Technical and Organizational Measures

The technical and organizational measures ("TOMs") below apply to standard service offerings provided by Infoblox Inc. and its affiliates (collectively, "Infoblox") except where Customer is responsible for security and privacy measures such as on-premises equipment deployment.

Product Controls and Measures

Measures of pseudonymization and encryption of personal data

Pseudonymization measures

Infoblox does not currently pseudonymize the DNS/DHCP/IP Address data processed for customers using our SaaS products. Infoblox also maintains contact information for system administrators / product users and billing contacts. This personal data is secured and is maintained according to our records retention policy.

Encryption measures

Data connections are encrypted using current industry standard protocols (e.g. TLS 1.2 for encryption in transit and AES256 for encryption at rest). Infoblox implements measures to support the security of the network as well as confirm the availability of computing environments and access to Customer Personal Data. Infoblox applies a Data Classification Policy to define the sensitivity of data elements. Personal data from customers or employees is always classified as Confidential which requires specific handling measures, including encryption at rest and encryption in transit, secure deletion, and limited access.

Measures for ensuring events logging

Infoblox utilizes comprehensive log collection for key events on our cloud applications and services. SaaS product-related events are correlated in a Security Event Incident Management (SEIM) tool which is monitored by the Product Security Incident Response Team. These logs are maintained for 90 days online and one year offline to support incident response investigations.

Corporate applications and devices are logged and monitored by the Infosec Security Operations Center (SOC). The SOC uses event logs in conjunction with a suite of security tools to detect compromise and support forensics investigation of incidents affecting corporate endpoints and IT-managed applications.

The architecture and policies related to Logging and Monitoring are coordinated between the two security teams and reviewed regularly by the Security Architects. The procedures for monitoring logs are well documented and periodically reviewed and updated, but are proprietary and not shared with Infoblox customers.

On-Premises NIOS, virtual NIOS, and NetMRI solutions capture access and activity logs. These logs can be downloaded to the customer's Security Event Incident Management tool.

Measures for ensuring data minimization

The data privacy team, including the Data Protection Officer, is involved in the Infoblox product development process to ensure only data that is needed to provide services is collected and processed. Periodic reviews of Infoblox products are performed regularly.

Infoblox uses a rigorous agile SAFe development methodology to prioritize product development.. This process ensures that new product features or requests for enhancements are carefully reviewed by relevant teams and appropriately prioritized. The Legal, Privacy, and Security teams are involved in reviewing the current and planned Program Increments along with business units such as sales and marketing. A Data Governance Committee reviews potential processing of internal and customer-derived data to ensure that it meets strict privacy standards.

Measures for ensuring data quality

Infoblox has internal quality control measures for the data we maintain and other programs. In terms of the cloud products, the Customer generates their data directly (in the form of DNS queries and access logs). This data is not curated or altered by Infoblox. Therefore, any quality control measures are the responsibility of the customer.

Infoblox cloud systems continually replicate to multiple geographically redundant data centers to ensure the integrity and availability of customer data.

Measures for ensuring limited data retention

Data is securely removed either by customer self-help functionality in the offering or by raising a ticket through the Infoblox Support Portal. Such tickets will be processed within 60 days. A certificate of destruction is available upon request. Individuals can also raise a deletion request of their personal information via the mechanisms set forth in the Infoblox Privacy Policy.

Measures for ensuring accountability

Infoblox uses measures to ensure that data is securely stored and processed. Technical and organizational measures such as encryption, vulnerability management program, and least privilege access principle are in place. All users access systems using unique access credentials.

Infoblox has a suite of data protection policies that govern compliance with all applicable data protection regulations (e.g. GDPR, and US state privacy laws).

Infoblox incorporates privacy by design principles for systems and enhancements at the earliest stage of development. Software engineers receive specific role-based training related to secure coding best practices, testing, and identification of key security issues such as the OWASP Top 10.

Infoblox, as a data processor, has entered into data processing agreements with our data sub-processors.

Infoblox maintains incident response, disaster recovery, and business continuity plans that provide thorough guidance and instruction in the unlikely event of a data breach.

Infoblox has assigned a Data Protection Officer.

