sonatype + Frontier

JAN 2026

Sonatype Repository Firewall Cloud

Service Definition

Contact for G-Cloud Enquiries: sonatype.gcloud@frontierhq.com / 0203 005 3237

Version 1.0



sonatype

Contents

1 Service Overview
2 Backup, Restore and Disaster Recovery
3 Onboarding and Offboarding Support
4 Service Constraints
5 Service Levels
6 After Sales Support
7 Technical Requirements
8 Outage and Maintenance Management
9 Hosting Options and Locations
10 Access to Data (Upon Exit)
11 Security

A Sonatype Workshops
B Customer Success from the Start
C Run Sonatype Anywhere

1. Service Overview

Sonatype Repository Firewall Cloud

Sonatype Repository Firewall Cloud prevents software supply chain attacks by automatically blocking malicious open-source components, malware, and vulnerabilities at the perimeter. Acting as a shield for your artifact repositories, it stops "next-gen" threats—including typosquatting, dependency confusion, and unknown "zero-day" malware—before they enter your SDLC.

Utilising advanced AI/ML behavioural analysis, Firewall enforces governance policies automatically, ensuring only secure, compliant, and high-quality components reach your developers. This shift-left approach reduces technical debt, accelerates DevSecOps pipelines, and ensures compliance with government security standards.





