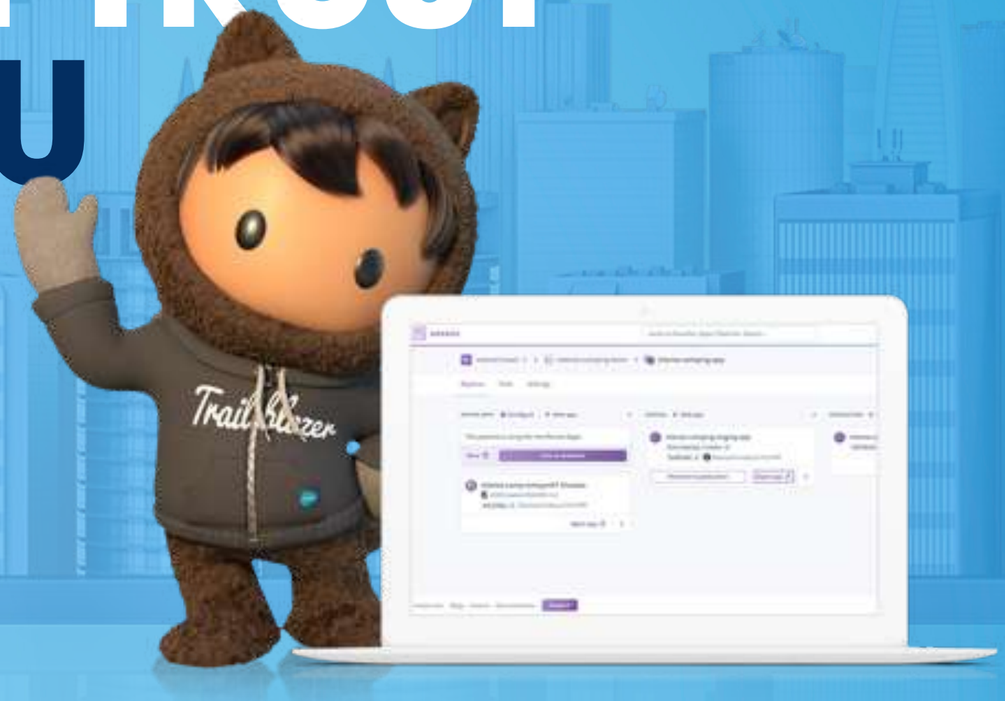
BUILD SECURE *and* COMPLIANT APPS YOU CAN TRUST *on* HEROKU



Contents

1

INTRODUCTION

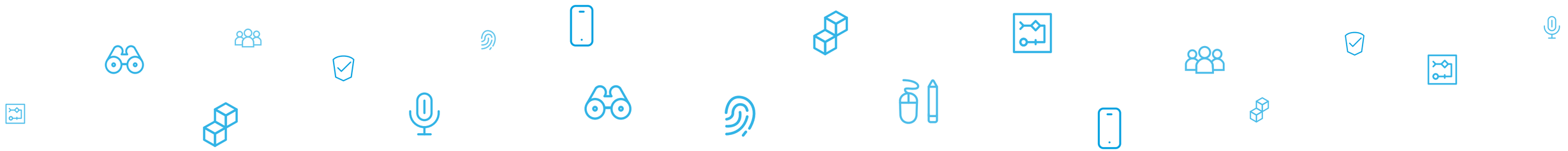
More Apps, More Choices ... More Problems?

The Fourth Industrial Revolution has ushered in an unprecedented era of digital innovation that is transforming every industry, business, and individual experience. In particular, mobile apps have accelerated this revolution by redefining the relationship between brands and their customers. Previously, brands held a monopoly over these relationships as they controlled the messages and channels they used to communicate to customers. But apps have redefined that dynamic by empowering customers with more choice, more information, and more control over their relationships with their favorite brands than ever before.

Leading companies such as Facebook, Amazon, Apple, and Netflix have capitalized on this new paradigm by delivering engaging experiences through innovative apps that have captured customers' hearts, minds, and dollars. These types of apps have paved a way for the app economy to grow into a ubiquitous presence in our daily lives, where the number of apps downloaded is projected to grow from 194 billion in 2018 to over **258 billion in 2022**, with gross consumer spend across all app stores to surpass $157 billion.

Yet, while mobile apps have redefined how we work, live, and play, they have also delivered an uncomfortable reality that comes with having more choice: **As the number of mobile devices and apps increases, so too does the attack surface that can leave companies vulnerable to cybersecurity attacks.** What's more, 62% of breaches and 39% of incidents occur at the web application layer. While it is unclear exactly how the web applications were compromised in some cases, it's assumed that attackers are scanning for specific web app vulnerabilities, exploiting them to gain access, inserting some kind of malware, and harvesting payment card data to create a profit.

Given how frequent and more sophisticated cybersecurity attacks have become, business leaders are starting to recognize that prioritizing cybersecurity is not a luxury but a strategic necessity. A failure to protect their organization and the customer data they possess from cybersecurity attacks has far greater consequences than just financial costs – it can also damage your company's reputation and erode the trust your customers have in you, which can take years to recover from.



Cybersecurity *and* Compliance Are Organizationalwide Responsibilities

Meeting the multifaceted challenges presented by cybersecurity threats and compliance is no longer considered a back-end job that is limited to chief information security officers (CISOs) and their security teams. Instead, it requires a comprehensive and organizationwide approach that brings together key stakeholders from all levels of the business.

Business leaders are responsible to ensure their organizations are best positioned to meet the cybersecurity and compliance demands of this digital age. **CEOs** must make these issues a top priority on their agendas and build a cybersecurity strategy that accounts for business continuity, brand protection, compliance, and bottom-line growth.

IT leaders, such as **CIOs** and **CTOs**, are responsible for investing in and implementing technologies that empower their organizations, departments, and employees to operate with speed and agility. They must not only ensure the confidentiality, integrity, and reliability of the technology platforms their businesses use, but must also closely align with **CISOs** to ensure these technologies are aligned to the organization's digital security initiatives in a comprehensive and integrated manner.

Developers play a critical role as they are in the front lines of enterprise application development. However, they face strong demand to meet rapid speed-to-market goals, enhance product quality with each update, and increase flexibility. This has led to complex, often fragmented development teams whose primary focus is on rapid development of features and functions, without consideration of the vulnerabilities they could be creating in the code they are so quickly churning out.

To build secure and compliant data-driven apps, developers need a platform that is built with security best practices in mind and can provide developers with the open languages, tools, and resources they need to seamlessly integrate security early and throughout the software development lifecycle.

Build Secure *and* Compliant Apps You Can Trust *on* Heroku

What is Heroku?

Heroku is a modern application platform that provides developers with the fastest path to go from an idea to a URL without having to manage infrastructure. Designed to optimize the developer experience, Heroku provides developers with the flexible tools, open languages, and frameworks to help them build engaging, custom applications at global consumer scale.

Heroku is for enterprises.

Heroku is designed and built to provide protection from cybersecurity threats by applying security controls and compliance across every layer, including application, infrastructure, networking, and data security. With these powerful security foundations in place, Heroku empowers IT and security teams to seamlessly protect customer applications and data, rapidly deploy security updates without customer interaction or service interruption, and deliver on their business objectives without having to sacrifice agility for security.

Heroku is for developers.

Heroku's inherent security and trust capabilities give developers a reliable platform to build consumer applications at scale. More specifically, developers can access Heroku's industry-leading secure application design tools, dedicated runtimes, and data integrations to rapidly build secure and compliant apps collaboratively and easily.

Extend the Power of Heroku *with* Salesforce Customer 360

Heroku is a core component of the **Salesforce Customer 360 Platform**, the **most agile and trusted way to innovate** and deliver digital transformation for your customers, your employees, and your partners. Customer 360 offers industry-leading trust, security, and availability with built-in compliance, integrated platform services, and automatic upgrades. These powerful capabilities allow companies of all sizes and industries to utilize Heroku to build engaging customer applications with Salesforce data that bring them closer to their customers.

Shared Responsibility *in the* Salesforce Trust Model

Our Promise

When developers build and operate mission critical applications on Heroku, they are entrusting Salesforce with critical and sensitive data about their businesses and their customers.

In an era when companies are under more scrutiny on how they are managing customer data, nothing is more important to us than honoring our custodial commitments in protecting the confidentiality, integrity and availability of your data, which is why **trust** has always been our *number one value*.

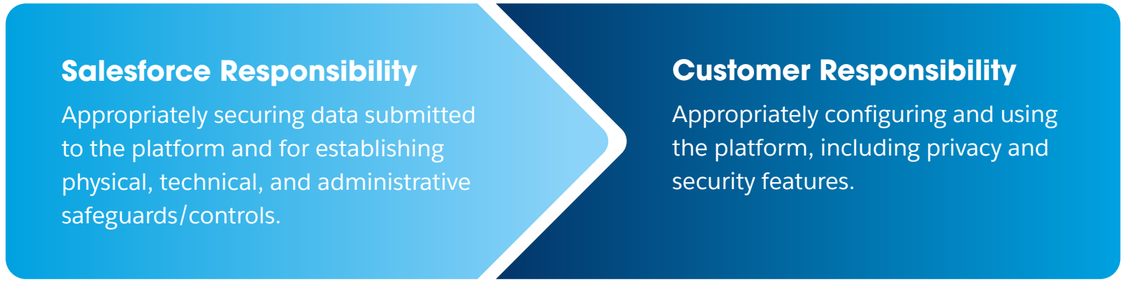
It is this radical commitment to customer trust that informs the decisions we make every day. We know that security and compliance are essential components of the customer trust journey, and we see them as the byproduct of a relentless focus on our security and engineering.

