New Relic®

Security Information & Policies

 | 188 Spear Street, Suite 1200, San Francisco, CA 94105 | www.newrelic.com

Table of Contents

Overview

This document is intended to provide a high-level overview of the New Relic Security Program and Practices, as well as an overview of the security features and functionality of the New Relic Service and Applications. It addresses the most common concerns customers may have about security and privacy, while outlining the security controls available within New Relic services. The security provided by New Relic allows for customers to install the service in many regulated environments.

CHAPTER ONE:

Security Program Overview

New Relic is committed to the security of your application's performance data. We use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure.

The New Relic security program is led by the Director of Information Security and Compliance and is responsible for the following areas:

- Application Security
- Compliance
- Privacy
- Corporate Security
- Physical Security

All New Relic employees are informed of their security responsibilities and receive annual security awareness training.

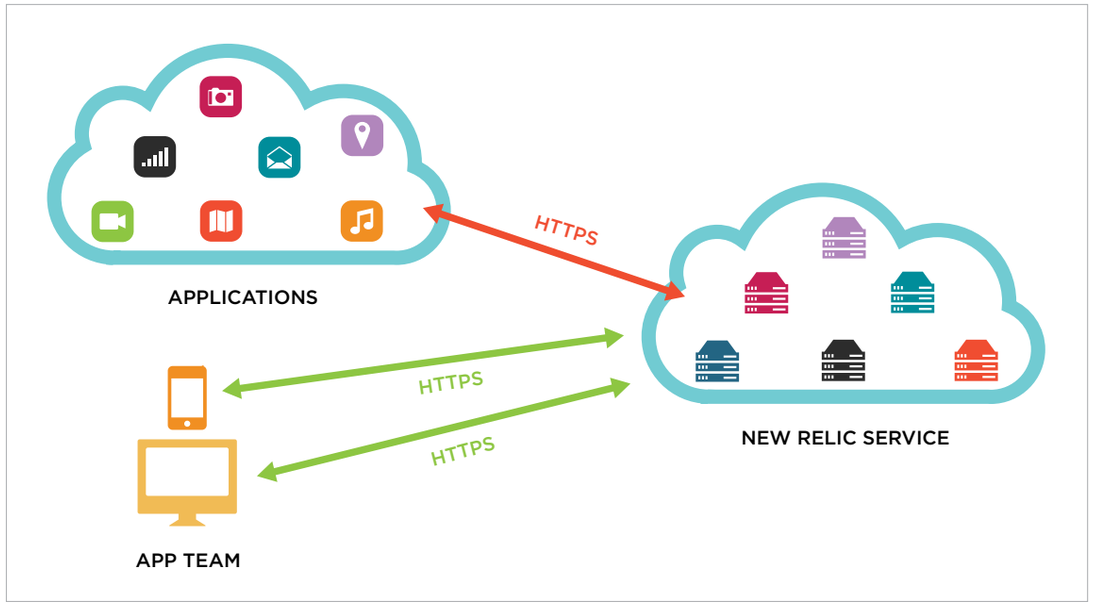
CHAPTER TWO:

Product Overview

New Relic collects performance data points from applications and systems, uploads those data points to the New Relic service, and presents application performance information through a secure website.

Basically, New Relic works like this:

- Run applications in data center, cloud, or hybrid environments.
- Install the New Relic Agent in applications and/or servers.
- The New Relic Agent sends performance data points to the New Relic service.
- The New Relic service aggregates and stores the application performance and data points in our tier 3 SSAE 16 certified data center.
- Visualizations of application performance data are available via New Relic's SSL-encrypted and password-protected website (https://rpm.newrelic.com) or via the New Relic mobile applications.



New Relic's optional Browser service (formerly known as RUM, or Real User Monitoring), meanwhile, collects data directly from your real users' browsers so you can understand their experience with your software from their perspective.

CHAPTER THREE:

Data Collected

New Relic collects performance data only for the applications and/or servers where the New Relic Agent is installed. In general, this includes aggregate time measurements for application transactions and webpage loading, application errors and transaction traces, and server resource-utilization statistics. By default, HTTP parameters are not included in Application Errors, and literal values in the "where" clauses of SQL statements are obfuscated.

The New Relic application monitoring agent collects:

- Application request activity, including view and controller breakdowns
- Database query activity, including create, update, and delete breakdowns
- View activity
- Requests that result in an error
- Process memory and CPU usage

New Relic Pro customers have the option to have the application monitoring agent collect application errors and transaction traces.

The New Relic server monitoring agent collects:

- CPU utilization
- Memory utilization
- Disk utilization and usage
- Network utilization

New Relic services do not collect any sensitive or personal information—nor any data used or stored by a monitored application. By default, New Relic is configured to not collect any HTTP parameters or any literal values in the "where" clauses of SQL statements. These values are removed before being sent to New Relic. Note that if Real User Monitoring is in use, then New Relic will see (but not store) end-user IP addresses.

CHAPTER FOUR:

Privacy & Confidentiality

New Relic is committed to protecting your privacy. We have been awarded TRUSTe's Privacy Seal signifying that our privacy policy and practices have been reviewed and validated by TRUSTe, an independent third party.

Application data we collect is primarily used to display application performance information back to the account user. It is also used by New Relic personnel to answer questions that customers may have about their account and to develop and improve our products.

We may also aggregate application data across multiple accounts and use this data to create and publish industry benchmarks or comparative application performance metrics. Individual transaction data collected by New Relic is obfuscated by default.

