EveryonePrint Security Health checks

To govern a high level of security for the EveryonePrint HCP solution we follow best practise for the industry. We have implemented a comprehensive compliance framework covering OWASP standards during our full software development process, SDLC and security tools protecting our Cloud infrastructure. We have had external consultants reviewing our Cloud architecture and doing quarterly PEN tests against our environment as well as offering customers and partners the option to perform their own PEN Tests.

Software Development Life Cycle, SDLC following OWASP

EveryonePrint recognizes the importance of application security to its customers and is dedicated to bringing products to market that meet high security standards. To meet the high levels of security, EveryonePrint has partnered with Security Innovation who has assessed the software development lifecycle (SDLC) and help defining security practices and activities for the development organization of the EveryonePrint Hybrid Cloud Platform (HCP).

We use OWASP guidelines for software design, vulnerability assessment and threat modelling. Possible security implications are identified and marked during design phase, the code is tested using static and dynamic code tools and analysis. Features with security tags are tested by the QA team and only released if passed.

EveryonePrint uses secure and mature coding languages, such as Rust and Java for software development. Secure coding guidelines for specific languages are also used by the development teams. Software security is mandated by EveryonePrint Software Development Security Standard (ISMS19 updated November 2020).

Cloud Security

Our production environment in AWS has been reviewed and evaluated by IBM Nordcloud in June 2021. Their report “Well-architected review” confirms a high level of operational excellence, security, reliability and performance efficiency for the HCP AWS production environment.

Protecting our Cloud environment in AWS we use several AWS professional tools, including:

- **AWS Security Hub** creates a bunch of AWS Config rules. These rules represent AWS Lambda functions that are created for a custom rule or a predefined managed rule. The function evaluates configuration items to assess whether the AWS resources comply with the desired configurations defined by the security standards mentioned above.
- **AWS GuardDuty** which is a threat detection service that continuously monitors for malicious activity and unauthorized behaviours to protect the AWS account.
- We run periodic **AWS Inspector** assessments in all the application environments. Amazon Inspector is an automated security assessment service

that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.
- **AWS IAM Access Analyzer** helps us to identify the resources in the organization, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. This lets us identify unintended access to our resources and data, which is a security risk.
- Additionally, we periodically monitor **AWS Trusted advisor** findings to keep best practices for cost management, high availability, security, and performance.

For more details about our cloud setup, please contact our Security Team.

Penetration Tests

EveryonePrint has external consultants performing quarterly penetration tests against its HCP Cloud environment addressing the OWASP Top 10 Application Security Risk. Schedule of penetration testing is mandated by EveryonePrint Security Testing Standard (ISMS-32).

During 2021 we have had 5 different 3rd party (red team) consultants performing PEN Tests against the HCP Cloud environment.

The results from all Penetration tests are being evaluated by the EveryonePrint security team, discussed and prioritised according to the risk score with the Product Management team. Remediations are then planed and implemented. According to the ISO27001 risk assessment framework, all critical issues are also added to our Risk Treatment table and have the attention of the EveryonePrint Compliance Committee.

Governance

EveryonePrint leverages best practices and sound security guidance from a wide variety of sources. The best practices that we consider as we continuously improve our security programs include the Cloud Security Alliance's Cloud Control Matrix, ISO 27001, GDPR, SD-PAC for our SDLC from Security Innovation Inc. and several others.

EveryonePrint considers all information, applications and underlying IT infrastructure as important assets which are supporting business processes and are being adequately protected. The scope of our IT risk includes the potential loss of confidentiality, integrity and availability of information assets due to inadequate controls or exploitation of security vulnerabilities.

Our Policy framework is approved by the Chief Executive Officer on behalf of the Executive Management at EveryonePrint and provides a management statement highlighting the key IT Security Principles for managing IT risk.

The following external audits and controls has been successfully completed:

Name of audit/controls	Scope	Month	Certification	3rd party auditor
ISO27001:2013 audit	HCP Cloud production environment and supporting organisation	April 2020	Yes	SGS United Kingdom Ltd
ISO27001:2013 surveillance audit	HCP Cloud production environment and supporting organisation	April 2021	Yes	SGS United Kingdom Ltd
SD PAC	Secure Development Life Circle	Februar y 2021	Yes	Software Innovation Inc
AWS Well-architected review	AWS Production environment	June 2021	No	IBM Nordcloud
Cloud Controls Matrix, CCM	Cloud application security controls and best practice	Septem ber 2021	No	NA (CAIQ)