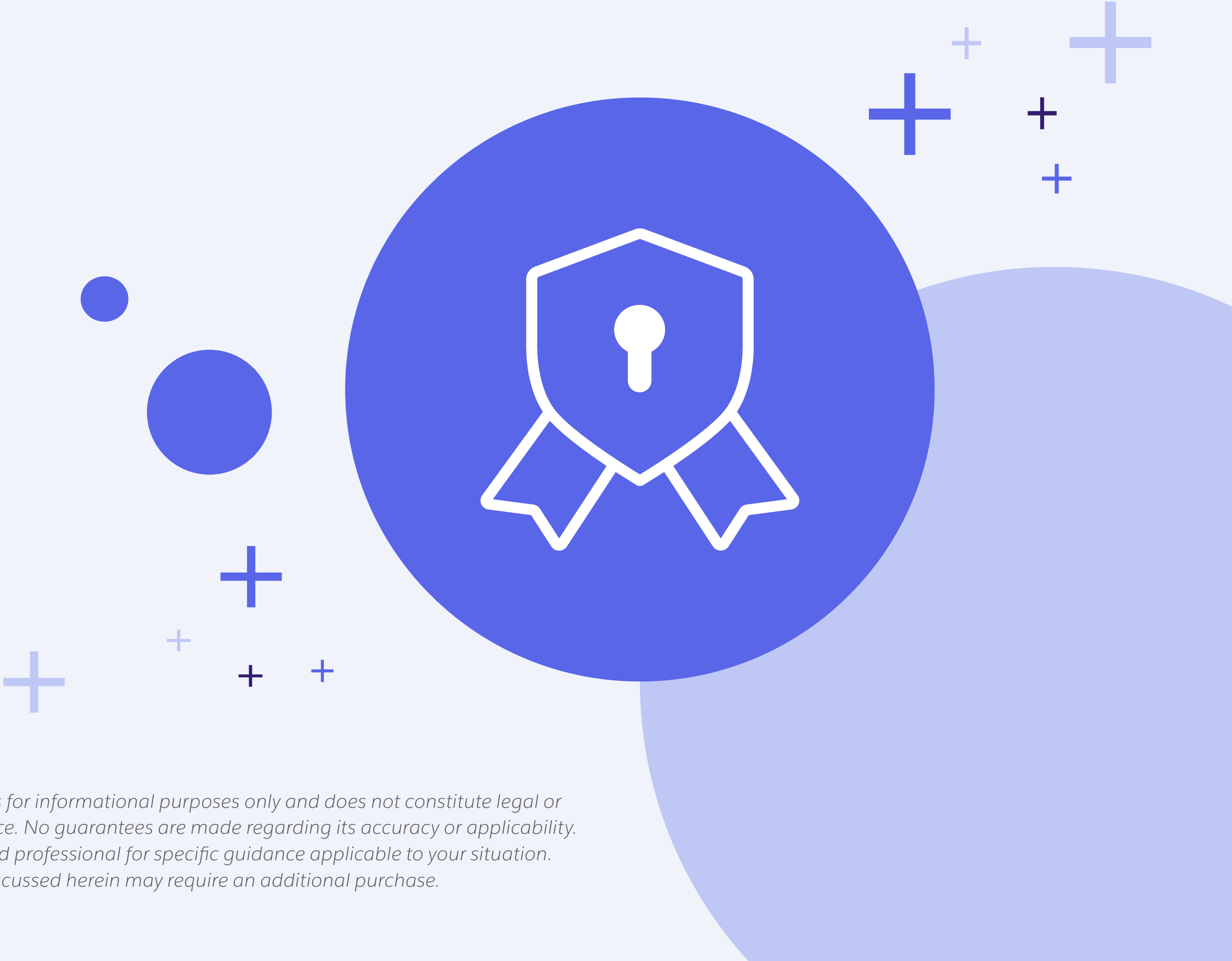
tableau
from Salesforce

Tableau Cloud on Hyperforce Security



This whitepaper is for informational purposes only and does not constitute legal or professional advice. No guarantees are made regarding its accuracy or applicability. Consult a qualified professional for specific guidance applicable to your situation. Some features discussed herein may require an additional purchase.

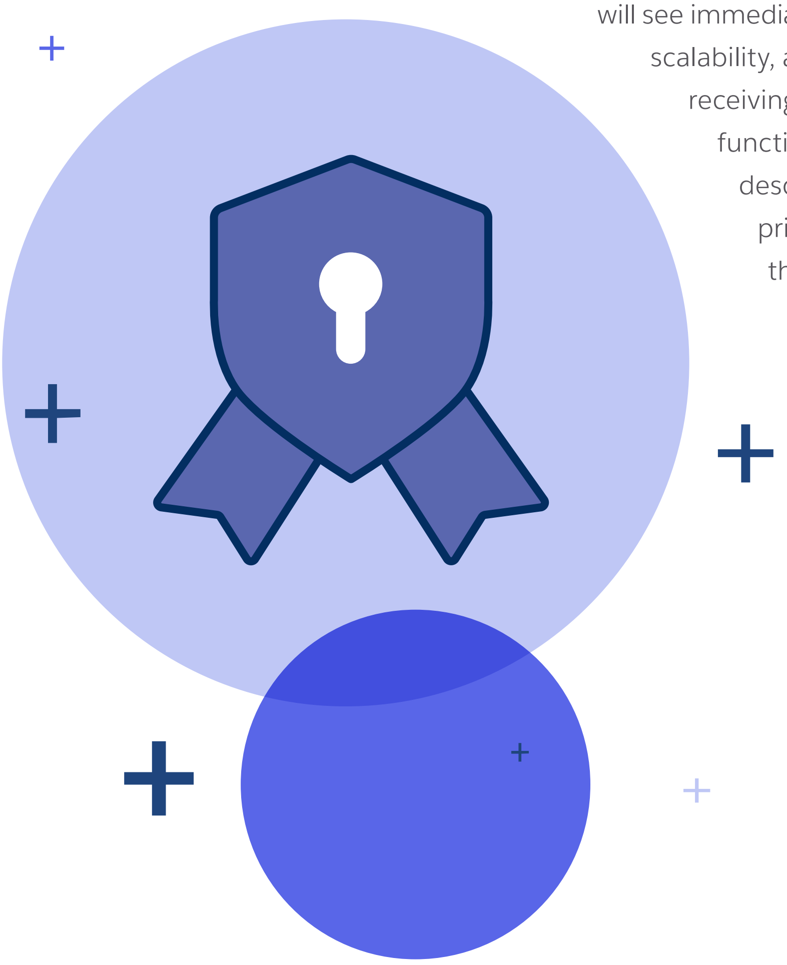
Contents

Introduction

At Salesforce, Trust is our #1 core value, which is why our data-centric strategy supports the company's commitment to run one of the most secure, trusted, reliable, and available cloud computing service. Customer success is the driving force behind our data center strategy, so delivering the highest standards in availability, performance, and security is our top priority.

Hyperforce is an integrated infrastructure platform with unified advanced standards for compliance, security, agility, scalability, and privacy. Hyperforce is built on the public cloud and currently, it's using AWS's capabilities. The platform is built on a foundation of code rather than traditional hardware, enabling rapid and reliable delivery of Salesforce applications to locations worldwide. As a result, customers gain enhanced choice and control over their data residency. By providing a common foundation for deploying our application stacks, Hyperforce accelerates Salesforce's ability to innovate across product clouds and deliver additional business value to customers.

With Tableau Cloud on Hyperforce, Tableau Cloud customers will see immediate benefits (such as security, availability, scalability, and privacy enhancements) while receiving the same user experience and functionality as before. This document describes in additional detail the security, privacy, and architecture of Hyperforce and the Tableau Cloud that operates on it.

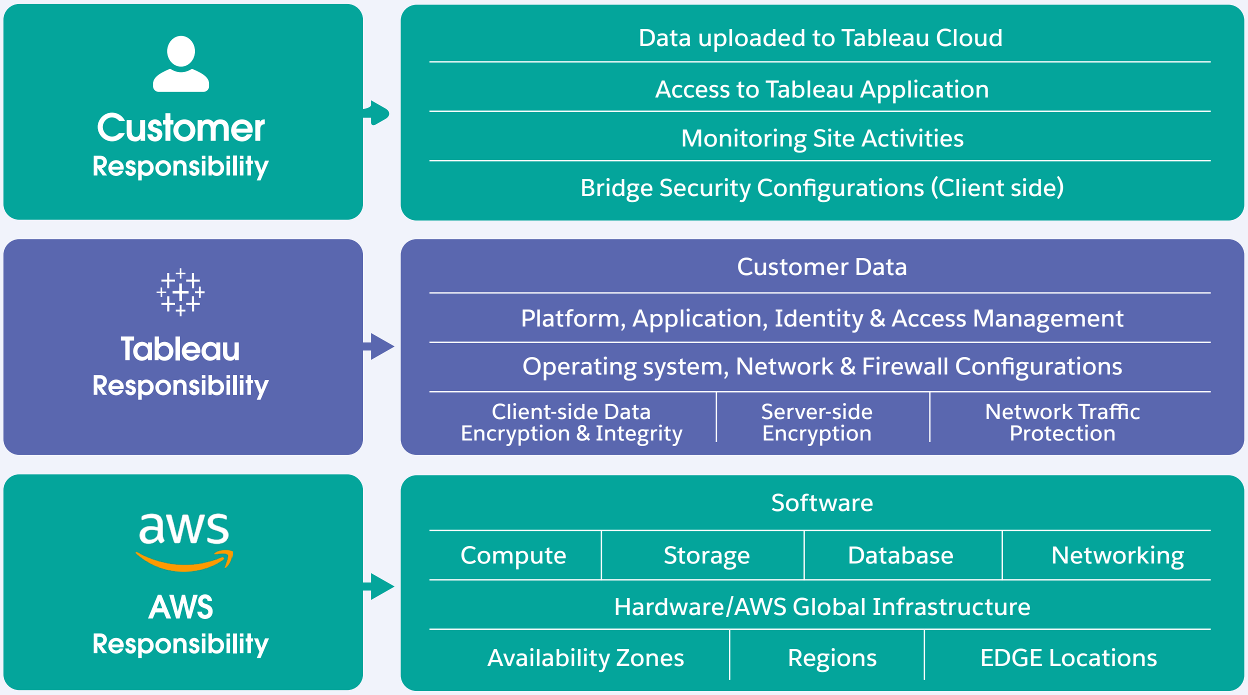


Shared Responsibility Model

The Shared Responsibility Model is a framework that defines the security and compliance responsibilities of both cloud service providers and customers. Under this model, cloud providers are responsible for the security and compliance of the cloud, while customers are responsible for securing their data and applications in the cloud. Understanding these roles is essential for maintaining a secure cloud environment.

