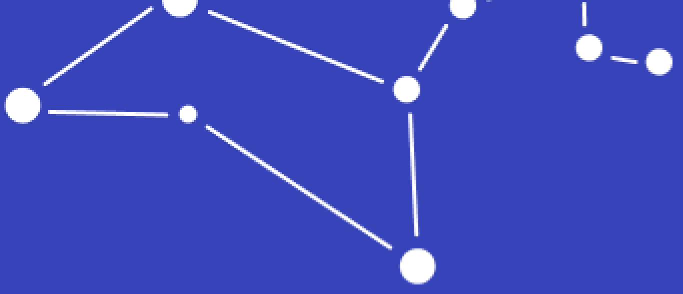
DevOps for FinTech

Unlocking the Benefits and Best Practices



gart.

Main Challenges Faced by FinTech companies without DevOps

01 **Regulated Industry**
One of the most regulated industry due to compliance standards **(SOC2, PCI DSS, ISO27001, etc)**

02 **Stability of Operations**
Delays in new features and updates deliver

03 **Siloed Teams**
Inefficient collaboration and lack of transparency between development, operations, and QA

04 **Frequent Downtimes**
Due to frequent updates and maintenance issues

05 **Data security**
Neglecting DevSecOps practices and compliance on early stage of development process.

Benefits of Using DevOps in FinTech

Better release cadence

Faster deployments

Increased reliability

Improved security and compliance

gart.

Better release cadence
Top DevOps teams deploy new code 208 times more frequently than WHOM.

Faster deployments
The best teams deploy 973x more frequently and have lead times **6750x faster** when compared to low performers.

DevOps practices enable FinTech companies to streamline and automate their software development and deployment pipelines. This, in turn, reduces time-to-market for new features and updates. In an industry where agility is key, this speed is a significant advantage, as it allows FinTech companies to respond swiftly to market changes and customer demands.

Increased reliability
Mature adopters have a 3X lower rate of failure.
The automated testing and continuous integration inherent in DevOps ensure that FinTech products and services are thoroughly checked for quality and reliability throughout the development process. With fewer bugs and issues, customers can trust in the consistency of services, promoting customer loyalty and satisfaction.

Improved security and compliance
High performers spend 50% less time fixing security issues compared to low performers thanks to better-documented development, testing processes, clear frameworks for application governance and security.

List of Standards Impacting DevOps Practices in FinTech

List of Standards Impacting DevOps Practices in FinTech

SOC2

PCI DSS

ISO 27001

FINRA

HIPAA

NIST

GLBA

CFTC

FERPA

BCBS 239

EU MiFID II

CCPA

PSD2

Compliance as Code

The FinTech industry is indeed one of the most regulated sectors, and adhering to various compliance standards is essential.

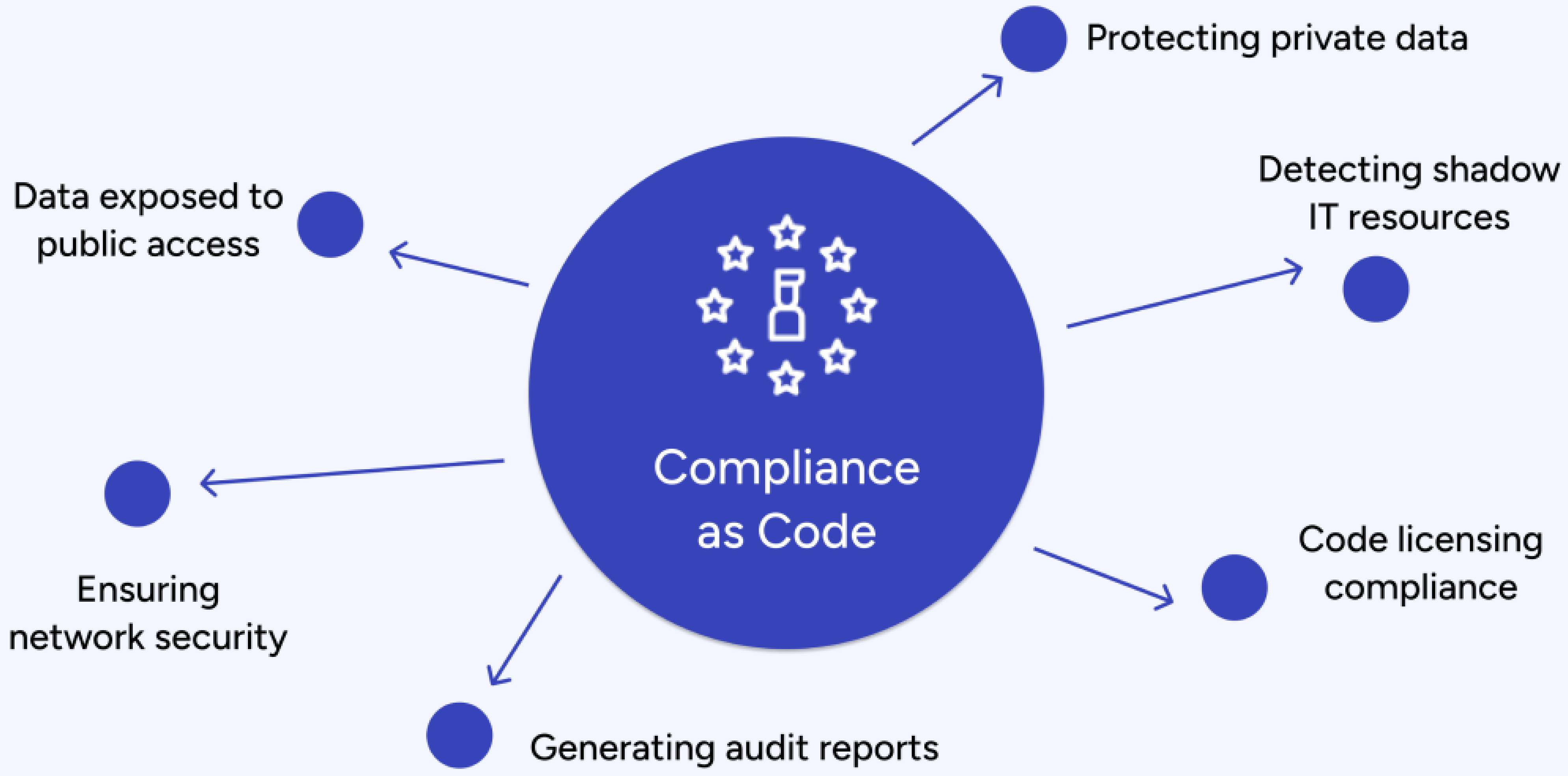
There are here lots of standards that can significantly impact DevOps practices in the FinTech industry:

SOC2 (Service Organization Control 2) is an auditing and reporting framework designed for service organizations, including those in the FinTech industry, to assess and demonstrate the security, availability, processing integrity, confidentiality, and privacy of customer data.

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to safeguard credit card data and prevent fraud. It applies to any organization that processes, stores, or transmits cardholder data, making it highly relevant to FinTech companies involved in payment processing.

ISO 27001 (International Organization for Standardization 27001) is an internationally recognized information security management system (ISMS) standard. It provides a systematic approach for managing information security risks and ensuring the confidentiality, integrity, and availability of sensitive information.

For FinTech companies, regulatory compliance is non-negotiable. To streamline compliance efforts, implement “Compliance as Code” by integrating regulatory requirements directly into your code and automation processes. This ensures that compliance is built into your software from the ground up, reducing the risk of costly violations.


Protecting private data
Data exposed to public access
Detecting shadow IT resources
Compliance as Code
Ensuring network security
Code licensing compliance
Generating audit reports

FinTech companies operate in a heavily regulated environment. Automate compliance checks, documentation, and reporting to ensure that your DevOps processes align with financial regulations. This helps in maintaining audit trails and ensures that your organization is always compliant.

gart.

Immutable Infrastructure for Security

Embrace the concept of immutable infrastructure, where servers and environments are treated as disposable entities that can be easily recreated. This reduces the risk of configuration drift and makes it simpler to maintain a secure and consistent environment.

