Contrast
SECURITY

UNIT4

Significantly Reduces False Positives and Speeds Devops Cycles with Contrast Application Security Platform

About the Company

Unit4's next-generation enterprise solutions power many of the world's most people-focused mid-market services organizations. Their state-of-the-art cloud platform, ERPx, delivers unified ERP, HCM and FP&A combining functionality designed for service-centric industries and user experience that puts people first. It supports rapid and continuous change while delivering individualized fit for customers at scale, delivering the right tools to unify the processes across their organization, and connect their people. Unit4 serves more than 6,000 customers globally including, Bravida, Havas, Migros Aare, Americares, Save the Children International, Action against Hunger, Metro Vancouver, Forest Research, Southampton City Council, Habitat for Humanity, Selkirk College, FTI Consulting, and Surrey County Council.

> "
>
> *With Contrast Assess we had an average of 7% of false positives against the 57% in the pen-test reports received from our customers."*
>
> – Jose Oca, Lead Quality Manager, Unit4

At a Glance

COMPANY OVERVIEW

Customer:
Unit4

INDUSTRY
Technology

LOCATION
Global

Kicking Off a Large-Scale Digital Transformation

In 2014, Unit4 embarked on an ambitious strategic initiative to adopt the DevOps methodology companywide, consolidate a patchwork of software solutions developed for different markets, streamline application security and quality control efforts, and move in the direction of a cloud-based delivery model for all its products.

As a part of this reorganization, a centralized quality assurance group was formed that reports to the CTO. José Oca, an 11-year veteran of the company, was asked to join that group. "We were all aiming to achieve a consistently high level of quality across the whole portfolio," he recalls.

Traditionally, each product operated in a silo with its own development and quality assurance functions. "Each area used different methodologies and different tools," Oca remembers.

Continuing the Innovation

Fast forward to today, Unit4's digital transformation is firmly on track. Oca explains. "We use Azure DevOps Services; we have built an entire microservices ecosystem to make this happen. This will enable us to release software continuously and localize our product offerings without maintaining separate applications for each iteration".

Evolving Application Security

In the past, application security was a part of the piecemeal approach, Oca and the Quality team began to look at how to streamline those efforts when the new team formed.

"We had a group of security experts in the Oslo office that took care of implementing the main security layers at the core-level technical platform level," Oca relates. "Among others, the main steps that were taken to ensure application security were initial and pre-release architectural reviews by the in-house security team, and manual penetration testing conducted by a third party".

Oca and the Quality team worked to standardize the process across all applications. "We developed policies and checklists that streamlined the process somewhat and made expectations clear for everyone. We created a complete security curriculum that was published in our internal training platform and distributed among all the engineering employees, to create a security culture that would impact the whole software development lifecycle", he says. However, it was clear that Unit4 needed to deliver an automated approach to the new digital transformation around application security tools and practices for its development process.

In a Nutshell

BUSINESS IMPACT

- Between 2 to 3 times faster remediation times.
- Estimated a reduction in false positive rate from 57% present in the pen-test reports compared to 7% in false positive reported by Contrast.
- Estimated saved around 72 hours in staff time in investigating false positives and preparing reports, whenever receiving a pen-test report from customers.

SOLUTIONS

- Contrast Assess
  – Integrations: Microsoft Teams.
- Professional Services
  – Technical Implementation, Knowledge Transfer/Training, Team Enablement Workshops, Vulnerability Management, Secure SDLC.

Deploying a Solution

Oca and the Quality team began evaluating a variety of application security tools, including traditional SAST, dynamic application security testing (DAST), and software composition analysis (SCA). "We started to create our own rules in some of these tools, but we quickly realized that using these tools requires a high level of expertise and a lot of customization. We knew we needed to externalize these capabilities.".

Late in the process, the team discovered **Contrast Assess** and requested a proof of concept. "It was one of the fastest proofs of concept that we had," Oca recalls. He quickly realized that Contrast Assess was ideal for their needs. "This was precisely the level of automation we were looking for, and it only required a pretty basic setup", he says. Unit4 deployed the solution, along with the native integrations with Microsoft Teams.

Contrast Assess uses instrumentation to conduct continuous security scanning from within the application. Immediately upon the creation of a vulnerability, whenever that functional area is exercised, the **Contrast Application Security Platform** sends an alert with contextual, actionable information that helps the engineer fix the problem right away, without involvement from anyone on the security team. Vulnerabilities can be remediated before additional layers of code are added, making remediation less complicated, time-consuming, and costly.

Realizing Tangible Benefits

Just a few months after deployment, Unit4 started to take advantage of the benefits. Among others:

- Instant notifications: Whenever a new critical, high, or medium-severity vulnerability pops up in our ERP product, a notification goes out on a Microsoft Teams channel that belongs to a specific product as well as the Quality team.

- Application merging: We run **Contrast Assess** in a vast ecosystem of microservices, which can sometimes lead to extra administrative effort, however **Contrast Assess** allows to merge applications, which facilitate handling different applications easily under a unique hood; as long as the merged applications have the same technology stack, so the security checks are correctly applied.

- Fewer false positives. Another big benefit is a reduction in false positives compared with penetration testing. With **Contrast Assess** we had an average of 7% of false positives against the 57% in the pen-test reports received from our customers.

"

The immediate feedback is very good at helping engineers learn not to create the same vulnerability twice. It is very didactical. Over time, our engineers learn to avoid a wide variety of vulnerabilities."

– Jose Oca, Lead Quality Manager, Unit4

"

Contrast's reports are great for communicating with C-level executives and people that might not have a deep security knowledge. Reports like the OWASP Top 10 communicates well and can be created with a click of the mouse."

– Jose Oca, Lead Quality Manager, Unit4

C Contrast
SECURITY

- Reporting capabilities. "Contrast's reports are great," Oca asserts. "For communicating with C-level executive and people that might not have a deep security knowledge, reports like the OWASP Top 10 communicate well".

  Risk officers appreciate the built-in reporting around the E.U.'s General Data Protection Regulation (GDPR), and security teams can build detailed telemetry reports.

  These automated reports can be prepared with a click of the mouse, which is faster than Unit4's previous reporting process, which involved manual correlation of data between Azure DevOps, security tools, and other sources. Oca estimates that an average of 72 of hours of staff time will be saved on report preparation, whenever having to process a pen-test report from customers.

- Grouping duplicated vulnerabilities: **Contrast Assess** allows to merge reported duplicated vulnerabilities, which usually happens when having a vulnerable parameter in a column of an HTML tables.

- Just-in-time training. Another tangible benefit is the just-in-time training that Unit4 engineers receive simply by using **Contrast Assess**, which is helping them to create more secure code over time. Oca contends "The immediate feedback is very good at helping engineers learn not to create the same vulnerability twice. It is very didactical. Over time, our engineers learn to avoid a wide variety of vulnerabilities".

Well-Positioned for the Future

Contrast Assess eased Unit4's digital transformation. By combining mid-sized experience – with a relentless focus on people – onto an industry-leading cloud platform, Unit4 has built finance and HR solutions to be just right 4U, and help transform the way people work. With Unit4 ERPx, the company introduces the next generation of smart cloud ERP.

"We have the right automation in place for our application security, and our engineers are learning to write more secure code," Oca concludes. "As a result, we are in a great place and the future is looking bright for us.".

> "
>
> *We have the right automation in place for our application security, and our engineers are learning to write more secure code."*
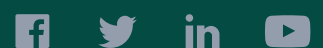>
> – Jose Oca, Lead Quality Manager, Unit4

Contrast
SECURITY

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

contrastsecurity.com