Go to **Trust.salesforce.com** to obtain real-time information on Salesforce's system availability, performance, security, and compliance.

Your Commitment

As a Salesforce customer and Trailblazer, you play an integral role in your organization's security story by making sure your apps are built with security and compliance best practices in mind.

You are responsible for implementing strong security measures in your application development process, evaluating the security and compliance capabilities of your third-party partners, and properly ensuring secure and compliant user access to your Heroku account and resources. Heroku offers a number of dynamic and robust security and compliance features to help make it easier for you to fulfill these responsibilities.



2

SECURE APPLICATION DESIGN TOOLS: BUILD ENGAGING APPS *with* SECURITY

Heroku Flow

Integrate Security Early *in the* Application Development Lifecycle

Developers face many demands to build and deploy the latest applications and features to help their organizations stay ahead of the competition. While 48% of developers who were surveyed acknowledge the importance of app security, very few feel they have the time to integrate security in efforts to meet rapid deadlines.

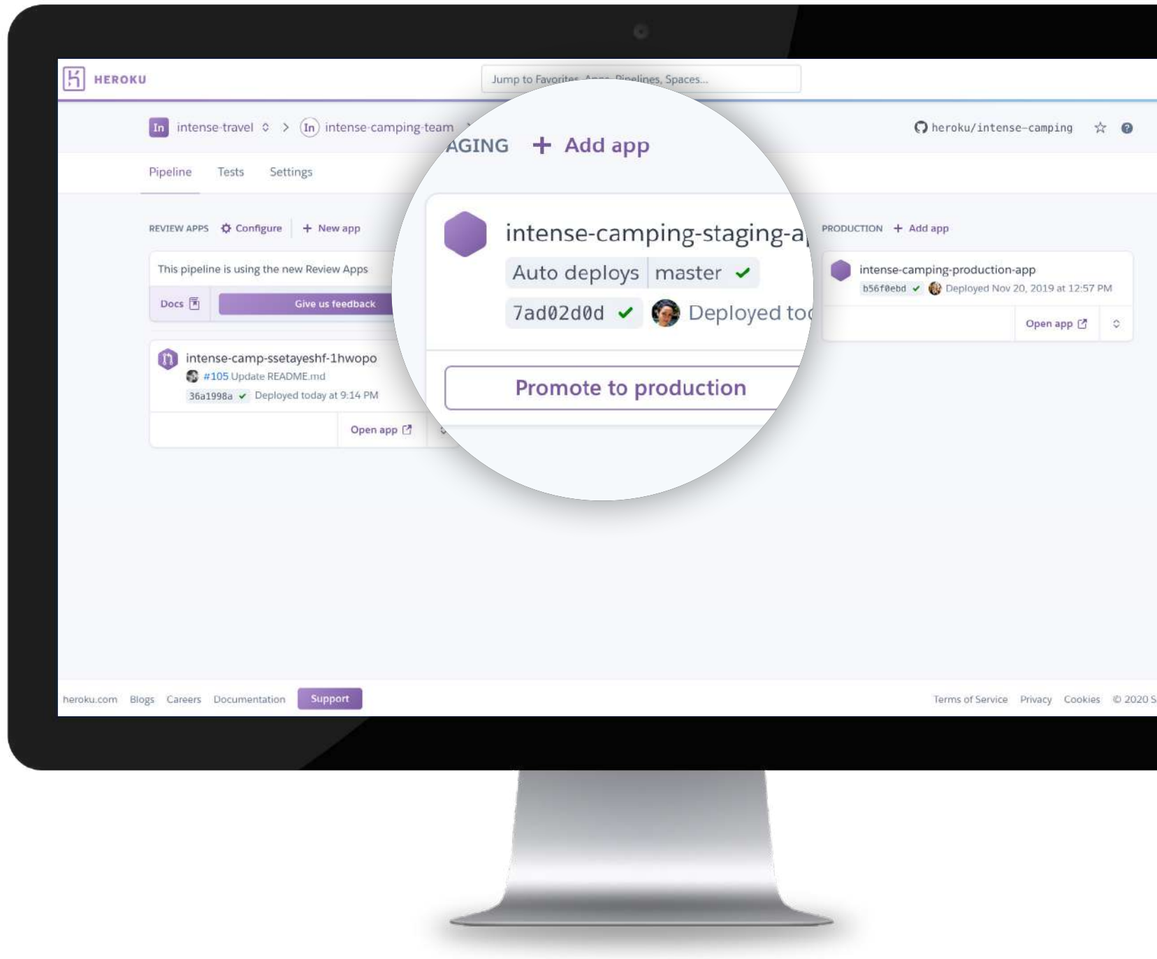
However, what developers don't realize is that it can be **six-to-15 times less costly** and time intensive to fix security bugs when they are detected early in the application design stages than it is when you are trying to patch dozens to hundreds of bugs that penetration testers find right before an app is due to go into production. More so, making changes to the codebase to address these defects later in the application development lifecycle can affect the application's functionality, which can add additional cost, time, and effort to fix. So it's important to find and fix bugs during the early stages of development.

Given this context, developers need a set of tools that will not only allow them to integrate sound security design principles and policies early in the application process, but also give them the flexibility and ease to collaborate with other teams to adjust their codebase when fixes need to be made.

Embed security early in the app development lifecycle with Heroku Flow

Heroku Flow is a flexible way to structure, support, and visualize continuous delivery (CD) for Heroku apps from development to production via a pipeline. A pipeline is a group of Heroku apps that share the same codebase. Apps in a pipeline are grouped into one of four distinct stages – review, development, staging, or production.

Each stage represents different deployment steps in a CD flow. There is a rich set of administrative controls that allow distinct control between stages of the software that are managed in Heroku Pipelines. Each app can have its own designated set of users with manage, deploy, and operate permissions. This allows broad collaboration for apps in the review and development stage, for example, but tighter governance and control of apps being promoted to staging and production environments.



The flexibility built into Heroku Flow gives developer teams a clear path to embed security and compliance features early in the application design process that can lead to the following benefits:

1. **Higher-quality apps:** Less time on repetitive processes means that developers can spend more time and attention on creating quality code, which inherently reduces bugs and issues. A regular release cadence allows product teams to loop in user feedback along the way. This helps further hone the app's feature set and user experience, and increases customer satisfaction.
2. **Improved team productivity and visibility:** Automated processes and environments reduce the time and expense of traditional manual testing. This allows app developers to focus on what they do best: development. Teams work at a faster pace, deliver more value to the business, and collaborate more effectively on solving problems. All members of the project, from design to production to marketing, can see changes sooner and participate in decision-making at each step of the process.
3. **Lower-risk releases:** Frequent releases allow teams to find and fix issues early in the development process, which means that code flaws are much less likely to reach production. The codebase stays clean and at a releasable state at all times. And with continuous delivery, repeated testing of deployment processes and scripts also happens earlier, before releases get to production.
4. **Faster time to market:** Continuous delivery enables a business to stay competitive by delivering new app features and updates into the hands of customers more quickly. Engineering teams can be more responsive to changing business needs and market trends, better manage their backlog of features, and be more able to release app fixes as soon as needed.

Click **here** to learn more about Heroku Flow.

"We're seeing organizations start to build security into each phase of the development pipeline ...

From pre-commit scans in the the IDE (my code), to build scans in the CI pipeline (our code), to deployment scans in the CD pipeline (production code), security testing will cover code from inception to production."

— Suzanne Ciccone, Veracode

" Heroku Pipelines have increased our small team's productivity. With review apps created after each PR, every developer can have their own testing environment and work on the same app simultaneously with much less friction."

