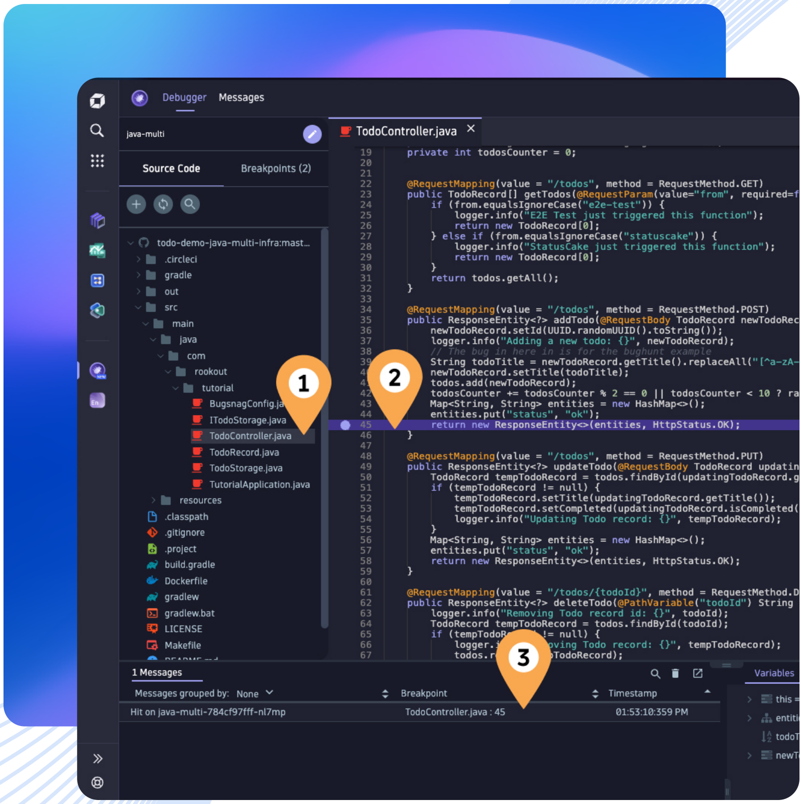
Live Debugger: Security and privacy

Dynatrace Live Debugger enables teams to identify and resolve IT issues more quickly—before they cost time, money, and before they affect users and data.



```
    private int todosCounter = 0;


    @RequestMapping(value = "/todos", method = RequestMethod.GET)
    public TodoRecord[] getTodos(@RequestParam(value="from", required=f
        if (from.equalsIgnoreCase("e2e-test")) {
            logger.info("E2E Test just triggered this function");
            return new TodoRecord[0];
        } else if (from.equalsIgnoreCase("statuscake")) {
            logger.info("StatusCake just triggered this function");
            return new TodoRecord[0];
        }
        return todos.getAll();
    }

    @RequestMapping(value = "/todos", method = RequestMethod.POST)
    public ResponseEntity<?> addTodo(@RequestBody TodoRecord newTodoRec
        newTodoRecord.setId(UUID.randomUUID().toString());
        logger.info("Adding a new todo: {}", newTodoRecord);
        // The bug in here in is for the bughunt example
        String todoTitle = newTodoRecord.getTitle().replaceAll("[^a-zA-
        newTodoRecord.setTitle(todoTitle);
        todos.add(newTodoRecord);
        todosCounter += todosCounter % 2 == 0 || todosCounter < 10 ? ra
        Map<String, String> entities = new HashMap<>();
        entities.put("status", "ok");
        return new ResponseEntity<>(entities, HttpStatus.OK);
    }

    @RequestMapping(value = "/todos", method = RequestMethod.PUT)
    public ResponseEntity<?> updateTodo(@RequestBody TodoRecord updatin
        TodoRecord tempTodoRecord = todos.findById(updatingTodoRecord.g
        if (tempTodoRecord != null) {
            tempTodoRecord.setTitle(updatingTodoRecord.getTitle());
            tempTodoRecord.setCompleted(updatingTodoRecord.isCompleted(
            logger.info("Updating Todo record: {}", tempTodoRecord);
        }
        Map<String, String> entities = new HashMap<>();
        entities.put("status", "ok");
        return new ResponseEntity<>(entities, HttpStatus.OK);
    }

    @RequestMapping(value = "/todos/{todoId}", method = RequestMethod.D
    public ResponseEntity<?> deleteTodo(@PathVariable("todoId") String
        logger.info("Removing Todo record id: {}", todoId);
        TodoRecord tempTodoRecord = todos.findById(todoId);
        if (tempTodoR      != null) {
            logger.i        oving Todo record: {}", tempTodoRecord);
            todos.r        TodoRecord);
```

```
Hit on java-multi-784cf97fff-nl7mp          TodoController.java : 45          01:53:10:359 PM
```

