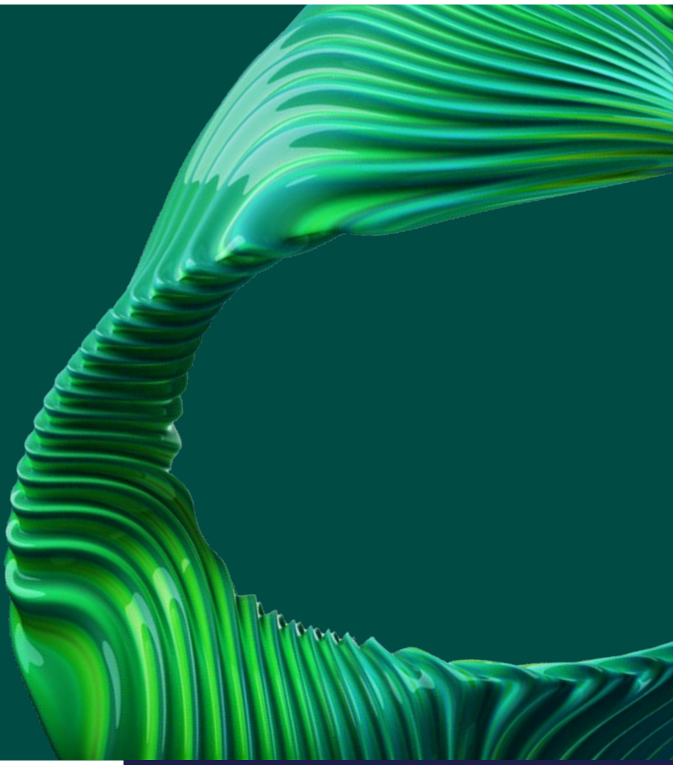

KAIZEN GAMING

Bets on Application Security Observability

About the Company

Kaizen Gaming is a leading GameTech company with headquarters in Greece, 750-plus employees, and more than 200 million annual customer transactions. The company operates two primary brands, Betano and Stoixman, and supports both casino and sports games. Kaizen games are available in six countries — Brazil, Cyprus, Germany, Greece, Portugal, and Romania.

Kaizen has a large development operation involved in developing new products and enhancing existing ones. The company uses the Agile methodology and currently has 28 fully staffed Scrum teams. The team's release cycle typically centers around two-week sprints by each Scrum team. In terms of languages, Kaizen primarily uses .NET Core and .NET Framework for application development.

> *"As soon as we turned Contrast Assess on, the tool immediately identified five vulnerabilities that had not been caught through penetration testing—three of which required prioritized remediation."*
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

At a Glance

COMPANY OVERVIEW

CUSTOMER:
Kaizen Gaming

INDUSTRY
Media & Entertainment

HQ
Athens, Greece

ACTIVE PLAYERS
450,000

CUSTOMER COMMUNICATIONS
1,500,000+

TRANSACTIONS
2,000,000+

SPORTING EVENTS
650,000+

Note: Metrics are annual numbers from 2019.

Aggelos Karonis started with the company's information security team three years ago and quickly assumed roles of increasing scope and responsibility. He is now manager of the team, holding the title of technical security manager. "The information security team reported to the chief technology officer when I began," Karonis explains. "But given the critical importance of our function, we now report to the board of directors." His five-person team is small, but most of the security programs they lead are cross-functional and involve stakeholders from other parts of the organization.

Late Identification of Vulnerabilities Caused Issues

Application security has always been a priority at Kaizen. Karonis' team conducts secure development training for all developers, and the Scrum teams have a formalized process of peer review through which more senior developers mentor more junior ones in writing secure code. The team previously did vulnerability assessments of their applications using a penetration testing tool and a dynamic application security testing (DAST) tool in the testing and production phases of the software development life cycle (SDLC).

"Penetration testing is a requirement for gaming applications in most of the countries where we do business, and it is also mandated by the Payment Card Industry [PCI] standards," Karonis notes. "Since we needed the solution for compliance, penetration testing was our first major application security investment."

But depending largely on penetration testing to deliver secure applications had its problems. "Needing to wait until the test phase to find vulnerabilities moved much of the remediation work until very late in the development process," Karonis states. "It added a lot of extra work and stress."