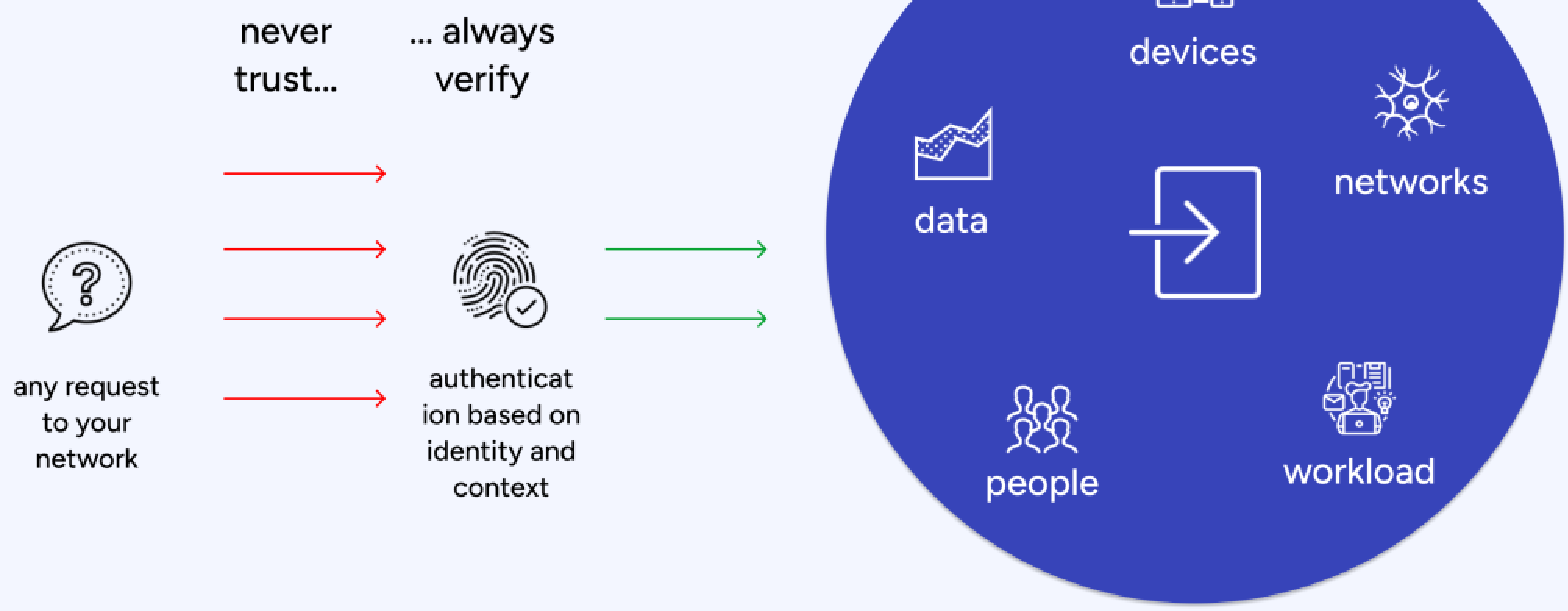
	Mutable	Immutable
pros	Does not need to build servers from scratch every time a change is required	• Declarative • Predictable state • Auditable • Easy to roll back • Modular
cons	• Incremental changes can fail • Indiscrete versioning	• Unable to modify in place • Misaligned with traditional IT practices

gart.

Zero Trust Security Model

Adhere to a “Zero Trust” security model, which assumes that threats can exist both outside and inside your network. Implement stringent access controls, multi-factor authentication, and micro-segmentation to protect sensitive financial data and critical systems.

Zero Trust Security Model



never trust...

... always verify

any request to your network

authenticat ion based on identity and context

devices

networks

data

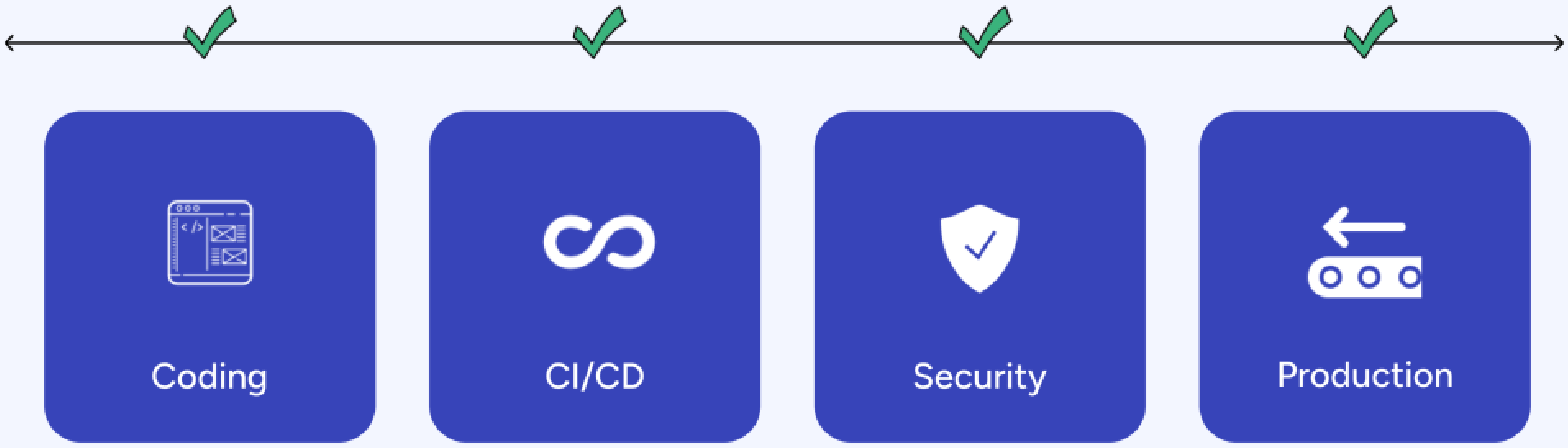
people

workload

Secure Software Supply Chain

In the FinTech industry, securing the software supply chain is paramount. Ensure that your DevOps pipeline is secure from end to end, including third-party dependencies, and utilize automated scanning and verification tools to prevent the introduction of malicious code.