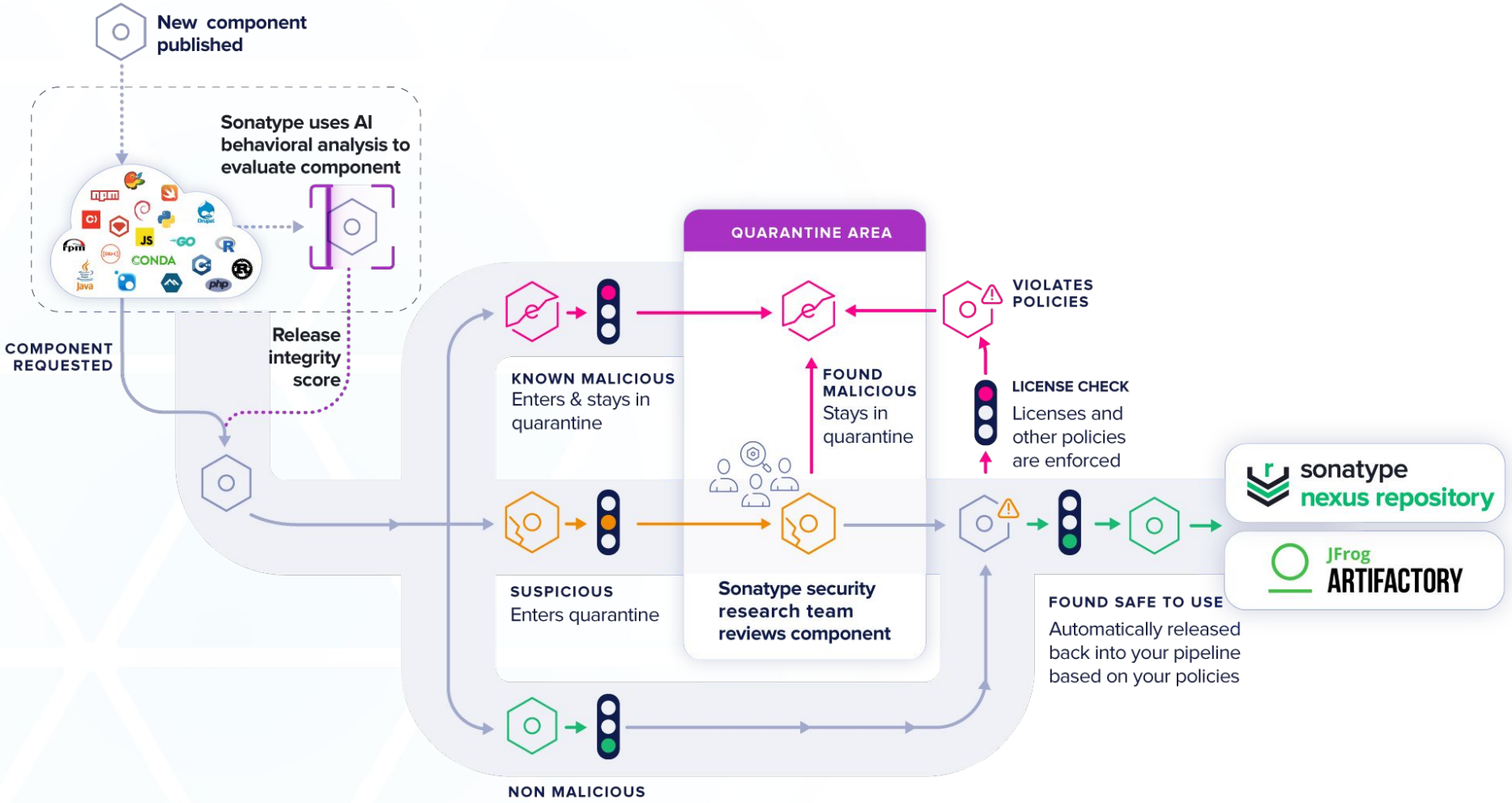
CLOUD | SELF-HOSTED | DISCONNECTED

Sonatype Repository Firewall is also available to run on customers' infrastructure or private clouds given Sonatype's "Run-Anywhere" approach.

For details on self-hosted and air-gapped installations - please contact us (sonatype.gcloud@frontierhq.com / 0203 005 3237).

Sonatype Repository Firewall

Powered by Proprietary AI/ML and the Industry's Best OSS Security Research Team



Block Growing OSS Malware Threat

2,941,296

Malicious Downloads Prevented by Sonatype

+3,300

malicious components added every 60 days in popular ecosystems like npm and PyPI

2. Backup, Restore, and Disaster Recovery

Sonatype Cloud

Disaster Recovery
In the event of a Disaster, our Disaster Recovery process is executed with the objective of restoring services in a different geographic region based on specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined per product. These objectives are measured from the point of formal Disaster declaration.

Sonatype's cloud platform uses AWS replication services to ensure minimum data loss when cutting over between regions. A Disaster is defined by Sonatype for losing an entire region of operational capabilities. In such an event, the following happens:

- An Incident is declared following the Incident Management process defined above;
- The databases that support the Sonatype cloud platform are automatically and continuously replicated to the designated fail over region;
- Runbooks are executed to stand up a replicate of the execution and application infrastructure in the failover region;
- Once service is restored, the Incident Management process is used to communicate restoring of service.

Because state is stored at the database level, the above process ensures we are able to recover at the closest possible state to the disaster level event. All tenants will be brought online at the same time with no preference given to one tenant over another.

All Disaster Recovery processes are tested with a full execution of the plan on a yearly basis. Execution of the Disaster Recovery plan follows the Incident Management process described above.

Solution	RTO	RPO
Repository Cloud	8 hours	1 hour
Firewall Cloud	8 hours	24 hours
Lifecycle Cloud	8 hours	24 hours
SBOM Manager Cloud	8 hours	24 hours

3. Onboarding & Offboarding

Sonatype Cloud

Onboarding

- Provisioning of the cloud instance is automated upon purchase
- Access to the Sonatype support portal and knowledge base is provided immediately
- Administrators are provided with documentation for configuring Single Sign-On (SSO) and connecting CI/CD pipelines
- Customer Success Managers (CSM) are available for enterprise tiers to guide initial configuration
- Additional Sonatype Workshops are available to get you up and running

Offboarding

- Customers are provided with a transition period to extract their data
- Upon contract termination, all customer data is securely deleted from the cloud environment in accordance with data protection standards (GDPR/Data Retention Policies)

4. Service Constraints

Sonatype Cloud

Maintenance

There are two types of maintenance performed on the platform:

1. Continuous Delivery
   The Sonatype Cloud platform is designed for continuous and seamless delivery of new features, capabilities and fixes. The vast majority of enhancements and version upgrades take place continuously providing an uninterrupted user experience and therefore require no down time nor maintenance window.