Hyperforce is built on public cloud infrastructure and currently Amazon Web Services (AWS) is the only provider. AWS is responsible for securing the physical infrastructure that powers Hyperforce. This includes the underlying hardware, software, networking, and data center facilities that support AWS's cloud services.

Shared Responsibility Model



Customer Responsibility

- Data uploaded to Tableau Cloud
- Access to Tableau Application
- Monitoring Site Activities
- Bridge Security Configurations (Client side)

Tableau Responsibility

- Customer Data
- Platform, Application, Identity & Access Management
- Operating system, Network & Firewall Configurations
- Client-side Data Encryption & Integrity | Server-side Encryption | Network Traffic Protection

AWS Responsibility

- Software
- Compute | Storage | Database | Networking
- Hardware/AWS Global Infrastructure
- Availability Zones | Regions | EDGE Locations

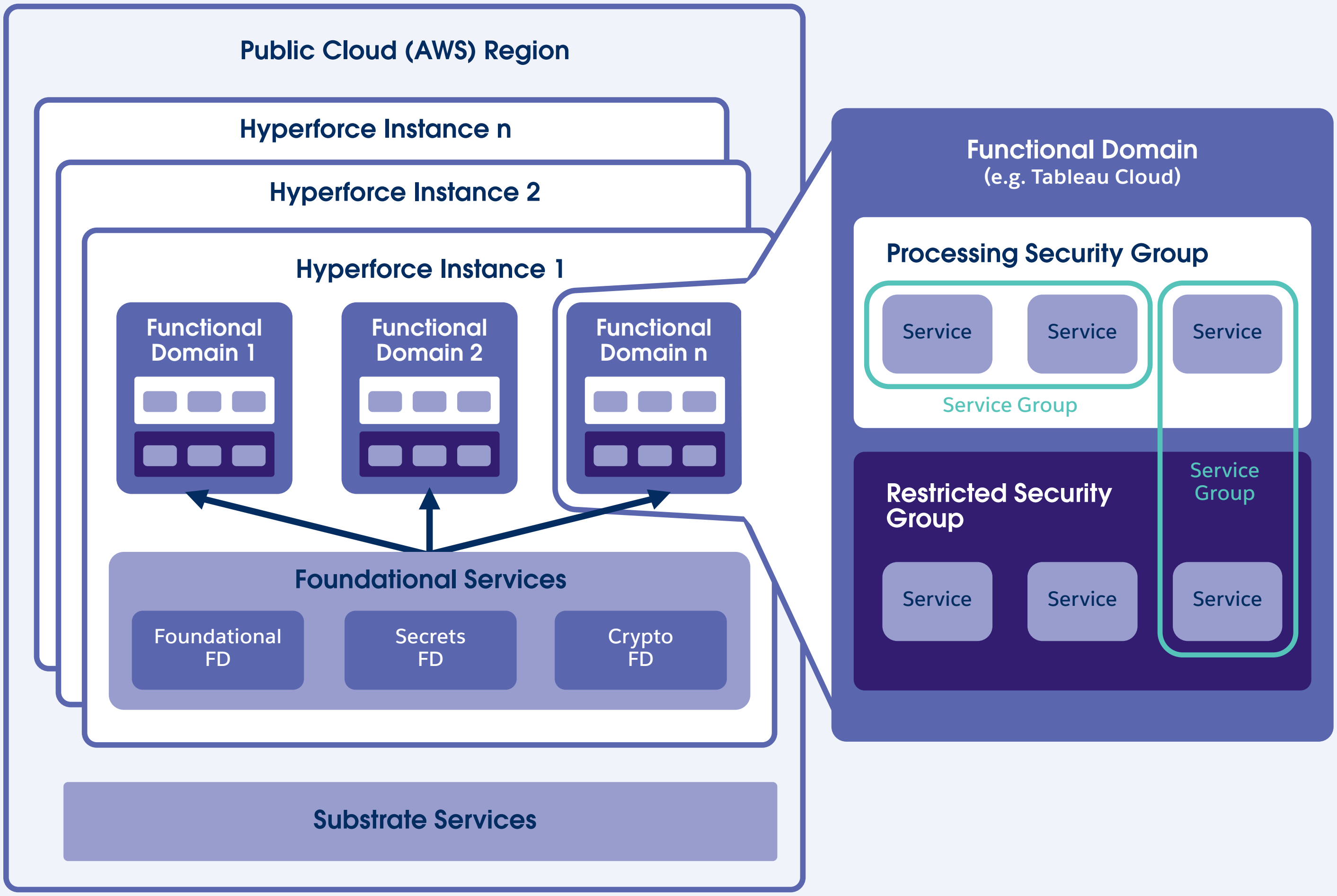
Tableau is responsible for the security of the platform itself. This includes, but is not limited to the logical security measures that protect the platform's operating systems, network and firewall configurations, application security, and identity and access management (IAM). Tableau maintains that the platform is securely configured to allow customers to safely use its services.

Customers maintain control over their data. Customers are the sole owners of the data they store in Tableau Cloud on Hyperforce and decide what data is submitted to the platform. Furthermore, customers are responsible for applying any additional security controls they need when using services like Tableau to meet their own specific privacy and security requirements.

Hyperforce Architecture Overview

Salesforce Hyperforce uses a Domain-Driven Design (DDD) approach to decompose business units into one or more Functional Domains (FDs). FDs group related functions while remaining decoupled. This approach reduces risk, enforces least privilege, improves scalability, and gives developers the flexibility to build secure, integrated, and loosely coupled services and applications.

Hyperforce Architecture Overview



At a high level, Hyperforce architecture includes:

Hyperforce Instance: An implementation of Hyperforce for a specific region and environment type. Each region has its own set of HIs.

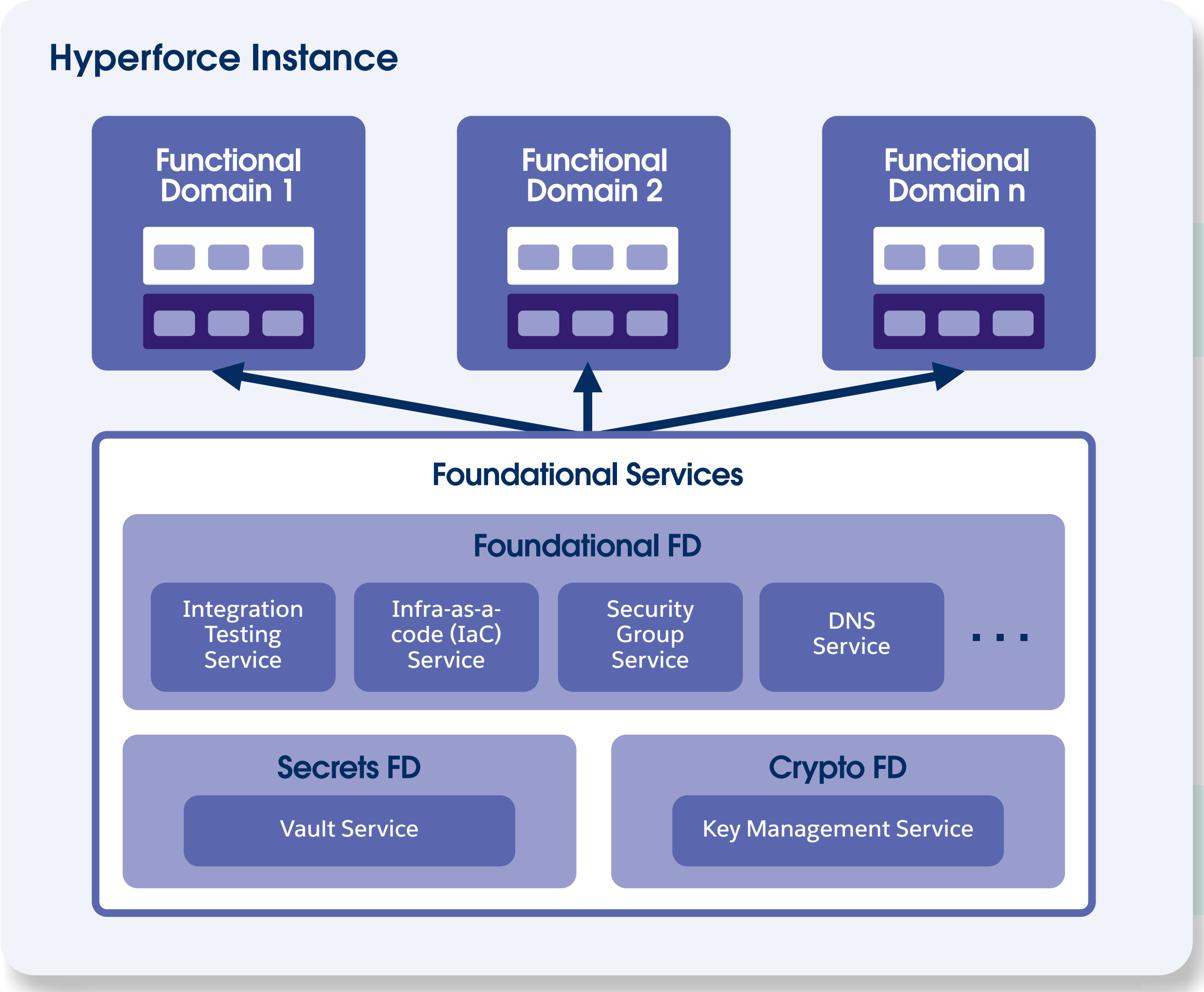
Functional Domain (FD): A boundaried set of capabilities, features, and services that's built and delivered independently of other FDs. Each FD acts as a set of cohesive business or technical use-case functionality. For example, Tableau Cloud is one of the FDs on Hyperforce Instance.

Service: A tool or a process – including pieces of our core app – that a team creates to address a specific business goal and that the team actively manages to meet that goal. A service can be used by or be dependent upon other services.