— Jane Philipps, The Information

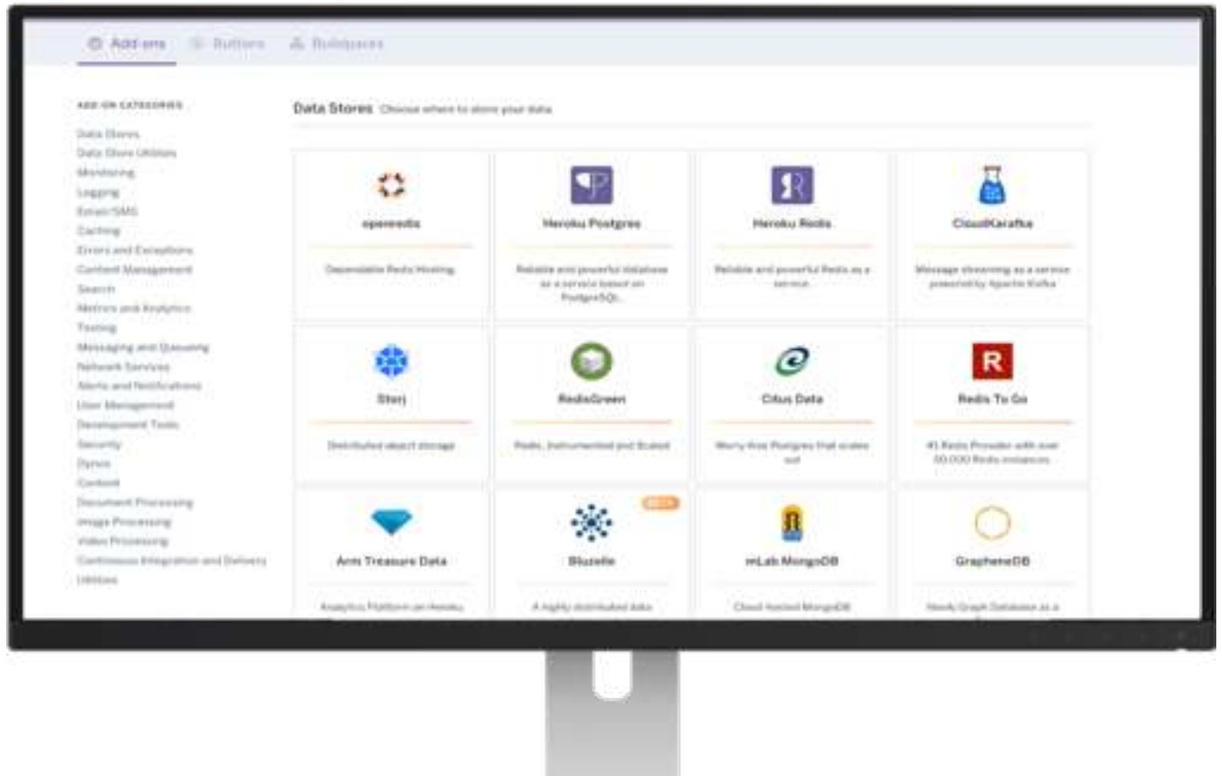
The Information

Heroku Elements Marketplace

Build Secure Applications *with* Add-ons

Building the next game-changing application with best-in-breed security can require features and capabilities that may be beyond the scope of your team's expertise. That may not be an issue for organizations with well-resourced development teams. But if you are a fledgling startup or small company that doesn't have a strong team of developers, where can you access those security features and capabilities in order to build and deliver fully functional and secure apps to customers quickly?

Fortunately, developers can source the key app features and capabilities they need through **Heroku Elements**, our marketplace that brings all of the pieces within our Heroku ecosystem together in one place. Heroku Elements allows developers to discover and select the best components to build secure and compliant apps fast by providing a variety of services such as the following:



1. **Add-ons:** Elements contains more than 170 fully managed services integrated for use with Heroku.
2. **Buttons:** Buttons provide the easiest way to get up and running with an example template or sample app on Heroku.
3. **Buildpacks:** Buildpacks are sets of open source scripts that are used for compiling apps on Heroku. With access to more than 900 buildpacks, customers can access any language or customizations when building apps on Heroku.

By leveraging add-ons, customers can more easily design applications that follow security best practices. For example, the Elements Marketplace includes several third-party components that support application monitoring, logging, and testing; network services such as static IPs and DNS management; alerts and notifications; user management such as authentication and single sign-on; and security services such as website security scanning, SSL encryption, and key management.

Note: Although Elements has a growing list of third-party providers, it is the customer's responsibility to do due diligence on whether these third-party add-ons meet their required level of security and reliability, and whether these third-party add-ons are updated with the latest security patches.

Heroku Enterprise Teams *and* Accounts
Managing Apps *and* Users with Secure Access Controls

There exists a popular perception that cybersecurity threats such as data breaches come from rogue states or individuals who are tucked in a private office wearing a hoodie.

While that may be true for the majority of cases, a growing number of data breaches are now coming from the inside via a company's own employees. While insider threats don't get the same attention on the news as cyberattacks caused by rogue states and hackers, they are a growing threat. The Verizon 2019 Data Breach Investigations **Report** states that as many as **34% of all breaches** are accidentally or intentionally caused by insiders. Given that insider-related incidents can cost a company on average as much as **$8.76 million** per year, it is important that internal security measures are in place to ensure that only the right people have the right access to the right resources and data.

> "97% of IT leaders are worried about insider data breaches."
> — Egress, 2020 Security Survey

This is especially relevant when it comes to building mobile applications that involve sensitive customer data. While business leaders need to ensure that only the right teams and individuals have authorized access to the right data and development resources, a challenge they face is how can they provide teams and developers secure access without slowing down the collaborative process that is needed to build an application?

Deliver unified administration, full visibility, and improved agility with Enterprise Accounts and Enterprise Teams

Heroku addresses these challenges by providing options that address the full range of administrative concerns, from team and user management to expense management, and finally, to the integration of team collaboration with continuous delivery workflows.

Heroku Enterprise Teams allows customers with the sophisticated collaboration needs of large organizations to manage their applications in secure, isolated environments and get access with customizable app-level permissions, along with daily and monthly usage reports. Admins can create an unlimited number of Enterprise Teams with up to 500 users per team.

With Enterprise Teams you can:

- Treat your apps as a shared collection
- Give a group of developers selective access to each app in the collection
- Monitor resource usage across the entire organization
- Seamlessly add new members and remove departing members, ensuring the right people have the right level of access to each app at all times

Learn more about Heroku Enterprise Teams here.

But as organizations expand their usage of Heroku Enterprise Teams, they need a way to manage multiple collaborative team environments, maintain visibility into projects to prevent security gaps, and keep track of high-risk activities and resource consumption. That's where Heroku Enterprise Accounts comes in.

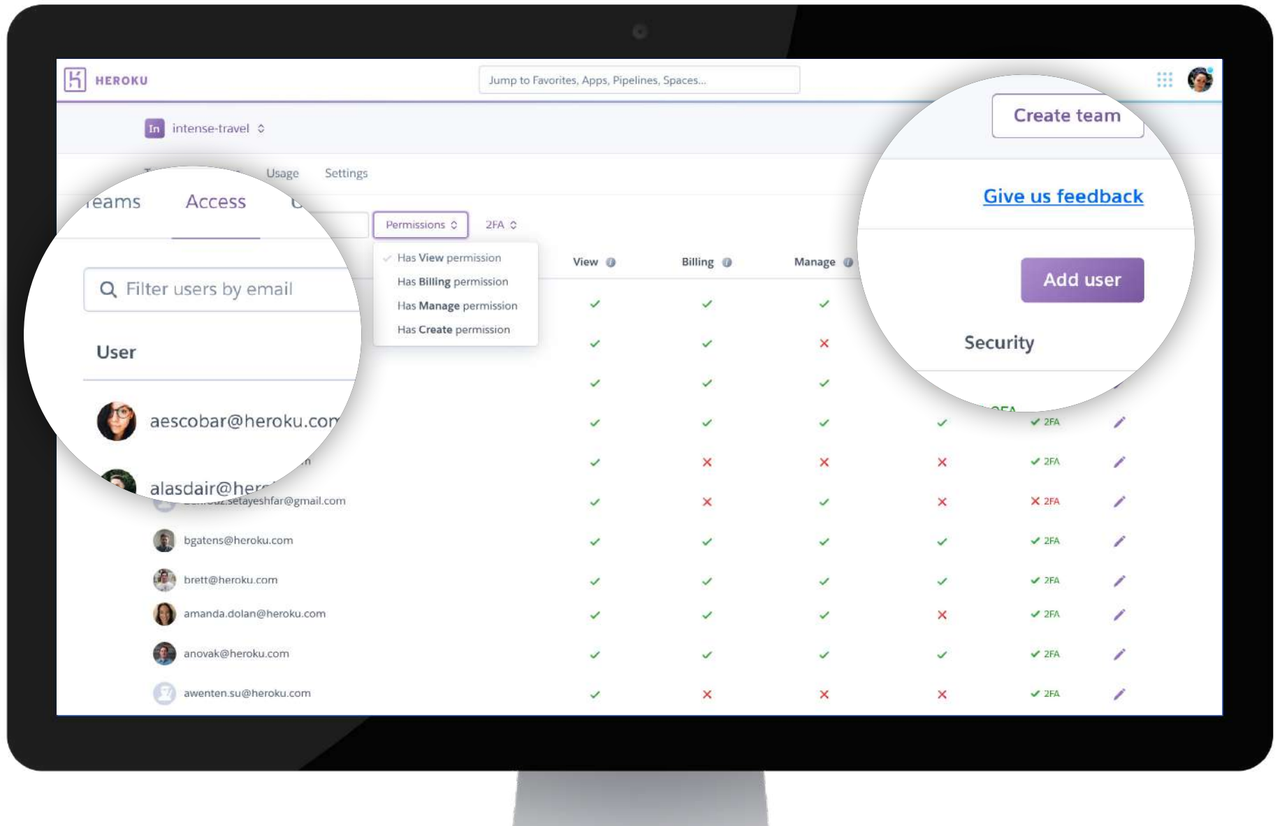
What is an Heroku Enterprise Account?

Heroku Enterprise Accounts is a new layer above Heroku Enterprise Teams that delivers higher-level visibility, accountability, and simple fast management of Enterprise Teams, users, and expenses.

How Heroku Enterprise Accounts adds value to customers:

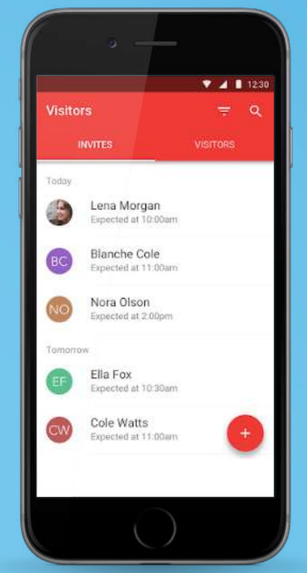
1. **Fast and easy management:** Delegated administrators have access to a variety of Enterprise Teams and user management tools. This makes creating new teams, modifying permissions, and onboarding and offboarding users simple and secure.
2. **Improved visibility with account-wide reports:** Billing admins can access daily and monthly usage reports to keep track of resource consumption across the company. There are also monthly auditing reports available to help customers get detailed information on sensitive activities across the company and meet their auditing requirements.
3. **Enhanced security:** Companies can set up single sign-on (SSO) at the Enterprise Accounts level that can be applied to all Enterprise Teams within an Enterprise Account. In addition, admins can check the security status of all Enterprise Account members under the Access tab and request users to enable SSO or 2FA.

