|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change | Author | Date |
| 0 | Added ChangeLog | Peter | 22/09 |
| 1 | Discussed which analyses to do and who would do them | Team | 29/09 |
| 2 | Added in the different context explorations from individual files | Peter | 7/11 |
| 3 | Discussed and highlighted findings from use context exploration | Peter | 8/11 |
| 4 | Added findings from research activity, competitor analysis | Victoria | 8/11 |
| 5 | Specified findings and conclusions | Peter | 8/11 |
| 6 | Reviewed | Cecilie | 9/11 |

Use Context Exploration

In order to properly understand the problem domain and existing knowledge, solutions and uses revolving around our future product, we need to conduct an exploration of the use context.

We initially brainstormed and discussed the following forms of domain analysis, represented in the table below. The cells that are shaded green reveal which analyses we ended up pursuing.

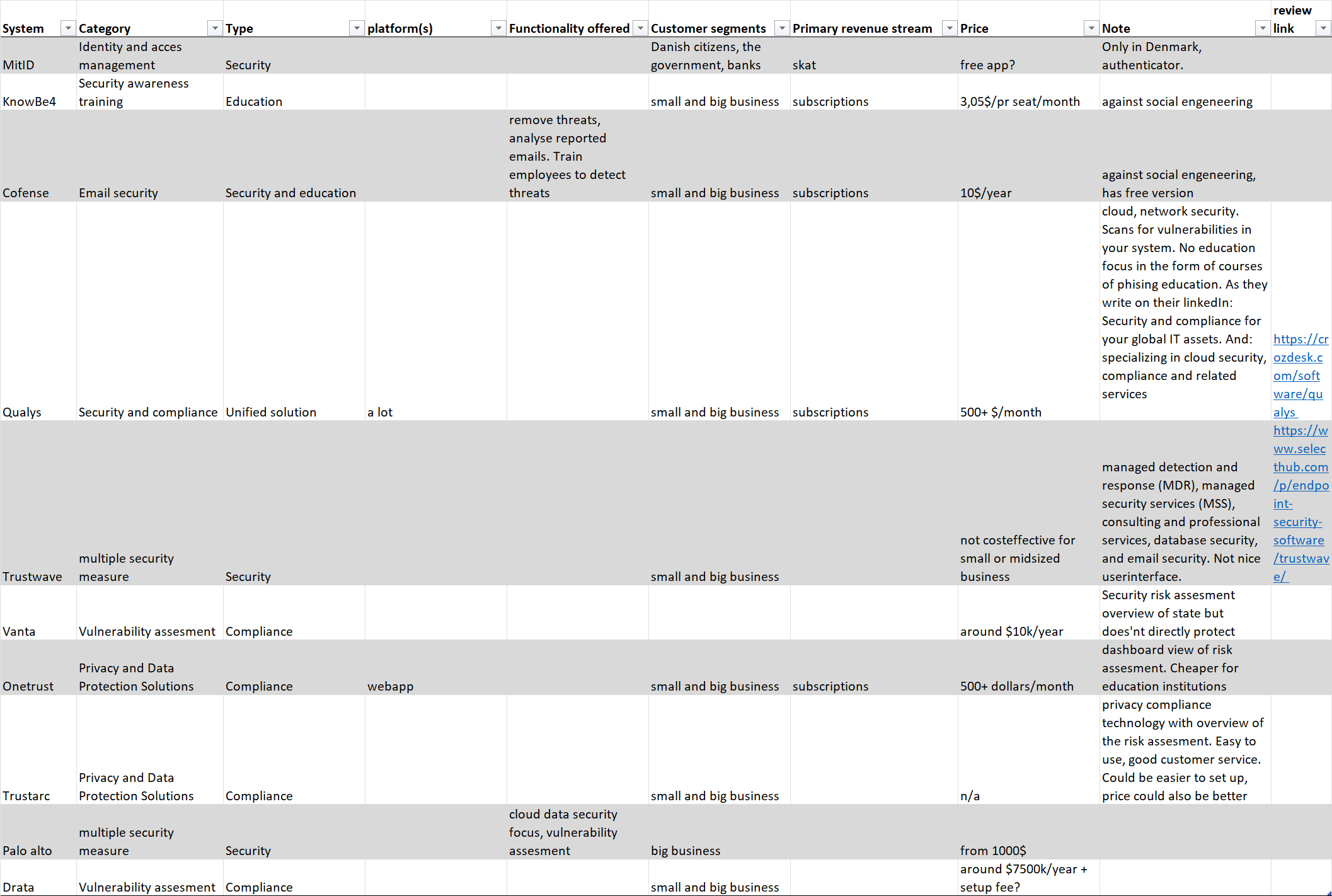
|  |  |  |
| --- | --- | --- |
| **Context** | **Item / Research** | **Description** |
| Tech | Existing systems +  other companies | We need to explore the existing solutions currently in the market. It can also be from different domain if it-is solving similar problem.  We may investigate how other companies in our sector conduct business in the form of a competitor analysis. |
| Tech | Legal regulations | The legal regulations should be investigated for a product of our nature, since it entails advising on critical infrastructure and practices. |
| Tech | Well-known/acknowledged problems (literature research) | Some information on the well-known problems for systems like ours has already been introduced in the case description. Information can be gathered by reviewing existing literature. |
| Social | Interview IT-security expert | Interview IT-security expert to get input on requirements and constraints |
| Social | Interview user | Interview small business owners to uncover their everyday needs and challenges. |
| Social | Participant observation | Visit small businesses and watch how they use their technology at the moment. Which security leaks are there? |
| Social | Survey | Send surveys to the users to figure out what issues they face with security and what their needs are |