Secure Software Supply Chain



Coding

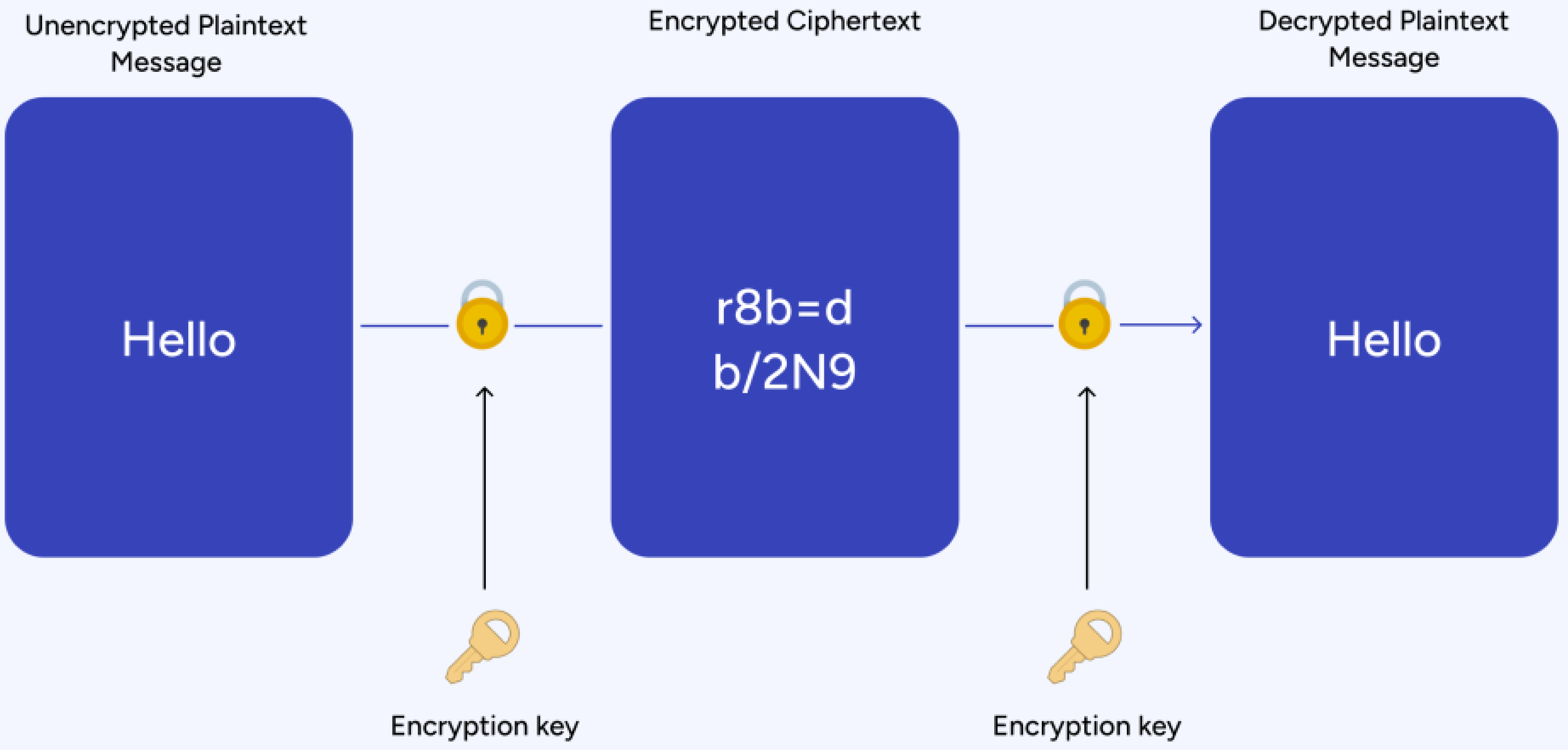
CI/CD

Security

Production

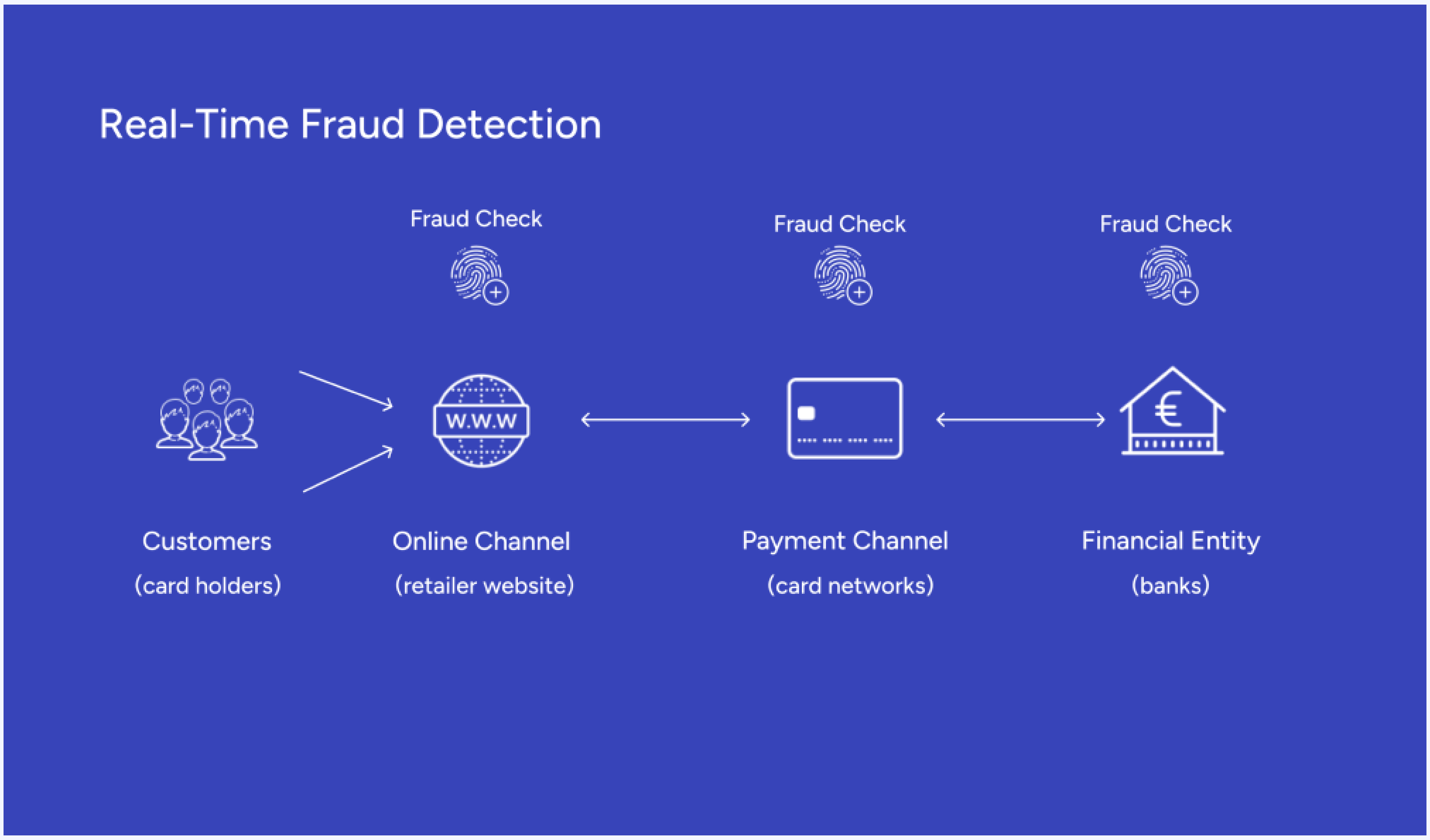
Financial Data Encryption

Encrypt financial data both in transit and at rest. Utilize strong encryption algorithms and enforce encryption protocols to protect sensitive information, ensuring it remains confidential and secure.



Real-Time Fraud Detection

Implement real-time fraud detection and prevention mechanisms within your DevOps pipeline. Utilize machine learning and AI to detect suspicious financial activities as they occur, helping prevent fraud in real-time.



Real-Time Fraud Detection

Fraud Check

Fraud Check

Fraud Check

Customers (card holders)

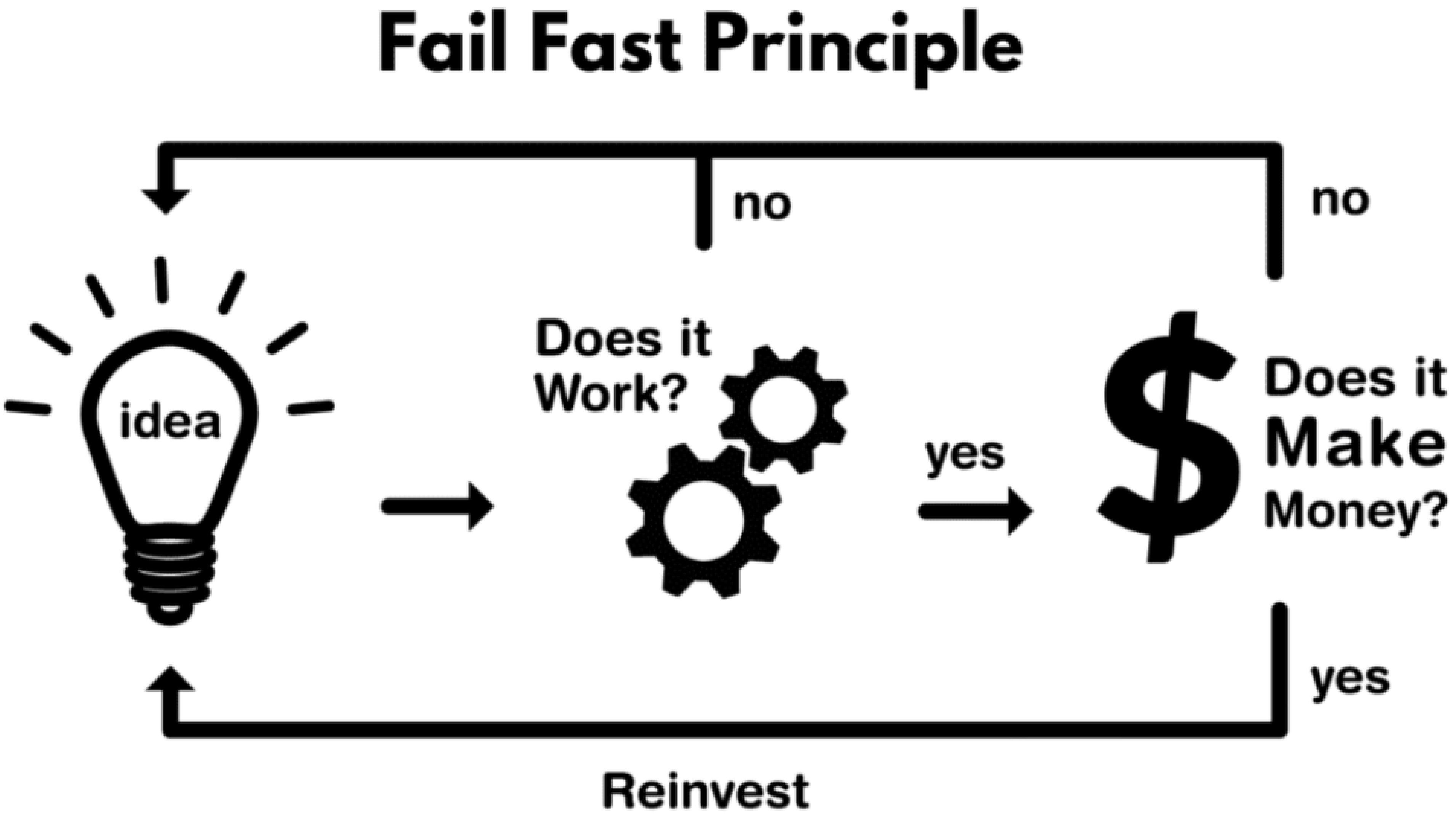
Online Channel (retailer website)

Payment Channel (card networks)

Financial Entity (banks)

Fail Fast, Learn Faster

Embrace a culture of experimentation and learning. Encourage teams to take calculated risks, with the understanding that failures are opportunities for improvement. Post-mortems and retrospectives are essential for continuous learning and enhancement of processes.