Introduction

Dynatrace Live Debugger is a cloud-native debugging and live data collection tool that allows software engineers to instantly access the code-level data they need to troubleshoot and understand complex, modern applications. Designed from the ground up for production environments, Dynatrace provides real-time answers to real-time questions, solving customer issues five times faster.

Architecture

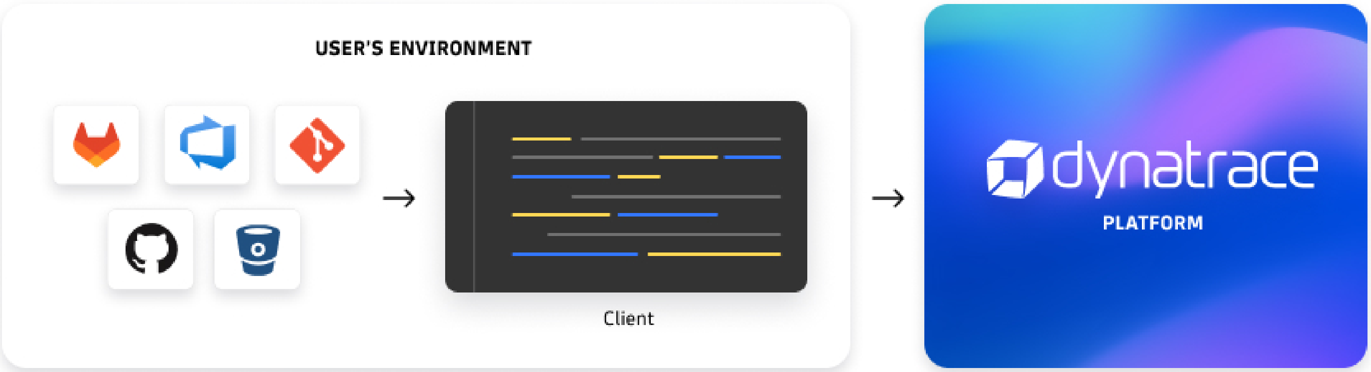
Software engineers use Dynatrace to securely connect to OneAgents deployed on application servers. This connection enables them to collect arbitrary application data using real-time instrumentation. Engineers can view the information using the Dynatrace web interface and/or designated integrated development environment (IDE) plug-ins for popular IDEs such as Visual Studio or JetBrains.

Real-time instrumentation collects new data without requiring engineers to write code or to redeploy or restart an application, drastically reducing time for data collection and troubleshooting.

Source code

Live Debugger integrates with source control management systems to display the correct source code revision and provide a seamless debugging experience. Designed from the ground up, this process aims to protect source code security and follow vendor best practices provided by the relevant vendors.

Source code is loaded only on an engineer's workstation, using engineer's privileges. Dynatrace servers never access, process, or store customer source code.



'*Data retention applies to Live Debugger only'.

Data security

Dynatrace provides teams with the following **security controls to prevent unauthorized access to data, maintain data accuracy, and ensure the correct use of information and its availability:**

