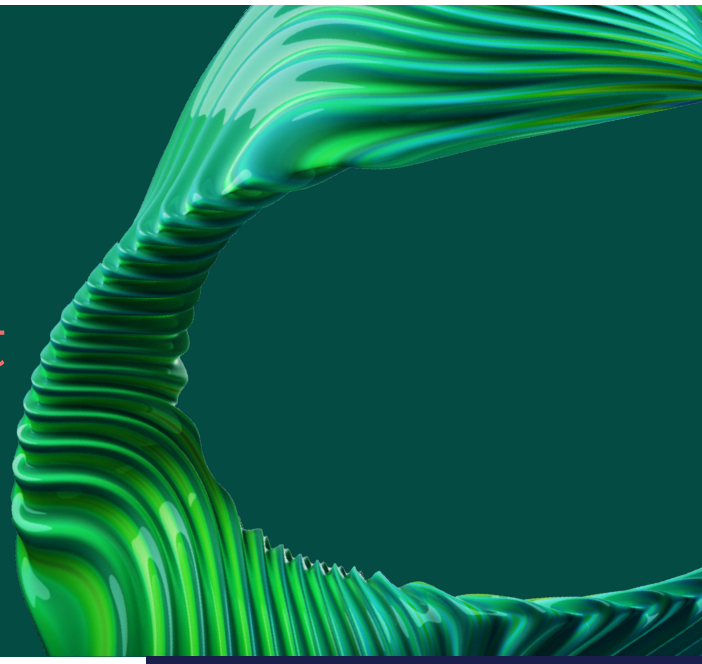
Contrast SECURITY

Visualizing what vulnerabilities were detected for each project

NTT DATA further strengthens security governance by enabling vulnerability detection and correction at an early stage of the web application development process



NTT DATA

Description of Business

With the frequent occurrence of security incidents caused by vulnerabilities in web applications both in Japan and overseas, customers are increasingly demanding the development of secure web applications that are free of serious vulnerabilities.

In order to ensure security while maintaining development schedules, NTT DATA has incorporated Contrast Assess into its development process to automatically detect vulnerabilities and correct them at an early stage in the development process.

At a glance

COMPANY PROFILE

COMPANY NAME
NTT DATA Corporation

MARKET CAPITALIZATION
¥142.52 billion

NUMBER OF EMPLOYEES
151,600
(group total as of March 31, 2022)

ADDRESS
Toyosu 3-3-3, Koto-ku, Tokyo

WEBSITE
www.nttdata.com

While expectations are rising for secure web applications, security diagnostics remain a bottleneck in development

As one of Japan's largest system integrators, NTT DATA has been designing, building and operating IT systems for many organizations and enterprises, such as the Japanese government, public offices, telecommunications and financial institutions. In recent years, the increasing number of sophisticated cyberattacks have made customers more security-conscious, leading them to choose NTT DATA as a partner that they trust —and expect — will ensure security.

"There are two aspects to security. One is to protect NTT DATA itself. The other is to provide security for our customers. Security is involved in various aspects, some by combining solutions to provide security as a business and others to keep the web applications we provide to our customers secure," said Hiroaki Kamoda, Head of Cyber Security Department, NTT DATA Corporation.

However, if the company is too rigidly bound by security, it risks putting a brake on innovation. "If we were to tie up the distribution of information too tightly, we might not be able to provide full services to our customers, so we have been aware of the need to strike a balance between ensuring information security and effectively utilizing information since we created the Security Governance Department in our company," Kamoda said.

This approach also applies to the systems NTT DATA provides to customers. "The security of the systems we provide is an important condition for our customers to be able to concentrate on their core business. We are required to provide secure systems to support our customers' business," Kamoda said.