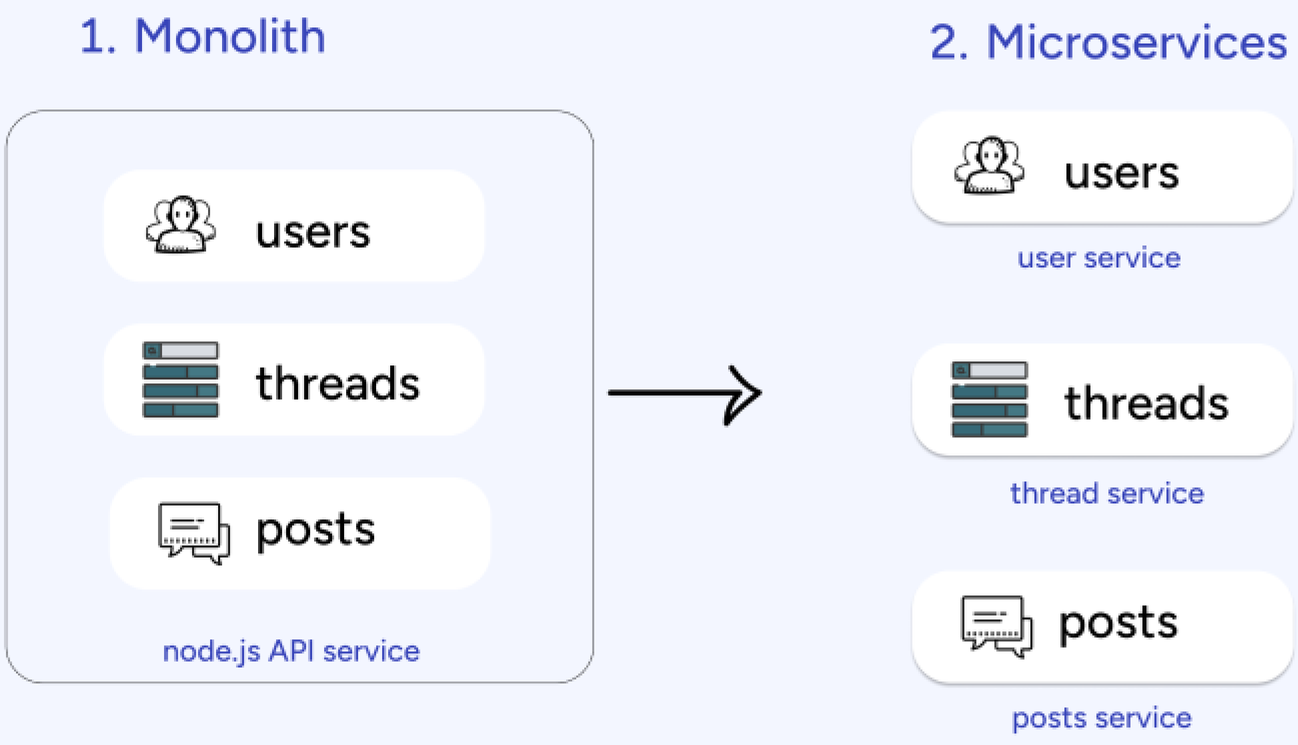


Microservices Architecture

SaaS solutions aren't constructed as large, monolithic applications that rely on a complex network of servers.

Microservice architecture is like building a digital system using small, independent building blocks (microservices) that work together. Each building block does a specific job, and they all communicate to create a complete, flexible, and efficient system.

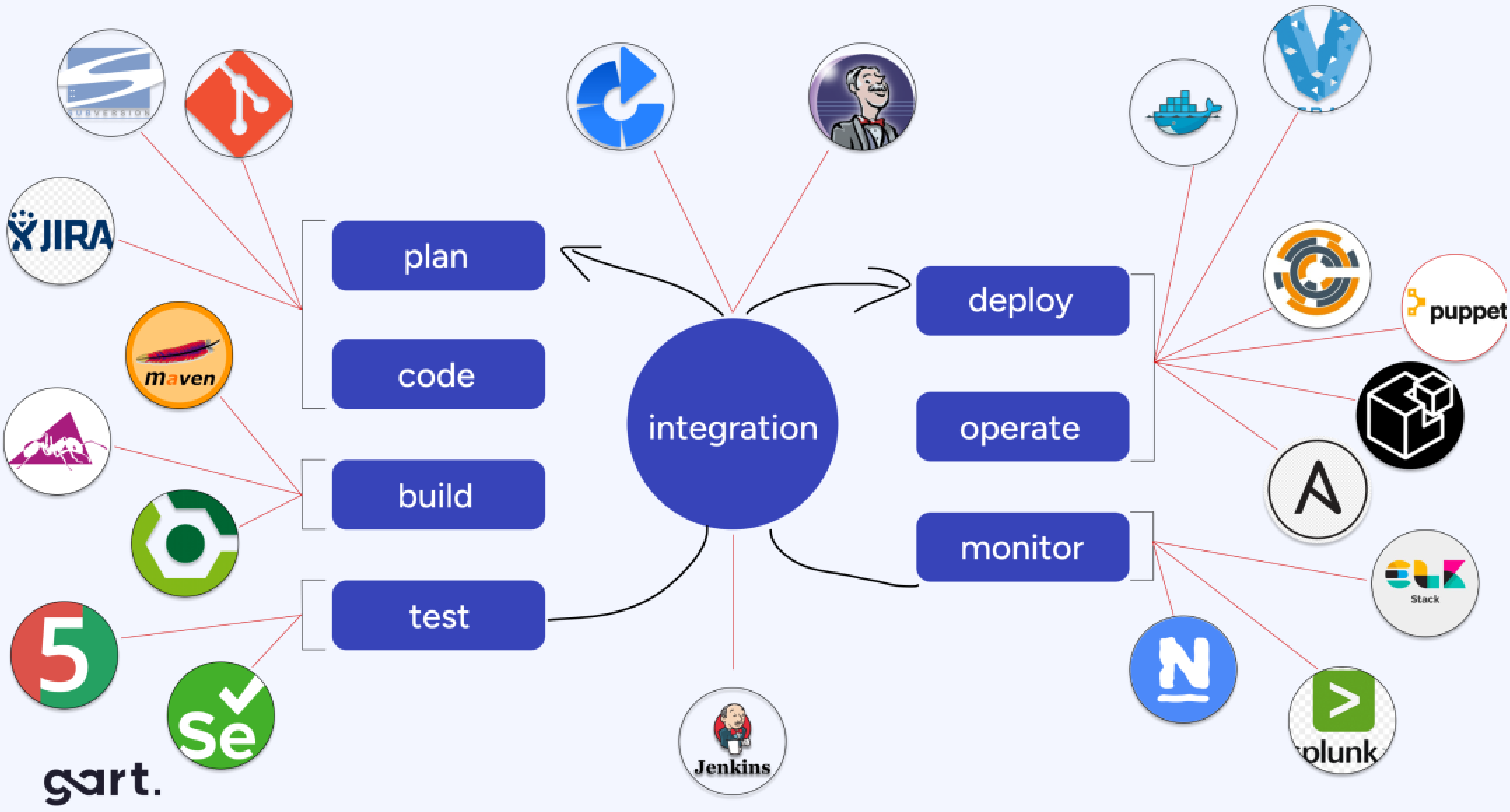
It's similar to assembling a collection of LEGO pieces to construct a complex structure, where each piece serves a unique purpose and can be changed or improved without affecting the entire creation. This approach makes it easier to develop, scale, and maintain software.



gart.

Real-Time Monitoring and Analytics

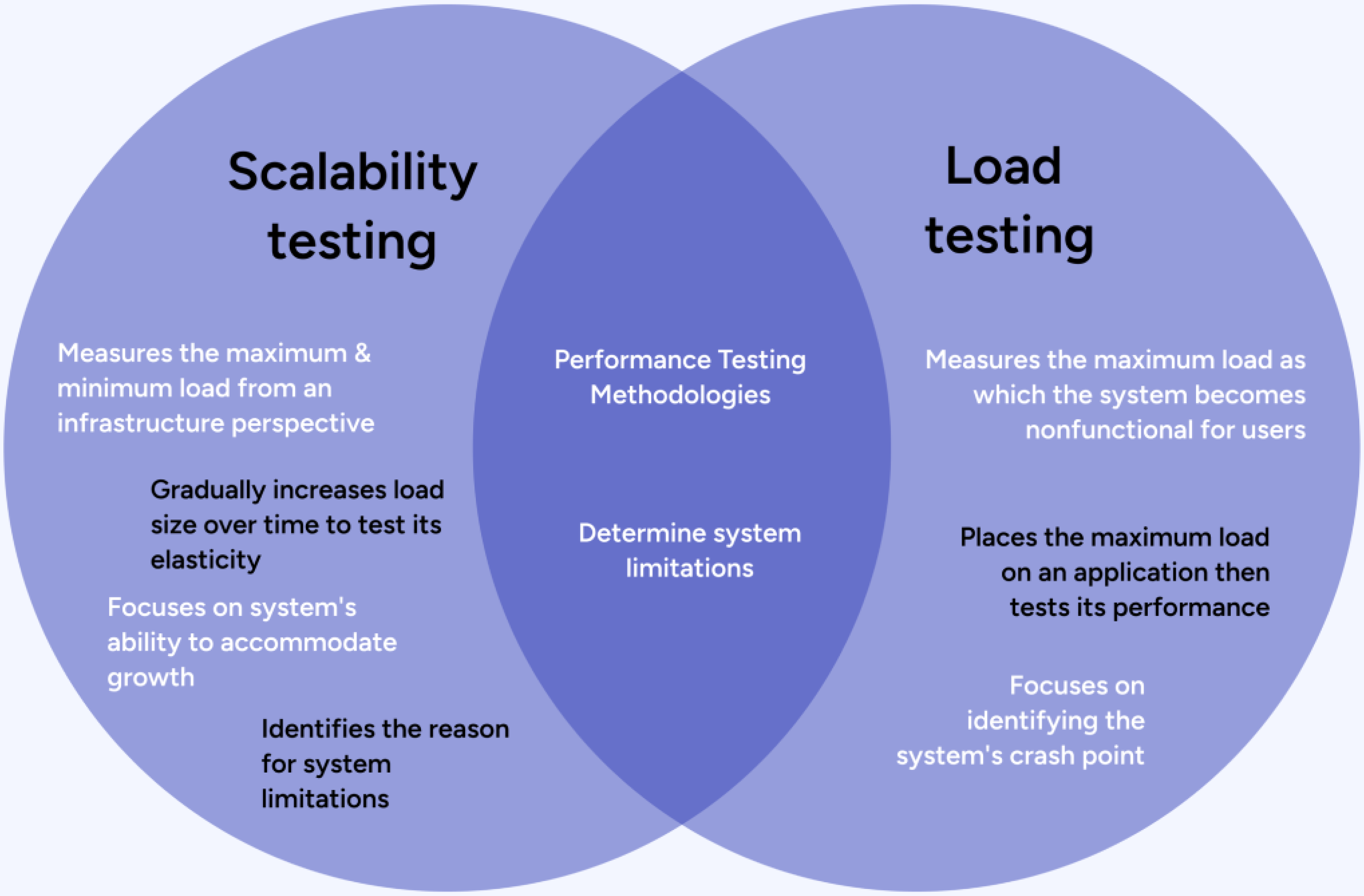
Fintech companies use DevOps for real-time monitoring and fast issue detection. The financial technology sector relies on real-time data to ensure the security, reliability, and scalability of their systems.