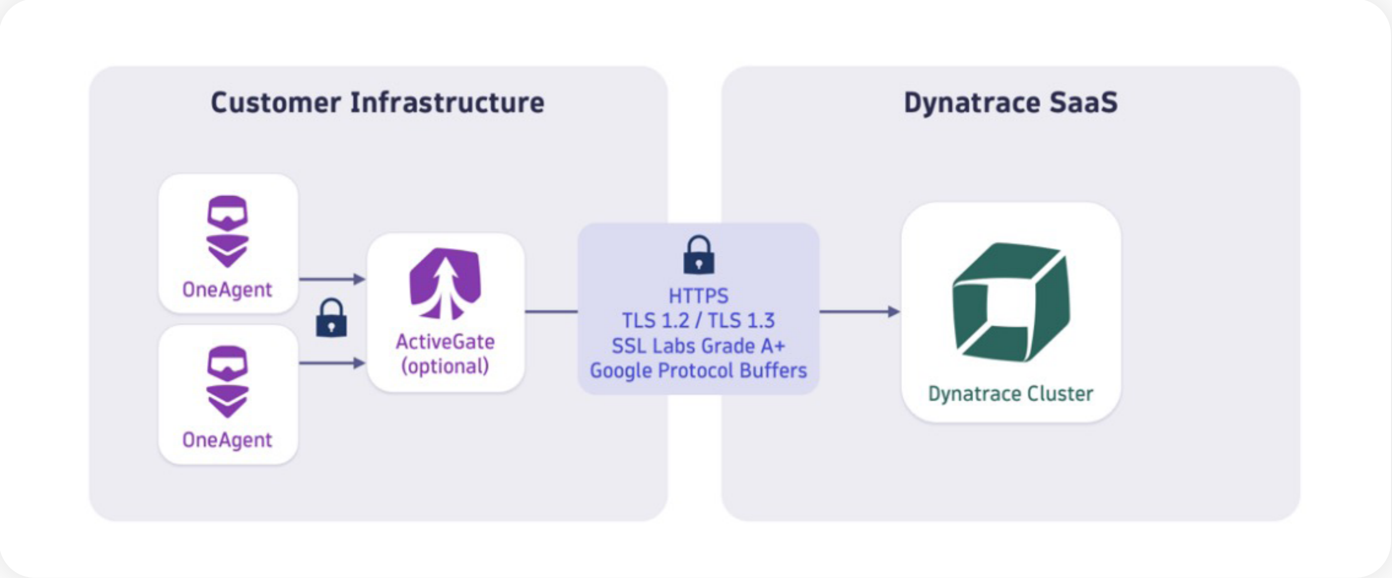
- **Infrastructure.** These security controls ensure that Dynatrace components (including OneAgent, ActiveGate, etc.) installed in an organization's infrastructure are always up to date and secure.
- **Dynatrace platform.** Dynatrace platform controls ensure that Dynatrace platform is securely up and running and that an organization's data is separate from other customers' data.
- **Your Dynatrace environment.** These security controls ensure that only authorized users can access the data in an organization's Dynatrace environment.

Data encryption. All data exchanged between OneAgent, ActiveGate, and Dynatrace platform is encrypted in transit. Dynatrace uses TLS 1.2 or TLS 1.3 (SSL Labs Grade A+).

Data at rest. Dynatrace is hosted in Amazon Web Services and Microsoft Azure, benefitting from the secure, world-class data centers. Dynatrace uses hardened configurations and ensure state-of-the-art AES-256 encryption and key management.

Comprehensive data security controls throughout Dynatrace platform. User authentication via single sign-on, or SSO. In Dynatrace SaaS, teams can manage users by setting up user groups and permissions with SAML.

Automatic integrity verification. Dynatrace signs every component that it builds to prevent man-in-the-middle manipulations. Such verification protects from supply chain attacks and validates that Dynatrace-provided software truly is from Dynatrace.



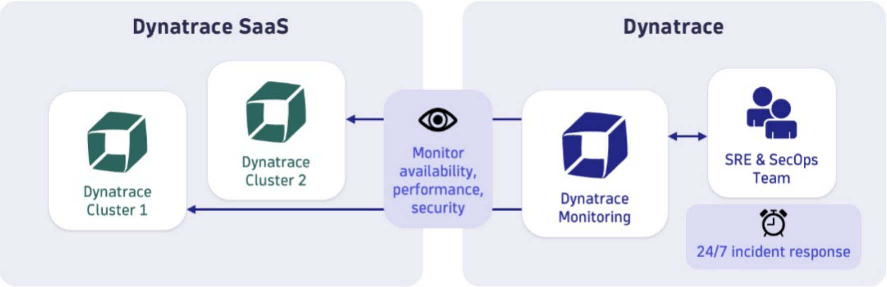
'*Data retention applies to Live Debugger only'.

Rollout of updates and hot fixes. The Dynatrace platform undergoes regular updates. Teams can control updates of OneAgent and ActiveGate. To keep an environment safe, hot fixes can be rolled out within a few hours.

Data access for Dynatrace support. Role-based access to Dynatrace SaaS environment ensures that only authorized users access the data. Audit logs provide full transparency over every instance of data access and changes. Soon, teams can require approval of every access to the user interface of a live environment by Dynatrace employees.

