Constant Company Security Whitepaper

Last Updated: 12/18/2024

Security Culture at Constant

Constant is committed to delivering robust, secure, and reliable cloud solutions for modern business infrastructure. Security remains our paramount concern as we strive to maintain trust of our customers. This whitepaper outlines Constant's comprehensive approach to ensuring the highest levels of security across our entire ecosystem.

At the core of our security strategy lies the principle of "Security by Design." We integrate security measures at every level in our infrastructure and operations. This proactive approach allows us to mitigate vulnerabilities early, minimize risks, and recognize security as a core business requirement.

Constant aims to provide our customers with a cloud environment they can trust. We recognize that security is an ongoing journey, and we remain committed to continuous improvement and adaptation in the face of evolving cyber threats.

Operational Security

Vulnerability Management

Constant is committed to a proactive approach to identifying and managing vulnerabilities within our cloud infrastructure. Our vulnerability management strategy encompasses a comprehensive set of practices to address both publicly known vulnerabilities and potential zero-day exploits.

Continuous Scanning: Our development pipeline integrates automated tools that continuously monitor our codebase and dependencies for vulnerabilities, ensuring timely updates to maintain a secure environment.

Infrastructure and Container Security: Regular scans of our infrastructure, including containerized environments, help us identify and address potential security risks across all layers of our platform.

Third-Party Assessments: Constant engages independent security experts for regular penetration testing and maintains a responsible disclosure program to further validate our security posture.

Customer Communication: In the event of significant vulnerabilities that could impact our customers, we promptly provide guidance and recommended actions through established communication channels.

Incident Management

Constant has a robust incident management process to swiftly address security events that may impact the confidentiality, integrity, or availability of our systems and customer data. Our security team regularly reviews and tests incident response procedures, ensuring readiness for notification, escalation, mitigation, and thorough documentation.

Security incidents are continuously monitored, logged, and prioritized to enable rapid response. In the event that customer data is impacted, we promptly notify affected clients and provide support to assist in their investigations.

Through these practices, Constant ensures a structured and responsive approach to managing security incidents, minimizing potential risks to our customers.

Physical Security

Constant partners with reputable third-party data center providers that implement stringent physical and environmental security controls, such as 24/7 on-site personnel, biometric access systems, and continuous video surveillance. These facilities are equipped with redundant power systems, advanced fire suppression, and precise climate controls to ensure consistent operational availability.

To maintain high standards, Constant exercises rigorous oversight of our data center partners through regular audits, compliance assessments, and strict contractual requirements aligned with industry standards, including ISO 27001 and SOC 2.

This partnership model enables Constant to provide a secure and resilient infrastructure foundation for our customers.

Malware Prevention & Monitoring

Constant employs a comprehensive suite of security monitoring tools across multiple data sources to protect client infrastructure and data. By analyzing network traffic, internal activities, and external threat intelligence, we proactively identify potential security risks.

Our global network utilizes advanced detection tools to inspect traffic for anomalies, while system logs are continuously monitored for unusual activity, such as unauthorized access attempts. In addition, Constant leverages both enterprise and proprietary tools for traffic analysis and log parsing, enabling timely detection and response.

Automated network analysis further enhances our ability to identify emerging threats and escalate concerns to our security team swiftly. This proactive and adaptive monitoring approach

allows Constant to maintain a high level of protection for our clients, ensuring a secure operating environment.

Technical Security Measures

With a strong focus on security, Constant provides a reliable service designed for customers seeking to adopt cloud solutions. Below is an overview of our essential security capabilities and controls:

Encryption in Transit

Constant prioritizes security in every aspect of our service, offering a dependable platform for customers adopting cloud solutions. Key technical measures include robust encryption protocols that ensure data remains protected throughout its journey within our systems.

Constant enforces strict encryption requirements for all data transmissions, securing customer interactions with the platform and safeguarding sensitive information across various access points.

Encryption at Rest

Constant employs robust encryption at rest across its data storage systems to protect customer data and ensure confidentiality. All data within Constant's infrastructure is encrypted to meet or exceed industry standards, providing a secure foundation for customer operations.

Our encryption practices include careful management of encryption keys and access controls, allowing only authorized systems and personnel to access stored data. Through these safeguards, Constant upholds a secure environment that aligns with industry benchmarks for data protection.

Network Security

Constant's network security strategy is designed with multiple layers of defense to protect against both external and internal threats. Our approach combines firewall protection, real-time threat detection, and logical segmentation to control and isolate internal traffic, reducing the risk of lateral movement and unauthorized access. Encryption and authentication are applied to all internal communications, preserving data integrity and confidentiality.

For clients seeking enhanced isolation and control, Constant offers customizable network configurations, including Virtual Private Cloud (VPC) options and dedicated interconnects. To maintain a strong security posture, we conduct regular security audits and penetration testing,

ensuring our network defenses adapt to evolving threats and provide a secure foundation for client operations.

Logical Data Separation

Constant enforces strict logical data separation across its platform, ensuring that each customer's data remains isolated and secure throughout all operational layers. Key components of this approach include unique data tagging, per-customer encryption keys, and isolated storage volumes, all designed to maintain clear customer-specific boundaries and prevent cross-access. These measures reinforce data privacy and integrity within our shared infrastructure, upholding Constant's commitment to secure data management.

