VTEX

The Enterprise
Digital Commerce
Platform

VTEX Security Posture

VTEX Security

Introduction 03
We Are Committed to Your Peace of Mind 04
How We Safeguard Our Clients and Systems 05
Information Security Program 06
Audit and Compliance 07
Education and Awareness 08
Asset Management 09
Access, Identification and Authentication 10
Data Security 11
Cryptographic Controls 13
Data Center Security 14
Host Security 15
Change Management 16
Security Monitoring 17
Threat Intelligence and Incident Response 18
Vulnerability Management 20
Perimeter Security 21
Secure Development Cycle 22
Third-Party Valuation Management 23
Security Risk Management 24
Business Continuity 25
Security Maturity 26
Conclusion 27
Resources 28

Introduction

With the exponential increase in remote work and ecommerce, companies have been urged to develop a safe and secure online environment. Although security has become a hot topic in the market, less than 1/3 of Brazilian companies have teams dedicated to cybersecurity.

Here at VTEX, we are committed to changing this scenario. We have developed a fully dedicated team to ensure that we provide everyone who is or will be part of our community with peace of mind, well-being, security, and trust when it comes to Security & Privacy. We understand the importance of adopting industry-leading security practices and technologies to protect customer data. Our security practices are embedded in all our technologies, people, and processes. Our clients rely on us to provide high levels of data integrity, confidentiality, and availability. For over two decades, we have worked with clients in highly regulated industries such as government, financial services, healthcare, and utilities — every client trusted VTEX with their data.

VTEX's Commitment

At VTEX, we are committed to following the most effective security practices and measures, ensuring that access is controlled and data is safe and secure.

Our Guidelines

To continuously improve our security posture, we use the ISO 27001:2013 standard to measure the maturity of our security programs. This standard is the international reference for information security management. We use this framework to evaluate and identify areas for improvement.

Our Values

At VTEX, we are committed to following the most effective security practices and measures, ensuring that access is controlled and data is safe and secure. We are reliable, secure, and scalable.

We are committed to your peace of mind

We are the Enterprise Digital Commerce Platform

We make bold decisions, putting ourselves at risk for our clients' success. We are a high-performance team, always learning by embracing uncomfortable challenges.

We are the backbone of connected commerce

At VTEX, we understand the importance of adopting the necessary security and technology practices to protect customer data. Our security measures are embedded throughout our technology, processes, and people.

VTEX is more than a commerce platform

We bring harmony between business and technology. We know that privacy and security are key to success in any business. In this document, we will provide an overview of our security posture — a starting point to demonstrate our commitment to our clients' security and our own.

Learn more details about our security processes by clicking here.

How We Safeguard Our Clients and Systems

Information Security Program

At VTEX, we have an information security program in place managed by a leadership committed to raising the level of security maturity for the entire VTEX ecosystem.

We have an information security policy that has been transmitted to the entire company through our internal communication channels. We review the policy annually in our document management process. Our information security policy is targeted toward the ISO IEC 27001 standard, frameworks with security best practices, data protection laws, and other obligations applicable to the VTEX context. Our clients can access our public version via the Store Administration Portal. All our documents are revised annually and can be managed through a policy management platform.

VTEX has a robust and specialized information security team that is structured and dedicated to supporting key security processes. Our security team works on call and in different time zones to ensure that our coverage goes beyond business hours.

Audit and Compliance

Internal Compliance Audits

Our internal audit team conducts internal compliance audits to prepare for external certification audits. They are constantly improving this process and automating control checks to have an active compliance dashboard.

External Compliance Audits

Certification audits are performed by independent companies and monitored by our internal audit team. Their results are used to improve internal compliance monitoring processes.

VTEX's Certifications

VTEX has a compliance program to manage and maintain security controls, which are audited by external companies periodically. We currently hold the following certifications:

Service Organization Controls (SOC 1)

Audit encompassing internal control over financial reporting systems.

Service Organization Controls (SOC 2 e 3)

Audit covering the Security, Availability, Integrity, Confidentiality, and Privacy processes of the platform.

Payment Card Industry Data Security Standards (PCI DSS)

A control validation of cardholder data to reduce credit card fraud.

