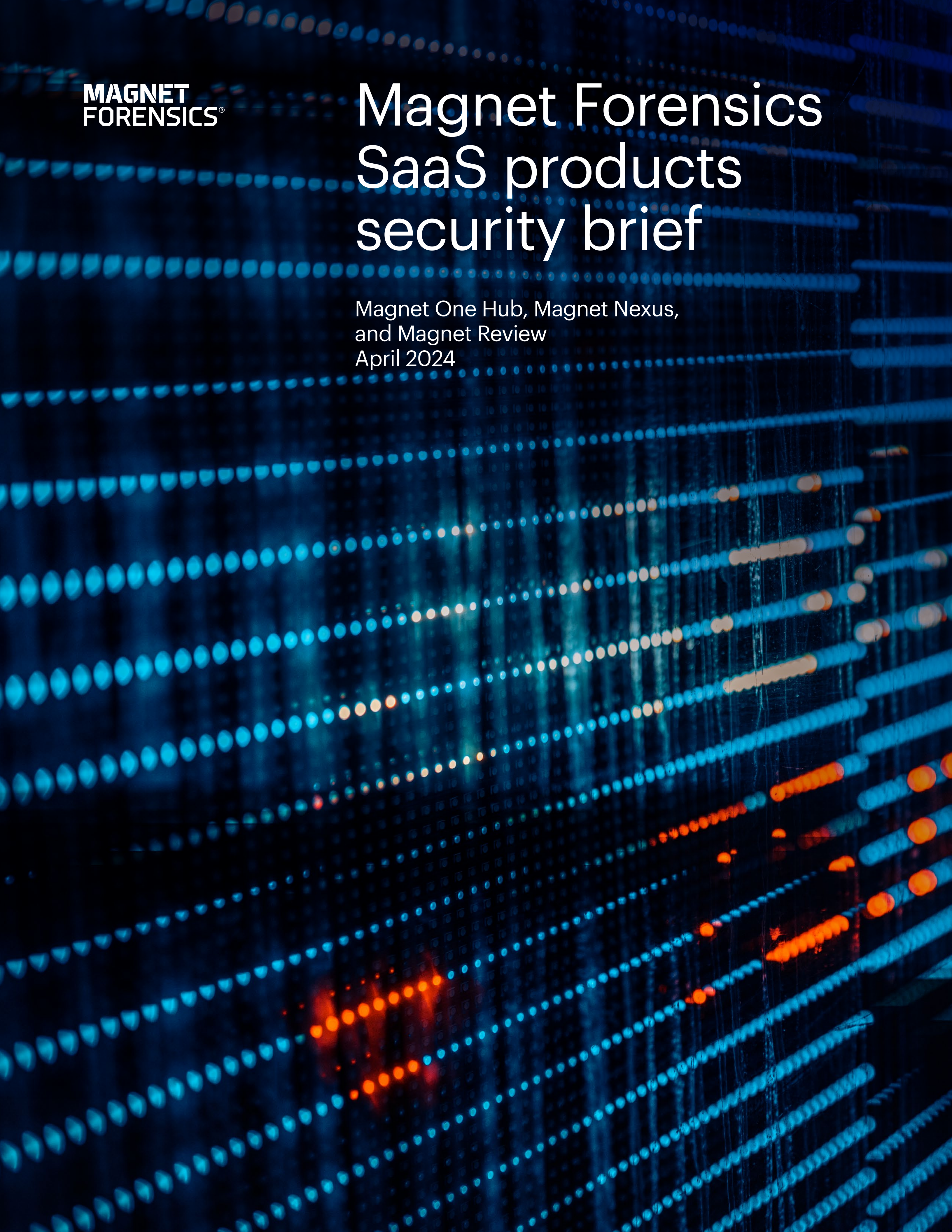


Magnet Forensics SaaS products security brief

Magnet One Hub, Magnet Nexus, and Magnet Review
April 2024

Introduction

Magnet Forensics takes the security and privacy of customer's data seriously. We work diligently to ensure that we’ve implemented and maintained proper security processes, standards, and procedures at all levels of our business.

This brief is aimed at providing you with information on our security infrastructure and practices as they apply to all generally available Magnet Forensics SaaS products.

For more details on how we handle any data we collect, please refer to our **Privacy Policy** and the data processing addendum to your SaaS agreement with Magnet Forensics. To learn more about our security practices, please visit **www.magnetforensics.com/security** or contact your Magnet Forensics sales representative.