Service Group: A group of related services that you can treat as a single software asset for some purposes. Service groups share security assessments, onboarding control validations, and more.

Security Group: A specific set of network segmentation rules that limit communication between services. These rules are explicit, declarative policies that broker connectivity between services with different risk profiles.

Foundational Services: Every Hyperforce instance includes Foundational Services that provide infrastructure and security services for the other FDs in that Hyperforce Instance. These foundational services are managed by dedicated teams and are shared across all the FDs in each Hyperforce Instance.

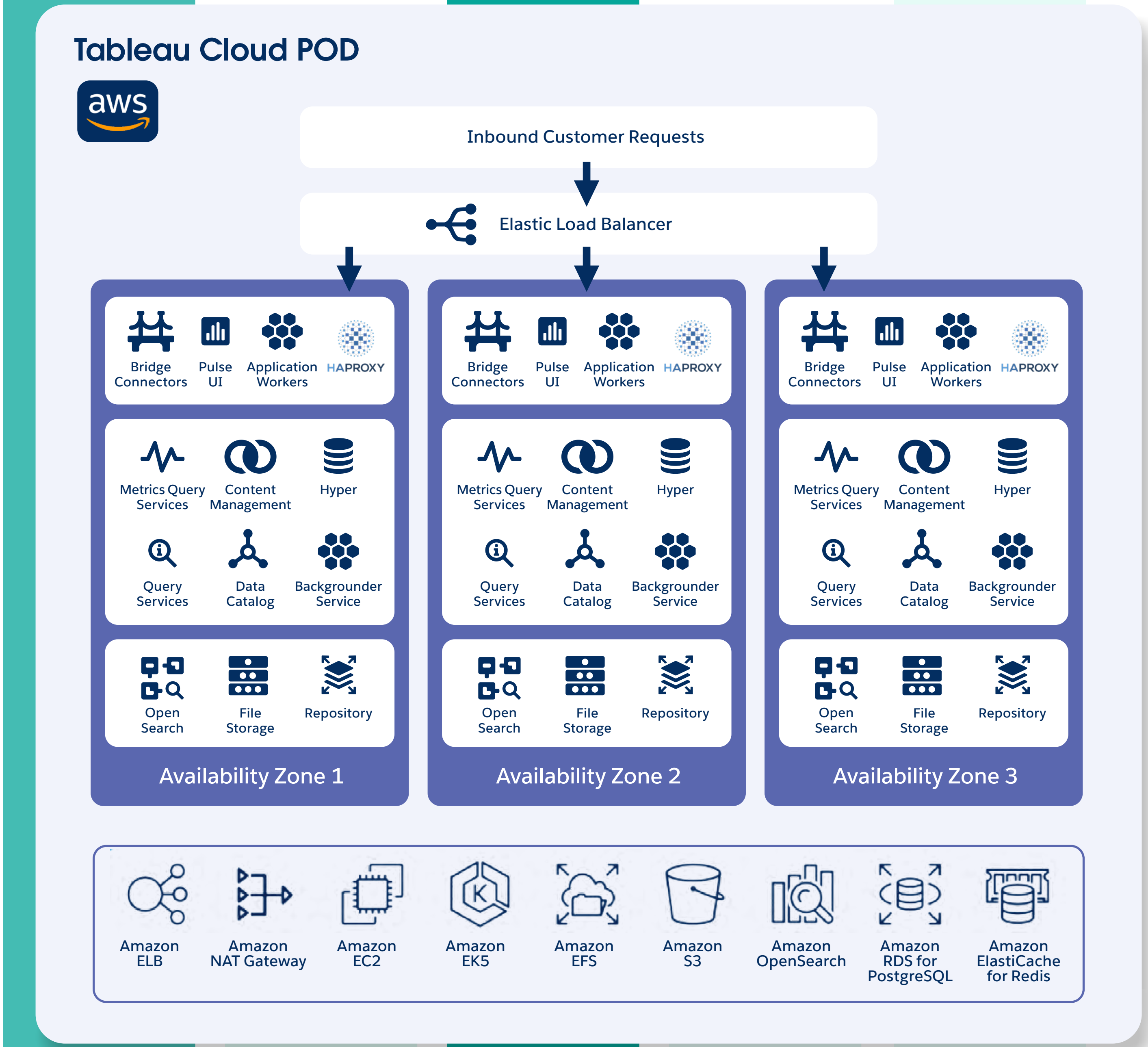


- Foundational FD contains the most shared infrastructure services, including FIT (Falcon testing platform), IAC, Soter (network security), and DNS.
- Secrets FD hosts an instance of Salesforce Vault for storing secrets.
- Crypto FD hosts key-management services.

Substrate Services: Public Cloud native features and services.

Tableau Cloud Overview

Tableau Cloud is a cloud-based analytics platform that's fully hosted on Salesforce's Hyperforce. It uses a variety of resources and services available within Hyperforce in multiple ways.



These resources and services are bundled into the following constructs:

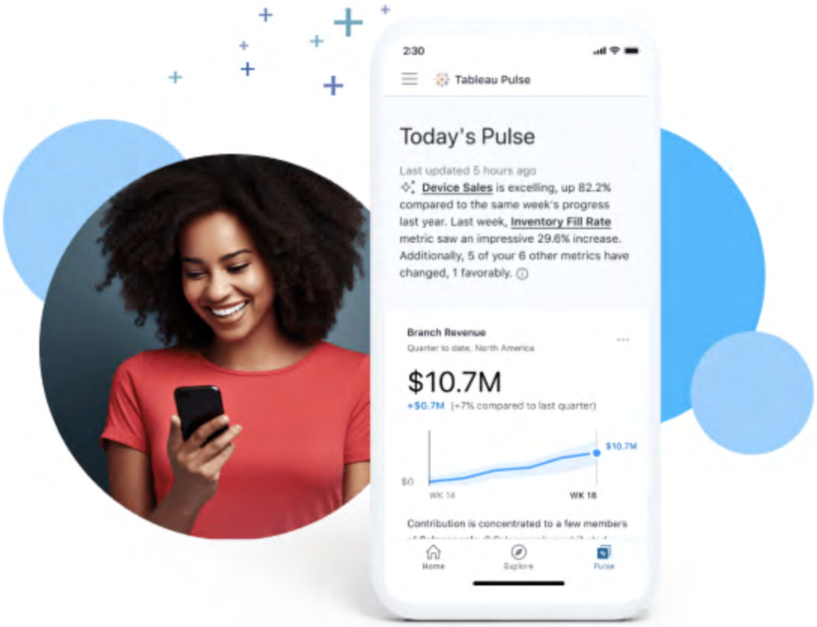
Workers: Workers are responsible for executing a variety of tasks, which include but are not limited to processing customer queries, managing interactions, and refreshing data extracts. Application Workers handle customer engagements in web authoring or establishing a connection to a live database. Background Workers handle background tasks such as scheduled extract refreshes, subscription management, and the execution of data-driven alerts.

Hyper: Hyper is Tableau's in-memory data engine, designed to efficiently manage large and complex datasets. It processes vast amounts of data in seconds, significantly speeding up queries and data extraction. With enhanced performance and the capacity to handle even larger datasets, businesses can tailor their data extraction to meet their specific requirements.

Storage: Tableau Cloud uses various AWS storage services to store all data. Customer data from their data sources is primarily stored as Hyper extracts on AWS S3. Custom views, temporary files, and Prep files are kept on AWS Elastic File System (EFS). The repository, metadata and credentials for data source connections are stored on AWS RDS (PostgreSQL). Lastly, the in-memory data store Amazon ElastiCache for Redis is used to provide low latency, helping to load workbooks efficiently by caching the results of previous queries and avoiding performance issues. This cache has a Time to Live (TTL) of 12 hours and is encrypted.

Bridge: Tableau Bridge is used to bring data from behind a firewall of a customer's site to Tableau Cloud. Customers can deploy Tableau Bridge within their own on-premises environment or within a VPC to securely connect to databases in the same environment.

Pulse and Agent: Tableau Cloud offers two powerful AI features: Tableau Pulse and Tableau Agent. Tableau Pulse provides personalized, contextual, and intelligent insights into the user's key business metrics. Users can follow these metrics, receive weekly digests via email and Slack, and dive deeper into the data through guided exploration and on-demand access. Tableau Agent enables users to create visualizations and perform data analysis using natural language prompts, making it easier to interact with their data.



Today's Pulse

Last updated 5 hours ago

Device Sales is excelling, up 82.2% compared to the same week's progress last year. Last week, Inventory Fill Rate metric saw an impressive 29.6% increase. Additionally, 5 of your 6 other metrics have changed, 1 favorably.

Branch Revenue

Quarter to date, North America

$10.7M

+$0.7M (+7% compared to last quarter)

Contribution is concentrated to a few members

When using Tableau Cloud to connect to data sources, there are two main options: live connections and extracts. With a live connection, users can web author or interact with a workbook that is directly connected to the data source, allowing them to work with live data. On the other hand, extracts are saved subsets of the user data that resides on Tableau Cloud. When a user uses a live connection for tasks like web authoring, the requests are sent from the browser to an application worker on Tableau Cloud. If the user's action triggers a database query, Tableau Cloud will directly query the data source. When a user schedules an extract, the request is sent to an application worker, which sets up a scheduled task in Tableau Cloud. At the scheduled time, Tableau Cloud assigns the task to a background worker. This worker connects to the data source, runs the necessary queries to build the extract, and then stores the completed extract on Tableau Cloud.

Regardless of whether users use live connections or extracts, the data is always transferred through encrypted channels and stored securely. Before users can start with either option, users need to connect their data source to Tableau Cloud. To facilitate this, customers have to allow connections to their databases from trusted Tableau Cloud's IP's. Salesforce IP Whitelist addresses can be found here.

Cloud Principles in Hyperforce

Following Hyperforce architectural patterns provides several benefits in terms of blast radius, the principle of least privilege, and scalability. Our architectural patterns provide flexibility, but we also follow a set of principles to maintain trust.

Infrastructure as Code (IaC): The process of managing and provisioning computer data center resources through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

Policy as Code (PaC): PaC extends the IaC approach by also covering rules governing the infrastructure and platform that manages it. PaC helps to validate your IaC templates, running checks against defined best practices and requirements before resources are deployed.