Measures for allowing data portability and ensuring erasure

Infoblox supports customer capability to remove their DNS data from the DDI product and transfer it to another provider. The records processed are IP addresses, MAC addresses, and hostnames. There is no data which a data subject would be able to transfer.

Infoblox will delete account data upon a customer request. Requests for account data deletion should be raised by submitting a request through the Infoblox Support Portal. Requests will be qualified through the authentication of the requester as well as validation of their authorization to make such a request. Infoblox leverages AWS practices and techniques to securely delete data stored in S3 buckets. Confirmation of the data deletion shall be provided to the requester if required and in accordance with the relevant contractual provisions.

Administrative Controls and Measures

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Infoblox maintains the security and privacy documentation related to the technical and organizational measures and periodically reviews the TOMs to ensure they are up-to-date, that they are enforced within Infoblox, and that the security of Infoblox systems meets or exceeds industry standard best practices.

Infoblox operates an enterprise risk-management program which includes performing an annual risk assessment. New threats and risks are continually added to the risk register and prioritized for remediation in a monthly review session. The risk register is reviewed quarterly by the executive leadership on the risk steering committee. The corporate security program is reviewed for effectiveness at least annually.

Measures for internal IT and IT security governance and management

Infoblox maintains a Written Information Security Program of policies and procedures that are integral to Infoblox's business and mandatory for all Infoblox employees and supplemental personnel. IT security policies are reviewed and approved annually. Infoblox will amend such policies as deemed reasonable to maintain protection of company data assets, employee and customer data. Infoblox's security program is consistent with NIST 800-53r4 standards and controls.

Infoblox maintains a vulnerability management program meant to identify, manage, mitigate and/or remediate vulnerabilities within Infoblox's computing environments. Security measures include:

Patch management

Anti-virus / anti-malware software

Threat notification advisories

Vulnerability scanning (all internal systems) and

Annual penetration testing (Internet facing systems) with remediation of identified vulnerabilities

Infoblox maintains policies and procedures designed to manage risks associated with the application of changes to both corporate IT systems and customer-facing products. Change Control Boards regularly meet to review and approve requested changes which are formally documented. Proposed product changes are reviewed using an Agile SAFe methodology which incorporates cross-organizational stakeholders, architectural review and design prior to developing the code.

Security Risk Management

Infoblox performs annual security risk assessments based upon the NIST Risk Management Framework, measuring the severity and likelihood of a particular vulnerability and risk to determine its relative risk ranking to the organization. Prioritization of remediation activities and new programs is determined by risk.

Infoblox has both an Enterprise Risk Management program and a robust IT Risk Management Program for prioritizing vulnerabilities and risks for remediation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

All vendors, customers and employees of Infoblox sign non-disclosure agreements prior to accessing any data or system.

Infoblox employees and contractors must sign the Acceptable Use Policy prior to obtaining access to internal systems.

Customers must acknowledge rules of behaviour or acceptable use statements prior to accessing the Customer Support Portal or SaaS products.

Data integrity for the cloud products is ensured by continual streaming backups which are periodically tested to ensure the recoverability of the system, and Infoblox utilizes built-in AWS technology to prevent DDoS attacks.

Technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter (Third Party Risk Management)

Infoblox maintains a third-party risk management program to review the security measures of potential new vendors, particularly those which will access employee or customer personal data. Third parties are examined to ensure that they have appropriate technical and administrative controls to protect our customer or employee data. Key vendors are monitored in real-time using independently collected security reputation metrics. Infoblox responds to changes in subprocessor security posture and works with vendors to ensure timely remediation of significant issues. Vendors are classified into High / Medium / Low risk depending on the type of data they process and the services provided to Infoblox. Sub-processors and other high-risk vendors are reassessed annually through either review of their audit documentation or responses to questionnaires. Records of these reviews are maintained within our GRC platform.

Infoblox has executed DPAs which include standard contractual clauses (as necessary) with select sub-processors as required under GDPR. Infoblox's list of sub-processors is available on the Infoblox Trust Center. Current customers may also subscribe to the list of sub-processors within the Customer Support Portal to be automatically notified of any changes (see https://support.infoblox.com/s/article/Infoblox-Subprocessors to subscribe).