2. Scheduled Maintenance
   On occasion, scheduled downtimes for tenants are needed to perform maintenance that would be disruptive to users and processes. When such downtime is scheduled, affected customers will receive a notification from Customer Success in advance.

Customization

As a SaaS offering, deep infrastructure customization (e.g., access to the underlying OS or database) is not permitted. Configuration is managed via the User Interface (UI) or REST API.

Storage Limits

Storage caps may apply based on the specific subscription tier purchased.

5. Service Levels

Availability

Service Level Objective

Sonatype cloud products and processes are designed to meet a Service Level Objective (SLO) of 99.9% uptime.

Maintenance

There are two types of maintenance performed on the platform:

1. Continuous Delivery
   The Sonatype Cloud platform is designed for continuous and seamless delivery of new features, capabilities and fixes. The vast majority of enhancements and version upgrades take place continuously providing an uninterrupted user experience and therefore require no down time nor maintenance window.

2. Scheduled Maintenance
   On occasion, scheduled downtimes for tenants are needed to perform maintenance that would be disruptive to users and processes. When such downtime is scheduled, affected customers will receive a notification from Customer Success in advance.

Customization

As a SaaS offering, deep infrastructure customization (e.g., access to the underlying OS or database) is not permitted. Configuration is managed via the User Interface (UI) or REST API.

Storage Limits

Storage caps may apply based on the specific subscription tier purchased.

5. Service Levels

Support—Your Success is Our Priority

Our team is committed to helping you maximize the value of your software investment by providing timely, tailored support.

From addressing standard inquiries and managing urgent escalations to delivering hands-on professional services, we are here to ensure your success.

	Standard	Gold
Cost	Included	Contact Sales
Support Hours^	08:00 - 17:00 (Mon-Fri) Customer Local Time	08:00 - 17:00 (Mon-Fri) Customer Local Time
Maximum Initial Response Time±	Sev-1: 3 Hours Sev-2: 5 Hours Sev-3: 6 Hours Sev-4: 8 Hours	Sev-1: 1 Hours Sev-2: 2 Hours Sev-3: 4 Hours Sev-4: 6 Hours
Authorized Support Contacts	4	10
Remote Troubleshooting	✓	✓
Support Portal and Knowledge Base	✓	✓
Extended Support§	Optional	✓
Ticket Routing to Senior Support Staff	-	✓
Phone Support	-	✓
Chat Support	-	✓
Sonatype Professional Services*	-	✓

^ Excluding Company-wide and Sonatype Regional Holidays.

± All times calculated based on business hours.

§ Extended Support provides assistance with Sev-1 - Production Outages only, 24x7x365.

* Includes delivery of 1 service offering during your contract period. Supported service offerings are available at https://www.sonatype.com/learn-training-workshops.

6. After Sales Support

Always by your side

sonatype

Sonatype provides continuous support throughout the contract:

- **Customer Success**: Dedicated managers for qualifying accounts to assist with adoption and value realization - read more about our Customer Success
- **Knowledge Base**: Access to a searchable repository of technical guides and troubleshooting articles
- **Community**: Access to the Sonatype user community for peer-to-peer assistance and best practices
  https://community.sonatype.com

7. Technical Requirements

Always by your side

Client Access

Users access the repository via a standard modern web browser (Chrome, Firefox, Edge, Safari) and standard developer tools (e.g. Maven, Gradle NPM, pip, nuget).

Build Tools

Integration requires standard build tools (e.g., Maven, Gradle, npm, pip) or container clients (Docker) configured to point to the Nexus Repository Cloud URL.