Learn more about Heroku Enterprise Accounts here.



"Heroku Enterprise Accounts has been a great help for us getting SOC2 compliance. Enterprise Account permissions are also a big step in security, allowing us to move toward the principle of least privilege for our organization while still being easy to use for our development team."

— Mike Chan,
VP of Engineering, Envoy



Envoy Mobile App

3

SECURE DEDICATED RUNTIMES: BUILD APPLICATIONS *within the* BOUNDARIES OF YOUR OWN SECURE NETWORK

1
2
3
4
5

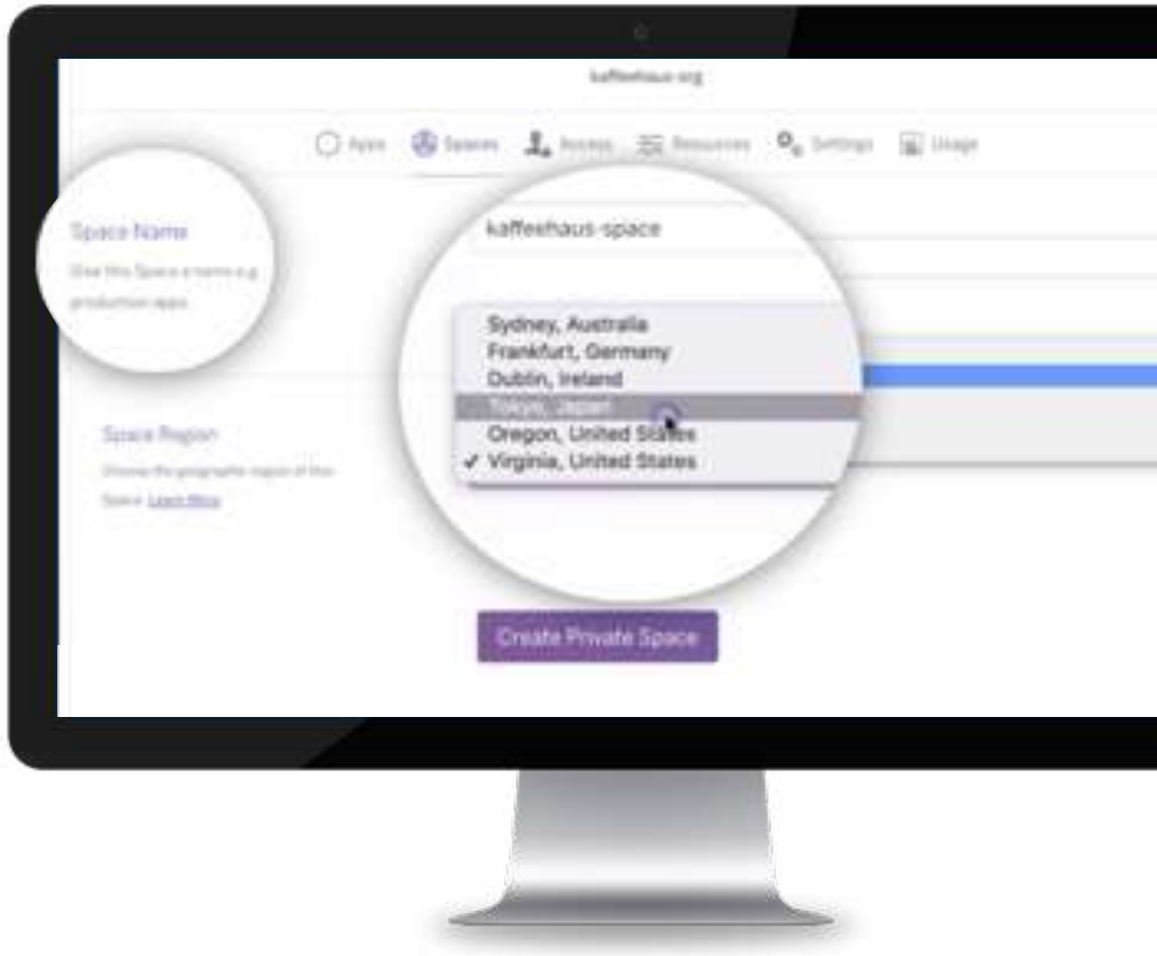
Heroku Private Spaces

Private PaaS, *delivered* as a Service

Many customers choose to build their apps on Heroku's mulitenant common runtime environment. But for customers who require additional layers of network security isolated from other tenants, Heroku Private Spaces delivers a network-isolated group of apps and data services with a dedicated runtime environment that is provisioned by Heroku in a geographic region specified by the customer. Each Private Space has a complete dyno runtime dedicated exclusively to the applications running in the space. This ensures the strongest level of isolation for applications, networking, and infrastructure resources, in turn enabling production apps to meet stringent security and trust requirements.

With Private Spaces, customers can build modern apps with the same powerful Heroku developer experience found in the common runtime environment while also getting enterprise-grade secure network topologies, which enables customers to securely connect to on-premises systems and other cloud services. The key benefits of building modern-day apps in a secure Private Space environment are summarized below:

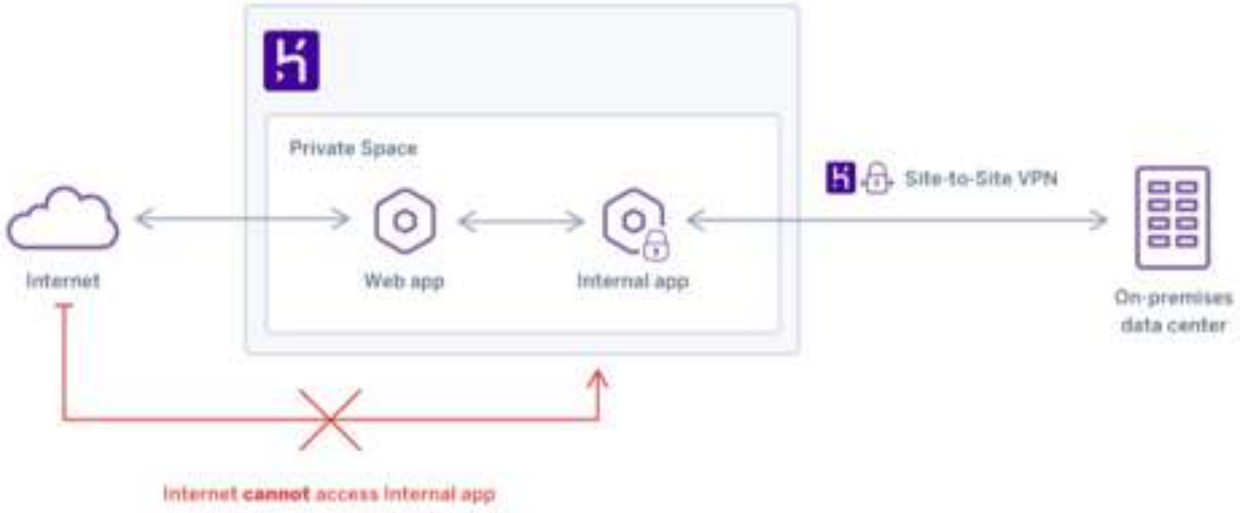
1. **Dedicated and isolated networks:** Private Spaces has a runtime dedicated to only your Heroku apps, ensuring even the highest-traffic apps deliver low-latency performance for every user. Easily set up private, isolated networks for internal services. With selectable regions, you can run apps in Dublin, Tokyo, Frankfurt, Oregon, Sydney, and Virginia.
2. **Private data services:** Keep customer data more secure and private in your internal network. The Heroku managed data service plan types private and shield are automatically provisioned to the same region as the Heroku Private Space and peered using a secure connection.



3. **Enhanced IP restrictions and improved control:** Securely connect apps to third-party cloud services and corporate networks. Each Private Space has a set of trusted IP ranges, and only clients originating from one of these trusted IP ranges can access web processes running in the Private Space. Only organization administrators can perform management functions such as creating, destroying, and changing settings on Private Spaces. Teams can also limit app access to users only on trusted networks.

4. **Seamless VPN support and internal routing:** Establish secure, site-to-site IPsec VPN connections between Private Spaces and on-premises data centers and third-party clouds. Build private apps and APIs with endpoints that are only routable within the Private Space and on VPC-and VPN-peered networks (see architecture diagram below).

Click **here** to learn more about Private Spaces.



"We already love Heroku Private Spaces. It builds on the power and flexibility of the service by giving us a higher level of security that our users expect when handling sensitive data."

— Jon Buckley, Mozilla Foundation Operations

Mozilla Mobile App

Heroku Shield

Create High-Compliance Apps *with* Speed and Trust

Industries such as healthcare and life sciences (HLS) or financial services have stringent regulatory and compliance standards such as HIPAA and PCI on how businesses manage customer data. Developers who are tasked to build applications in these regulated industries can often face complex tradeoffs where they feel they have to choose between building complex regulatory and compliance standards apps at the expense of speed and innovation.

