Behind the SOC 2 Report: An Interview with Devolutions' CSO and Director of Legal Affairs, Risk and Privacy

Devolutions

WE HAVE SUCCESSFULLY COMPLETED OUR SOC 2 COMPLIANCE AUDIT

As we announced last week, we have successfully completed our SOC 2 compliance audit. Many of our technical and business staff members worked with Ernst & Young's team on the SOC 2 auditing of Devolutions Password Hub and its ecosystem, including Lucid, our authentication and identification service. In order to tell you a bit more about the whole process, I've interviewed Martin Lemay, our Chief Security Officer, and Guillaume Beaupré, our Director of Legal Affairs, Risk and Privacy. Both Martin and Guillaume were deeply involved in the entire audit process. Here's what we discussed:


Chief Security Officer


Director of Legal Affairs and Privacy

What exactly is SOC 2?

Martin Lemay: The Service Organization Controls 2 (SOC 2) report is a third-party audit of a provider's service and the trustworthiness of its system description, its security controls, and, optionally, its availability, processing integrity, confidentiality, and privacy controls. In other words, an organization that has completed the audit exercise will have a compliance report issued that details the auditors' level of confidence in the security and consistency of the service provider's controls.

There are two types of SOC 2 reports. Both provide a description of the system and its controls. The difference between them is that Type-I is for compliance assurance at a given date, while Type-II assesses controls for a given time range. The latter type is better, because it asserts that controls were audited for correctness over a specified period of time and not only at one point in time. Our SOC 2 report is a Type-II for the period of October 1 to December 31, 2019. We plan to cover a full year with our next report in 2021, for the period of January 1 to December 31, 2020.

Guillaume Beaupré: Apart from the SOC 2 report itself, the SOC 2 audit process is also beneficial internally, since the organization is compelled to elaborate, implement, and (most importantly) control on a continuous basis a wide range of organizational, physical, and technical security measures in order to get (and maintain) a clean SOC 2 report, as the audit process is repeated on an annual basis. The audit process therefore helps the organization foster and develop a genuine information security culture among its management and employees.

What was audited?

ML: The organization's SOC 2 Type-II scope included the Devolutions Password Hub service and related components, such as Password Hub Core and Lucid. It specifically aimed to meet security criteria related to the organizational environment, staff, cloud services, infrastructure, and application code supporting these services. It means that not only were Password Hub technical controls audited, but so were the team and business environments behind them. It required us to implement nearly 50 controls in such a way that we could prove to our auditor that those controls had been met and were working as intended. This means that nearly a hundred of evidence were collected and analyzed by our auditor to produce the report.

GB: Actually, the SOC 2 auditing process is integrated with the COSO framework (Committee of Sponsoring Organizations of the Treadway Commission), which is specifically used to assess the design, implementation, maintenance, and effectiveness of an organization's internal controls relating to its control environment, risk assessment, information and communications, monitoring activities, and existing control activities. Such internal control components are themselves divided into 17 internal control principles that need to be met, along with some additional criteria that address cybersecurity risks, including logical and physical access controls, system operations, change management, and risk mitigation.