In addition, penetration testing did not provide real-time, holistic observability into Kaizen's overall application portfolio at a given time. "It created a lot of blind spots," Karonis recalls. "Vulnerabilities would come up in the final review process that had not been detected in the past, and this resulted in inefficiency in how the problems were tackled. It also meant that we spent a lot of extra time remediating vulnerabilities at the end of the process."

In a Nutshell

CHALLENGES

- Move discovery and remediation of vulnerabilities earlier in the SDLC (shift left)
- Eliminate security-related delays to development for 28 Scrum teams and speed release cycles
- Simplify reporting for auditors and for communication to business leaders • Support operational efficiency for small information security team

SOLUTIONS

- Contrast Assess
- Contrast Support Services

BENEFITS

- Lowering Application Risk
  - Reduced MTTR by 15 days
  - 5 vulnerabilities discovered immediately when Contrast Assess was turned on, 3 that required immediate remediation
  - Significant improvements in time to remediation and reduction to security debt
  - Automated prioritization of vulnerabilities by risk, improving application security posture
- Realizing Operational Efficiencies
  - Time savings of up to 1.5 days each time a report must be generated for management or auditors
  - Significant time savings for security team to interpret and provide feedback on penetration testing reports
  - Accelerated deployment releases into production by shifting application security left

Seeking an Automated, Efficient, and Scalable Solution

Karonis and his team knew that this state of affairs was unsustainable and that they needed to deploy an application security solution that covers the entire SDLC. “We needed to catch vulnerabilities earlier in the process, but we did not want to slow down our developers,” he explains. “We have a very distributed development team, and any delays create a lot of downstream impacts.”

In addition, Kaizen’s financial team strongly preferred a pricing model that charges by the application rather than by the developer. “We have a large development team and just one application,” Karonis notes. “Our business runs on tight margins, and we knew that paying by the application would suit our model better.”

Karonis’ team wound up doing extensive evaluation of 10 different solution options—quite a feat for a five-person team. The team assumed that they would be acquiring a static application security testing (SAST) tool, but opened the proof of concept (POC) to a variety of solutions. “We started out with something different in our heads, but as we saw the capabilities of Contrast Assess, we determined it was a better option for us,” Karonis remembers. “We found other good solutions, but they did not fit our needs as fully as Contrast.”

> “It previously took between a half day and a full day to pull figures for auditors, and between a full day and a day and a half to put something in a form that could be consumed by business leaders. With Contrast, we simply click a button.”
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

Rolling Out a Modern Instrumentation Approach

Contrast Assess uses security instrumentation to do continuous vulnerability scanning from within an application. The scanning happens in the background, eliminating interruptions to the development process and providing continuous feedback to developers when a vulnerability is detected. In addition, the Application Security Platform on which Contrast Assess is built provides complete, ongoing security observability for the entire application infrastructure.

Kaizen deployed Contrast Assess with Contrast Support Services. “We had some things that were not designed correctly on our end, and the support engineers worked with our engineers to get everything working correctly,” Karonis reports. “Overall, we were able to deploy the POC in one day, and it took another half day to go to production. The Technical Support team was instrumental in making things happen this fast.”

Kaizen uses the native integration with Jira that is built into the Application Security Platform, and is looking to deploy the integration

> “We do not have to wait for the next quarterly penetration test to detect a vulnerability, so that can shorten remediation time by months.”
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

with Slack. “Our teams use Jira for project management and Slack for communication and collaboration,” Karonis explains. “Once the Slack integration is rolled out, my team can raise something that needs to be fixed in Slack for feedback and remediation.”

In addition to using Assess during the development process, Karonis’ team uses it with its application in production as well. “This allows the tool to perform real-life testing on our application,” Karonis relates. “In this way we have automated the identification of vulnerabilities in our code and made it continuous, whereas previously it was delivered through penetration testing on a periodic basis.”

Kaizen also includes three critical application programming interfaces (APIs) in the continuous scanning that is done by Contrast Assess. “Many of our APIs are externally controlled, such as those associated with payment gateways,” he notes. “For the ones we control, we want to make sure they are free of vulnerabilities.”