Immutable infrastructure: A system-management approach in which deployed services and applications are never modified. Instead, new instances of the service or application are deployed to replace them.

Zero Trust Architecture: A security concept that dictates an organization shouldn't automatically trust anything inside or outside its perimeters without verifying its identity first.

Detection and Response Logs: All Network Flow logs are sent to Detection & Response endpoints.

Security-approved container/VM Images: Services must only use operating-system images that have been scanned by Security and meet the baseline requirements for securely running workloads within Salesforce.

Security-approved container creation path: Each image component, such as the base image or modules, must be scanned and verified that they meet the baseline requirements for securely running workloads within Salesforce.

Trust Root Certificates: Private root certificates that establish secure connections between internal services.

Data security: Encryption-at-rest and in-transit using Salesforce keys and certificates.

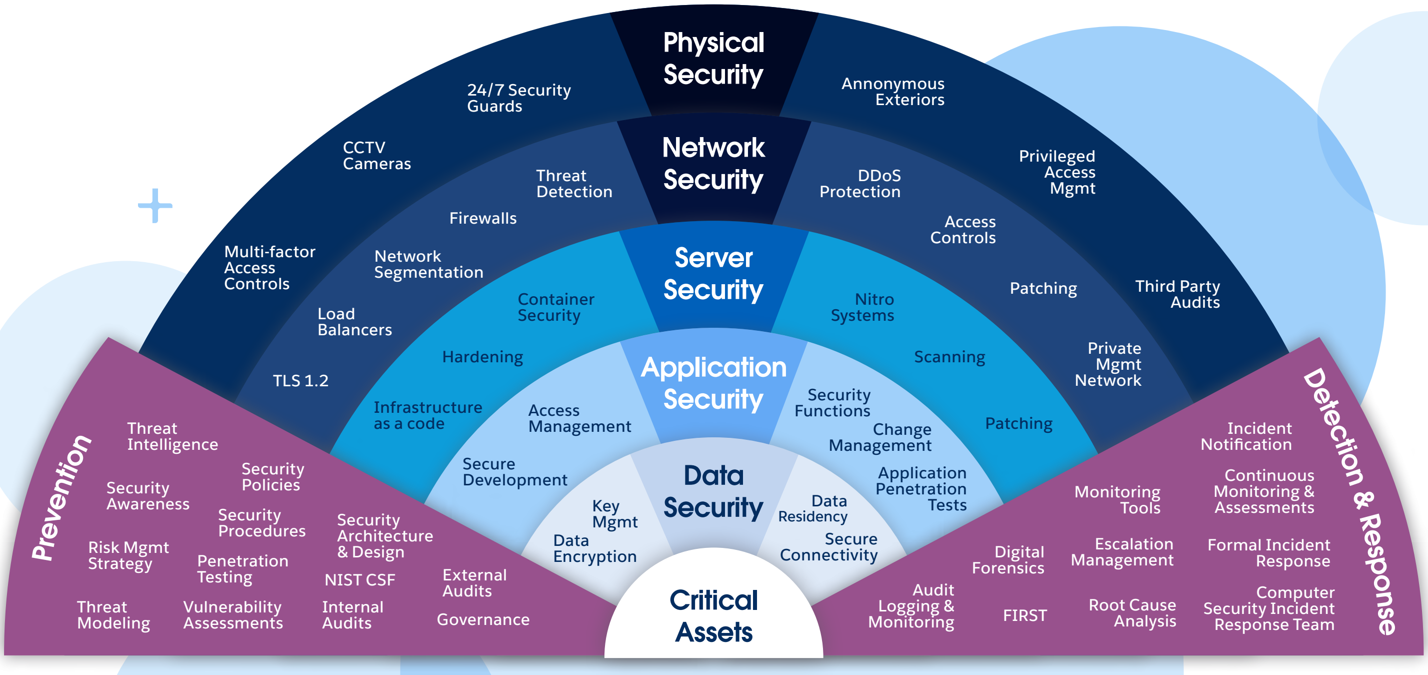
Managed Mesh: Managed Mesh helps provide authentication and authorization protection by enforcing as many policies as possible as a service. Falcon usually uses mTLS for this purpose.

Change control: Changes to production environments, including stage, are gated by Change Cases.

Production environment security: Hardware encryption MFA devices enforce access to production environments. Bastion environments gate access.

Defense-in-Depth Hyperforce Security

Salesforce Hyperforce employs a multi-layered approach to security, known as Defense in Depth, encompassing various measures and practices to safeguard our infrastructure, platform, and services. In this chapter, we'll discuss the security measures of each layer, starting from the outermost layer of Physical Security and progressing inward to the final layer – Logging and Monitoring.



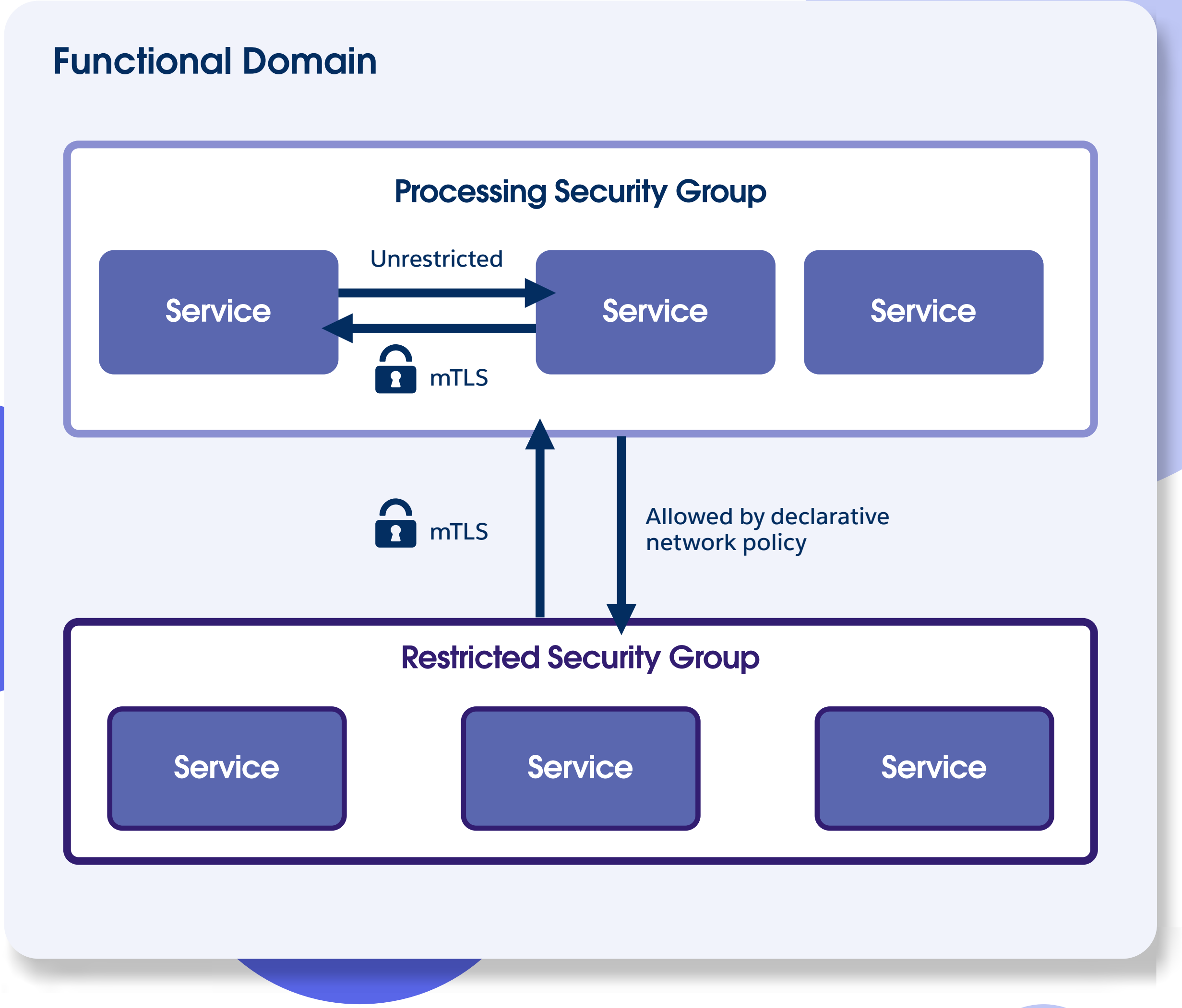
Physical Security

Hyperforce currently uses Amazon Web Services (AWS) as its third-party cloud provider for Infrastructure as a Service (IaaS). The AWS physical infrastructure is hosted and managed within Amazon's secure data centers and uses AWS technology. AWS is responsible for protecting the physical data center, both for physical and environmental controls. AWS maintains controls that test the design and operating effectiveness on a regular basis (as stated in the AWS SOC 2 Report). Salesforce's security teams regularly audit and evaluate AWS datacenter controls to confirm they meet key processes and contractual obligations. This ongoing review helps maintain our commitments to availability, confidentiality, and security. These evaluations follow the Vendor Audit Criteria which are grounded in compliance frameworks such as PCI DSS and ISO 27001, as well as best practices outlined by Salesforce's internal requirements.

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high-impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stores customer data isn't removed from AWS control until it's been securely decommissioned

.