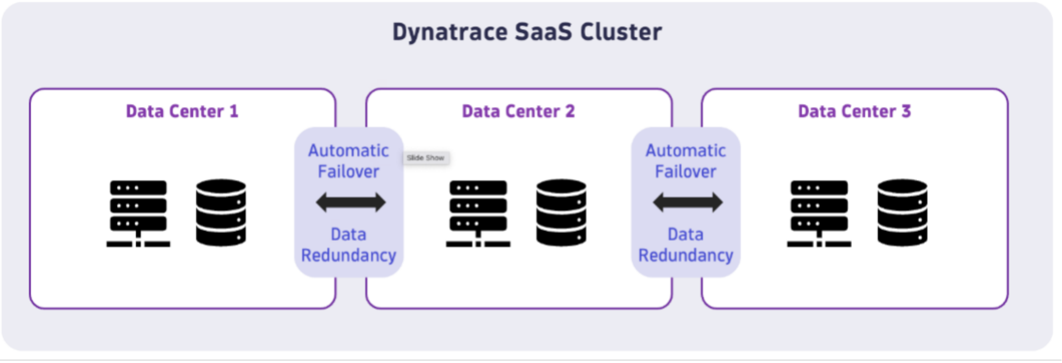
Data backups and disaster recovery. Regular backups (which occur every 24 hours) and backup that includes data for at least 30 days keep data protected from unexpected accidents.

Business continuity and high availability. Dynatrace SaaS uses a clustered architecture, multiple availability zones (data centers), and automatic fail over mechanisms to ensure high availability (with 99.5% availability in each service level agreement).



Infrastructure monitoring. A dedicated Dynatrace self-monitoring cluster monitors availability, performance, and security of all SaaS clusters.

Data segregation between customers. Dynatrace SaaS allocates one dedicated environment per customer account. Organizations' data is segregated logically from other customers' data.



'*Data retention applies to Live Debugger only'.