Security Awareness

Infoblox employees and contractors' complete security and privacy education at hire and annually. All workforce members also certify each year that they will comply with Infoblox's code of ethical business conduct and Infoblox's Employee Handbook. Additional training is provided to persons granted privileged administrative access to security components, by role and systems accessed, and as required to maintain compliance with regulations and certifications.

Hiring Practices

Infoblox performs employee background checks prior to hiring employees worldwide. Depending on the position, these background checks include identity and address related confirmation, criminal background checks, credit checks, education, prior employment and professional license verifications. All employees are checked against Politically Exposed Parties and sanctions lists. Employees who leave the company and return more than 90 days later undergo new background checks.

Security Incidents and Investigations

Infoblox maintains an incident response program within the Infosec Security Operations Center (SOC). The SOC regularly monitors security logs and investigates anomalous or suspicious events. The SOC maintains and exercises Incident Runbooks to effectively respond to incidents. Documented procedures are followed to escalate to appropriate management channels, and to the Infoblox Legal department for review and data breach notification to the Data Controller without undue delay where a breach is known or reasonably suspected by Infoblox to affect Customer's Personal Data.

The Product Security Incident Response team monitors logs of the Infoblox SaaS products and also performs security penetration testing on both on-premises and Cloud products. The two teams work together to validate whether Infoblox is affected by specific vulnerabilities which may be announced by US-CERT, software vendors, or other news sources.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Availability of data is ensured through Business Continuity and Disaster Recovery planning which supports Infoblox's documented risk management guidelines. Infoblox has a robust business continuity and disaster recovery program consistent with industry standards, such as ISO 23301. Business Impact Assessments and Business Continuity Plans are reviewed with business owners and updated annually. Business Continuity and Disaster Recovery Plans are tested annually with lessons learned from the exercises incorporated into the plans for continuous improvement. An

overview of Business Continuity / Disaster Recovery is available upon request to customers and prospective customers.

Technical Controls and Measures

Measures for ensuring physical security of locations at which personal data are processed

Infoblox protects the physical security of Infoblox facilities, including use of appropriate access control and visitor procedures. Corporate offices require proximity badges with photo ID. Allocation of badges or keys is strictly controlled by the Facilities Department. Infoblox takes precautions against environmental threats, power disruptions, and natural disasters. Infoblox validates that contracted data centers and AWS have appropriate physical controls in place by annual review of their SOC 2 Type II reports, certifications, and other security documentation. Access to the data center and controlled areas within Infoblox-controlled facilities such as wiring closets is limited by job role and subject to authorized approval. Visitors to Infoblox offices must follow specific protocols as defined by the Physical Security Policy, including being escorted by an Infoblox employee at all times.

Measures for user identification and authorisation

User access management

Infoblox maintains proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications containing Personal Data. Only employees and contractors with clear business need to access Personal Data located on servers, within applications, or databases will be granted access on a need-to-know / least privilege basis. All access requests for corporate systems are approved by the individual's manager and the business owner for the application or resource. Entitlements are reviewed on a regular basis for continued business need and applicable role.

All systems require unique login credentials which may not be shared. Wherever possible, multi-factor authentication is deployed to ensure that the person attempting access is authorized. Systems are configured with the following password restrictions:

Minimum password length of 8 characters and complexity of three of four types of characters – upper case, lower case, special characters, and numbers.

Password expiration 90 days

Automatic lock out after five bad login attempts

Application and workstation sessions timeout after 15 minutes, requiring re-authentication to resume access. On-premises NIOS / virtual NIOS / NetMRI allow the customer to define the password policies, inactivity timeout, and lockout policies as desired.

Remote Access

Access to Infoblox internal network resources requires use of VPN and multi-factor authentication (one time password). Critical SaaS services require Single Sign-On (SSO) and multi-factor

authentication. Minimum configuration standards are enforced for connectivity between computer systems and for utilization of Application Programming Interfaces (APIs).