Learn more about all VTEX's certifications.

Security education and awareness

We consider our employees a critical line of defense in protecting the data of our company and our clients. We have a dedicated team that drives awareness, engagement, and education of our employees on security best practices and the adoption of security features at VTEX. Our comprehensive programs include new employee integration and annual security training.

We train employees to identify frequently used attack vectors, such as phishing emails, and how to report them. This applies to all employees and third parties, and we measure the effectiveness of security awareness programs through performance indicators.

Every year we establish a schedule for our education program. In addition, we constantly review our content, considering the latest scenarios and attack vectors and vulnerabilities.

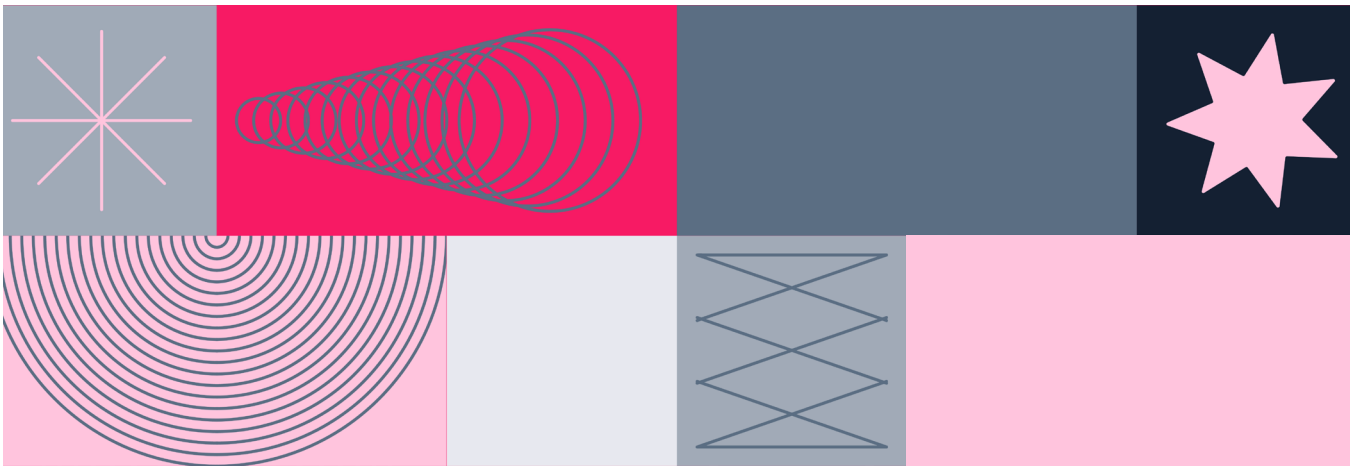
We provide an ethics channel for reporting inappropriate behavior. In addition, we have a sanctions process for employees who do not comply with the established information security policies and standards.

Asset Management

Assets are centrally managed through an inventory management system that stores and tracks their owner, location, status, maintenance, and descriptive information. Once acquired, we check and track all assets and inspect and monitor assets under maintenance for ownership, status, and resolution. It is also worth mentioning that VTEX operates 100% in the cloud and is the largest AWS (Amazon Web Services) partner in Latin America. Thus, there is no need for physical asset inventory for the resources in the AWS cloud. We use the AWS Systems Manager for software inventory, which provides visibility into our AWS computing environment.

The media storage devices used to store customer data are classified as critical and of high impact and treated as such throughout their life cycles.

AWS uses strict standards on installing, maintaining, and eventually destroying devices when they are no longer useful. When a storage device reaches the end of its useful life, it is decommissioned using techniques detailed in NIST 800-88. The media used to store the client data is not removed from the control until safely deactivated.



Access, Identification, and Authentication

VTEX strictly controls and monitors access to our production environments. Only employees whose job functions require access can qualify to access our systems. This guideline is aligned with our practice of the principle of least privilege and separation of duties, in which access is granted based on legitimate need. Privileged VTEX employees, such as platform reliability engineers, need to use multiple layers of two-factor authentication to access a segregated environment and manage systems using only applications hosted on a secure remote desktop client, Virtual Desktop Infrastructure (VDI). Administrators with logical access to the systems do not have physical access to the data centers. Logical access to the service systems is restricted to VTEX's Site Reliability Engineering team. Repositories with the platform code are private. Adding and removing users from the organization is part of the hiring and firing processes. Only VTEX's Development Engineers have access to the code repositories.