gart.

Load Testing for Scalability

Load testing is a critical component of DevOps in the fintech industry, where scalability and reliability are paramount. Fintech applications and systems need to handle high volumes of transactions, often with stringent security and compliance requirements.



Scalability testing

Measures the maximum & minimum load from an infrastructure perspective

Gradually increases load size over time to test its elasticity

Focuses on system's ability to accommodate growth

Identifies the reason for system limitations

Performance Testing Methodologies

Determine system limitations

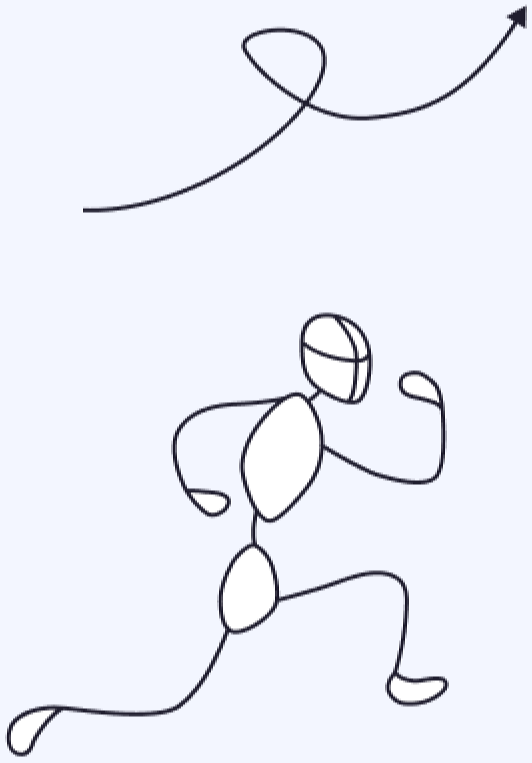
Load testing

Measures the maximum load as which the system becomes nonfunctional for users

Places the maximum load on an application then tests its performance

Focuses on identifying the system's crash point

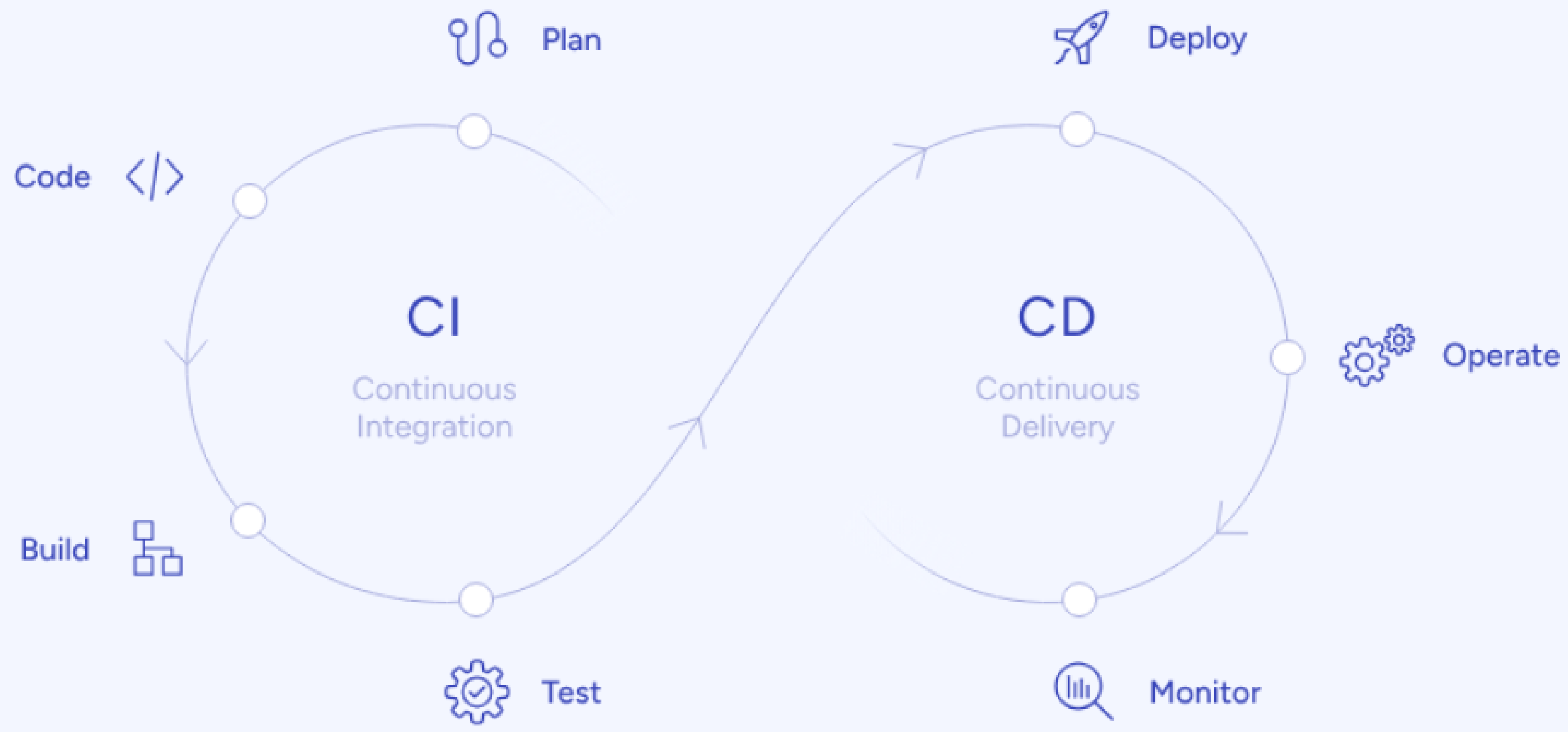
Top 10 DevOps Practices for FinTech



gart.

CI/CD for financial institutions

Implement CI/CD pipelines to automate the build, test, and deployment processes. This accelerates development and reduces the chance of errors in the production environment. Frequent deployments also make it easier to implement necessary updates and security patches promptly.



The adoption of Continuous Integration (CI) and Continuous Delivery (CD) for FinTech and financial institutions promising swifter, more stable, and highly predictable code deployments.

Benefits of CI/CD

- **Faster Time to Market**

Embracing automation paves the way for rapid code deployment into production, free from any service interruptions.

- **Agility and Responsiveness**

CI/CD empowers you to build and test swiftly within a secure sandbox environment. It enables your teams to experiment, detect and resolve bugs and integration challenges promptly, ensuring the release of fully refined and functional software.

- **Increased Productivity**

Implementing CI/CD allows the development team to stay more productive. CI/CD for FinTech eliminates rework and wait time. By automating routine processes, developers can focus on other more crucial tasks, such as code quality or security.