We chose to analyse the existing systems and solutions made by other companies, to understand what offerings are currently available on the market, and to inform our own approach. This analysis also helps us scope what is possible and sought after in the cybersecurity landscape. We concurrently chose to conduct a literature review to further strengthen our knowledge on this subject area that is somewhat alien to the novice and to use. This would also help us identify differences and similarities between the scholarly procured issues found in research and the solutions that our potential competitors offer. Finally, we had the unique possibility to interview a security specialist in our area, who had profound insights into our customers, their business and IT structures and the scenarios they encounter on a daily basis, allowing us to bridge the technical domain analysis to an understanding of social and practical dynamics as well.

The results of our use context analyses can be found below.

Competitor analysis

When selecting systems to analyse we weighted having different kinds to represent different solutions. This should give a better understanding of what is available on the market, their distinctness and similarities. Our competitor analysis resulted in the following table, which can be found in a larger format in Appendix A:



**Findings**

Numerous companies specialize in various domains such as security, compliance, or education. However, few of these companies integrate these areas seamlessly, leaving a gap in the market. While unified compliance and security measures are available, none offer a comprehensive solution that encompasses all three aspects.

Many companies provide protection against multiple forms of threats by implementing a combination of security measures.

In the realm of compliance and vulnerability assessment, Vanta and Drata are favoured by some, although they have both proponents and critics. These platforms offer yearly subscriptions and a feature known as the yearly auditor.

Pricing details for these services are often not transparent. Typically, prices are tailored to the specific needs of each company, which can make price discussions challenging.

Pricing models are predominantly subscription-based, with options for monthly or annual billing, and costs per user. Typically, a lower per-user cost is associated with more users, which may not be cost-effective for smaller companies.

Notably, Drata stands out by offering a more explicit plan designed for startups, a rarity in this industry.

Some systems offer special pricing options tailored to schools and educational institutions, such as Onetrust.

The abundance of options in the market can make it challenging to navigate and select the right solution for your specific needs.

Literature review

During our literature review, we reviewed the following texts:

* Bada, Maria, and Jason R.C. Nurse. 2019. “Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs)”. *Information & Computer Security* 27.
* Dinkova, Milena, et al. 2023. “Should Firms Invest More in Cybersecurity?” *Small Business Economics*.
* Gafni, Ruti, and Yair Levy. 2023. “Experts’ Feedback on the Cybersecurity Footprint Elements: In Pursuit of a Quantifiable Measure of SMBs’ Cybersecurity Posture”*.* *Information and computer security*.
* Hall, Joanne, Tam, Tracy, and Asha Rao. 2021. “The Good, the Bad and the Missing: A Narrative Review of Cyber-Security Implications for Australian Small Businesses”. *Computers & Security* *109.*
* Loshchenko, Vitaly, and Olga Zvereva. 2022. “Integrated Approach to Cybersecurity of a Small-Sized Business System”.
* Raineri, Ellen M., and Jessica Resig. 2020. “Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses”. *The Journal of Applied Business and Economics*, vol. 22, no. 12.
* Walsh, Karen. 2023. “Security-First Compliance for Small Businesses”. CRC Press.

For an overview of the initial findings for the individual texts, see Appendix B.