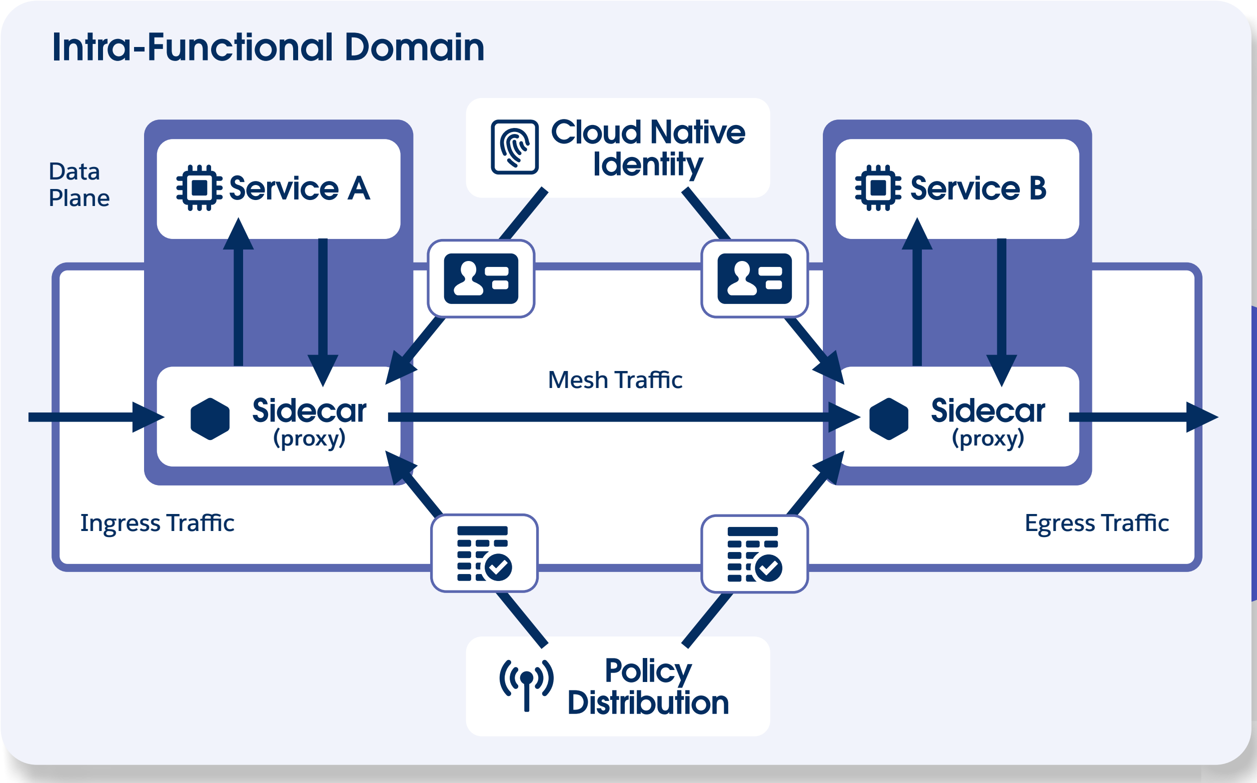
Network Security


Functional Domain
Processing Security Group
Service
Unrestricted
Service
Service
mTLS
mTLS
Allowed by declarative network policy
Restricted Security Group
Service
Service
Service

Intra-Functional Domain (FD) Communication

Security groups are used to control intra-FD connectivity. Security groups are a declarative model for enforcing network segmentation by grouping similar risk service profiles. Traffic inside a security group is unrestricted, but traffic between security groups is restricted by a declarative network policy.

Also, istio-based service mesh is used for both egress and ingress communications within FDs. A service mesh is an infrastructure layer that manages communication between microservices, providing capabilities such as traffic routing, observability, and fault tolerance. It enhances security by enforcing policies such as mutual TLS 1.2 for encrypted communication, service authentication, and fine-grained network policies across services.



Inter-Functional Domain (FD) and External Communication

The Ingress Gateway serves as the entry point for traffic from the public internet into Hyperforce, offering crucial security and traffic management benefits. It protects against unauthorized access, mitigates Distributed Denial-of-Service (DDoS) attacks, and prevents data leaks by securing endpoints. Additionally, it improves traffic management at the ingress points, supporting a smoother and more efficient flow of data into the system.

The Egress Gateway serves as the exit point for outbound traffic, directing data to the public internet and other Falcon Functional Domains. It plays a key role in preventing data exfiltration by blocking unauthorized outbound connections and securing traffic to external services. It improves visibility into outbound traffic, providing better monitoring and strengthening overall security by allowing only authorized connections. Additionally, Hyperforce uses auto-managed point of presence (PoP) external internet protocols (IPs). Network access is only granted through a set of predefined restricted IPs, thus minimizing the risk of unauthorized data exfiltration to unknown locations.

DNS Security

Hyperforce uses Private and Cloud DNS for internal (inter-/intra-FD) communications, and Public DNS for external (customer-facing) communications. Hyperforce network controls enhance DNS security by protecting against spoofing attacks, supporting reliable DNS failover, and reducing DNS latency across regions. Additionally, it supports accurate DNS record management across all domains, providing a robust and efficient DNS infrastructure.

Server Security

Infrastructure as Code

Infrastructure as Code (IaC) is a method of using code to define and manage a system infrastructure, instead of manual processes. Hyperforce uses Infrastructure as Code (IaC) to provide a secure, declarative approach for creating and managing infrastructure. This method reduces the risk of configuration drift and maintains consistency across environments. By automating setup processes, IaC minimizes manual errors, enhances operational visibility, and fosters a more reliable deployment pipeline.

Nitro Systems

An AWS Nitro System is a collection of hardware and software components that deliver high-performance, security, and efficient resource utilization for Amazon EC2 instances. One of the key security features of the Nitro System is its design to prevent unauthorized access to customer data by Amazon employees. They can't log in to the underlying host, access customer content on the host, or access customer content in instance storage. Management API access requires authentication and authorization, and such access is always logged. Hosts can only run tested and signed software deployed by authenticated and authorized deployment services. Amazon employees can't directly deploy code to hosts.

Container Orchestration

Hyperforce uses Kubernetes for its container orchestration platform, offering numerous benefits:

Scalability: Automatically scale applications up or down based on demand, supporting optimal resource utilization.

High Availability: Distribute workloads across multiple nodes to ensure applications remain available even if some nodes fail.

Automated Rollouts and Rollbacks: Simplify updates and rollbacks of applications, enhancing minimal downtime and consistent deployment.

Resource Efficiency: Optimize resource usage by efficiently scheduling containers based on resource requirements and availability.

Self-Healing: Automatically restart failed containers, replace and reschedule them when nodes die, and kill unresponsive containers.

Service Discovery and Load Balancing: Automatically expose containers using DNS names or IP addresses and distribute network traffic to support stable deployments.

Consistent Environments: Maintain consistent development, testing, and production environments, reducing the "it works on my machine" problem.

Container Scannings

Static Container Scanning: performs comprehensive checks to verify that containers and their components are safe before they enter the production environment.

Base Image Analysis: examines the foundational images for vulnerabilities.

Dependency Scanning: scrutinizes third-party libraries and packages for security issues.

Security Configurations: checks for sensitive information in environment variables, hardcoded secrets, and proper file permissions.

Compliance Checks: Conducts checks to ensure adherence to regulatory and organizational security standards, such as CIS Benchmarks.

Dynamic Container Scanning: protects containers from various attack vectors by identifying vulnerabilities in all container components. Each Kubernetes cluster has an agent installed on the host to report data on running containers to the console, highlighting any vulnerabilities.

Runtime Behavior: Monitors and analyzes the container's actions and processes during its execution to detect anomalies.

Network Traffic: Inspects incoming and outgoing network connections to identify suspicious or unauthorized communication.

File System Integrity: Continuously checks the container's file system for unauthorized changes or tampering.

Resource Utilization: Tracks the container's usage of CPU, memory, and other resources to detect unusual consumption patterns.

Application Security

Change Management

All changes to the production infrastructure and applications follow a formal change control process. This process includes development, testing, review/approval, delivery, and roll-back controls. Salesforce utilizes several platforms to make our change management process as effective as possible.

The review and approval platform centralizes, automates, and tracks all necessary control owner approvals before deployment. The platform supports developers throughout the development and release phases, requiring that all approvals from control owners (such as Legal, GRC, and Security) are obtained for production releases in all operating zones.

The Continuous Integration (CI) platform automates Docker image builds, unit testing, and the early detection of third-party vulnerabilities (3PP). The platform supports early detection of 3PP vulnerabilities through CVE reporting, automates CI tasks to minimize human error, and speeds up issue detection, thereby accelerating development. Additionally, it automates testing to uncover security risks and promotes uniformity across builds, reducing inconsistencies.

The Continuous Delivery (CD) platform centralizes development within the Hyperforce environment. It reduces deployment risks by providing successful rollbacks, maintains consistent and secure environments across deployments, and enforces compliance through standardized deployment processes.

Hyperforce features an asynchronous feature-toggle framework that allows Salesforce to turn features on and off in production without redeploying code. This capability significantly reduces risk by enabling the rollout of features with minimal impact, accelerates deployment velocity while maintaining control over production environments, and simplifies feature management in these settings.

Identity & Access Management

Hyperforce offers a comprehensive suite of Identity & Access Management services designed to enhance security and streamline authentication processes. The services use Kerberos for system authentication, and Matlock provides YubiKey-based multi-factor authentication for production engineers. The Product Remote Access (PRA) service acts as a gateway for accessing production systems via a dedicated VM that connects to a bastion, providing secure access to production servers. Quantum-K serves as a secure token service for connected applications, using both Matlock and LDAP. Additionally, the Public Cloud Secure Kernel (PCSK) features Just-In-Time (JIT) access, giving only the amount of time that is needed to access the production environment.

Secure Development

Salesforce built a Secure Software Development Lifecycle (SSDL), which integrates security requirements throughout the software development and deployment process following industry-best secure coding practices, including the OWASP Top 10 and the MITRE CWE Top 25. Operating on the concept of Secure by Design, Salesforce applies its SSDL across all of its products and services from initial ideas through feature releases. As part of the SSDL, Salesforce employs threat modeling through security assessments and uses a variety of tools to identify the security risks, threats, and vulnerabilities of the proposed design early in the development process to create security mitigations against our requirements.

Customer Security Functions

Authentication and Authorization: Most customers prefer their authentication controls over application-provided authentication mechanisms. Tableau Cloud does have a default authentication mechanism for securely accessing customer sites. If the customer wants to integrate their Identity provider, they can do it using SAML. Tableau also supports SCIM to automatically update Tableau Users from the IdP as it updates. Tableau supports SCIM, natively, for the major IdPs such as Okta and Azure AD. Tableau Cloud doesn't store any user credentials when a customer configures their organization's IdP or SSO.

Roles and permissions: Tableau Cloud supports RBAC (Role-Based Access Control) and permissions can be configured per user or group in a manner that restricts access to only the functions needed for any particular role. The customer is responsible for managing the permissions within the application.