Network

Outbound internet access via HTTPS (Port 443) is required to reach the service.

If you wish to self-host, or are on an air-gapped network - please see our Run Anywhere details.

8. Outage and Maintenance Management

sonatype

Status Page

Real-time service status, incident history, and scheduled maintenance details are to be published on a public status page at https://status.sonatype.com.

Incident Management

In the event of an unplanned outage, Sonatype's engineering team follows a formal Incident Response Plan to identify, triage, and resolve the issue. Root Cause Analysis (RCA) is available upon request for major incidents.

9. Hosting Options & Locations

sonatype

Cloud Provider

Sonatype's Cloud services are hosted on top-tier public cloud infrastructure (primarily AWS).

Data Residency

Options are generally available for hosting in the United States or the European Union (EU) to meet data sovereignty requirements.

Tenancy

The environment utilizes a secure multi-tenant architecture with logical data separation.

i If you wish to self-host, or are on an air-gapped network - please see our Run Anywhere details.

10. Access to Data (upon exit)

sonatype

Customers retain full ownership of their artifacts and metadata.

Data Export

Data can be retrieved via the standard Sonatype REST APIs.

Format

Artifacts are exported in their native formats (e.g., .jar, .tar.gz). APIs respond in JSON.

11. Security

Sonatype Cloud is built with a "Secure by Design" approach.

Certifications

The platform is SOC 2 Type II compliant. Sonatype also holds ISO-27001 certification.

Encryption

Data is encrypted at rest (AES-256) and in transit (TLS 1.2+).

Access Control

Support for SAML 2.0 and OIDC for Single Sign-On (SSO). Granular Role-Based Access Control (RBAC) allows administrators to define precise permissions for users and groups.

Vulnerability Scanning

The underlying infrastructure is subject to regular vulnerability scanning and penetration testing.

sonatype

A: Sonatype Workshops

A1 Sonatype Repository Firewall Health Check
A2 Sonatype Repository Firewall Advanced Deployment
A3 Sonatype Repository Firewall Policy Workshop

A1: Sonatype Repository Firewall Health Check

sonatype

A focused professional services engagement led by Sonatype experts that assesses your Sonatype Repository Firewall deployment.

KEY ACCOMPLISHMENTS:

- Establish a baseline of hardware specifications and application configuration
- Optimization of application and system configuration for stability, performance, and issue prevention
- Create maintenance strategy
- Learn administration best practices
- Post-session Health Check Report

DURATION

1-2 days
expert review

SCOPE

Expert review
config and usage

OUTPUT

Format report
and roadmap

RECOMMENDED FOR:

Ideal for organizations seeking to review existing deployments, evaluate configuration and alignment with best practice, identify risks prior to scaling, upgrades or migrations.

sonatype
repository firewall

A2: Sonatype Repository Firewall Advanced Deployment

sonatype

A comprehensive, multi-session virtual engagement where a Sonatype expert will jump start and accelerate your enhanced Sonatype deployment by guiding your team through planning, designing, implementing, and configuring the product in an optimal and supported environment.

KEY ACCOMPLISHMENTS:

DURATION

1-4 weeks
expert review

- Documented deployment and business requirements
- Documented architecture designs
- Deployed Sonatype environment with tailored configuration
- Integrated supported CI/CD tooling
- Documented Business Continuity Plan
- Documented next steps, maintenance, and best practices

RECOMMENDED FOR:

Ideal for organizations seeking to optimally deploy the Sonatype solutions and accelerate their timeline through the direct and hands-on assistance of Sonatype subject matter experts. Participants should include System Administrators, Architects, DevOps Engineers, and Program Managers.

sonatype
repository firewall

A3: Sonatype Repository Firewall Policy Workshop

sonatype

Introduces the core concepts of Sonatype Firewall policies that drive guidance and enforcement. This one-day workshop focuses on defining and configuring the rules for policy use and learning best practices for continuous policy-based component governance.

