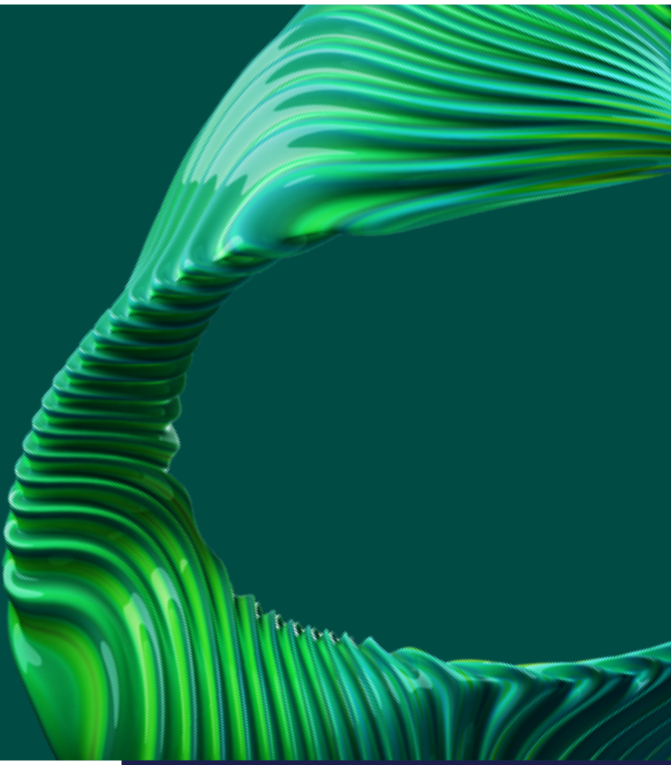
Contrast SECURITY

CM.COM

Improves Security and Efficiency while Reducing Risk



About the Company

CM.com was founded in 1999 by Jeroen van Glabbeek and Gilbert Gooijers as ClubMessage. They introduced group SMS messaging to the marketplace. Early customers included discotheques in the Benelux region, which engaged with their customers by texting out information about guest DJs, timetables, contests, discounts, and more weekend news—right at the exact moment it mattered for the visitor. More than two decades later, CM.com has become a global leader in cloud software for conversational commerce that enables businesses to deliver a superior customer experience. Their communications and payments platform empowers marketing, sales, and customer support to automate engagement with customers across multiple mobile channels, blended with seamless payment capabilities that drive sales, gain customers, and increase customer happiness.

> *The process for finding the typical vulnerability has literally gone from days to minutes, and the developer time required to remediate each vulnerability has also declined.”*
>
> – Sándor Incze, CISO, CM.com

At a Glance

COMPANY OVERVIEW

CUSTOMER:
CM.com (AMS: CMCOM)

INDUSTRY
Technology

HQ
Breda, Netherlands

Sándor Incze joined CM.com a decade ago and has held positions in sales and engineering for the firm. Two years ago, he was appointed CISO. “We were a small company when I joined,” Incze recalls. “We were all in the Breda office, and cybersecurity was easier because we all knew each other and were constantly reminded to cultivate a culture of security. Things have changed over the years as we have expanded internationally, but we still strive to practice good security hygiene and deliver safe applications.”

From an application security perspective, Incze’s small team has been augmented by one or more security leads from each of the company’s 10 development teams. “We also work cross-functionally with the IT department and the risk management team, and try to make cybersecurity a cross-functional effort,” he explains. The company has ISO 27017 and ISO 27018 certifications, and Payment Card Industry (PCI) compliance is critical for the company, as its revenue model includes monthly subscriptions charged to corporate credit cards.

Struggling with Application Security

Until recently, the primary application security strategy at CM.com consisted of penetration testing and static application security testing (SAST). When Incze started in the CISO role, he realized that these tools consumed considerable time on the part of both his team and the development teams. “In addition to the additional time required for tests and scans, the reports had to be analyzed by our security team,” he relates. “Then a ticket would be created for each vulnerability that needed to be fixed.” It would often be days after the test before developers received feedback on what to do.