We have implemented secure configurations and a robust password policy to access our systems, such as a minimum number of characters and special characters, periodicity for changing passwords, not using previous passwords, session control, inactivity, and more.

When an employee is fired, the Human Resources notification triggers a set of tasks that protect access to the production system. After the termination, privileged accounts are blocked, active connections are closed, and two-factor authentication tokens are removed. Our access control team periodically reviews logical access and checks if terminated users have been removed from the respective systems via an internal ticketing system. We also review employee transfers and ensure that network, server, and database access to production systems are still appropriate for their new job function. And if you still want to know more about the platform's security features, click here and get to know our identity provider, VTEX ID.

Data Security

Data Classification and Protection

For us at VTEX, data is classified according to its impact level — high, moderate, or low — regarding confidentiality, integrity and availability. This structure will result in three possible classifications: restricted, confidential, or public. For example, the following types of data are considered confidential and critical within our information rating scale:

- Payment Card Information (PCI-DSS)
- Personally Identifiable Information (PII)

Therefore, we adopted strict security measures to classify and protect this data, we are committed to keeping your data safe and secure.

Our critical information must always be encrypted, in transit and at rest. Therefore, all confidential data is encrypted. Data in transit is encrypted with TLS 1.2 or higher and data at rest with AES-256 or RSA algorithms using keys of at least 2048 bits.

Data Retention

VTEX does not actively delete any proprietary data from our clients without their express expression of will. This also includes cases of termination of the customer's contract with VTEX, where we are asked to delete customer data, including personally identifiable data.

Secure Data Transfer

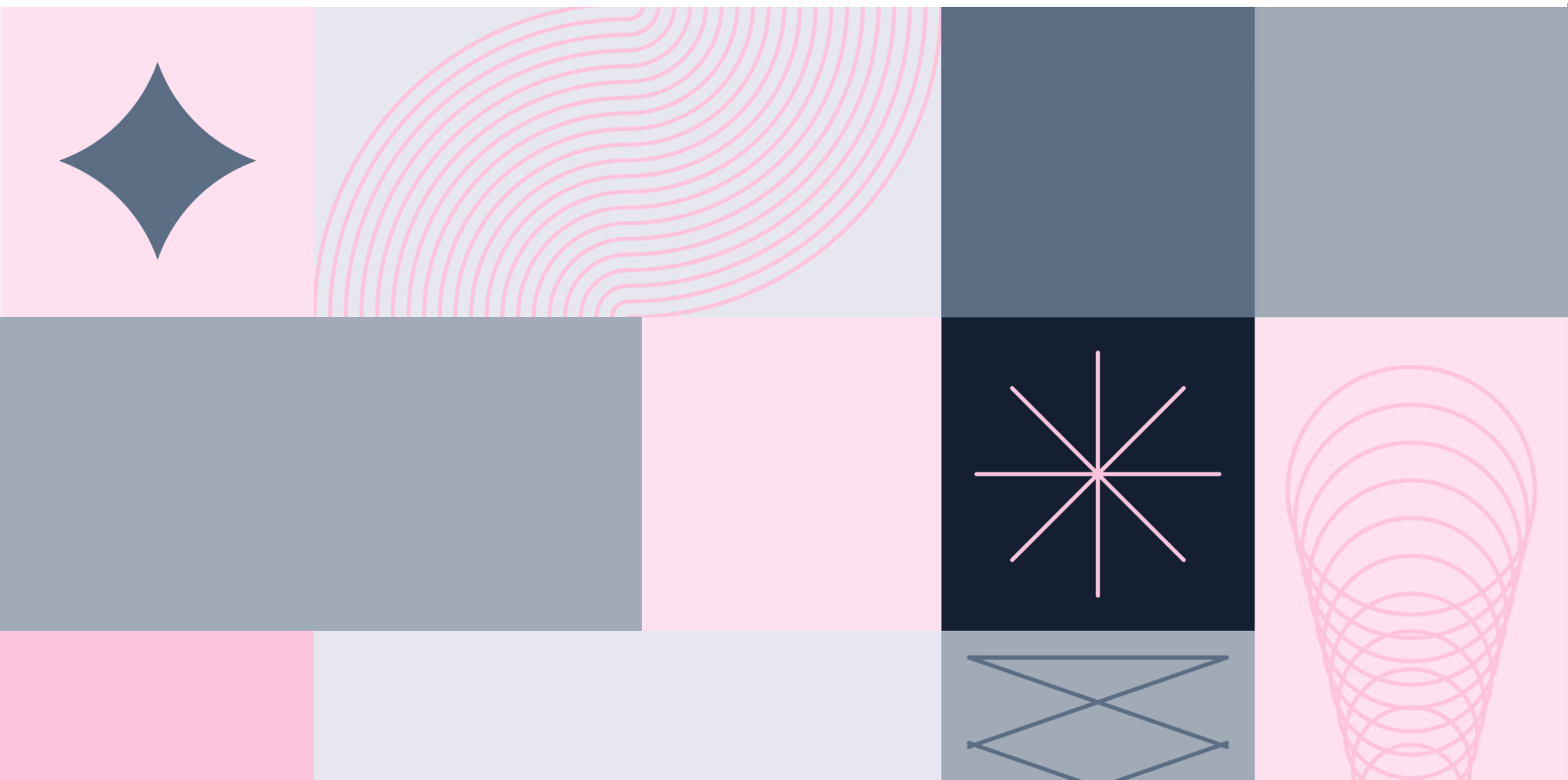
As previously stated, for VTEX, our clients' data is extremely valuable, and we preserve its integrity and confidentiality throughout its lifecycle. VTEX does not transfer or disclose customer data except to provide its services and prevent or resolve technical or service problems upon request by the client regarding support issues or as required by law. We comply with governance obligations under a variety of regional privacy and data protection regulations, such as the EU General Data Protection Regulation (GDPR), Brazilian General Data Protection Law (LGPD), and California Consumer Privacy Act (CCPA).