In such situations, NTT DATA has taken measures to ensure the security of systems for customers and to monitor the status of vulnerability response, mainly through the Information Security Office, one of the groups that form the information security management team. Specifically, NTT DATA has formulated the Security Quality Standards — a set of guidelines defining the procedures for secure system development — and has established a rule that all web applications must be checked by an external diagnostic service before release to ensure that applications go live with no serious vulnerabilities.

However, the company gradually began to feel the impact on the development projects. "If multiple vulnerabilities are found just before release as a result of security diagnosis, the release may get postponed. On the other hand, security testing cannot be performed until the application is completed to some extent. As a result, security tests to ensure secure development had become a bottleneck that slowed down the development speed," according to Satoshi Seimiya, Assistant Manager of the Information Security Office, Cyber Security Department, NTT DATA Corporation.

In addition, due to various factors such as budget and release timing, the company had no choice but to limit the scope of testing to only a portion of the web application. The risk of vulnerabilities remaining in areas outside the scope could not be ruled out if they might lead to a security incident.

In parallel, NTT DATA had been training security engineers with the skills to perform security assessments and was also working to ensure project security. However, "The number of projects NTT DATA is involved in is extremely large, and it is difficult to assign personnel to all projects in an organized manner. In addition, since false negatives inevitably occur when monitoring by humans, it was difficult to completely cover all the vulnerabilities," Kamoda said.

The key is to enable vulnerability testing during the development process with a high level of accuracy and to monitor it in real time.

Around 2019, when NTT DATA was looking for a solution to automate security testing to solve such issues, Interactive Application Security Testing (IAST) began to catch attention in the security testing market.

"Until then, we had been using DAST [Dynamic Application Security Testing] for diagnostics, but it was causing the problem of affecting our development schedule. In some projects, we also used SAST [Static Application Security Testing] to diagnose code during the development process, but this inevitably resulted in detecting a large number of false positives and false negatives," Seimiya said. NTT DATA saw the potential of IAST and narrowed down the IAST solution candidates from several perspectives.

"First of all, if we were going to use it as SaaS [software as a service], we needed to be able to use a dedicated instance for NTT DATA at a tenant in Japan, not a shared instance," Seimiya continued. "In addition, some projects are developed in environments without internet access, so vulnerability testing needed to be performed in an on-premise environment. The third requirement was that the governance team should be able to monitor in real time 'what vulnerabilities are being detected now,' and also it should be the same level of accuracy as the security testing service provided by NTT DATA INTELLILINK Corporation, which was being used at that time."

Contrast Assess emerged as a candidate to meet these requirements. NTT DATA further conducted an evaluation test along with other candidates to confirm its performance of vulnerability detection.

"NTT DATA has been analyzing trends in vulnerabilities detected during web application development. We checked whether the vulnerabilities from this analysis could be detected by Contrast Assess and also evaluated whether there were any false negatives or false positives using the OWASP Benchmark. As a result, we determined that Contrast Assess was able to detect high-risk vulnerabilities with a lower false positive rate than other tools, minimizing the need to respond to false positives," Seimiya summarized. In addition, Contrast Assess was chosen after confirming that it could meet those non-functional requirements mentioned previously, as well as having an easy-to-use management console. The fact that NTT DATA's cloud-native platform iQuattro® already had been using Contrast Assess was an additional reason for the decision.

Visualize vulnerability detection and release applications after fixing them completely

NTT DATA has officially introduced Contrast Assess after a two-year trial. Since FY2022, the company has also made it a rule to conduct vulnerability tests using Contrast Assess at the integration test phase for all web application development projects that meet the policy requirements.

“Before using Contrast Assess, security testing was mandatory, but in some cases it depended on the project. However, as a result of introducing Contrast Assess, we are now able to test for vulnerabilities during the development process, and we no longer have to release a product before all the fixes get complete,” Kamoda said.

When a new development project begins, first it gets checked by Contrast Assess to see if it is subject to vulnerability testing. If it is determined that the project is eligible, the Information Security Office, which is the governance unit, dispenses a Contrast Server account, and the person in charge of each development project conducts the vulnerability test in the development process. When new functions are added, they get tested in the same manner.