These security-related delays created friction in the development process and increased complications and delays tied to fixing vulnerabilities that were identified in the process. They also resulted in resentment on the part of developers. “They complained, ‘Security is controlling every step of what I do, and wasting a lot of my time,’” Incze recalls.

Improving the Application Security Architecture

Scan and penetration reports revealed something else to Incze; there was a great deal of room for improvement in the quality of the outputs of the development process. He decided to roll out a secure software development life cycle (SDLC) initiative at the company. But he knew that the team’s current application security toolset was inadequate, and unable to facilitate the improvements he was seeking.

Business Impact

VULNERABILITY REMEDIATION

- MTTR reduced significantly due to continuous scanning and remediation help
- Developer time for remediating vulnerabilities decreased significantly through catching vulnerabilities earlier in the SDLC

OPERATIONAL EFFICIENCY

- Projected faster development cycles due to fewer security-related delays
- Anticipated decrease in security team time for analyzing SAST and penetration testing reports
- Time to prepare reports for compliance and the board of directors reduced from hours to minutes

COST SAVINGS AND RISK REDUCTION

- Lower cost via paying fewer bug bounties
- Reduced license risk and risk of dependency confusion vulnerabilities due to automated settings in Contrast SCA

SOLUTIONS

- Contrast Assess
- Contrast SCA
- Contrast Professional Services

When researching possible solutions, he identified Contrast Security as a possible option. He especially liked the fact that Contrast—in the form of its automated Application Security Platform—offered a comprehensive DevSecOps approach. The ability to continuously monitor application code using instrumentation was a big plus for him. “I compare Contrast to the continuous spell check feature in Microsoft Word,” Incze describes. “Immediately upon typing a word incorrectly, users see it marked in red with an alternative spelling suggested. Similarly, developers receive immediate feedback when a vulnerability is detected, including actionable information about how to fix it. It helps developers learn to build better code.”

Incze launched into the project by purchasing licenses for Contrast Assess. Recognizing that application security must take place within development workflows, Incze notes that Contrast’s ability to integrate into various development tools used by the CM.com development team was also a major factor in Incze’s decision to select Contrast. “Our developers use various tools—Docker, Visual Studio, Jira, and Microsoft Teams—and the native integrations in the Contrast platform make for a seamless process,” he relates.

> “*By identifying and remediating more vulnerabilities before releasing applications into production, we believe there will be fewer problems that are spotted by the ethical hacker community”*
>
> – Sándor Incze, CISO, CM.com

Overcoming Adoption Hesitancy

Incze’s team faced some early challenges in convincing CM.com developers to use Contrast Assess. “We found that developers were initially resistant to adding another application security tool, as they assumed that it would create even more delays in the development process,” Incze explains. “We informed them it would actually make their jobs easier.”

In response, Incze collaborated with CM.com’s chief technology officer (CTO) to add application security metrics to the key performance indicators (KPIs) by which developers were evaluated. “In addition to a requirement that all developers use Contrast Assess for all programming languages that it supports, we just launched a Quality Improvement Program that is included in individual KPIs,” he says. “All developers will score themselves periodically for the quality and security of the code they produce, on a scale of 1 to 5. Everyone will start at Level 1, but developers who are still at Level 1 in a few months will need to explain why they have not progressed.”

Another adjustment that Incze made was to have developers do their own onboarding for Contrast Assess, using instructions that are posted internally—rather than his team setting up each user as was done initially. “We found that this is the best way for developers to see the added value they can realize from using the tool,” Incze explains. “Developers who take the time to understand the solution realize how it helps them to write more secure code more quickly.”

Tackling Open-Source Security

When CM.com initially engaged Contrast Security, the proof of concept (POC) included Contrast SCA along with Contrast Assess. Incze's team opted to focus on deploying Assess first, but they acquired a license for OSS so they could start working on securing their open-source libraries. Now the team is using OSS to protect the third-party code in one of its key applications.