Cloud infrastructure overview

Magnet Forensics SaaS products leverage cloud infrastructure and services offered by Amazon Web Services (AWS) to deliver processing, storage, and management capabilities to our clients. AWS's infrastructure, encompassing meticulously designed facilities, current network technology, and high-performance hardware, is at the heart of our SaaS offerings. This foundation is complemented by a comprehensive operational software suite that supports our system's provisioning and robust hosting.

Security and compliance practices

In addition to leveraging AWS infrastructure, Magnet Forensics has implemented a set of procedures, policies, technologies, and standards to help protect your more sensitive data.

- The AWS infrastructure was designed to offer industry-leading security measures, in compliance with standards and industry best practices. (For more details, please refer to https://aws.amazon.com/compliance/data-center/controls/).
- **SOC2 compliance** We aim to have all SaaS products undertake SOC2 compliance evaluations by authorized third-party auditors. Reports for each product are available upon request. For more information, please contact your Magnet Forensics sales representative.
- **AWS services** are used to monitor for threats, track and remediate vulnerabilities, patch systems in a timely manner, and ensure secure configurations throughout our environment to meet industry and Magnet Forensics standards. (CIS 1.4, NIST 800 53 v5, AFSBP).
- **Audit Logs** for both the application and infrastructure are gathered and written to an isolated, high-privilege location for audit purposes and to maintain integrity.
- The principles of least privilege and maximum workload isolation are used to limit Magnet Forensics staff access to only resources strictly required.
- **Data is encrypted** both in transit and at rest (AES-256 or higher for symmetric encryption, SHA-2 family for hashing, and RSA 2048 or longer key length for asymmetric encryption are our minimum standards). Additional controls are in place to further protect customer data by using separate encryption schemes and further limiting access to only people and systems who are required to have access.
- **Third-party audits**, including both penetration testing and compliance, are completed for each SaaS application on a yearly basis and as needed to ensure the security of our products as we add new features and functionality.
- Magnet Forensics routinely evaluates and tests our incident response practices including tabletop exercises to ensure robust familiarity across cooperating teams so they are prepared to react in the event of an incident.
- Risks to our products are constantly being evaluated and mitigated by building threat models, reducing attack surface, both external as well as internal, and are developed for our applications to build a structured approach to securing them.

Authentication and authorization

- Federation of users originating in customer directories is possible using either LDAP or SAML (depending on the Magnet Forensics application.)
- Multi-factor authentication (MFA): All users are encouraged or required to undergo multi-factor authentication, combining something they know (password or PIN), and something they have (security token or smartphone app).
- The system requires users to create strong passwords.
- Our solutions are built with role-based access control and least privilege in mind. Customers are encouraged to assign roles based on job functions, ensuring users have access only to the information and functionality necessary for their duties.

Availability practices

We have implemented robust measures to help provide smooth service delivery and uptime.

- Multiple region and availability zone support. Within each zone, auto-scaling enables the systems to recover from outages, downtime, or errors in the various web services.
- Full and incremental backups which are routinely captured and tested. Point-in-time-recovery (PITR) is available for many of our services to ensure even the latest data is recoverable in the event of a disaster or failure.
- Disaster recovery plans for all SaaS products and failover mechanisms that are routinely tested to ensure that important data is not lost.

Development and supply chain practices

Magnet Forensics has implemented the following development and supply chain practices to help ensure high standards of reliability and security:

- Magnet Forensics software is developed according to our Secure Development Lifecycle. This follows patterns established by both the **NIST 800-218 standard and the Microsoft SDL Practices.** (NIST 800-218 attestation available.)
- All code and system changes are reviewed and tested by both automated systems as well as manual peer reviews prior to merging into any product.
- All production **infrastructure is treated as code** to ensure that it can be stood up and torn down quickly and as frequently as needed. This also ensures all configurations are reviewed and tested to ensure any security and compliance requirements are met prior to deployment.
- **To reduce the risk of supply chain attacks**, Magnet Forensics rigorously reviews third-party software that is used to build Magnet applications for vulnerabilities, both at the time of original inclusion and on a continual basis allowing us to identify new threats and vulnerabilities quickly by knowing what components are in our products instantly.
- **Our development teams follow OWASP best practices** and guidelines to ensure that our software is built with security in mind–protecting against common web application vulnerabilities.
- **Vulnerability Disclosure Program**—with this program, we accept, review, and address disclosed software vulnerabilities in a timely fashion. Vulnerabilities can be reported at **securityconnect@magnetforensics.com**.