Since there are a wide variety of factors that affect the development schedule, it is difficult to measure how much time has been shortened specifically by using Contrast Assess. However, “It is certain that we have been able to release the applications with zero high-risk vulnerabilities, which were all detected by Contrast Assess,” said Seimiya.

“Typical vulnerabilities such as SQL injection are detected and fixed early by the tool. In addition, as in the past, security tests are conducted by a testing service provider prior to release, so that vulnerabilities that cannot be detected by the tools, such as Broken Access Control, can be found and fixed quickly in time,” Seimiya added. Instead of being rushed just before a release, the Information Security Office is able to check for vulnerabilities early in the development cycle and provide advice as needed.

The Information Security Office has already been using Contrast Assess in dozens of projects, and the developers involved in those projects have generally given it high marks. “The ease of implementation, which requires only placing the agent file on the application server and slightly rewriting the configuration file, has been receiving a positive impression,” Seimiya said.

Furthermore, “Since the interface is easy to understand even for those who are not security experts, multiple members are able to discuss [issues] by looking at vulnerability information and reference information,” Seimiya said.

The Information Security Office also feels the benefits of this system. “From the perspective of security governance, the office is now able to visualize what vulnerabilities are detected, how many are detected and how well they are handled through the dashboard on a daily basis. Developers are able to confirm high-risk vulnerabilities at an early stage and check that all detected high-risk vulnerabilities have been confirmed and addressed, which in the past would sometimes be discovered just before a release,” Seimiya said.

Contrast SECURITY

NTT DATA has also been satisfied with Contrast Security's support service. "The daily support has, of course, been very good, but they also respond promptly when we have a problem. We have been able to work out issues with a mutual consensus on how to approach them, and Contrast has also been addressing our unique requests with sincerity," said Seimiya. He has trust in Contrast's support team in Japan — especially now that Contrast provides the Japanese version of product updates almost at the same time as the English version.

Currently evaluating Contrast SCA to further establish supply-chain security

As the Apache Log4j vulnerability showed, in recent years, it has become a challenge to address not only vulnerabilities in web application code, but also vulnerabilities in the open-source libraries used in those applications. NTT DATA has turned its attention to this area as well. To tackle the issue, NTT DATA has begun working on supply-chain security, beginning evaluation of Contrast SCA in FY2021.

"Contrast SCA allows us to verify whether or not a zero-day vulnerability has been identified in an OSS [Open-Source Software] library or component and whether or not the component is being used, as well as whether it can be affected or not. Since Contrast SCA also has a function to output a [Software Bill of Materials (SBOM)], we are currently evaluating whether we can utilize the SBOM in the software supply chain using Contrast SCA," Seimiya said. In this way, the company is exploring ways to efficiently manage SBOMs and vulnerabilities while involving partners and customers.

Even before the introduction of Contrast Assess, NTT DATA had been monitoring and analyzing the types of web application vulnerabilities detected through their development projects. "Since we started using Contrast Assess, we have been getting a good feeling that we are able to analyze in real time what kind of vulnerabilities are detected, how long it takes to fix them, and how much damage could be created if the vulnerabilities were left unfixed, depending on the timing of security tests and characteristics and scale of the project. By visualizing such data, we expect that NTT DATA as a whole will have a greater sense of urgency, which will lead to improvements in the level of secure development," Kamoda said.

Based on these results, NTT DATA plans to establish rules for vulnerability tests by IAST tools, such as Contrast Assess, not only at the NTT DATA headquarters but also at group companies, so that the entire group can work together to ensure the security of web applications. In addition, while utilizing Contrast SCA, they plan to work on the maintenance of SBOMs, ensuring traceability across the entire development supply chain and prompt vulnerability response, with continued faith in the power of Contrast Security.

Contrast SECURITY

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333

Contrast SECURITY

contrastsecurity.com