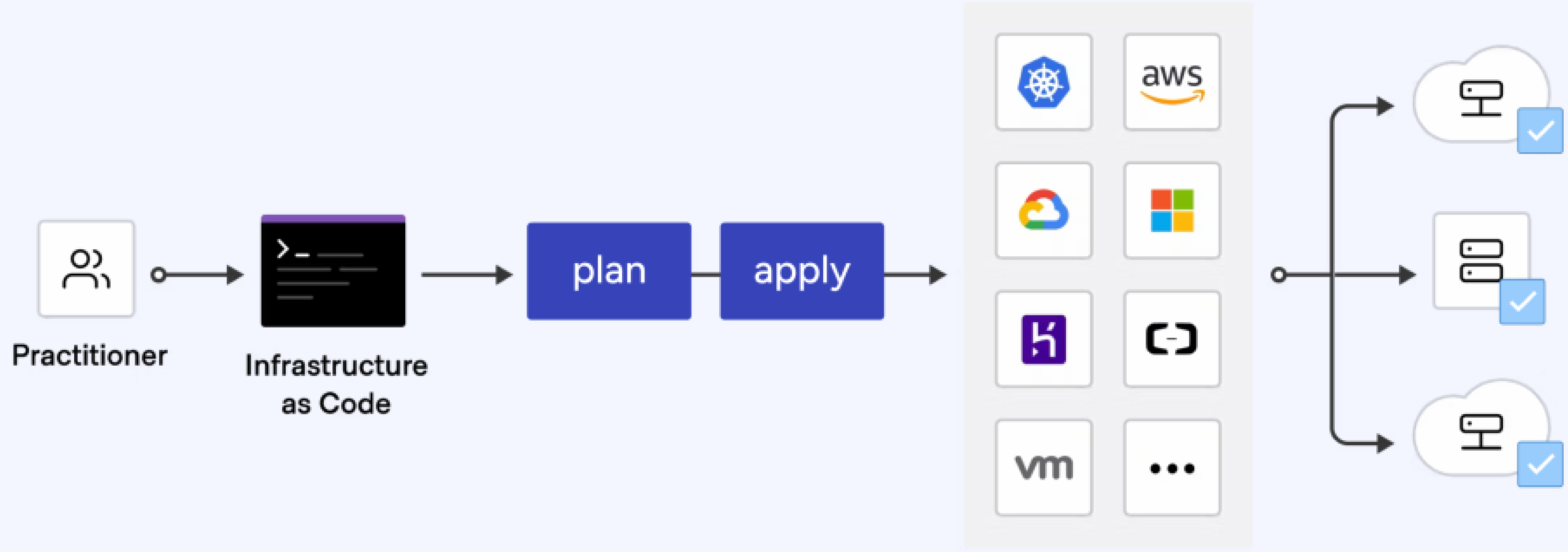
- **Superior Product Quality**

CI/CD's seamless automation guarantees heightened reliability, early error detection and meticulous risk assessment, enhancing the overall quality of the end product.

Infrastructure as code (IaC)

Instead of programming configurations manually, testing and deploying – with IaC your teams can build up the environment you need to develop and test new products in one click and with less risk.

Infrastructure as code (IaC)



Treat infrastructure components as code, allowing for automated provisioning, configuration, and management of resources. This approach ensures consistency across environments and facilitates disaster recovery and scalability.

Benefits of IaC for financial application development

- **Faster development and deployment**

IaC accelerates team performance at every stage of the SDLC. Provision CI/CD and testing environments in moments and streamline deployments as the application and production infrastructure are packed into one unit.

- **Consistent product quality**

No manual infrastructure provisions – no security vulnerabilities and non-compliance — the least desirable scenarios for finance.

- **Enhanced testing**

Test applications in a production-like environment at any stage of the SDLC — prevent common deployment issues caused by configuration drift, missing dependencies, or integrations.

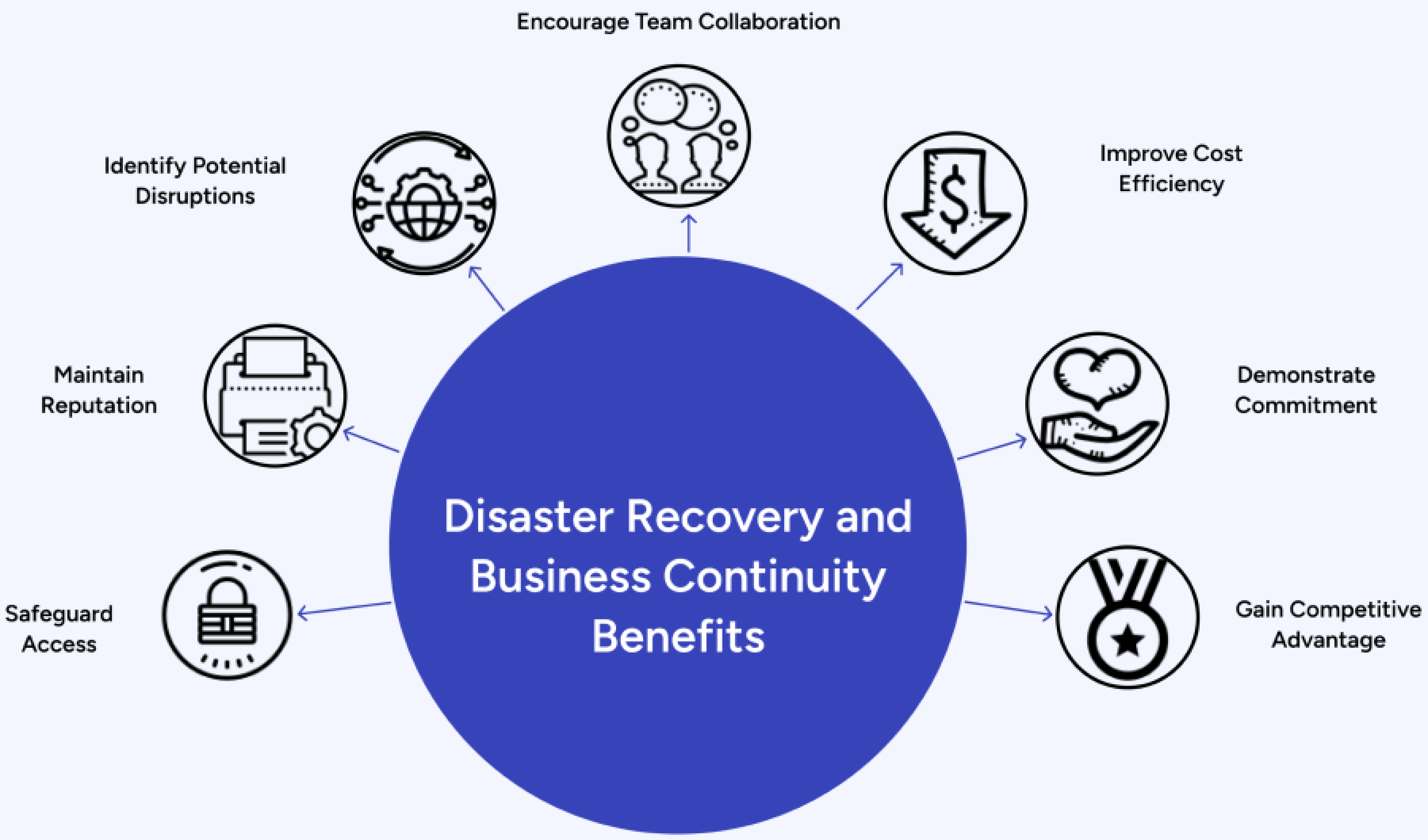
- **Cost optimization**

IaC helps optimize cloud computing bills through targeted optimization, dynamic provisioning and teardown of environments.

Backup and Disaster Recovery

Develop robust backup and disaster recovery plans to safeguard against data loss and ensure business continuity in the event of unforeseen disruptions.

Regularly test your disaster recovery plans to guarantee that, in the event of a major disruption, you can swiftly recover and maintain financial operations. DevOps should facilitate automated failover and rapid recovery processes.