"Most of our development teams use .NET Core, which has less complexity when it comes to open-source libraries," Incze notes. "However, our payment application is written in Java and is quite old with numerous libraries embedded. Its security standard is also higher, given that it houses payment card and financial information."

Previously, CM.com depended on its traditional SAST and penetration testing solutions to identify outdated open-source libraries. As with custom-code vulnerabilities, the process for remediating outdated libraries was lengthy, requiring analysis of scan reports and the creation of a service ticket. In addition, these legacy tools did not differentiate between active and inactive libraries and library classes; the result was that significant time was wasted in updating code that was not even used by the application.

With Contrast SCA, Incze can see at a glance open-source code that is used by an application, what vulnerabilities exist in those active libraries and classes, and which libraries need to be updated. "When we first ran OSS on our payment application, we found library versions that went back as far as 2012," Incze remembers. "It took a lot of work to update these libraries without breaking the application, but the result is a more secure piece of software.

"Contrast SCA also helps CM.com to minimize licensing risk in our applications by enabling me to block libraries that have risky copyleft licenses. I configured OSS to disallow such licenses, so developers do not need to do anything proactive," Incze explains. There are also protections against newly discovered dependency confusion vulnerabilities, through which attackers can create a malicious package with an identical name to an internal library used to "trick" applications into using the wrong library.

> *When we first ran OSS on our payment application, we found library versions that went back as far as 2012."*
>
> – Sándor Incze, CISO, CM.com

Realizing Tangible Efficiency Gains

In the short time since Incze and his team deployed the Contrast Application Security Platform, CM.com anticipates significant business value from the deployment. Mean time to remediation (MTTR) is one area where CM.com expects to see tangible value, with serious vulnerabilities identified earlier in the SDLC. "We also expect developer time required to remediate each vulnerability to decline, as they no longer have to go back through layers of added code to fix something from several days ago," says Incze. In addition to the efficiency gain, CM.com has lowered its risk; fewer vulnerabilities in development equate to fewer vulnerabilities in production.

Contrast
SECURITY

Efficiency gains also extend to the full range of application security processes. “My team members spend less time analyzing SAST and penetration testing reports, as we no longer need that information to fix vulnerabilities,” Incze says. “It is also easier to produce compliance reports, and we can produce a report customized for the board of directors with a few mouse clicks,” he adds. Previously, many reports could take hours.

Incze expects these different efficiency improvements to translate into faster development cycles for CM.com. “We are already seeing fewer delays in moving to production,” Incze reports.

Saving Costs and Reducing Risk

CM.com has also seen cost savings because of its Contrast deployment. Incze has recently noted a recent downturn in the amounts paid to security researchers through CM.com’s bug bounty program. “By identifying and remediating more vulnerabilities before releasing applications into production, we believe there will be fewer problems that are spotted by the ethical hacker community,” Incze predicts.

Now that Incze’s team is starting to use Contrast SCA, he believes his team and developers will spend less time triaging and diagnosing security alerts and remediating vulnerabilities. “The reality is that we are wasting time on vulnerabilities in code that is never exercised in runtime because of the application security tools we’ve used before,” he notes. And while it is too early to quantify a number in terms of time saved annually, Incze is confident it will be significant. “This is time that my team can spend on threat-hunting or more strategic security activities tied to risk mitigation,” he adds. “We also are lowering our risk connected to vulnerabilities such as developer confusion.”

Delivering Secure Applications

Looking back, Incze and his team—as well as the CTO—see their secure SDLC initiative to be a huge success. “Thanks to Contrast, we are delivering highly secure applications while lowering costs and speeding up development,” Incze concludes. “You cannot ask for more than that.”

> “
> *Thanks to Contrast, we are delivering more secure applications while saving costs and speeding up development.”*
>
> – Sándor Incze, CISO, CM.com

> “
> *My team members spend less time analyzing SAST and penetration testing reports, as we no longer need that information to fix vulnerabilities.”*
>
> – Sándor Incze, CISO, CM.com

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast
SECURITY

contrastsecurity.com