DURATION

1 day
expert lead

KEY ACCOMPLISHMENTS:

- Understand key policy creation and management concepts
- Test the policy to ensure actionable findings
- Develop strategies to refine policies over time
- Learn about approaches to ongoing enforcement

RECOMMENDED FOR:

- Ideal for any new user that is involved in policy creation and management including open source review board members, application security staff, architects, and the legal/compliance team.

sonatype
repository firewall

sonatype

B: Customer Success: Success from the Start

We are by your side

U.S. DEPARTMENT OF ENERGY

sonatype

BOTTLENECKS

The laboratory faced severe delays with security approval cycles lasting up to six months, which hindered productivity and forced costly context switching for developers working on sensitive nuclear energy software.

ACCELERATE

By implementing the Sonatype Platform to "shift security left," the organization automated the verification of open-source libraries and code quality, drastically reducing security review times from weeks to just a few hours.

ADOPTION

The initial success and flexibility of the tools inspired a grassroots DevSecOps movement, where different teams voluntarily adopted the platform and integrated it into their unique workflows without needing a top-down mandate.

Weeks → Hours

Processes that on average took weeks, were down to just a few hours.

"We have teams that go from concept to deployment in less than 24 hours, and that frequent incremental delivery of business value makes us incredibly productive."

See all our Customer Stories at https://www.sonatype.com/customer-stories.

sonatype

C: Run Anywhere

Run Anywhere

sonatype

Sonatype is the only Artifact Repository, Application Security Testing (AST) and Software Composition Analysis (SCA) tool flexible enough to run wherever you need. Simplify software supply chain management with a choice of three deployment options:

CLOUD

Get enterprise-grade security.

Our SOC and ISO 27001 certifications mean that security is built into every layer of our Cloud deployment.

Maximum benefit with minimal effort.

Let Sonatype Cloud take care of maintenance and infrastructure.

SELF-HOSTED

Host it your way.

Use Sonatype's platform with granular user control and host our tools under your preferred conditions.

AIR-GAPPED

For your most sensitive environments.

Our disconnected deployments are cut off from the public internet and are compatible with air-gapped environments.



Contact Us to discuss Self Hosted and Air-Gapped offerings in more detail.