Data Security

Data Encryption

Encryption-at-Rest: Customer data from the customer's data source is stored as Hyper extracts primarily on AWS S3. Custom views, Temporary files, and Prep Files are stored on AWS EFS (Elastic File System). AWS RDS stores metadata and encrypted extract keys. Finally, AWS Secrets Manager stores credentials for connectivities, tokens, and other secrets. All data on Tableau Cloud is encrypted at rest with AES-256 used by AWS's encryption functions for native services.

Encryption-in-Transit: All traffic over public networks is encrypted in transit using TLS1.2 using TLS 1.2 with 2048-bit certificates. Within the Hyperforce boundary, traffic is encrypted with mutual TLS (mTLS) by the Service Mesh architecture.

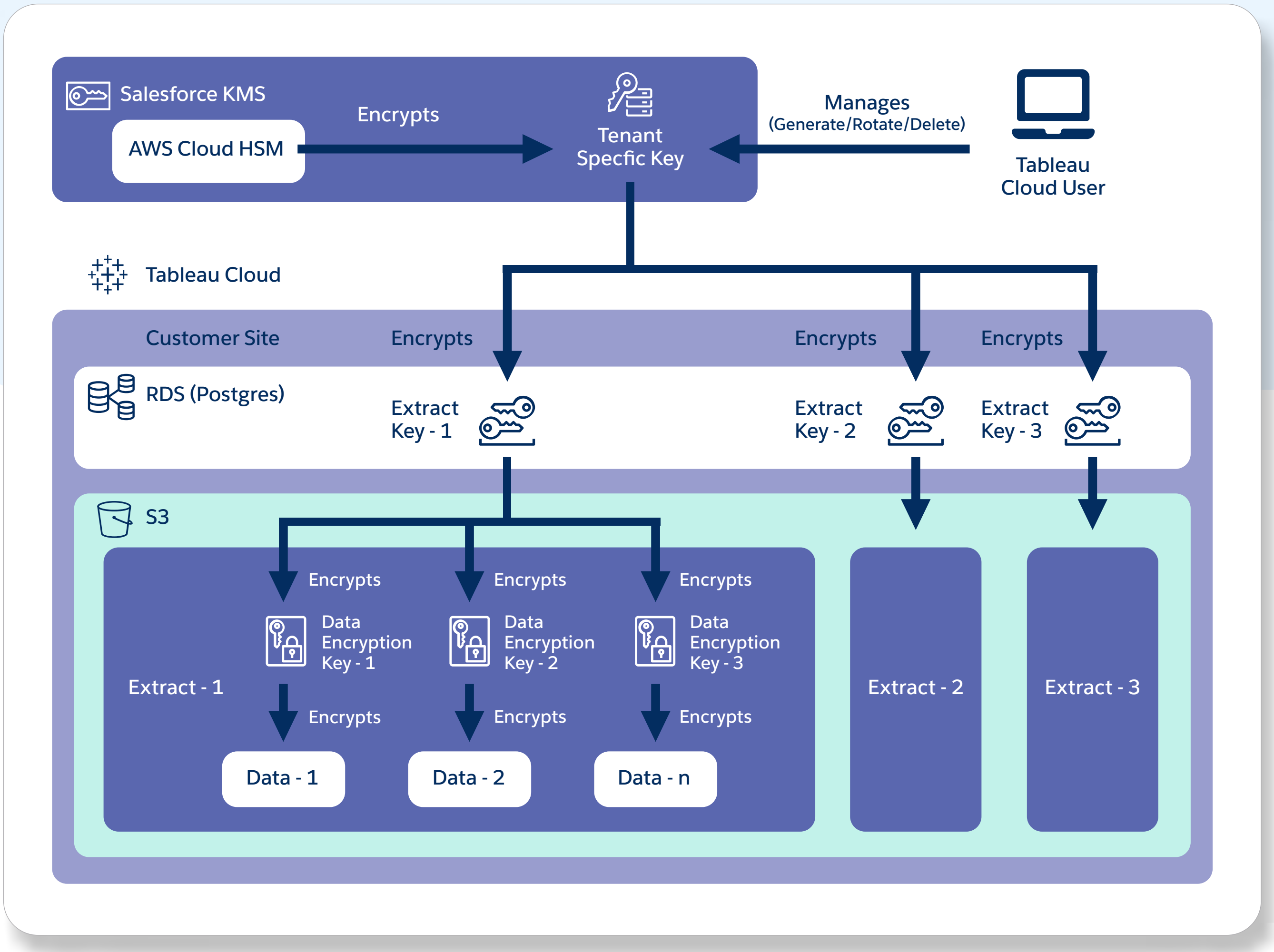
Encryption Key Management

Encryption Key Management by Tableau: Salesforce uses AWS KMS (Key Management Service) to manage its encryption keys, with CloudHSM to make sure that only Salesforce has access to these keys. The public cloud provider can't access the encryption keys or the decrypted versions of customer data stored in Hyperforce's environment.

Customer-Managed Encryption Key (CMEK): Customers can choose to have an add-on Customer Managed Encryption Key (CMEK). Customer-Managed Encryption Keys give customers an extra level of security by allowing them to encrypt their site data extracts with a customer-managed site-specific key (Tenant Key). The Salesforce Key Management System (KMS) instance stores the default Tenant Key for anyone who enables encryption on a site. Here's a more natural version of the process for generating and using a Customer-Managed Encryption Key to encrypt and decrypt the customer data in extracts:

> **Tenant Key Generation:** When a customer enables the Customer-Managed Encryption Key (CMEK) feature on their Tableau Cloud site, an RSA2048 asymmetric encryption key is created as the customer's per-site key, known as the Tenant Key, in the Salesforce KMS database. This Tenant Key is then encrypted using CloudHSM and never leaves the Salesforce KMS database.
>
> **Encryption Process:** When new extracts are created and published, an AES-256 symmetric encryption key, called the Extract Key, is generated. The plain-text version of the Extract Key is kept in memory, while an encrypted version (encrypted with the Tenant Key) is stored in RDS (Postgres) along with the extract's metadata. Next, one or more Data Encryption Keys (DEKs), also AES-256 symmetric encryption keys, are created to encrypt the data in the extract. The extract is then encrypted with the DEK, and the DEK, itself, is encrypted with the Extract Key and stored with the extract.

Decryption Process: To decrypt an extract, Salesforce KMS decrypts the Extract Key. The decrypted Extract Key is then used to decrypt the DEK, and the decrypted DEK is used to decrypt the encrypted extract. Finally, the decrypted extract is returned.



Credential Encryption

When a workbook or data source is published with credentials in Tableau Cloud, it's crucial to securely persist these credentials for future connections. Tableau Cloud uses keychains to achieve this. Keychains store authentication secrets and transient connection information, enabling data sources to connect to databases. These keychains are serialized and encrypted when saved in PostgreSQL (AWS RDS) powered metadata databases in Tableau Cloud.

Keychains are created when a new workbook/datasource (publishing/web authoring) are created; then they're encrypted and serialized to PostgreSQL. When a workbook/datasource is to be used, the keychain is decrypted, then augmented with additional authentication or connection information, and finally it's turned back into an XML string and used to allow the database connections.

The Asset Key (AES-256) is used to encrypt keychains within the application before they are stored in PostgreSQL. These asset keys are never saved in plaintext on disk or in any insecure database; they exist in plaintext only in memory. The keys are generated and stored securely in a Vault within the Secret Functional Domain on Hyperforce and are never moved out of this secure environment. They're always transmitted securely over the network using TLS 1.2. Additionally, asset keys are rotated every 90 days. During the key rotation process, each keychain is decrypted with the old key and then re-encrypted with the new key. PostgreSQL uses AWS RDS encryption turned on by default to provide volume level encryption.

Tenant Data Isolation

Tableau Cloud is a multi-tenant SaaS which means customers share a system with all other customers using the same POD. Customer data in a POD isn't segregated by instance or database, but application logic. Every customer's site has its own GUID value (so-called "Site ID"). Customer data within the site is tied to the Site ID. Tableau Cloud application logic limits user actions (read, update, and delete) so that they can be performed only on the data that is tied to the particular Site ID. When a user gets authenticated, Tableau Cloud stores the session token and the Site ID that was authenticated in PostgreSQL. Every time the user makes an action, the user's session token value from their client side will be compared with the one in the server's PostgreSQL to prevent tampering. If they are matching, the queries will be made with a scope of the data with the same site ID. Additionally, the returned data will be filtered based on the user's access privileges and permissions. Secure Software Development Lifecycle (SSDLC) practices, including threat modeling and internal security assessments, are conducted to confirm that OWASP issues aren't present in the application. Also, external penetration tests are regularly performed.