The healthcare industry is living proof of how challenging it is to modernize application delivery while meeting strict HIPAA compliance requirements. All you have to do is compare the user experience of most healthcare apps with what you have come to expect from apps in less regulated industries like ecommerce, productivity, and social networks. Developers may find it too hard to build modern healthcare apps today because they are delivered using outdated, legacy platforms and practices.

However, with **Heroku Shield** developers have a simplified path to building high-compliance apps. **Heroku Shield** delivers a premium set of integrated services for managing regulatory security and compliance built natively in Heroku for customers.

Heroku Shield reduces the risk, complexity, and costs of managing compliance requirements and accelerates the app development process for a company's most transformative customer-facing apps. It allows companies to safeguard and audit customer data while enabling a 360-degree view of the customer. And, in a matter of clicks, developers can support compliance requirements for apps that must adhere to regulations stipulated by HIPAA, PCI, and the like. Heroku Shield includes five core components:

1. Shield Private Spaces: Heroku Shield Private Spaces enables you to build high-compliance, customer-facing apps for regulated industries like healthcare and life sciences that require a BAA. Shield Private Spaces includes additional trust controls for high compliance: keystroke logging for production access auditing, logging at the space level that you control, encryption at rest for ephemeral data, and strict TLS enforcement.

2. Shield Connect: Using Heroku Connect's bidirectional synchronization between Salesforce and Shield Postgres, you can extend your CRM to your Heroku apps and safely share protected health information (PHI) or personally identifiable information (PII) data, including contacts, account data, and other custom objects, in a secure environment.

3. Shield Dynos: With Shield Private Dynos, our isolated containers for running code include an encrypted ephemeral file system, and restrict SSL termination from using TLS 1.0. Heroku also automatically captures a high volume of security monitoring events for Shield Dynos and databases, which helps meet regulatory requirements without imposing any extra burden on developers.

4. Shield Postgres: Shield Postgres further extends Heroku Postgres to guarantee that your sensitive data is always encrypted, both in transit and at rest. Shield Postgres databases are meant for situations where meeting compliance is a goal of your application and business.

5. Apache Kafka on Heroku Shield: Apache Kafka on Heroku Shield is a fully managed data service certified for handling PHI-, PII-, and HIPAA-compliant data. This enables teams to build high-compliance apps powered by real-time event streaming. This newest managed data service unifies Heroku Shield, which allows enterprises to easily work with real-time data in a secure, trusted, and compliant environment. Apache Kafka on Heroku Shield is available in all six Heroku Shield Private Spaces regions: Dublin, Frankfurt, Sydney, Tokyo, Virginia, and Oregon.

Learn more about Heroku Shield **here**.

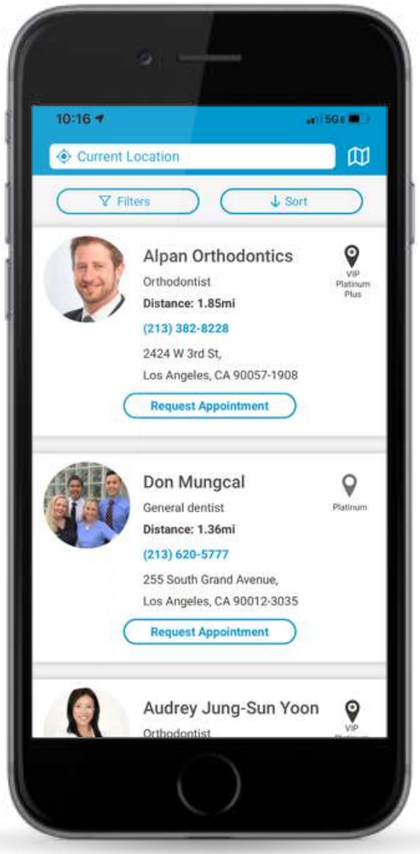
1
2
3
4
5

Build Elastic Engaging Apps *that* Meet Industry Regulations

"Heroku Shield makes HIPAA compliance easier to execute, so now my dev teams can focus on building great apps using a modern app-dev tool set, refer to customer-sensitive data with added confidence, and ultimately provide our customers with an engaging experience that differentiates Align Technology in the marketplace."

— Leela Parvathaneni, Director of Customer-Facing Applications Align Technology

align



Provider Locator App

SmileView App

4

TRUSTED DATA INTEGRATIONS: CONNECT TO DATA STORED *in* OTHER ENVIRONMENTS

Data Protection *in the* Digital Transformation Era

The lifeblood of any application is customer data, and that data can be stored in many different locations. Given how vital data is to any organization's digital transformation efforts, customer data is more valuable than ever before. Information that may have previously seemed trivial to the everyday consumer will actually hold significant value for stakeholders and hackers across the spectrum. Adversaries or real-life data bounty hunters will hunt for new ways to exploit it, governments will seek better ways to access it, enterprises will adopt stronger security measures to protect it, and end users will demand better privacy to secure their personal information.

Customers who use Salesforce and Heroku can rest assured that we will strive to relentlessly protect their important and regulated data within the secure walls of the Salesforce Trust boundary.

However, as app architectures are increasing in complexity, so too are the number of data sources and use cases. No longer are data resources that are used to build customer-facing apps exclusive to just one provider such as Salesforce, but they are now housed in different locations such as on-premises data centers and public cloud providers such as Amazon Web Services (AWS), Google Cloud Platform, and others.

This presents a challenge as developers want the flexibility to have seamless and secure access to these app and data resources while businesses must also ensure that vigilant safety and security standards are met.

Data is key to creating the immersive experiences that engage today's customers. Developers need fast access to data and insights so they can bring the most compelling and relevant apps to market.

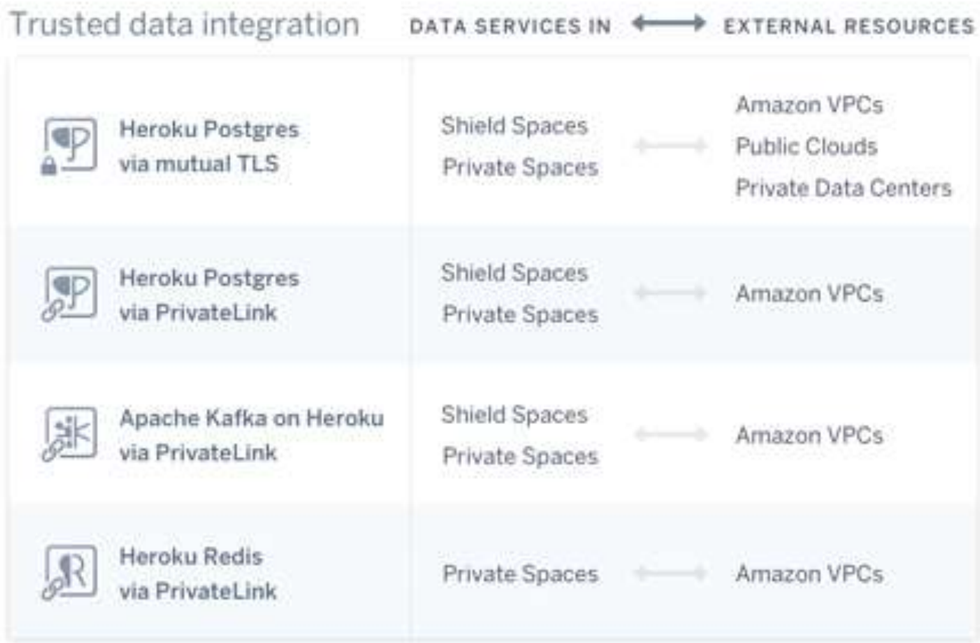
Extending the Value *of* Heroku Postgres

Data is key to creating the immersive experiences that engage today's customers, and developers need fast access to data and insights so they can bring the most compelling and relevant apps to market.

Developers who build apps on Heroku and want to access data resources that are located elsewhere can start with Heroku Postgres. **Heroku Postgres** sits at the heart of most apps deployed on Heroku because it's deeply integrated with four key developer workflows:

1. First, the **"app + Heroku Postgres database"** integration is the original design pattern that drove the first decade of cloud development. It remains a key driver in helping developers scale from an emerging startup to a high-growth company to a massive enterprise on Heroku.
2. Second, the **Salesforce CRM data integration with Heroku Postgres** is the next design pattern that enables developers to build highly personalized apps and experiences. The bidirectional sync of Heroku Connect makes it possible to securely and seamlessly work with and enrich Salesforce CRM data in Heroku.
3. Third, the **Heroku data services (that is Postgres, Redis, Apache Kafka on Heroku) via PrivateLink** integration is the emerging design pattern that unlocks an ecosystem of data resources. With this release, we are providing customers greater architectural choice for building data-centric applications.
4. Finally, **Heroku Postgres via Mutual Transport Layer Security (MTLS)** integration helps developers access data resources that are stored in other public clouds and private data centers in secure ways.

These evolving models of integration now allow Heroku to provide developers with more secure and versatile means to access data resources to build more personalized apps and engaging experiences.