Early Business Value Identified

Karonis’ team realized a quick win as soon as Contrast Assess was activated. “As soon as we turned Contrast Assess on, the tool immediately identified five vulnerabilities that had not been caught through penetration testing—three of which required prioritized remediation,” Karonis recalls. “These vulnerabilities should have been caught by penetration testing, but they were not.” This improved Kaizen’s security posture by eliminating vulnerabilities that might have gone undetected into production.

Reporting also became measurably easier as soon as the solution was rolled out. “It previously took a lot of manual work to produce a report listing all the issues for presentation to the board, executive management, or auditors,” Karonis remembers. “It previously took between a half day and a full day to pull figures for auditors, and between a full day and a day and a half to put something in a form that could be consumed by business leaders. With Contrast, we simply click a button and produce a report that includes everything the different audiences require.”

Another early success for the team was a significant reduction in the amount of time required for the security team to interpret penetration test results and provide detailed feedback to developers. “We only need to review the findings from Contrast Assess and forward them to the teams,” Karonis says enthusiastically. “Once we are able to quantify those savings, I believe we will see a significant improvement.”

> “
> *There is a certain elegance and simplicity in the real-time feedback from Contrast Assess, which is sorted by the level of risk that each vulnerability poses to an organization—with a suggested resolution just one click away.”*
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

> “
> *We started out with something different in our heads, but as we saw the capabilities of Contrast Assess, we determined it was a better option for us.”*
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

Reducing Security Debt

While it is too early to track improvements to the speed of remediation, the anecdotal feedback from members of his team is that remediation is much faster and security debt is going down. “We are still fine-tuning our remediation processes, so we have not yet measured this impact. But we know that vulnerabilities are being taken care of more quickly,” Karonis describes. “We do not have to wait for the next quarterly penetration test to detect a vulnerability, so that can shorten remediation time by months. I expect that we will eliminate our backlog of unresolved vulnerabilities quickly.” Karonis indicates that his team is already seeing a reduction of around 15 days in mean time to remediate (MTTR) and expects this to reduce even more in the future.

Time to remediation is also helped because Contrast Assess has been very easy for developers to adopt. “To be honest, finding the best way to communicate the launch of the new tool was more difficult than helping our developers understand it,” Karonis asserts. “With so many Scrum teams—some fairly new—making everyone aware of the tool has been a challenge. But the feedback is so intuitive that little training was required once awareness was there.”

Easy prioritization of vulnerabilities with Contrast Assess is another benefit for Kaizen. “There is a certain elegance and simplicity in the real-time feedback from Contrast Assess, which is sorted by the level of risk that each vulnerability poses to an organization—with a suggested resolution just one click away,” Karonis says.

Dealing with vulnerabilities in real time throughout the SDLC makes deployment of applications into production a much easier process. “We always built substantial extra time into our timelines at the end of the process to resolve vulnerabilities, so we rarely deployed behind schedule,” Karonis explains. “But we were always pushing hard against the deadline. With Contrast Assess, deployments are now much easier and stress-free. We do not have to be like a passenger train coming in exactly on time. Deploying on time is no longer a headache.”

Vision for the Future

Kaizen’s applications include code from approximately 300 open-source libraries and frameworks, and Karonis is considering adding Contrast OSS to bolster and automate risk management for those elements in the Kaizen application. “We have stayed on top of open-source code so far, but it is getting more complex,” Karonis admits. “I would like to have a better way of monitoring and staying up to date on patches and licensing issues. And though it is not required in our jurisdictions, presenting the feedback from such a tool to regulators would show that we take open-source security seriously.”

> *“Overall, we were able to deploy the POC in one day, and it took another half day to go to production. The Technical Support team was instrumental in making things happen this fast.”*
>
> – Aggelos Karonis, Technical Security Manager, Kaizen Gaming

Kaizen's developers also have big future plans, with cloud-native initiatives on the near-term horizon. "We use microservices with some applications now, and I expect us to embrace things like serverless technology in the relatively near future," Karonis reports. "It is good that Contrast is developing solutions for that space."

Karonis is pleased with the success his team has achieved with Contrast Assess. "There are many benefits, but I think they are best summarized with one word—observability," Karonis concludes. "You only see how valuable that visibility is once you have it in place."

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

Contrast SECURITY

contrastsecurity.com