Access to Data

Constant enforces strict access controls to protect customer data, adhering to the principle of least privilege to minimize unauthorized data exposure. Role-Based Access Control (RBAC) is used to assign permissions based on job functions, ensuring access is limited to authorized personnel only. All access attempts are logged and continuously monitored, with any unusual activity automatically flagged for investigation.

For troubleshooting or technical support, Constant requires explicit customer consent before accessing customer environments. This access is granted on an as-needed basis, with restricted duration and scope, maintaining customer control and prioritizing data privacy.

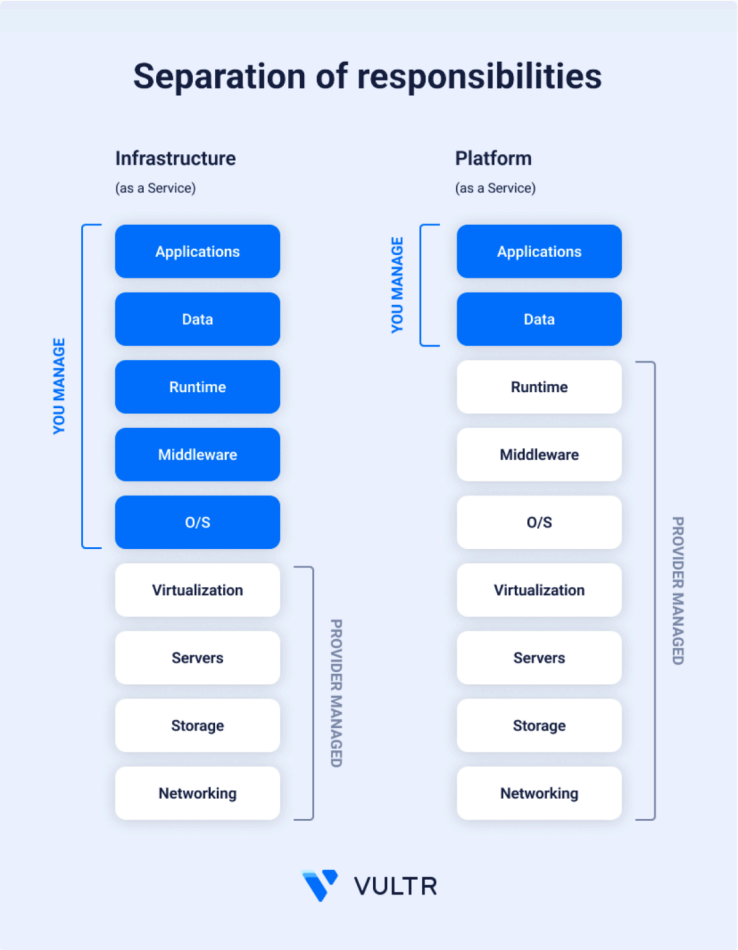
Data Deletion

Constant follows a stringent data deletion policy to ensure customer data is securely and permanently removed once the retention period specified in the customer contract has ended. Our data deletion practices align with industry standards, including NIST 800-88 guidelines, to ensure secure and thorough disposal.

Customer data is securely deleted through automated processes that remove and destroy both raw data and associated metadata. This approach ensures compliance with secure deletion protocols and upholds Constant's commitment to data privacy and protection.

Shared Responsibility

The shared responsibility model at Constant defines a clear division of security, compliance and operational duties between Constant and its customers, tailored to specific service types—Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).



At a high level, security and operational duties are divided between customers and Constant in the following manner:

- **Constant's Responsibilities (Provider-Managed)**: Constant manages and secures foundational infrastructure elements, including networking, storage, servers, and virtualization.
- **Customer Responsibilities (Customer-Managed)**:
    - **For IaaS**: Customers manage their operating systems, applications, data, and security configurations.
    - **For PaaS**: Customers maintain responsibility for their applications and data, while Constant handles the operating system, middleware, and runtime, allowing customers to focus on application-level security.

To support these responsibilities, Constant offers certain key administrative functions our customers can utilize:

1. **Create Roles for Users**: Administrators can define and manage user roles within the Constant platform, enabling precise access control by assigning permissions based on specific job functions.
2. **Whitelist IPs**: Administrators can implement IP whitelisting by specifying trusted IP addresses or ranges allowed to access the platform, reducing exposure to unauthorized locations.
3. **Manage Server SSH Keys**: Administrators can add/remove SSH keys that can be used when deploying new servers.
4. **Implement Backup Strategies**: Administrators are responsible for establishing and managing backup strategies, such as data forwarding or storage replication, to ensure data availability and continuity in the event of disruptions.
5. **Manage Firewall Groups**: Administrators can create firewall groups that can be applied to servers.
6. **Manage API Access**: Administrators can refresh/disable keys and limit IP access.

Compliance, Certifications, and Attestations

Constant is committed to maintaining a strong security and compliance posture by continuously acquiring and upholding industry-recognized certifications and attestations. These certifications demonstrate our adherence to globally recognized standards and our dedication to safeguarding customer data.

Our compliance framework includes a variety of certifications, which include standards such as SOC 2 Type II, ISO 27001, PCI-DSS, HIPAA, and others, relevant to our customers' security and regulatory needs. Constant regularly undergoes rigorous audits and assessments to ensure that our security practices meet or exceed industry requirements.

For the most current information on our certifications and compliance status, please refer to our compliance page here.