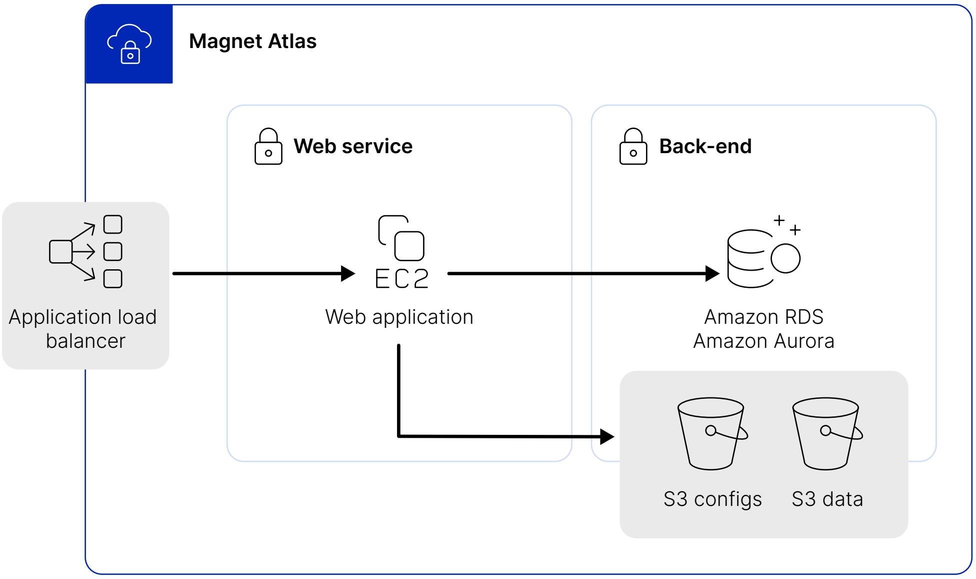
Region support

The table below provides a snapshot of current region support across Magnet Forensics SaaS products. This is subject to change as we add or consolidate regional support.

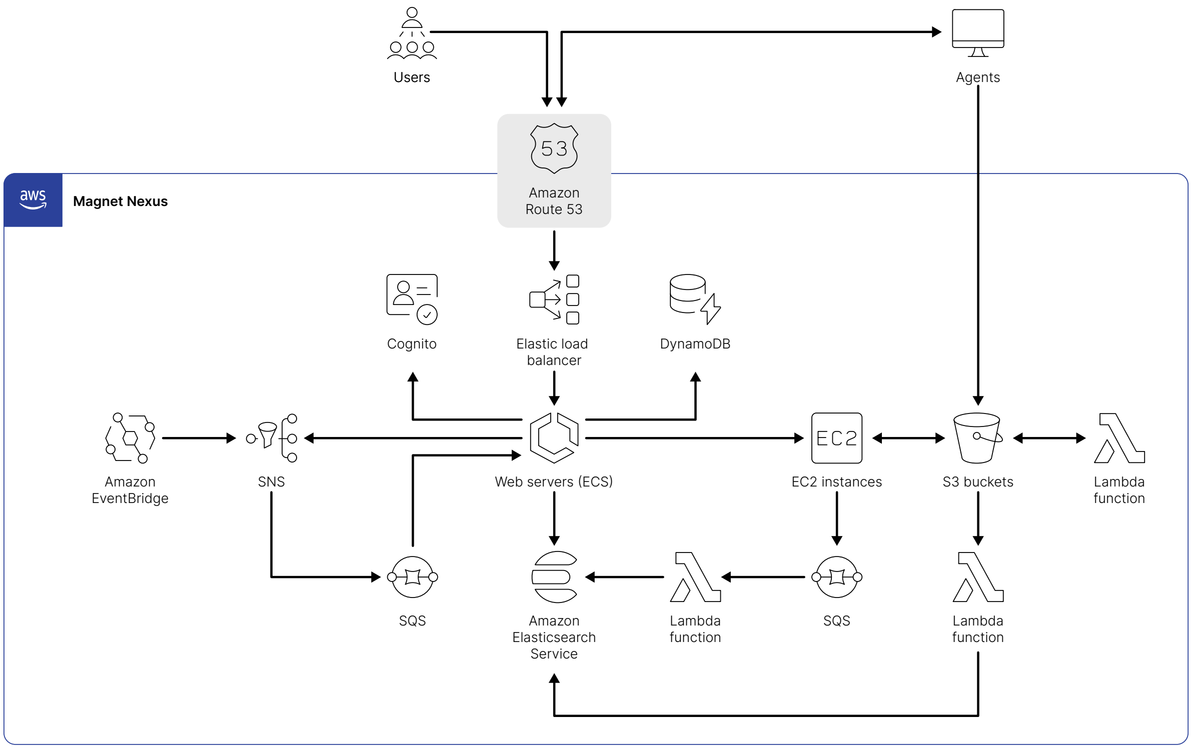
Customer case data is guaranteed to stay in the customer's selected region. User management functionality may store information in us-east-1 including Name, Email, Role, and Organization. Billing data may also be centralized in us-east-1.