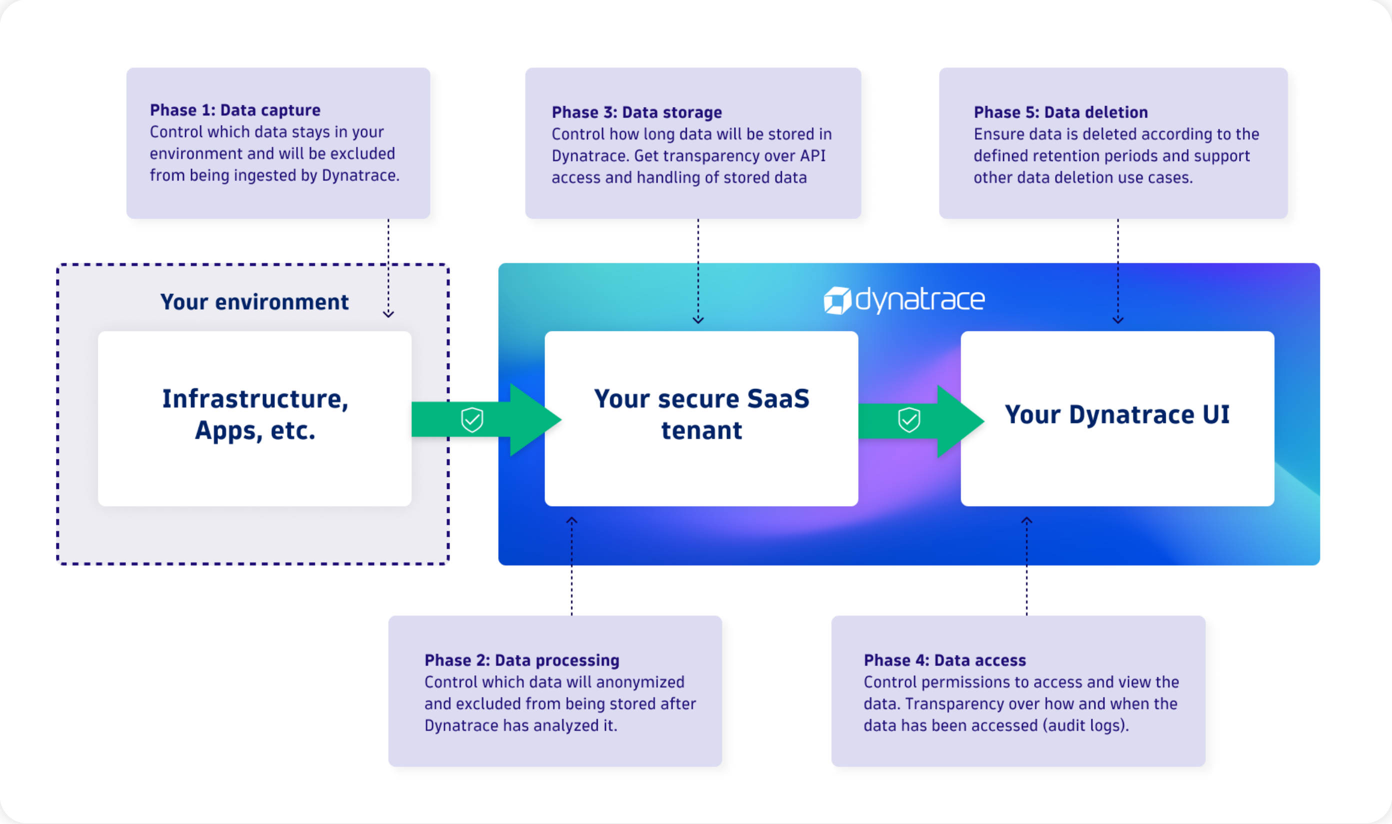
Data Privacy

Dynatrace protects data end to end. The Dynatrace platform is built and operated with strong privacy by design and privacy by default in place. Additional privacy configurations are available to enable you to maximize the value of the platform and meet the strictest privacy requirements.

1. Data masking: Protecting sensitive data on three levels.

Easily protect sensitive data and limit the data shared with Dynatrace.

- **Masking at capture.** This capability masks data at first contact with Dynatrace. The raw data does not leave the monitored environment.
- **Masking at ingest.** Implementing masking at ingest sends the data to Dynatrace for optimal analysis. The data is masked before it's stored.
- **Masking at display.** Masking at display stores data in its original form but limits certain fields' accessibility to the users of your choice.


Phase 1: Data capture
Control which data stays in your environment and will be excluded from being ingested by Dynatrace.
Phase 3: Data storage
Control how long data will be stored in Dynatrace. Get transparency over API access and handling of stored data
Phase 5: Data deletion
Ensure data is deleted according to the defined retention periods and support other data deletion use cases.
Your environment
Infrastructure, Apps, etc.
dynatrace
Your secure SaaS tenant
Your Dynatrace UI
Phase 2: Data processing
Control which data will anonymized and excluded from being stored after Dynatrace has analyzed it.
Phase 4: Data access
Control permissions to access and view the data. Transparency over how and when the data has been accessed (audit logs).

'*Data retention applies to Live Debugger only'.

2. Data access. Control access to data ingested by Dynatrace.

Flexible management of user permissions for sensitive data and monitored applications and services as well as transparent audit logging enable teams to automate control of access to organizational data.

Access to all functionalities within Dynatrace is managed using IAM (identity and access management), whether it is about collecting or reading data.

With IAM, customers can configure which users are allowed to place breakpoints within particular applications and environments.

Further access restrictions can be imposed for reading snapshot data with Grail, which is the Dynatrace data lakehouse. These restrictions use Grail's existing user permission system on a per-record level.

- **Access management:** Permission for users and user groups can be managed on globally on both levels
- **Account level:** Levels involve settings, users, billing, and so on.
- **Environment level:** This level involves monitoring environment, logs, configurations, and so on.
- **Audit logging:** Each access is logged, time-stamped, and made available in an automated way via the Dynatrace REST application programing interface or API.

3. Data retention*: Data is kept for 10 days to minimize privacy implications

4. Privacy rights: Efficient execution of customers' privacy rights Executing privacy requests of your customers to delete, amend or access their data is supported via

- **Customer support**
- **The Privacy Rights App (coming in 2024)**
- **Record-level hard deletion (coming in 2024)**

Compliance

Dynatrace provides independent verification that data security and privacy controls that Dynatrace implemented follow industry best practices and address compliance requirements: HIPAA, FedRAMP, StateRAMP, SOC 2 Type II, FIPS 140-2, ISO 27001 , TISAX, GDPR, IRAP, CSA , External pen-tests, AWS PrivateLink, PIPEDA, CCPA, Red team pen-tests, Hackerone, etc.

'*Data retention applies to Live Debugger only'.

Learn more

visit the Trust Center or explore documentation.

dynatrace