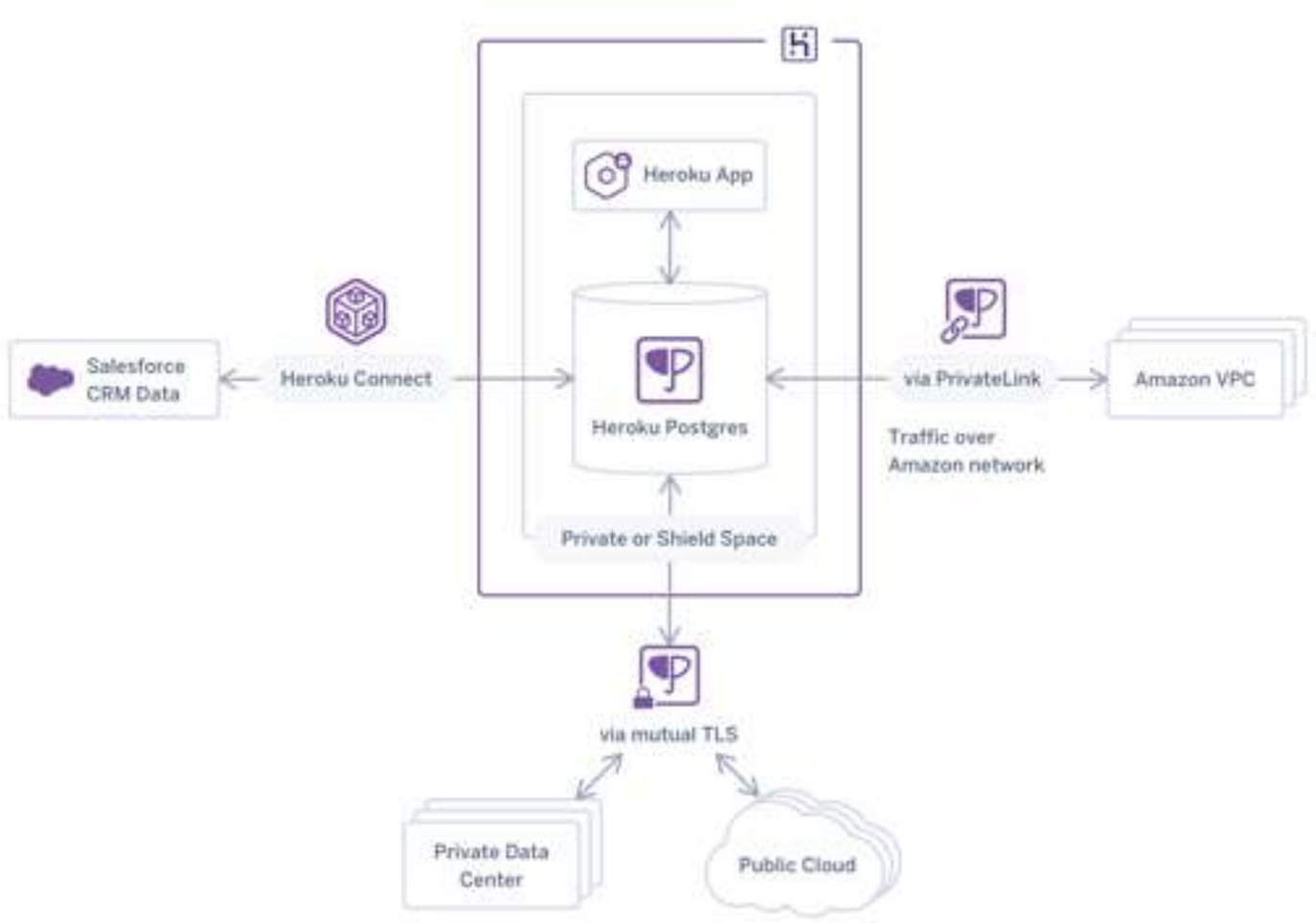


Heroku Postgres via MTLS:
Trusted Data Integrations *with* Other Public Clouds *and* Private Data Centers

This integration allows customers to easily encrypt and mutually authenticate connections between Private and Shield Postgres databases and resources running in other public clouds and private data centers.

Heroku Postgres via MTLS requires that both the server and the client verify their certificates and identities to ensure that each one is authenticated and authorized to share data. For additional security, Heroku requires a whitelisted IP or IP range for the client and valid Heroku Postgres credentials. We also log the creation of a MTLS connection, notify admin members on the account, and periodically send reminder notifications as long as it is live.

The entire MTLS configuration and lifecycle is managed by Heroku to maintain security and meet compliance standards. It's designed to be configured once and updated every year with new certificates, so the integration recedes into the background of the developer workflow. Get started with Heroku Postgres via MTLS.



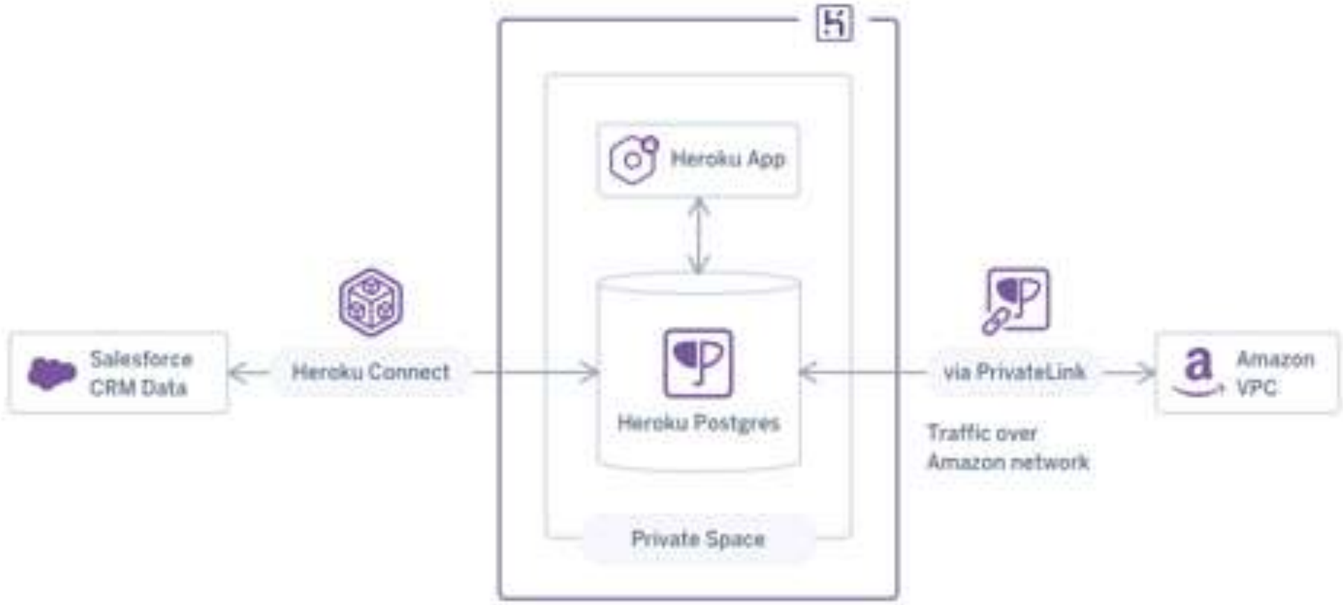
Trusted Data Integrations Between Heroku *and* Amazon Web Services (AWS)

Heroku Postgres via PrivateLink

Heroku Postgres via PrivateLink provides customers with secure, scalable, and durable connections because traffic to and from Heroku Postgres stays on the Amazon private network. Once a PrivateLink is set up, customers have greater architectural choice when it comes to building data-centric applications with resources in both Heroku and AWS. This makes Heroku Postgres an even more powerful presence in distributed app architectures for the following reasons:

- Developers can now create more scalable and secure external connections to Heroku Postgres.
- Developers can now build more sophisticated app architectures that combine resources running on Heroku and AWS. Anything that runs in an Amazon VPC is now accessible to Heroku Postgres via PrivateLink.
- Developers can now access complimentary AWS resources for use cases like OLAP, archive, and more, all directly from Heroku Postgres. These same AWS resources can write back to Heroku Postgres to enrich and increase the value of CRM data.

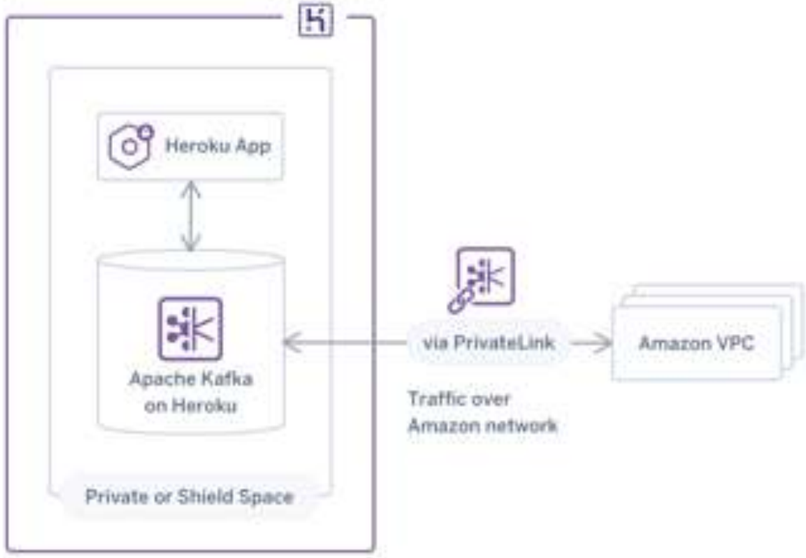
Heroku also provides PrivateLink support for **Heroku Postgres in Shield Spaces**, so that sensitive and regulated data can flow securely and seamlessly between Heroku and AWS. We now log the creation of a PrivateLink, notify admin members on the account, and periodically send reminder notifications as long as it is live. We have also applied these changes to the Private Space version. **Get started with Heroku Postgres via PrivateLink**.