Region	Magnet One Hub	Magnet Review	Magnet Nexus
us-east-1(US)	Yes	Yes	Yes
eu-central-1 (EU)	Yes	No	Yes
ca-central-1 (Canada)	Yes	No	No
ap-south-1 (India)	No	No	Yes

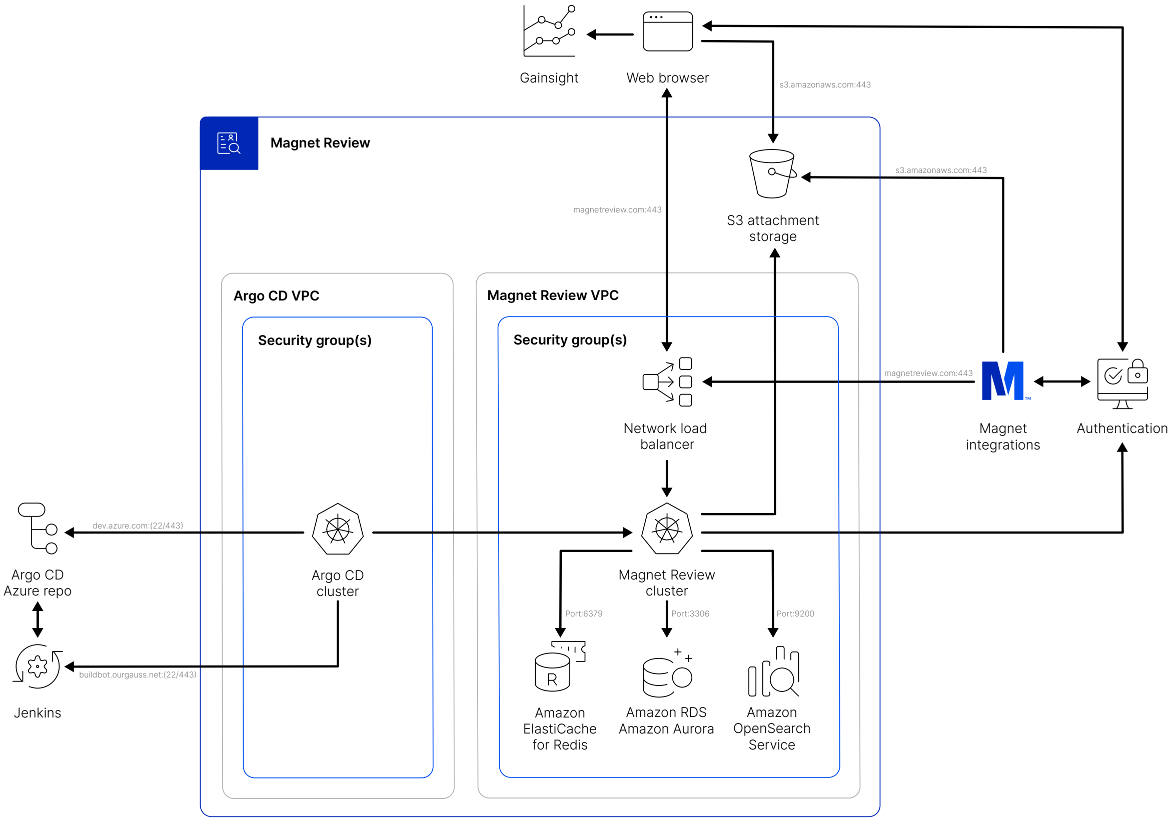
Magnet One Hub architecture diagram



Magnet Nexus architecture diagram



Magnet Review architecture diagram



MAGNET FORENSICS®

Learn more at magnetforensics.com

Book a demo today, call us at 1-844-638-7884 or email sales@magnetforensics.com