Disaster Recovery and Business Continuity Benefits

Encourage Team Collaboration

Improve Cost Efficiency

Demonstrate Commitment

Gain Competitive Advantage

Safeguard Access

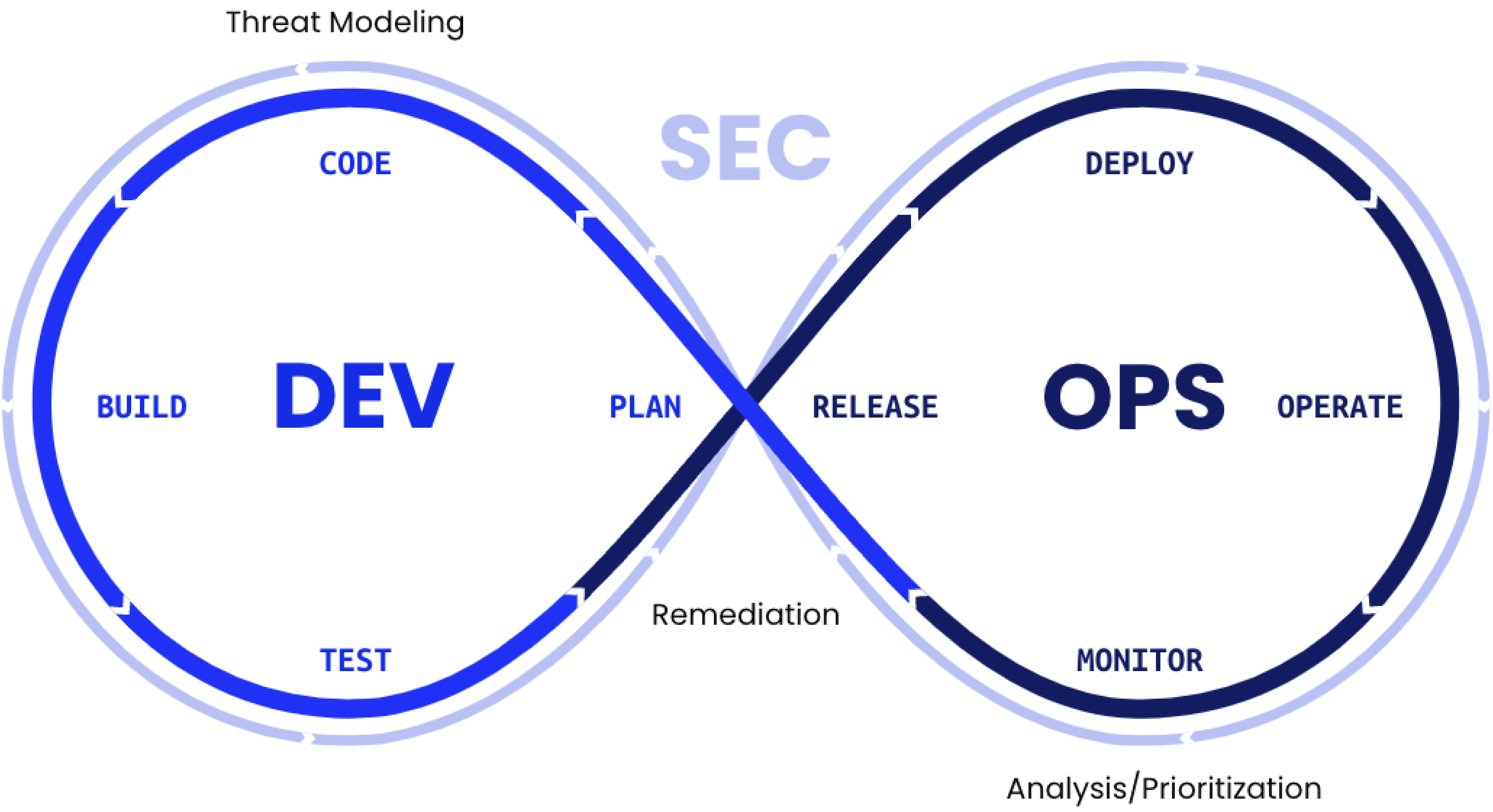
Maintain Reputation

Identify Potential Disruptions

Secure DevOps

DevSecOps is aimed at infusing automated security best practices at every stage of the SDLC.

Embed security practices into your DevOps pipeline. Employ tools and techniques for automated security testing, vulnerability scanning, and code analysis. Regularly update dependencies to patch vulnerabilities and adhere to security protocols at every stage of development and deployment.



Collaboration and Communication

Foster a culture of collaboration and open communication between development, operations, and security teams. Promote transparency and the sharing of knowledge to enhance the overall effectiveness of DevOps practices.

Capacity Planning and Scalability

Regularly assess your infrastructure’s capacity and performance. Use metrics and historical data to plan for scalability, ensuring that your FinTech services can handle increased loads and remain highly available.

Redundancy and High Availability

Design your DevOps infrastructure for redundancy and high availability. FinTech services must be accessible 24/7. Implement automated failover mechanisms and data replication to ensure minimal downtime and data loss in case of system failures.

Threat Intelligence Integration

Integrate threat intelligence feeds and monitoring into your DevOps pipeline to stay ahead of potential security threats. This proactive approach helps in identifying and mitigating emerging risks.

Comprehensive Audit Trails

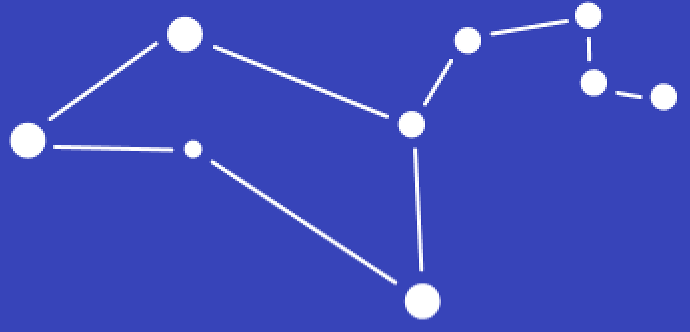
Maintain comprehensive audit trails of all changes made in your DevOps pipeline. This is vital for tracking any unauthorized modifications and for meeting regulatory compliance requirements.

Data Privacy and GDPR Compliance

If your FinTech company operates in regions subject to the General Data Protection Regulation (GDPR), ensure that your DevOps practices align with GDPR principles, including data protection impact assessments and data subject rights.

Perfect Cloud Partner for Your FinTech

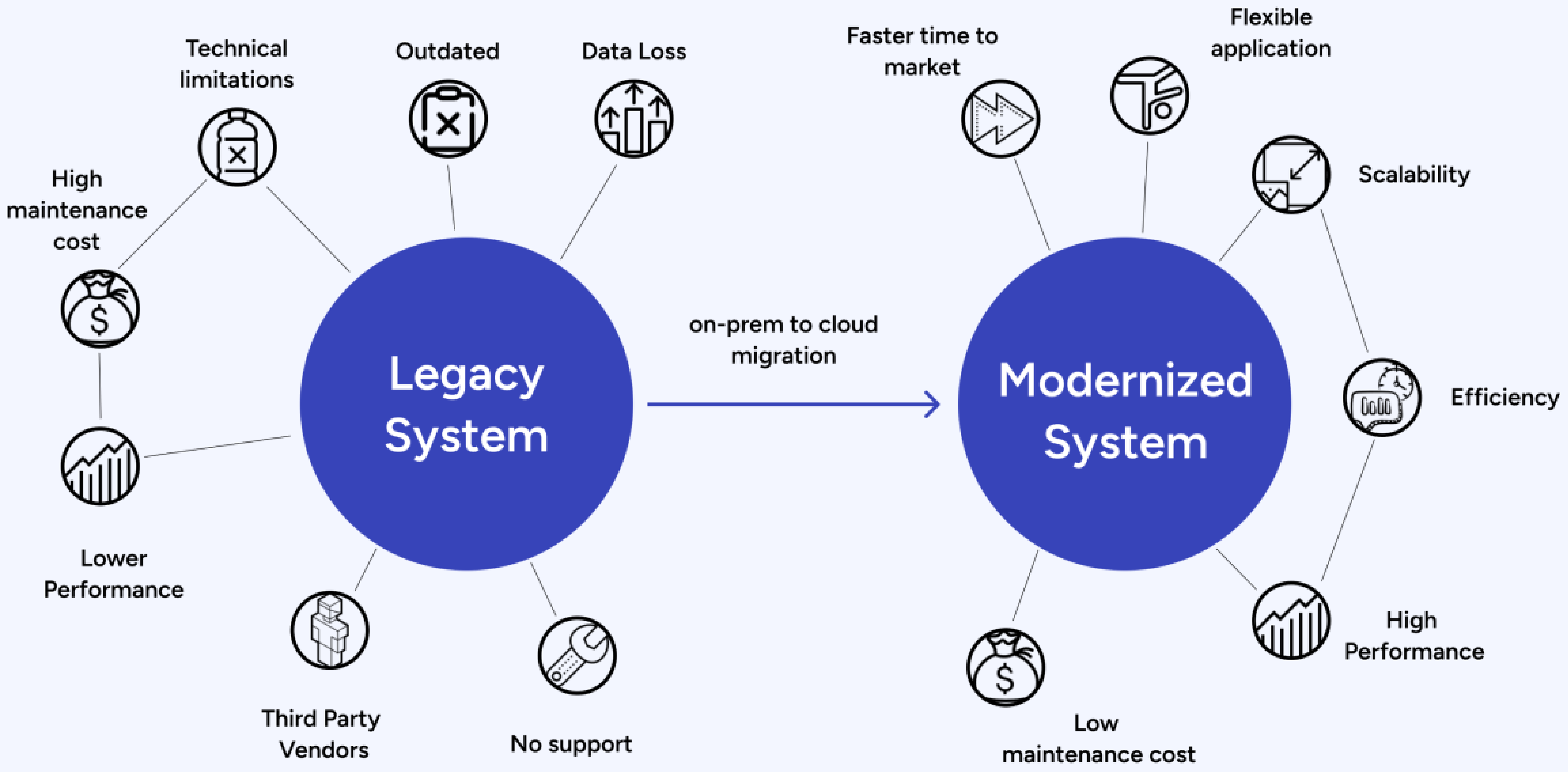
The Specific Requirements of the Financial Industry



gart.