VTEX is fully committed to complying with Data Protection Regulations; that is why we are constantly updating our personal data security and privacy procedures in compliance with all applicable data protection laws in the countries where we provide services.

Cryptographic Controls

VTEX deals with critical customer data, so encrypting this information is essential. TLS and its predecessor, SSL, are encryption protocols to secure communication over computer networks. They are the S of HTTPS. This technology does not prevent criminals from intercepting the connection between consumer and store. Still, it makes it impossible to read this data, which can only be unscrambled inside your server using the private key generated by the system. VTEX has encryption standards for all its clients for data at rest and data in transit.

The AWS service provides encryption keys. Access keys are stored in a segregated environment with proper cryptographic protection. To manage the cryptographic keys, we use AWS Key Management, which stores and protects the encryption keys to make them highly available while providing robust and flexible access control. AWS KMS keys are the key feature in AWS KMS. You can use a KMS key to encrypt, decrypt, and re-encrypt data. It can also generate data keys to be used outside of AWS KMS.



Security of the VTEX data center and offices

Our data and our clients' data are hosted on Amazon (Amazon Web Services), a public cloud infrastructure service provider. VTEX has agreements with these providers to ensure physical security and environmental protection baseline to run our services. Before choosing a site, AWS performs initial environmental and geographic assessments. Data center sites are chosen carefully to reduce environmental risks such as flooding, extreme weather conditions, and seismic activity. Our availability zones are designed to be independent and physically separate from each other.

AWS allows only approved employees to have physical access to the data center. All employees who need access to the data center must first request access and present a valid justification. It is also worth noting that AWS operates its data centers in compliance with Tier III+ (UpTime Institute) guidelines.

VTEX has offices all over the world. We have physical security control such as monitoring and access control at all VTEX offices. Professional security staff controls physical access at the building's entry points using surveillance systems such as turnstiles and other electronic means. This equipment registers the exits and entrances of authorized people.