Secure Data Source Connectivity: Tableau Bridge

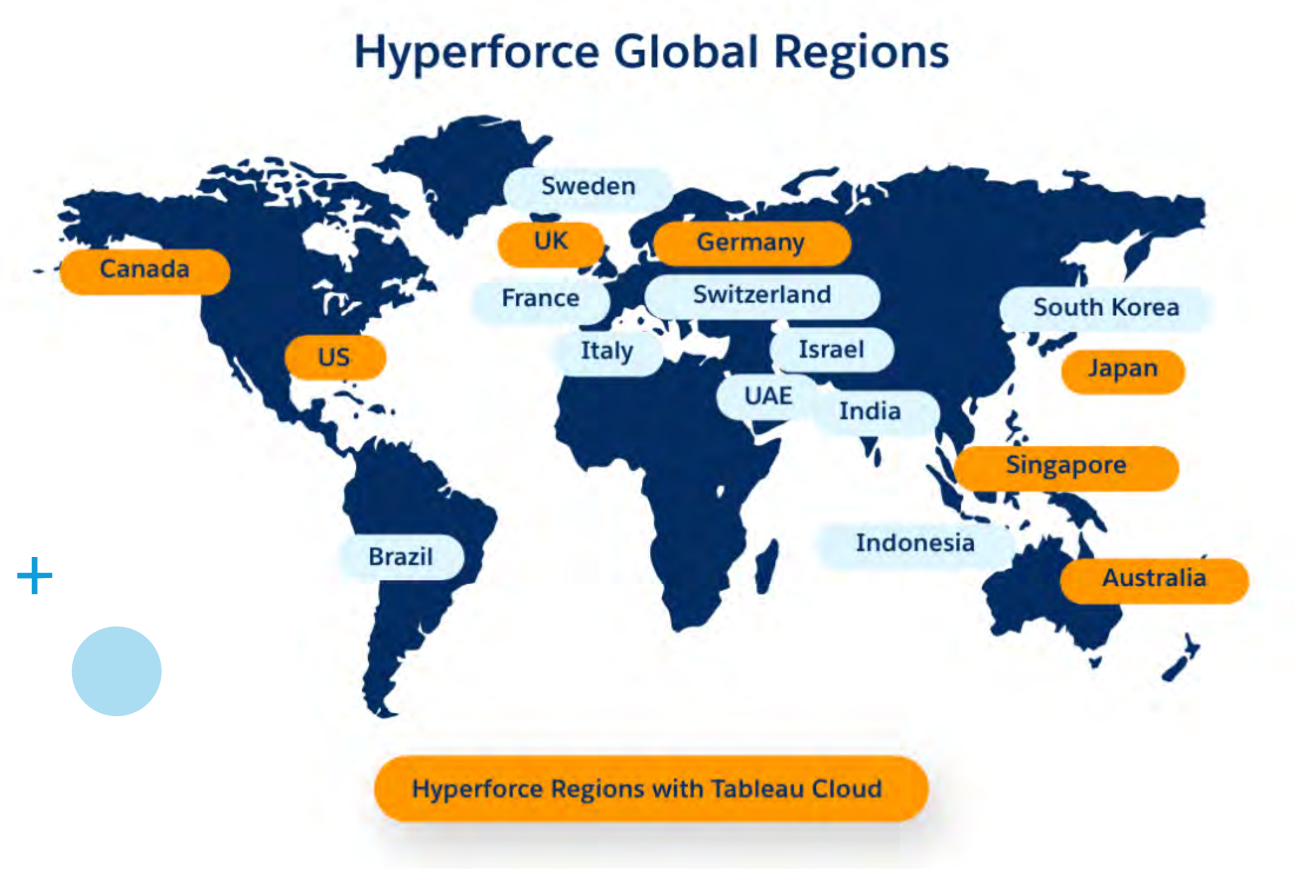
Many customers run databases like SQL Server on-premises and need to bring data from them to Tableau Cloud. Tableau Bridge is a product built by Tableau to support exactly this need. Tableau Bridge then communicates with the customer's Tableau Cloud site from behind their firewall, handling both scheduled extract refreshes or live queries of their published data sources.

As an administrator or creator, users can install a Tableau Bridge in the same environment as an on-premises database, connect it to the database, at which point Tableau Cloud can start querying the connected database. Tableau Bridge is a Windows and Docker-based program that lives in the same network as the customer's on-premises data.

To set up Bridge, an administrator or creator needs to download Bridge and then run it locally in "application mode" or run it in "service mode" in a separate account. After Bridge is launched, a user can authenticate with the name and password for their Tableau Cloud site to pair Bridge to a site. After Bridge is paired, it creates an encrypted channel through a long-running WebSocket between Tableau Cloud and the user's environment. Users can then configure live connections or extracts to databases within the same network environment as Bridge.

In terms of security, live connections or scheduled extracts via Bridge are very similar to a cloud connection, with Bridge just acting as an intermediary. In this case, a schedule is executed locally on a Bridge agent. When the time comes, the Bridge agent will connect to a database and build an extract locally. The connection is fully controlled by customers and happens within the customer network environment. After being built, the extract is sent to a background worker in Tableau Cloud over an encrypted channel. A background worker with encrypted volumes is responsible for storing the extract on a file server, which is encrypted at-rest. Like with cloud connections, all data is encrypted in-transit and at-rest.

Data Residency



Customers can choose their Tableau Cloud region. Customer data won't be transferred to other regions while using Tableau Cloud, except for Generative AI features and as otherwise described in the Documentation. Hyperforce delivers data residency benefits by providing customers with local data storage and processing options, which can help them comply with local regulations. Currently, Hyperforce instances are running in 17 regions and Tableau Cloud is running in 8 regions in 7 countries:

Sydney, Australia
Tokyo, Japan
Quebec, Canada
Frankfurt, Germany
London, UK
Virginia, US
Oregon, US
Singapore, Singapore

Logging & Monitoring

Security Logging and Monitoring

Salesforce's Computer Security Incident Response Team (CSIRT) uses a security event logging and management system to manage the security alerts and logs generated by services, computing, and network components on Hyperforce. The system consists of a central database, management server, and distributed agents. The distributed agents receive events from network flow and systems (application logs, system logs, DNS logs, file access logs, hosts, file integrity, and database monitoring) on the network, and compress, encrypt, and transmit the data to the management server and database for processing. Correlated events are configured to generate alerts and logs, which are monitored on a 24/7 basis. Firewalls and network services are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of 1 year.

Incident Response and Management

Salesforce has a structured Incident Management Process to guide its CSIRT in handling investigations, management, communication, and resolution activities. If there's a security breach that leads to unauthorized disclosure of customer data, Salesforce will promptly notify the affected customer. This notification could come via a phone call from Salesforce Support, an email to the customer's administrator and Security Contact (if provided), or a public announcement on trust.salesforce.com. Regular updates will be given to all involved parties until the issue is resolved. All incidents are tracked and managed through an internal ticketing system. If the CSIRT needs extra help with a complex or severe incident, Salesforce can call on external incident response consulting firms with which they have a relationship.

Availability Logging and Monitoring

Every aspect of the services and applications is monitored. The five key metrics are listed below and are termed **READS**:

Request rate: The number of requests per second received by a service. This metric indicates demand and can be used to detect unusual activity.
Errors: The number of errors that occur in a service. This metric helps identify failure cases.
Availability: The percentage of time a service is available and able to provide its defined functions. This metric is a combination of availability and reliability. Availability means a service is up, while reliability means a service is healthy.
Duration/latency: The time it takes for a service to complete a transaction.
Saturation: How close a service is to exceeding its headroom. This metric varies with the service's constraints. For example, a memory-constrained system will measure memory usage, while an IO-bound service will measure IO.

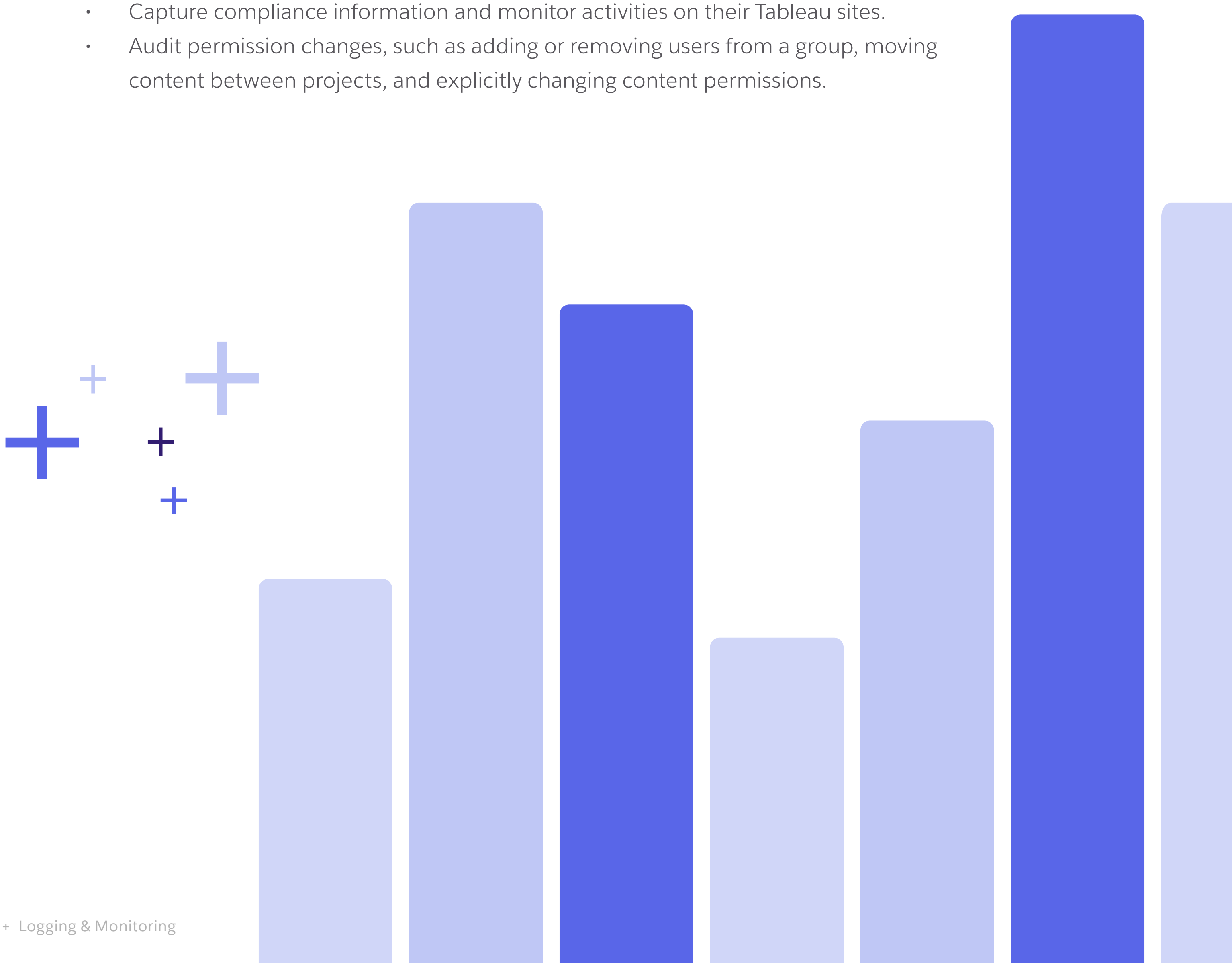
Every service reports these metrics and is measured to drive decisions, maintenance, and improvements. This capability enables Salesforce to address any issues related to service availability, performance, or responsiveness even before our customers can experience and report.

Customer Site Logging and Monitoring

Admin Insights is a Tableau Cloud feature that helps customers to track the activities like site traffic, adoption, reach, User roles & sign-in activity, and publishing-related activity for their account or site. This feature is available to customers by default for their sites.

Activity Log is an enhanced logging and monitoring function that allows customers to send log events to their own Amazon S3 for further analysis and auditing. Events may take up to 15 minutes to appear in the S3 bucket after they occur. Each event includes a timestamp and the ID of the actor who performed the action. If applicable, the ID of the affected content is also included. With the Activity Log, customers can:

- View detailed event data for Tableau Cloud.
- Capture compliance information and monitor activities on their Tableau sites.
- Audit permission changes, such as adding or removing users from a group, moving content between projects, and explicitly changing content permissions.