We may share your application data with third parties to provide technical support or to provide specific services. If you are using New Relic via one of our partner companies, we may provide application data to that partner company on a confidential basis in order to assist them in providing customer support.

New Relic may disclose application data if it believes that such disclosure is necessary to comply with relevant laws or to respond to subpoenas or to protect the rights or property of New Relic or its users.

Except as otherwise stated in our privacy policy, we do not sell, trade, share, or rent the personal data collected from our services to third parties. You expressly consent to the sharing of your personal data" as described in this policy. We do not use the data for marketing or sales purposes.

More information on our privacy policies is available at https://newrelic.com/privacy.

CHAPTER FIVE:

Data Center Security & Location

New Relic is hosted in the U.S. at our secure tier 3 SSAE 16 certified data center with fully redundant power backup systems, fire suppression systems, security guards, and biometric authentication systems.

CHAPTER SIX:

Data Protection

New Relic encrypts performance data in transit.

SSL encryption is enabled by default for data being sent to New Relic (data in transit). Data collected and stored by New Relic (data in storage) is not encrypted. By default, New Relic services do not collect or store any sensitive customer data.

The New Relic agent does not open a hole in customer firewalls.

All communication from agents to the New Relic servers is outbound on either port 80 or 443 and can be configured to use a proxy server. New Relic agents do not need to listen for incoming connections.

New Relic does not have the ability to auto-update agents installed on your servers.

All updates must be manually installed by our customers.

Upon termination of New Relic services, all data will be expired out of New Relic systems (including backups) within 90 days.

CHAPTER SEVEN:

EU Considerations

New Relic is E.U. Safe Harbor Certified. New Relic is hosted in the U.S. at our tier 3 SSAE 16 certified data center.

New Relic believes that RUM (Real User Monitoring) cookies comply with the spirit of the EU Privacy and Electronic Communications (EC) Directive because they are not persistently stored, they are not used to personalize content, and they could be considered “strictly necessary” as they are used to monitor the health of the application.

By default New Relic does not collect any personal information from our customers’ customers. If Real User Monitoring is in use, then New Relic will see (but not store) end-user IP addresses; the IP address is immediately translated into a geographical region and then discarded.

CHAPTER EIGHT:

Application Security

New Relic maintains a robust application security program. Developers receive application security training in areas including the OWASP Top 10, all projects go through a mandatory security review by the security team, and we perform continuous application vulnerability scanning on both our staging and production environment. We have also implemented automated static code analysis and perform regular third-party security assessments.

CHAPTER NINE:

Security Policy

New Relic maintains a robust set of Security Policies that are updated annually. These cover the following areas:

- **Information security program management**
- **Information security policy management**
- **Information security compliance**
- **Information asset management**
- **Personnel security**
- **Physical security**
- **Mobile device security**
- **Network, system, and operation security**
- **Access management**
- **System and software lifecycle**
- **Vulnerability management**
- **Security monitoring**
- **Security incident and events**
- **Business continuity and disaster recovery**

CHAPTER TEN:

Audits & Certifications

New Relic undergoes annual SOC 2 Type II audits to provide ourselves and our customers with independent, third-party assurance that we are in fact taking the appropriate steps to protect our systems and our customer's data. In addition, data is stored in a tier 3 SSAE 16 certified data center.

New Relic is also a member of the Cloud Security Alliance (CSA) and has proudly published the results of our Security, Trust & Assurance Registry (STAR) self-assessment on the CSA website. These results, which include detailed information about New Relic security controls, can be found at https://cloudsecurityalliance.org/star/.

CHAPTER ELEVEN:

User Management

New Relic uses email addresses for customer usernames. Passwords must be a minimum of eight characters and must include at least one number or special character. No password expiration requirements are enforced. User passwords are stored in an industry standard encrypted hash format.

New Relic supports single sign-on (SSO) via Ping Identity, Okta, OneLogin, Auth0, and SiteMinder, and should work with any other identity provider that supports SAML 2.0.

New Relic allows an unlimited number of authorized users to be associated with an individual account. Users can be assigned to one of the following roles: Owner, Admin, User, and Restricted User.

Customers are responsible for managing their own accounts, including provisioning and de-provisioning their own users.

CHAPTER TWELVE:

Security Configurations

New Relic offers the following security configuration options:

- Transaction traces can be configured to either obfuscate (remove) literal values in the “where” clauses of SQL statements (this is the default), or to not send any SQL statements.
- Agents can be configured not to collect HTTP parameters (this is the default).
- Enterprise Security mode can be set to force SQL obfuscation, force filtering of HTTP parameters, and force the use of SSL. Once set, Enterprise Security mode can be disabled only by the New Relic support team. This is to prevent users from accidentally disabling these security controls.

CHAPTER THIRTEEN:

Disaster Recovery & Planning

New Relic maintains a Disaster Recovery (DR) plan for our SaaS service. This plan is updated and tested annually.

CHAPTER FOURTEEN:

Compliance

New Relic can be installed in a PCI-compliant environment. By default, New Relic does not receive any cardholder data. In addition, the New Relic agent can be configured to run behind a proxy to satisfy the PCI requirement to not allow any direct connections between the Internet and the cardholder data environment.

If installed properly, New Relic can be safely deployed in a healthcare environment without impacting HIPAA compliance obligations. By default, New Relic will not receive any protected health information.

Customers running New Relic in compliant environments should strongly consider enabling High Security Mode.