Our offices have Closed-Circuit Television (CCTV) cameras. Images are maintained following legal and compliance requirements. We also have power and fire suppression controls aligned with industry-leading measures to help prevent outages and power surges.

Host Security

VTEX services are powered by operating systems configured and implemented according to the industry's security best practices. We create environments using the latest AMI provided by AWS for each deployment service. In doing so, we leverage our security in the protection that AWS already provides for instances deployed by its services. We complement this security practice with the following measures:

- Applying critical security patches to operating systems when they are not provided as an updated AMI by AWS;
- Activating and centralizing system logs not to lose important information from the systems;
- Monitoring changes to critical configuration files to notify us of changes to these files;
- Activating local firewalls configured only with secure ports, such as HTTPS, TLS 1.2, or higher.
- Removing unnecessary and standard processes, accounts and protocols to reduce the attack surface.
- Installing anti-malware software.

These settings are applied during the deployment of a new environment. If the new installation module needs to be added to our servers, the baseline installation will automatically be added to the devices.

Capacity and Change Management

Change management in our organization follows a documented process, as required. This domain aims to define how we control changes made to information systems. What the domain wants is for the organization to manage these changes so they do not act as improvisations. However urgent it may be, even if the need appears last minute, change management requires our organization to evaluate the change and its consequences. These consequences are not always very clear and may conceal serious damage. By doing this analysis, the organization increases the chances of choosing the best idea and not the first one, and, moreover, of not being negatively surprised afterwards.

Therefore, VTEX has established a procedure to control changes. This procedure includes a study of the alternatives for making the change and its consequences. In addition, every move must be authorized by someone responsible for it. To prove this procedure is being followed, VTEX keeps a record of the conclusions about each assessment and the person responsible for authorizing the change.

Security Logging and Monitoring

The information security monitoring system consists of a series of resources — Information Technology software — used to prevent third parties from accessing and using important data. That's why we continuously monitor our resources in our environment on a 24/7 basis.

Our critical services are monitored to identify possible anomalies and cyber threats. Event logs from VTEX's internal infrastructure and infrastructure providers are collected and centralized by our detection and response system. Alerts are generated through pre-defined rules and using correlated detection logic. When this occurs, our incident response team investigates the causes of these alerts using standard processes and procedures.

In addition, we periodically evaluate the effectiveness of threat and risk identification and resolution, leading to improvements in our automated processes, making them increasingly efficient.

Threat Intelligence and Incident Response

Our priority is to protect our clients' data. To do this, we have complex procedures in place to ensure our resources are properly monitored. Our main objective is to identify potential threats quickly and effectively respond to them. Our detection and response team is dedicated to developing threat intelligence through research and analysis related to security incidents. Our incident response plan has been structured according to the four main stages of the response process:

Preparation

Before any response plan, our focus must be on incident prevention. This requires environment risk assessment, implementation of security baselines, patch updates, minimum access assurance, perimeter security safeguards, malware prevention and security education campaigns.

Containment, Eradication and Recovery

Before starting any corrective action, collecting, preserving, protecting, and documenting evidence is essential.
No evidence can be deleted. No asset involved in the incident can be changed or deleted without proper approval.
If the evidence contains confidential information, it must be encrypted. After containing an incident, assess whether other environments are exposed or have already suffered the same type of attack to resolve the problem at the root cause. The team in charge must reestablish uncompromised safeguards.

Incident Identification

Anomalous behavior is confirmed as an incident if it directly affects the availability, integrity and confidentiality of information, systems and services or if it results from improper access or a direct attack.

Post-Incident Activities

This is an important stage of the process, in which learnings and improvements will be collected for the security controls when preparing and managing future incidents. The objective is to analyze what happened, what has been done to intervene and whether the intervention worked properly.