Business Continuity Plans & Disaster Recovery plans (BCP/DR)

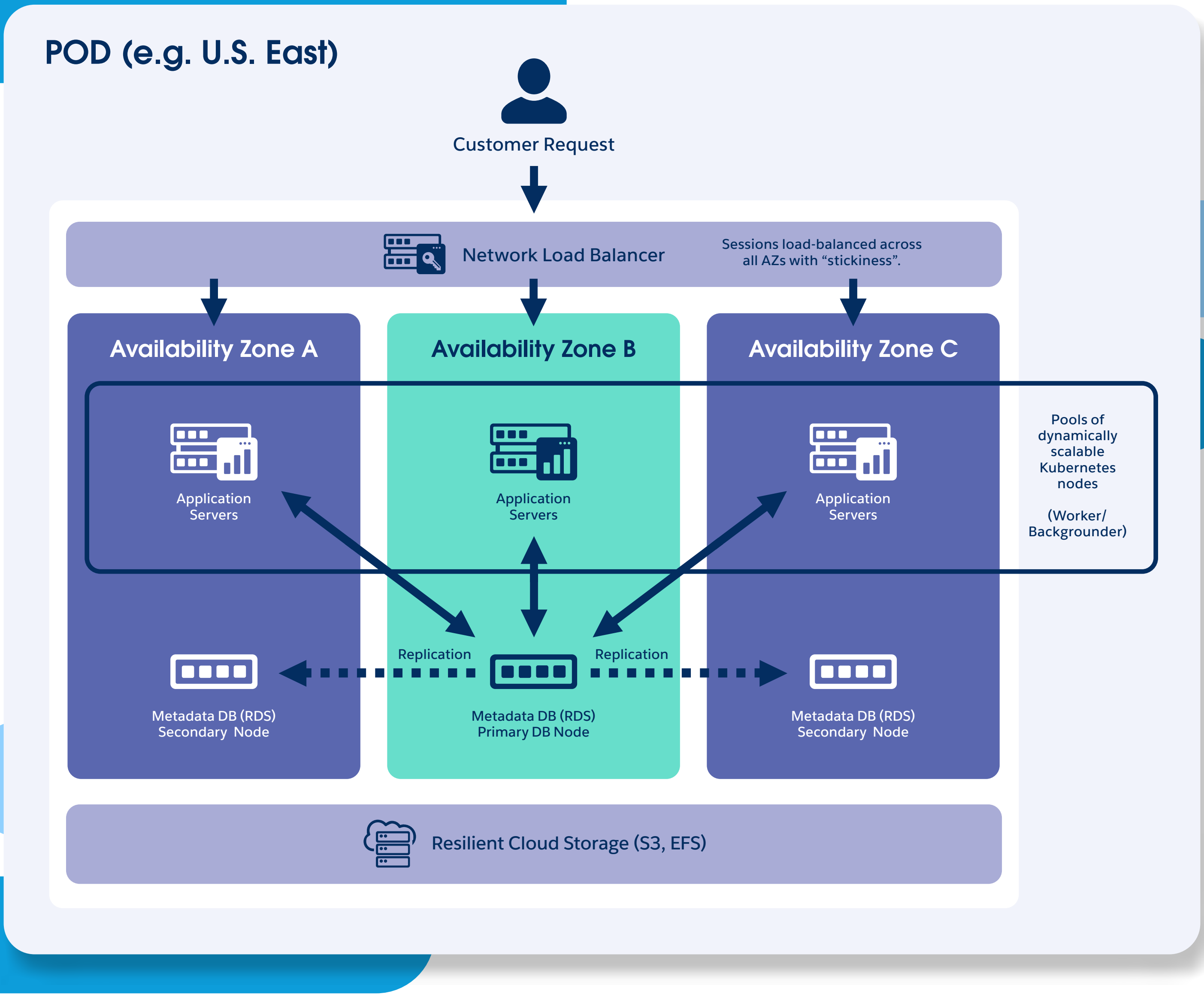
Salesforce has Business Continuity Plans and Disaster Recovery Plans (BCP/DR) in place and exercises them at least once per year. Exercises verify the accuracy of its content and make updates to the plan as necessary. Results are documented and evidence is retained, incorporating lessons learned as appropriate.

High Availability and Disaster Recovery

The 3 Availability Zone (3AZ) architecture of Hyperforce is a fundamental design principle aimed at enhancing the platform's high availability, resilience, and performance. Availability Zones are distinct, physically separated data centers within a specific geographic region - each equipped with its own power, cooling, and networking infrastructure. In the event that one AZ fails, the other two are designed to continue operating without interruption. All services securely hosted on the Hyperforce platform adhere to the same design and deployment principles as those applied to other services within Hyperforce.

By following the key disaster recovery principles and practices outlined below, Hyperforce can withstand a range of potential disaster scenarios and uninterrupted service delivery, even in the face of adverse situations:

- 3 Availability Zone (3AZ) Model
- Continuous Data Replication
- Regular Data Backups
- Highly Redundant Infrastructure
- Monitoring and Alerts
- Disaster Recovery Testing
- Automated Failover and Recovery


POD (e.g. U.S. East)
Customer Request
Network Load Balancer
Sessions load-balanced across all AZs with “stickiness”.
Availability Zone A
Availability Zone B
Availability Zone C
Application Servers
Application Servers
Application Servers
Pools of dynamically scalable Kubernetes nodes
(Worker/ Backgrounder)
Replication
Replication
Metadata DB (RDS) Secondary Node
Metadata DB (RDS) Primary DB Node
Metadata DB (RDS) Secondary Node
Resilient Cloud Storage (S3, EFS)

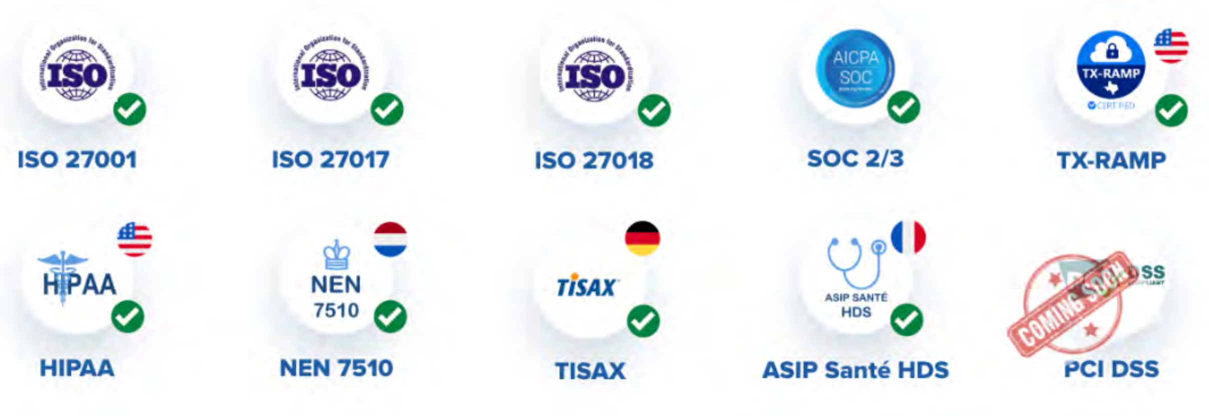
Data Backup

Tableau Cloud uses the AWS Backup Service to backup system and customer data. Backups are encrypted and stored securely. Access to the backup is restricted to approved administrators. Backups are monitored regularly. Failures are investigated and resolved in a timely manner. The below is the Data backup frequencies and scopes:

- Daily incremental backup of customer data
- Weekly synthetic backup of customer data
- Monthly full backup of the entire system data

Compliance

Here are the compliance certifications and 3rd-party audits that Tableau Cloud on Hyperforce has achieved. Customers can download the certifications or 3rd-party audit report from our Salesforce Compliance site.



Conclusion

At Salesforce, we build security into every aspect of our business and systems. Tableau Cloud is built upon our #1 core value, Trust, because our customers depend on us to safeguard and protect their customer data and to make sure that our platform and services consistently meet our performance and security requirements. For additional details and information, review the following Tableau Cloud Security Compliance Documentation section or contact your Salesforce account executive.

Salesforce Security Compliance Documentation

Tableau Cloud Compliance Documents:

Tableau Cloud Compliance
AWS SOC 2 Report
Vulnerability/Penetration Report Summary

Tableau Help Articles:

Security in the Cloud
Site Authentication
Monitor Site Activity
Manage Users and Groups
Manage Content Access
Keep Data Fresh
Use Tableau Bridge
Activity Log
Customer-Managed Encryption Keys (CMEK)

Tableau Cloud Hyperforce Migration Articles

Tableau Cloud Migration to Hyperforce
Introducing Tableau on Hyperforce - General Information & FAQ
What to Know About Tableau Cloud Migration to Hyperforce

Salesforce Compliance Documents

Salesforce Corporate Services SOC 2 Report
Vulnerability/Penetration Report Summary

Legal

Trust and Compliance Documentation
The Infrastructure & Sub-processors (“I&S”)
Tableau Cloud Security, Privacy and Architecture
Hyperforce Security, Privacy and Architecture
Data Processing Addendum (DPA)

This whitepaper is for informational purposes only and does not constitute legal or professional advice. No guarantees are made regarding its accuracy or applicability. Consult a qualified professional for specific guidance applicable to your situation. Some features discussed herein may require an additional purchase.

About Tableau from Salesforce

Tableau is the world's leading AI-powered analytics platform. Intuitive data experiences, backed by generative and predictive AI capabilities, elevate insights where you work most. Offering a suite of analytics and business intelligence tools, Tableau turns trusted data into actionable insights so you can make better decisions every time. Tableau offers the most choice and flexibility for your architecture as your technology and AI strategy evolve. With security, data governance, and compliance in mind, your organization can maintain agility as new demands on data arise.

Tableau is committed to supporting the unique needs of organizations around the world with the largest partner and success ecosystem, including the passionate Tableau Community that can teach, support, challenge, and celebrate you at every stage of your AI journey. The future is limitless when you start with data and move forward with Tableau. For more information, visit www.tableau.com.