Sonatype for Air-Gapped Networks

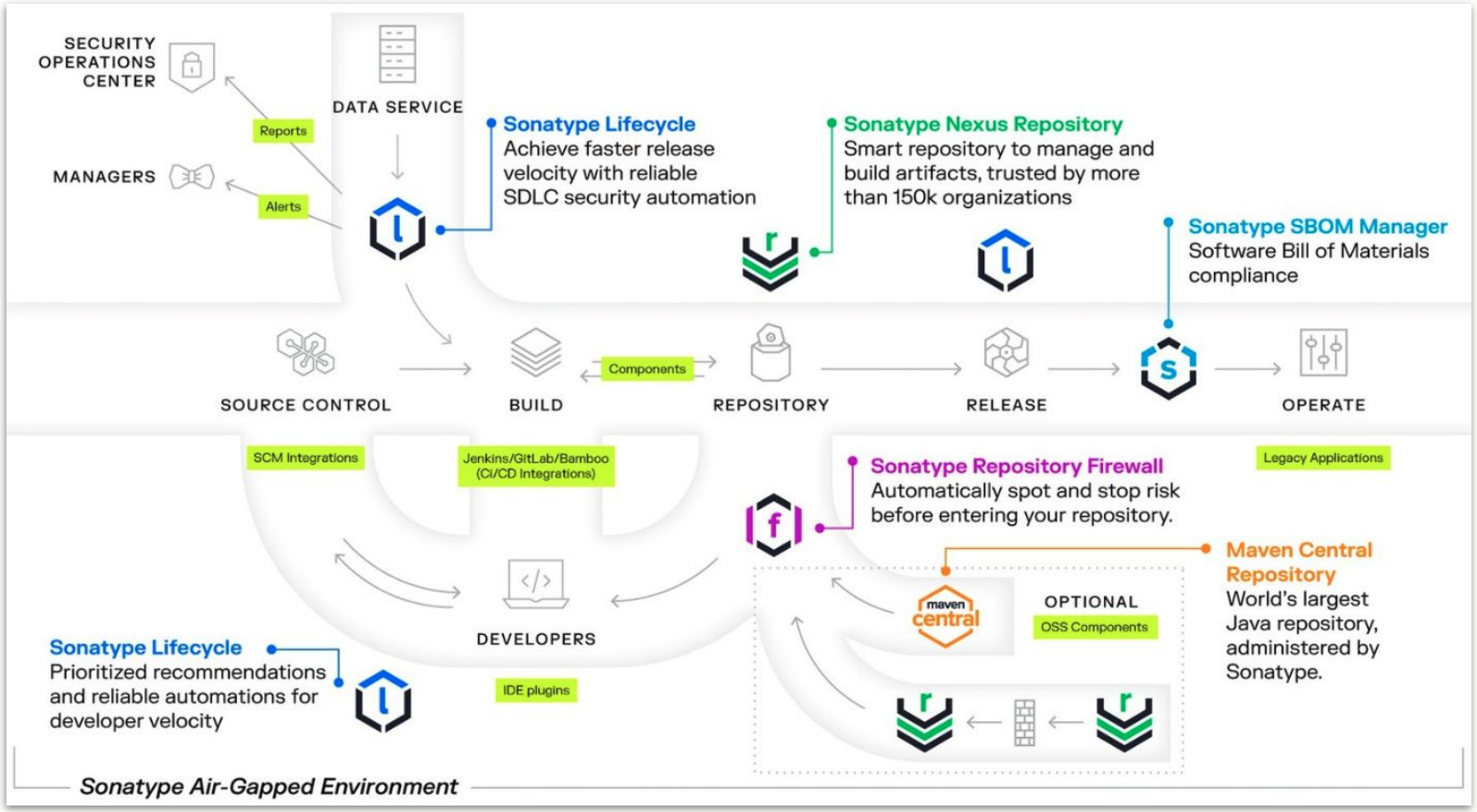
For teams with air-gapped DevOps Environments who want to utilize the full range of Sonatype's Platform without connection to the internet.

Sonatype Air-Gapped Environment (SAGE) is distributed as RPMs for 64-bit Red Hat 8 and 9. Specific tooling is additionally provided to obtain and apply data updates.

Requires:
- Java 17
- MySQL 8
- PostgreSQL 16

Storage Requirements:
- Data Service: ~5TB
- Maven Central: ~75TB

Daily Update Sizes:
- Data Service: ~15GB
- Maven Central: 5-75GB





+



Sonatype is the leader in secure software development built on open source and AI. As the maintainers of Maven Central and creators of Nexus Repository, Sonatype has spent two decades pioneering how the world manages and secures open source software — making Sonatype the trusted authority for modern software supply chains. With unmatched open source visibility and a unified product suite built for modern software development, Sonatype gives enterprises the intelligence and automated governance they need to harness the full potential of open source and AI. Sonatype handles the complexity behind the scenes: guiding component and model selection, blocking harmful malicious code, automating dependency and vulnerability management, and ensuring faster, more reliable builds — so developers spend more time on innovation and less time on remediation and rework. Trusted by more than 15 million developers, Sonatype helps power secure, modern software development at nearly 2,000 global organizations including 70% of the Fortune 100. To learn more about Sonatype, please visit **www.sonatype.com**.

Frontier is a platform engineering company who enable organisations to operate predictably and innovate safely by integrating technology that's secure by default, resilient, scalable, observable, maintainable and cost-effective. Frontier are experts in Kubernetes, Cloud, Data & AI, Security and Automation. They're trusted by major global organisations like Mastercard, HSBC, Fidelity International, and SITA. To learn more about Frontier, please visit **frontierhq.com**.