Sales Management Vulnerabilities

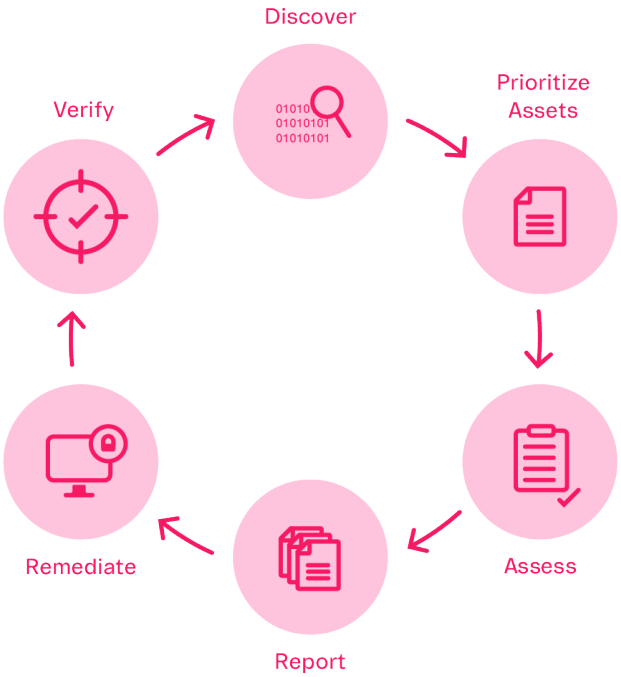
VTEX rigorously evaluates resources by testing and identifying vulnerabilities by performing scans and penetration tests in our environments.

We have a schedule for vulnerability checks. They occur periodically and according to the criticality of the scope.

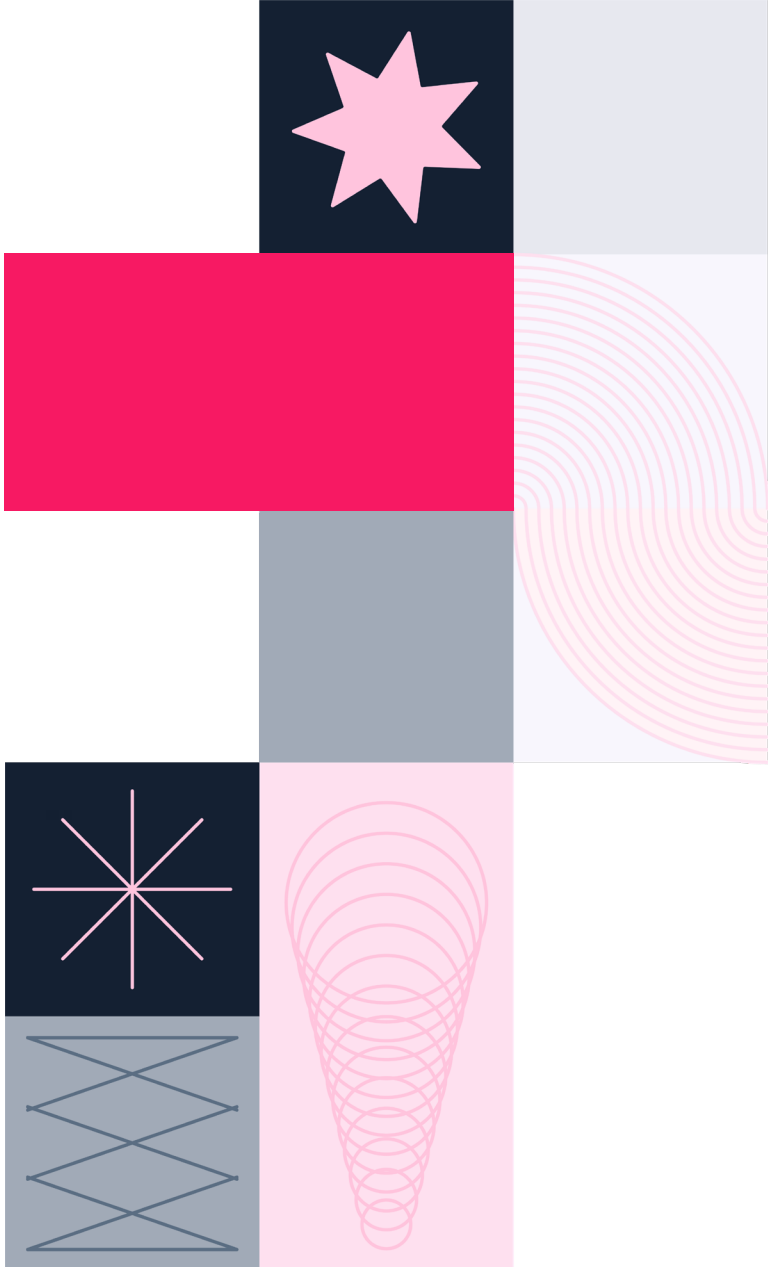
We address vulnerabilities identified in our vulnerability management process and manage them properly throughout their lifecycle.