Apache Kafka on Heroku via PrivateLink

We also now provide the same PrivateLink support for Apache Kafka on Heroku in Private and Shield Spaces. In addition to **Apache Kafka on Heroku Shield**, Apache Kafka on Heroku now has the ability to integrate with Amazon VPCs for true multicloud architectures and best-of-breed solutions. We log, notify, and remind customers as long as this integration is live.

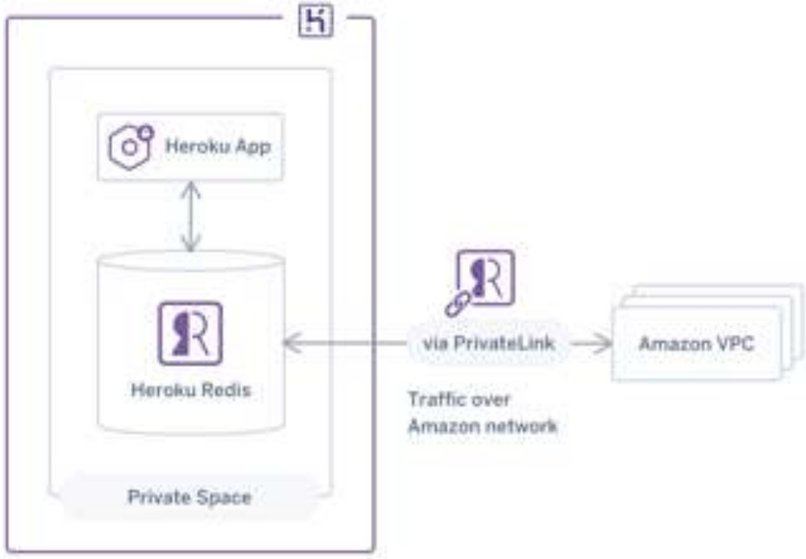
Get started with Apache Kafka on Heroku via PrivateLink.



Heroku Redis via PrivateLink

Finally, we now provide the same PrivateLink support for Heroku Redis in Private Spaces. Likewise, we log, notify, and remind customers while the integration is live.

Get started with Heroku Redis via PrivateLink.



5

HEROKU'S SECURITY *and* TRUST FOUNDATION

1
2
3
4
5

Application Security

Customer Application Isolation

Each application on the Heroku platform runs within its own isolated environment and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using Linux containers, while host-based configurations restrict applications from establishing local network connections.

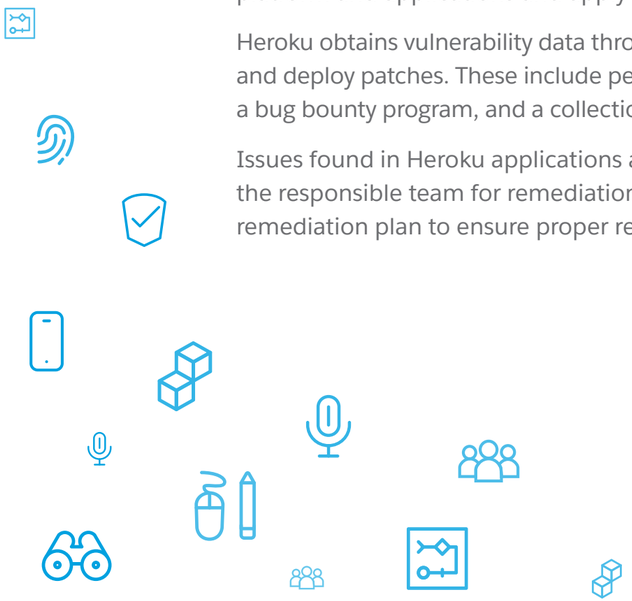
For additional technical information, see **devcenter.heroku.com/articles/dyno-isolation**.

Secure Software Development Lifecycle (SSDLC)

Heroku undergoes extensive internal penetration tests, vulnerability assessments, and source code reviews to assess the security of the application, architecture, and implementation. Third-party security assessments cover all of Heroku's platform surface area, and tests for Application Security classifications, including testing for OWASP Top Ten, WASC Threat Classification, and customer application isolation. Heroku works closely with external security assessors to review the security of its platform and applications and apply best practices.

Heroku obtains vulnerability data through a variety of sources to detect vulnerabilities and deploy patches. These include periodic, external and internal penetration tests, a bug bounty program, and a collection of open-source community vulnerability data.

Issues found in Heroku applications are risk ranked, prioritized, and assigned to the responsible team for remediation, and Salesforce's security team reviews each remediation plan to ensure proper resolution.



Heroku practices a secure development lifecycle, and the Salesforce security team works closely with the engineering team, from architecture review through source code review and penetration testing of all high-risk features. The security team is included in quarterly planning to track the security implications of upcoming feature work and identify the highest-risk projects. Projects identified as high risk are tracked for security team review. The process includes an initial security assessment, guidelines for secure coding, periodic, and external and internal penetration tests, all performed or supervised by the security team.

Heroku leverages a platform integration testing service that runs end-to-end tests from the perspective of external Heroku users, a process that exercises the different services needed to deliver user-facing functionality. This service supports both one-off test runs and continuous running of tests for monitoring purposes. Heroku also uses third-party testing tools for repository-level testing of platform software components.

Patch Management

The Heroku platform itself is continually upgraded and improved, usually with no effect on a customer's running application. If downtime is required for noncritical patches of a Heroku Postgres database, customers are given the opportunity to schedule their maintenance window for upgrades. OS patches can be deployed rapidly and invisibly to the customer. The vulnerability management process is designed to remediate risks with minimal customer interaction or impact.

Patch Notification

Heroku patches continuously, and as needed. Typically, Heroku does not notify customers about minor patches, but posts notifications to the Heroku Changelog for more important releases. If patches have a customer-facing impact – for example, a database upgrade that might require downtime – Heroku notifies customers in advance and provides a maintenance window.

These changes are also communicated on the Heroku status site: **status.heroku.com**.

Network *and* Infrastructure Security

Server Hardening

Heroku hardens its OS images (stacks) by turning off all services and components by default, and only enabling those that have a justified business and operational purpose. These stacks are constantly enhanced and used to regularly refresh systems components. This utilization of immutable servers provides a current and constantly updated underlying operating system environment for all Heroku components that almost entirely eliminates configuration drift.

Dyno Container Hardening

Heroku takes several precautions within the kernel to reduce the risk that a kernel bug could lead to the compromise of a host. Heroku filters syscalls using secure computing mode (seccomp), a security facility that provides application sandboxing in the Linux kernel. Containers are configured to explicitly deny root inside containers and drop several capabilities while executing inside containers, including the ability to mount filesystems or load kernel modules.

There are some distinctions between the Heroku Common Runtime environment and the Heroku Private Spaces/Shield Private Spaces Runtime environment. Heroku Common Runtime is a blend of both multitenant and single tenant architecture, and containers leverage tools that utilize Linux Security Module to restrict programs and protect Linux services.

Heroku Private Spaces/Shield Private Spaces Runtime provides substrate account-level complete isolation between tenants.

Secure Network Architecture

Heroku's Private Space network architecture is publicly documented, and network services are isolated based on the classical n-tier architecture to limit any potential incident's blast radius.

Host-based configurations restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based configurations also provide the ability to further limit inbound and outbound connections as needed.

Data in Motion

All data in transit between instances is encrypted by default via SSL/TLS. This means that all traffic between single-tenant dynos and Private Spaces Runtime are encrypted, but communication between multitenant dynos running within the same instance may be unencrypted unless you've configured your application to encrypt such traffic. Encryption algorithms are chosen by browser/endpoint negotiation. All internet traffic is encrypted by default.

Distributed Denial of Service (DDoS) Mitigation and Intrusion Prevention & Detection

Heroku is built on IaaS by major public cloud providers that have strong mitigation in place for network-layer DDoS attacks. Our operations and security teams are able to quickly respond to events and enable additional DDoS mitigation controls on a progressive basis when an attack is underway. As a customer, you may consider enabling additional controls to protect against flaws in your deployed code, including the use of a content delivery network (CDN) with additional features potentially available in your application framework.

Heroku utilizes the following capabilities, along with the DDoS mitigations, together to provide preventive and detection controls that are traditionally covered by intrusion detection and prevention appliances:

- Heroku monitors various threat intelligence channels for notifications of disclosed defects or vulnerabilities, and the availability of mitigating configuration guidance or software patch availability to constantly enhance base images used to regularly refresh system components on immutable services.
- Heroku maintains a mature secure software development lifecycle (SDLC or SSDLC) process that includes requirements and guidance for secure coding practices and patterns, initial and ongoing security review of new features and functionality, internal and external penetration testing, as well as periodic red-team assessments. Each stage in this process is proactively monitored and managed to drive the remediation of discovered defects, vulnerabilities, or misconfigurations within well-defined time lines. In addition to our own efforts to uncover items in need of remediation, we operate a public Bug Bounty Program and strongly encourage our customers to work with us to identify issues as they encounter them through the process of testing their own applications running on the Heroku platform.
- Heroku utilizes a number of related processes and techniques for detecting and managing misuse, abuse, crime, and malicious utilization of the platform itself. As a Heroku user, running your code on our platform is precisely what we do, and sometimes, malicious actors run their code on our platform. Our dedicated Computer Security Incident Response Team (CSIRT) and Abuse Team have built capabilities into the platform that provide effective assessment and disruption of malicious actors.

Man in the Middle and IP Spoofing

Managed boundary restrictions prevent spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure, including the hypervisor, which will not deliver traffic to an interface that it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further mitigate risk at all levels.