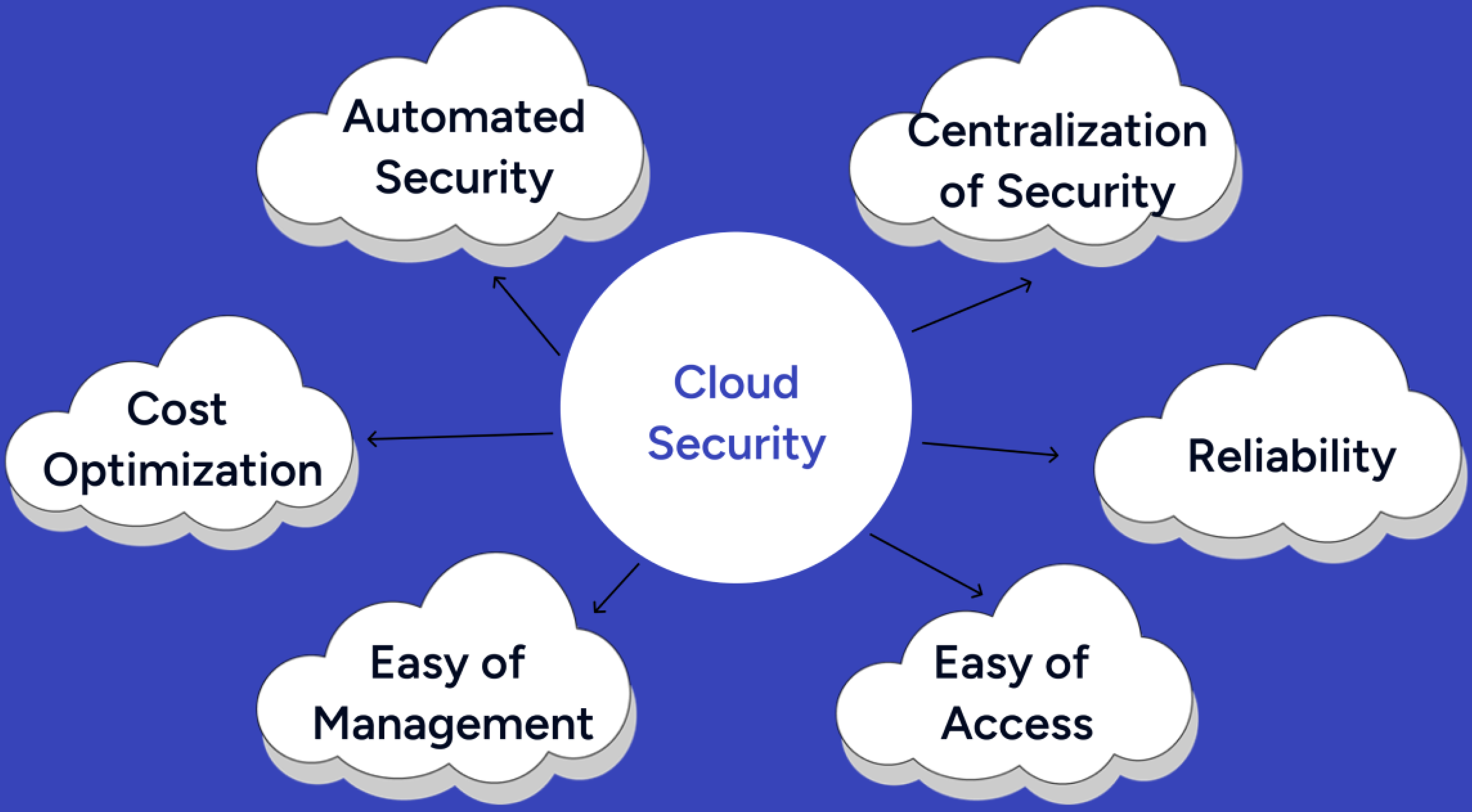
Integration with Legacy Systems

Cloud services must seamlessly integrate with these existing systems, enabling a smooth transition to modernized infrastructure.



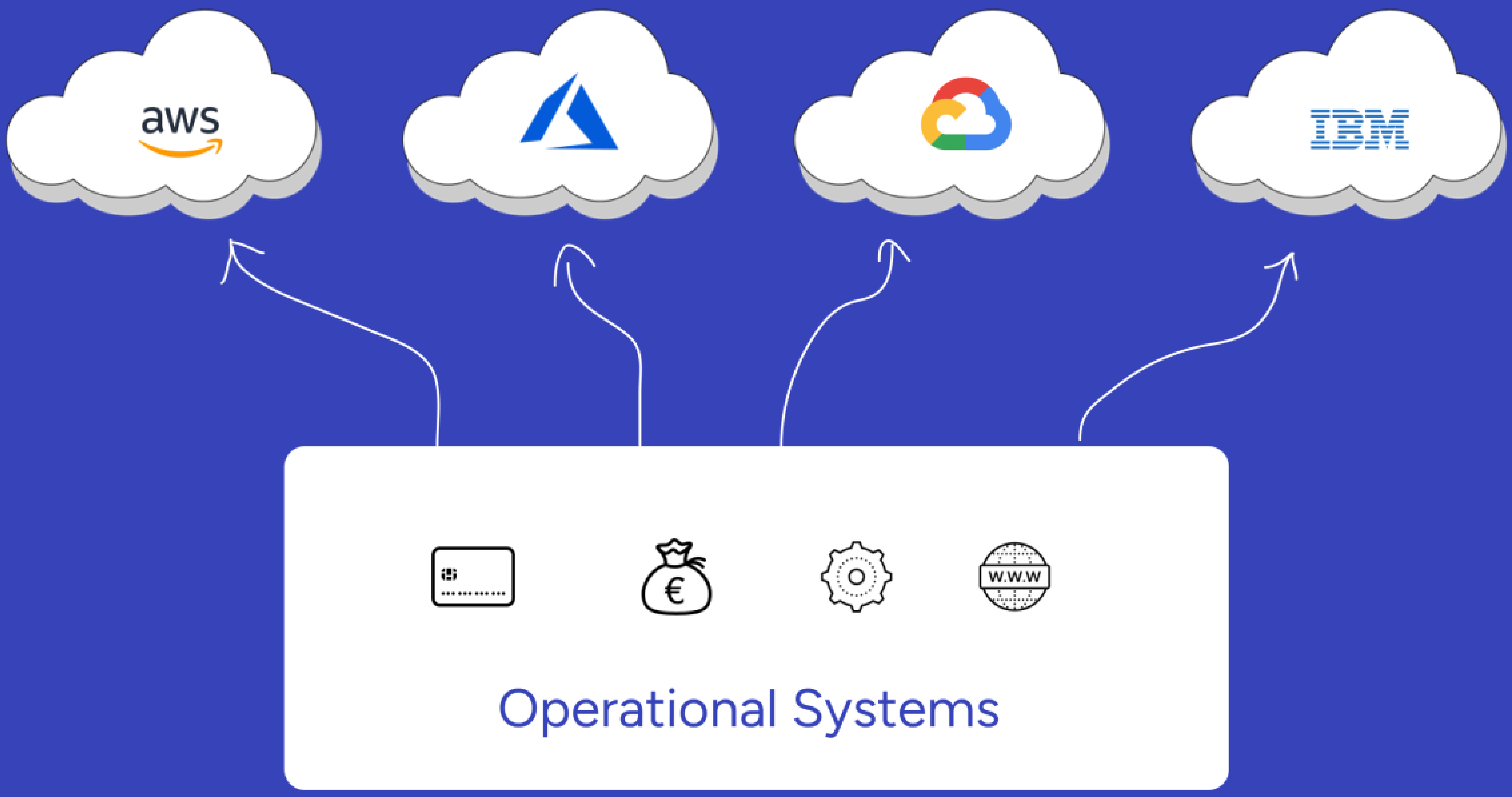
Data Security and Privacy

To safeguard sensitive info, financial firms and FinTech need robust encryption, access controls, and authentication. Security is non-negotiable with the ever-present threat of breaches.



Multiple Cloud Providers (Optional)

Consider adopting a multi-cloud strategy to leverage the strengths of different providers for various aspects of your business.



Speed & Growth

Financial tasks churn out vast data. Systems need top-tier processing and analytics. Plus, as FinTechs expand fast, cloud infrastructure must scale without slowing down.

Low Latency

In high-frequency trading and real-time decisions, low-latency data access is a must. Delays mean lost opportunities and financial losses.

Comprehensive Compliance Reporting

Financial firms and FinTech must tackle intricate audits and reporting. Cloud services should provide tools to streamline compliance reporting, saving time and effort.

The best cloud services provider for your FinTech company depends on your unique business requirements, such as regulatory compliance, data analytics, scalability, and geographic presence.

It’s recommended to conduct a thorough assessment and consider consulting with IT experts to determine which provider aligns best with your specific goals and needs.

Additionally, many FinTech companies use a multi-cloud approach to leverage the strengths of multiple providers for various aspects of their business.

When to Choose DevOps Outsourcing?

- You need a DevOps development team with unique skills, but you cannot select suitable candidates.
- You aim for shorter development cycles with better quality, less risk, and no additional costs.
- You are a startup that needs DevOps expertise, but has no need to hire full-time professional
- You want to offload some specialist.

The adoption of DevOps practices has become a strategic imperative for FinTech companies aiming to thrive in the digital age. Its ability to deliver speed, quality, security, and cost-efficiency has made DevOps a game-changer in the industry.

As customer expectations and market dynamics continue to evolve, FinTech companies leveraging DevOps will be well-positioned to provide innovative, reliable, and secure financial services that cater to the needs of today’s digitally connected world.