In addition, our clients are free to conduct tests in their stores openly and transparently. In a multi-tenant solution like VTEX, this means that the entire platform is constantly tested throughout the year.

Our clients should report any vulnerabilities they identify in the VTEX platform. We have a process to receive and evaluate reports from our clients. If the VTEX security team confirms a vulnerability, it will be addressed internally for correction, always considering its level of criticality and risk to the platform.



Perimeter Security



VTEX uses a multi-layered approach to protect resources, adopting processes such as network segregation, firewalls, and edge routers as the mechanism for perimeter and network protection.

We have an IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) solution as network layer protection. We continuously monitor network traffic for anomalies, both in our internal network and on the Internet. This solution acts in the mitigation of DDoS attacks. When an event associated with a DDoS attack is identified, traffic is redirected to ensure that it is clean and our clients can continue their operations normally.

Our clients' information is contained in a store account and is isolated from different accounts by the VTEX process and storage implementation. There is no integrated method of accessing data from different accounts, even for internal VTEX use. The only ways to access the data require the explicit indication of a specific account.

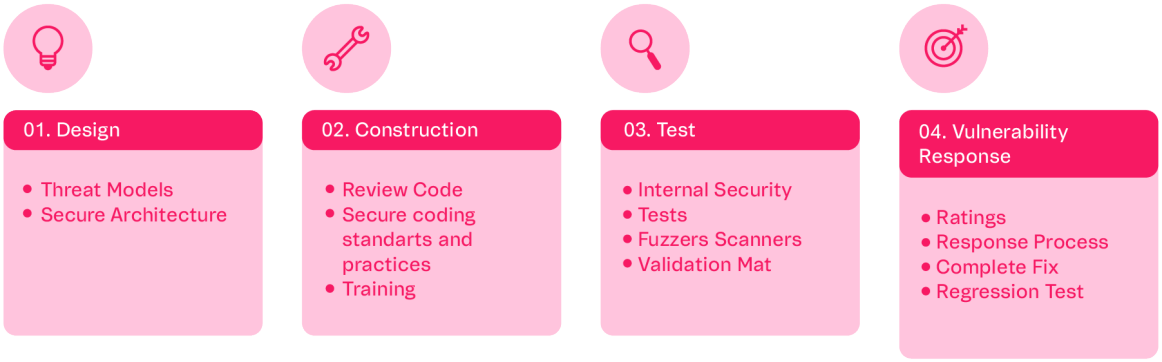
Secure Development Cycle

At VTEX, we integrate security requirements into every stage of the platform development cycle, using the Secure Software Development Lifecycle (SSDLC) process.

Through this methodology, our development engineers work with agile processes, taking into account our products' security issues and concerns. We innovate considering the constant market demands. An example of this is VTEX IO, a native platform that provides enterprise solutions with more agility and security. Learn more about VTEX IO.

We care about following the best market guidelines for secure development. That's why VTEX engineers follow OWASP Top 10 methods to prevent any malicious code.

In addition, VTEX has a code scanning system in the repository that acts by catching possible vulnerabilities and errors within the software development cycles.



Third-Party Valuation Management

VTEX ensures that its outsourced providers respect and follow the same security policies offered by VTEX. Here is a list of all of our third-party infrastructure providers: https://vtex.com/br-pt/subprocessors/

VTEX has an established security risk analysis process for critical suppliers responsible for handling confidential data.

We assess these vendors' maturity and security posture to understand the possible risks and gaps and address these issues to make the appropriate internal decisions. In addition, all suppliers go through the risk assessment flow for compliance with data protection laws and business risk analysis. After all the necessary assessments and with an adequate level of maturity, we proceed with the hiring.