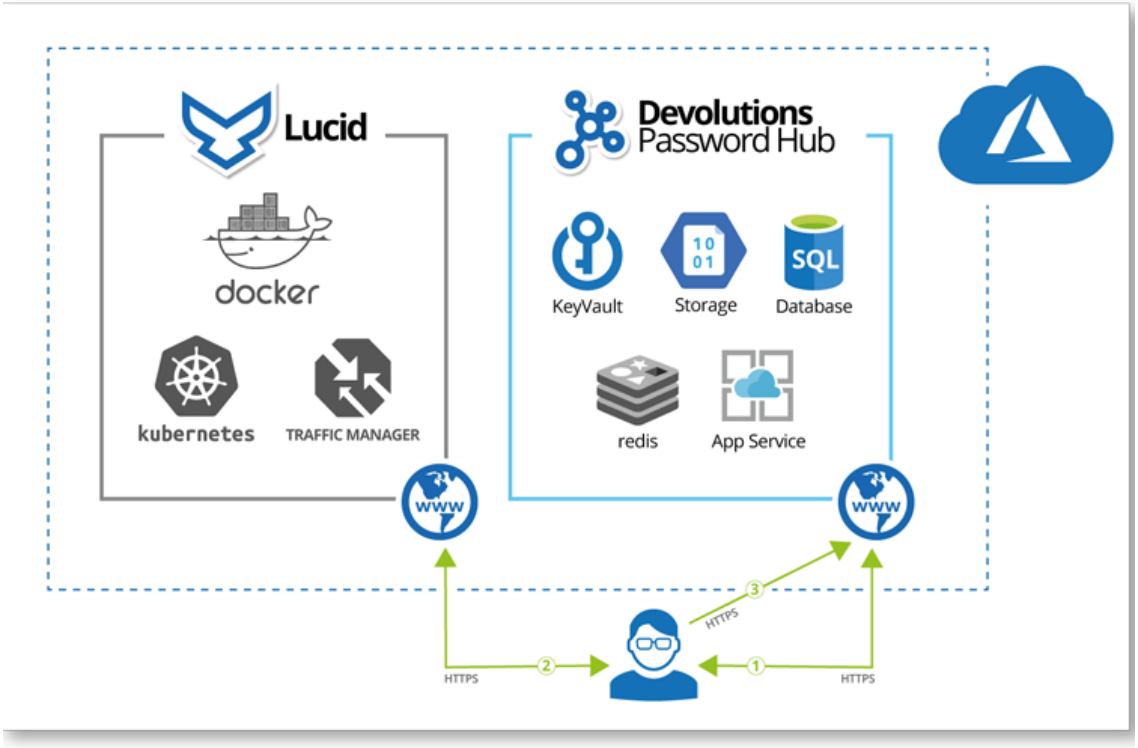

Diagram 1 - Password Hub Architecture Overview

How were you involved in this project? What were the challenges?

ML: I was responsible for managing the whole SOC 2 project and was deeply involved in the design and implementation of security controls with IT Operations and Engineering teams. The challenges were not necessarily technical since we have a great pool of talented engineers at Devolutions that work hard to deliver high quality products and services. However, changing the way they were working was a true challenge. As an example, Engineering and IT Operations teams had to start documenting their work in tickets, version control, and pipeline systems in a way that every code and infrastructure change to production was easily traceable. It is hard for humans to change their behavior at someone else's request. But it had to be done, and we succeeded by leveraging organizational culture, productivity requirements, tooling availability and enhancement, executive commitment, risk management, and transparent communication.

GB: For my part, I was mainly involved in the design and implementation of organizational and risk assessment / mitigation controls. This included having all required information security policies and procedures drafted and approved, implementing a thorough risk management and mitigation program, and making sure that our upper management remained committed and aligned with our SOC 2 requirements during the whole process. Regarding this last point, I must say that we received tremendous support from our management team, which was an important factor in the timely achievement of our SOC 2 objectives.

What was the result of the audit? Did we pass?

ML: At the end of the day, the deliverable of the SOC 2 audit is a detailed report that includes the opinion of our auditor on the system description and the consistency of the controls, our description of the system and its environment, a management assertion, and the result of each tested control within the scope of the audit. There is no real notion of pass or fail during this exercise since all the facts are included in the report. Our customers and partners will therefore have to judge, based on the content of the report, the level of confidence they can have in us based on the integrity of our auditor and ours. But to this date, we've had no significant deviation from all the controls we were audited for.

GB: "It's not the destination, it's the journey", as we often say. Well, I couldn't agree more here. Putting aside the report (which is in itself very positive), I think that, from an internal point of view, the most valuable input of this whole SOC 2 process for our organization was (and still is) how we increased our global awareness and commitment to information security within our company. There is now a common understanding among our management team and employees that information security is not just a simple feature that needs to be taken into account, but that it is rather a strong value which must guide all our processes and decisions. This represents a major shift in our business culture and the SOC 2 process really helped us to get there.

Do customers have access to the complete report?

ML: Yes, they do. They simply have to visit our security portal available from our website and directly download it from there.It is also important to note that an SOC 2 report is complex and is intended for an audience that can understand such a document.

GB: I will simply add that given the confidential nature of the information disclosed in the report, each person requesting a copy of our SOC 2 report will be asked first to review and accept the terms of our non-disclosure agreement to preserve the confidentiality of its contents.