Measures for the protection of data during transmission

Remote connectivity to Infoblox computing environments requires use of encrypted sessions, such as VPN, and multi-factor authentication. Data connections are encrypted using current industry standard protocols (such as TLS 1.2). Infoblox implements measures to support the security of the network as well as confirm the availability of computing environments and access to Customer Personal Data. Network security measures are deployed within Infoblox, such as firewalls, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring. Lab or Development networks are segmented from production networks by firewalls. Data processing operations are physically or logically separated. The cloud products are multi-tenant with strict logical controls in place to prevent one customer from accessing another customer's data.

Measures for ensuring system configuration, including default configuration

Infoblox utilizes standardized CI/CD tools and processes to ensure a default secure system configuration for our infrastructure and code. Configuration management tools are used to ensure that images or systems do not drift from the standard approved baseline configuration.

Security measures defined in the default configuration include:

Removal or renaming of system administrator accounts

Changing of default passwords

Disabling unnecessary services

Review and disable unnecessary ports / protocols

Ensure host is entered in the CMDB or other asset tracking system

Applications which will be Internet-facing have additional security requirements, including a vulnerability scan prior to go-live. Corporate applications are deployed using CIS Benchmarks as a standard. A vulnerability management platform is used to monitor and verify configuration of new and deployed systems on an ongoing basis via monthly scanning.

Endpoint Protection

Infoblox implements protections on end-user devices and servers. Devices are monitored to ensure they remain in compliance with the security standard requiring hard drive passwords, screen saver, antivirus software, firewall software, vulnerability scanning software, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate endpoint compliance deviations. Mobile Device Management software is used to manage the Windows and Macintosh laptops.

Media Handling

Infoblox implements protections to secure portable storage media from damage, destruction, theft or unauthorized copying. Use of USB or portable media drives is not allowed for storage of customer data. Backup data intended for off-site storage is encrypted prior to transport.

Measures for the protection of data during storage

Infoblox's family of Software as a Service (SaaS) products reside in multiple data centers in the AWS East Region, United States, and for applicable offerings, in the AWS Frankfurt Region, Germany. Infoblox relies upon Amazon for the physical security of the AWS resources, including data carrier control, Internet connectivity, redundant power, and fire suppression. The AWS SOC 2 Type 2 and ISO certifications can be shared with Infoblox customers under mutual NDA. AWS certifications are reviewed annually by the third party risk management team.

At the infrastructure as a service (IaaS) layer, the SaaS Platform is built in a cloud-native environment. It consists of a control plane, the applications infrastructure and related services, such as event logging, messaging, programming interfaces and a user interface (UI). It is built using industry-leading open source technologies, such as Kubernetes (k8s), Docker and Core DNS, and is container-based for scalability and extensibility.

Data integrity is ensured by continual streaming backups which are periodically tested to ensure the recoverability of the system.

Periodic disaster recovery exercises are performed including functional testing of the failover of the AWS environment which supports the cloud products.

Secure Destruction

Infoblox will securely sanitize physical media such as laptop harddrives which are intended for reuse prior to such reuse or will destroy media prior to retiring it. Media must be overwritten in a fashion consistent with NIST 800-88 standard to render the data unrecoverable. Infoblox requires our hosting services to also perform secure file deletion.

Measures for certification/assurance of processes and products

Infoblox's flagship product is a DNS / DHCP / IP Address Management solution which is delivered on a hardware appliance or as a virtual machine. The NIOS/Trinzic appliance is Common Criteria EAL-2 Certified. Infoblox on-premises solutions are included on the Defense Information Systems Agency (DISA) Approved Products List (APL) for DoD infrastructure. The Common Criteria certificate and FIPS 140-2 Crypto certificate for NIOS / Trinzic appliances are available upon request.

Infoblox has attained FedRAMP Moderate level certification of the BloxOne Threat Defense GovCloud security product, a specific version of the SaaS security tool which will be made available to United States Government entities only. Companies which attain FedRAMP certification must demonstrate compliance with NIST 800-53 R4 which is a comprehensive set of security controls covering everything from Access Control, Contingency Planning, Incident Response, Physical & Environmental Protection, Personnel Security, and Risk Assessment. Within the 17 control families are 325 specific control objectives which have been tested by a third-party auditor and will be audited annually. Infoblox is also in the process of achieving Soc2TypeII certification.

Last updated October 2024