Security Risk Management

Our risk management program provides visibility into potential security threats and helps us make decisions aimed at corporate objectives. We use risk mapping processes for assessing the likelihood and impact of threats that may affect our strategic capability.

Identifying risks allows us to improve our monitoring and notification systems to deal with their eventual materialization. This can be done by notifying the people handling risks or triggering automated actions to mitigate or eliminate these risks.

We use a management process that addresses the entire risk lifecycle and ensures that identified risks are addressed, mitigated and communicated according to their relevance. Our process comprises five main steps.

Business Continuity

We have a definitive commitment to our clients to prove that we are a safe and reliable platform. That is why we have implemented a business continuity plan designed to prepare the company to deal with the effects of an emergency. Our goal is that following the steps set out in the plan will provide the basis for a relatively quick and easy return to the day-to-day operation of our business, regardless of the cause.

Our disaster recovery plan focuses on ensuring continuity of operations and the availability of critical resources in the event of a disaster. It contains instructions on what actions to take and how to respond to unplanned incidents characterized as crises. These incidents can be related to natural disasters, cyber attacks, and any other disruptive event.

Security Maturity

To continuously improve our security posture, we use the ISO 27001:2013 standard to measure the maturity of our security programs. This standard is the International standard and benchmark for information security management. We use this framework to evaluate and identify areas for improvement. The standard's structure is domain-based and was developed in 1992 by a British government department that established a code of practices related to information security management.

Over the years, thousands of professionals have contributed with their know-how and experience to establish a stable and mature standard, which will undoubtedly continue to evolve.

Adopting the ISO 27001 standard helps organizations use a suitable model to establish, implement, operate, monitor, review and manage an information security management system.

This information security management system (ISMS) is, according to the principles of ISO 27001, a holistic approach to security that is independent of brands and technology manufacturers.

We perform self-assessments periodically using the ISO 27001 controls as guidelines, and based on the gaps identified, we build a roadmap for implementation and adaptation. It is also possible to set a score to our current state of maturity. By assessing current and desired ISO 27001 results, we can quantify and track the overall maturity of our security posture over time.

Conclusion

At VTEX, our biggest commitment is the security of our clients. We are leaders in accelerating digital commerce transformation in Latin America and are expanding globally. Our platform is designed for enterprise-level standards and capabilities. Approximately 80% of our GMV comes from large, top-tier enterprises (i.e., clients with more than $10 million GMV per year). We are trusted by more than 2,000 clients with over 2,500 active online stores in 32 countries to connect with their consumers in a meaningful way. We are reliable, scalable, and secure. We understand that our clients depend on the security, performance, and transparency of VTEX systems and services.

We offer high-security services that help our customers innovate to meet market demands, which drives mutual growth. To support our customers' success, we also share and promote security best practices with them using a variety of channels, including our website, blogs, social media, tools and features.

Companies choose us as a strategic partner to accelerate digital commerce transformation and deliver revenue-generating initiatives. Our platform is available through a subscription revenue model that includes GMV-based fixed and variable components.

What does all this success represent? Even after 20 years and all the impact we've delivered to the ecommerce ecosystem, we still keep the mindset that got us here from day one.

We are on a never-ending journey of connecting the world through the way people trade, so we invite you to step into our future and be a part of that journey!

So remember, #WeAreTrusted.

Resources

Security Help Center
This site is a public channel that serves as a help desk for VTEX clients and prospects. It provides solutions to a variety of questions and has a broad information base.

VTEX Trusthub
The VTEX Trust Hub is our public site for addressing concerns involving legal, compliance, privacy and security issues.

Security FAQ
This space is the only private one. Only VTEX clients can access it using their login and password. This is a reserved portal where we provide our answers to the most frequently asked security questions to support the resolution of doubts and the completion of the Risk Assessment.

VTEX Healthcheck
VTEX HealthCheck is a public page to monitor the status of our platform's services. The Healthcheck has over 100 tests running per minute. In this dashboard, you can track the health of each module in real time.

Status VTEX
In VTEX Status, you can track the platform's stability in real time and access the entire history of incidents. Our team reports events whenever our automatic monitoring system identifies an instability in the platform modules.

See more at: vtex.com

The Enterprise
Digital Commerce
Platform