Customer Data Security

Customer Data Storage

Customer data is stored in Heroku Postgres, which is a managed database service with access-controlled logically segregated databases. Each Heroku Postgres database requires a unique username and password valid only for that specific database. Customers with multiple applications and databases are assigned separate database instances and accounts.

Customer connections to Postgres databases require SSL encryption to ensure a high level of security and privacy. When deploying applications, Heroku encourages customers to take advantage of encrypted database connections. Stored data can be encrypted by customer applications in order to meet data security requirements. Customers can implement data storage, key management, and data retention requirements when developing their application.

Customer Data Encryption

Heroku's paid Heroku Postgres plans, Apache Kafka on Heroku and Heroku Redis, encrypt data at rest by using AES-256, block-level storage encryption. Data encryption is implemented using the AWS EBS disk encryption feature. Encryption keys are fully managed by AWS and are not visible to Heroku or Heroku customers. Postgres access credentials are also encrypted at rest.

Customer Data Retention and Destruction

Heroku customers define the data that is stored by their applications, and it is the customer's responsibility to purge data from databases to comply with data-retention requirements. If a customer deprovisions an application and any associated database, Heroku maintains the database's storage volume for at least one week, after which time it is automatically destroyed, rendering the data unrecoverable within 30 days. Physical storage volumes are securely destroyed at their end of life.

Security Monitoring

Privileged Access

Heroku-managed privileged access to the production infrastructure hosting Heroku Services requires use of secure SSH connections, strong passwords, and several layers and types of multifactor authentication. Heroku staff does not access or interact with customer data or applications as part of normal operations. There may be cases when Heroku is requested to interact with customer data or applications at the request of the customer for support purposes or when required by law. Customer data is access-controlled and all access by Heroku staff is accompanied by customer approval or government mandate, reason for access, actions taken by staff, and support start and end time.

Heroku employee access is logged, and our security operations team is continually identifying better ways to identify, investigate, and report on those types of actions. Pointedly, state machines managing the databases make a lot of noise, and operator access is rather rare at scale.

Logging and Network Monitoring

Heroku security and engineering staff monitor various tools and log feeds to detect anomalous behavior. The teams review authentication events, sudo requests, data traffic patterns, and other data sources.

From a network perspective, Heroku collects access logs and continually reviews them for indications of abuse or inappropriate access. Heroku also receives abuse data from its infrastructure-as-a-service provider.

The Heroku logging stream is based on logplex, a logging router that shuttles logs around to their eventual destination (called a "drain"). Heroku hosts a single-tenant instance of a log aggregation and analysis tool as the drain of record and analytics engine for logs.

Business Continuity *and* Disaster Recovery

The Heroku platform is designed for stability and scaling. The platform inherently mitigates common issues that lead to outages while maintaining recovery capabilities. The platform maintains redundancy to prevent single points of failure, is able to automatically replace failed components, and is deployed across multiple data center availability zones. In the case of an outage, the platform can be recovered using current system images and data stored in backups. After any service-impacting incident, the Heroku team determines root cause, impact to customers, and improvements to the platform and processes to prevent future incidents.

In the event of an interruption of Heroku services, details on severity, impact, and duration are posted on the status page: **status.heroku.com**.

As a business unit of Salesforce, Heroku adheres to Salesforce's global Business Continuity Management program, which includes business continuity plans (BCPs) for critical departments and functions across the organization that are integrated and aligned with site-specific emergency response plans (ERPs) and crisis management plans (CMPs) at a regional and global level. Heroku also maintains a disaster recovery plan, which is updated and tested continually as Heroku creates and removes computing resources. The operations teams review capacity and availability metrics on a daily basis to ensure that the platform is highly resistant to any outages.

Compliance *and* Privacy

As consumer data and its monetization potential grow in significance, so do the privacy challenges wrought by current and new regulations. In Europe, the **General Data Protection Regulation (GDPR)** that went live in 2018 places pressure on multinationals to ensure that customer data that is captured is handled in a compliant and secure manner. And in the U.S., regulations such as **HIPAA, PICA,** and the new **California Consumer Privacy Act (CCPA)** that went live in 2020 place additional responsibility on companies to ensure that their management of their customers' personal information meets the strict compliance standards set forth by these regulations. Failure to do so can lead to costly penalties and the loss of consumer trust.

Heroku's Compliance and Privacy Credentials

Compliance is an essential component of the trust we have with our customers, and we see compliance as the byproduct of a relentless focus on security and engineering excellence. Heroku is not secure because we are compliant; we are compliant because we are secure. This is evident in the list of compliance certifications that make Heroku world class.

Please refer to our compliance website for additional details regarding these security and privacy-related audits and certifications: **heroku.com/compliance**.

PCI DSS Level 1 | Service Provider
The Payment Card Industry Data Security Standard (PCI DSS) is a widely understood and accepted security standard for cardholder data.

HIPAA | Protected Health Information
The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. Customers who want to build healthcare applications on Heroku that comply with U.S. HIPAA requirements should contact their account representative about completing a Business Associate Addendum with Heroku.

ISO 27001 | Security Management Controls
ISO 27001 is a widely recognized and internationally accepted information security standard that specifies security management best practices and comprehensive security controls following ISO 27002 best practices guidance.

ISO 27017 | Cloud Specific Controls
ISO 27017 is a standard that provides additional guidance and implementation advice on information security aspects specific to cloud computing.

ISO 27018 | Personal Data Protection
ISO 27018 establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect personally identifiable information (PII) in accordance with defined privacy principles for public cloud computing environments.

SOC1 Type 2 | Internal Controls over Financial Reporting Systems
SOC1 Type 2 is an independent examination of the IT general controls and controls around availability, confidentiality, and security of customer data process by the Heroku platform relevant for the financial reporting of customers.

SOC2 Type 2 | Security, Availability, and Confidentiality Reports
The restricted-to-use SOC2 Type 2 report is an independent examination of the fairness of presentation and the suitability of the design of controls relevant to security, availability, and confidentiality of the customer data processed by the Heroku platform.

SOC3 | Public Report of Security, Availability, Integrity, Confidentiality, and Privacy Controls
The general use SOC3 report is an independent examination of the fairness of presentation and the suitability of the design of controls relevant to security, availability, and confidentiality of the customer data processed by the Heroku platform.

Case Study: Remediation of Meltdown *and* Spectre Security

One of the most significant challenges that CIOs and CTOs continue to face is protecting and ensuring that the technology environments they are responsible for consistently deliver the business-critical solutions their organization and teams need to achieve their work. Given that customers no longer tolerate downtime, let alone data breaches, IT leaders are tasked to work closely with CISOs and their security teams to better anticipate, safeguard, and prevent potential threat vectors ahead of time in order to preserve the trust of their customers.

Heroku is a powerful component of Customer 360 built on a deep security foundation designed to protect customers' trust. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including the protection of customer data. The following case study highlights some key security components and use cases we have in place to protect your customer data on the Heroku platform.

On January 3, 2018, researchers disclosed a security vulnerability affecting side-channel analysis of speculative execution on modern computer processors (CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754). These became known as Meltdown and Spectre.

Heroku's product security team follows emerging trends and partners closely with the research community. We invest heavily in facilitating conversations regarding vulnerabilities and keeping our customers safe via community partnerships.

In the case of emerging and recently announced vulnerabilities (including those embargoed or leaked to the press), we have a proven methodology for ingesting, processing, and prioritizing mitigation work. Our team utilizes these methods to address vulnerabilities as material or actionable information is made available.

Our security and platform teams worked closely with AWS and Canonical (makers of the Ubuntu Linux operating system) to investigate and patch any affected systems related to the Meltdown and Spectre announcements.

On January 5, 2018, 13:30 PT, **AWS completed its patch deployment** addressing tenant isolation threats. AWS reported it had restored the expected multitenancy protections similar to dedicated hardware, which left Heroku to address the kernel vulnerabilities in runtime host operating systems.

Heroku Performance, Private, and Shield dynos feature varying degrees of isolation from potentially hostile neighbors. However, the shared Common Runtime carries our highest priority for Meltdown (variant 3) mitigation work due to the nature of its shared infrastructure.

The ideal fix was to deploy the updated kernel from Canonical prior to the release of functional proof-of-concept exploit code for this vulnerability. As this patch was not yet available, the Heroku security team opted for a more rapid response.

Heroku engineering prepared our own upstream kernel deployment as an aggressive measure to protect the shared Common Runtime. We began deploying this update as quickly as possible.

Heroku fully deployed this update to the U.S. and EU shared Common Runtime, which was replaced when the official **Canonical update** was made available.

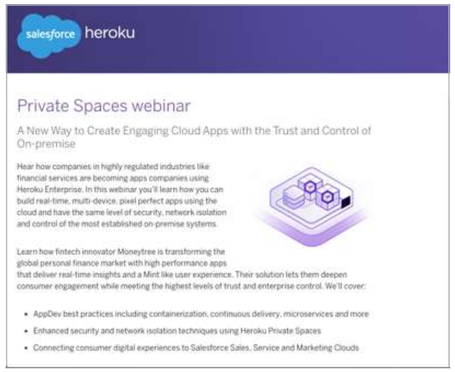
Learn more about Heroku

See Trailhead

Learn to Develop Apps with Heroku

See Webinar

Architect HIPAA and High-Compliance Apps with Heroku Shield



See Webinar

Private Spaces Webinar: Cloud Apps with the Trust and Control of On Premises


salesforce