The findings from this particular part of the use context analysis resulted in a lot of insights from existing research into the subject area. Notable highlights include:

**Insights and definitions for SMBs**

SMBs (Small and medium-sized businesses) are the target customers for our security solution and as such an integral part of not just the process, but also the final design of our product. The literature generally defines SMBs as businesses with 19 or less employees (Hall et al. 2021).For ease of translatability, we have adopted this definition. Building upon the initial findings from the *Explore your case* section, several texts highlight the following:

* A large number of SMBs experience cyber-attacks and data breaches (Gafni and Levy 2023; Hall et al. 2021).
* SMBs do not have the resources for hiring a security officer or similar specialist (Dinkova 2023; Hall et al. 2021; Walsh 2023).
* SMB owners generally have limited or no understanding of security risks, and concurrently lack confidence in the area (Hall et al. 2021; Raineri and Resig 2020).
* SMB owners are very interested in staying compliant and having a strict data policy, although they do not know where and how to start (Bada and Nurse 2019; Hall et al. 2021; Walsh 2023).
* SMB owners overwhelmingly use cloud services for data storage and computation (Hall et al. 2021).
* Due to lack of company equipment, many SMB owners and employees use private devices to access company data (Hall et al. 2021).
* Customers value a company’s data privacy policies highly when making purchase decisions (Walsh 2023).
* In a data leak, the type of data is much more important than the volume (Gafni and Levy 2023).

**Analysis and derivations**

The literature reveals that cyber-security attacks towards small and medium-sized businesses are common and on the rise (Gafni and Levy 2023; Hall et al. 2021). Meanwhile, business owners feel lost in the digital security landscape and lack both the necessary awareness and education to deal with present issues. This leads to low confidence and self-efficacy when approaching the subject, and concurrently results in inaction and glossing over security risks. For this reason, much of the literature focuses on educational aspects of cyber-security and proposes that education of the business owner has a profound effect on their cybersecurity efforts (Bada and Nurse 2019; Raineri and Resig 2020). Initial increases in awareness typically leads to an increase in attack reports, as attacks that would previously go unnoticed are suddenly discovered (Dinkova 2023), but seems like a necessary step towards increasing data security.

Another finding relates to the fact that most businesses use cloud services for data storage (Hall et al. 2021). Coupled with existing local anti-malware software, the company’s data is quite well-protected from technical means of attack (Zvereva and Loshchenko 2022). Instead, attacks are primarily related to social or psychological means, for example via a phishing attack in which an employee of the business grants an adversary access to the company’s data. The literature endorses two primary methods of countering this approach:

* Increased employee awareness via education (Bada and Nurse 2019; Zvereva and Loshchenko 2022).
* A strict access control structure (Zvereva and Loshchenko 2022).

These findings directly inform the decisions we are going to make in relation to project requirements and our concurrent use case diagram.

Interview

Our third and final use case exploration was in the form of an interview of a technical expert. The interview guide and interview notes can be found in Appendix C.

The interview was held in order to gain knowledge about what security risks a small business owner may face. As we want to develop an application that can help such users with improving their IT security, we saw that a discussion with an IT specialist about how such a system may work would be beneficial.

The informant has previously worked as head of IT Security and CEO of a small software company. The informant tells us that the IT setup for small businesses varies based on the size and nature of the business. There are lots of different software products available that can fulfill the businesses’ needs.

Small businesses’ IT setups have more in common with larger businesses’ now than they did earlier. This is because more easily manageable software products are available to small businesses today. However, the business's IT setup depends on what service the company provides. A hair salon only offers a service that takes place physically without IT systems. IT only supports the business in terms of bookings and handling money and customer data. Whereas a software company has another kind of offering, more dependent on IT. However, data protection is important to comply with any local regulations any business may have. Awareness is most important in general as this is the first step in creating internal processes and policies that describe how to navigate IT internally, and how the business will react if there is an attack.

The threats that a small business faces differ from those a larger business face. Attacks with malicious intent may not attack hair salons because their data isn’t as important. But phishing attacks are likely to happen to hair salon owners and employees, just as they happen to regular individuals as well. Therefore, having awareness training about concepts such as phishing and social engineering is really important, as most attacks are done through these methods and humans are the weakest part of a company’s IT security.

Our informant believes that customers usually look for a piece of software that can either advise on security or compliance, which is why these are separated. However, if a provider suddenly offers another branch of awareness in the existing software, then customers wouldn’t mind.

The informant tells us that our app shouldn’t be intrusive, as we don’t want the business owners to think that this is a big undertaking that takes too much of their time to learn. A great idea to improve the app is to gamify it and give the business owners trophies for completing tests.

Lastly, the app shouldn’t share the statistics with employees in the company, as bad performance from an employee shouldn’t be laid out. Instead, the employees should want to talk about and brag that they have completed a new test successfully.

Conclusions

As we review our use context exploration, several issues and considerations are highlighted repeatedly and identified by various actors. These findings will guide our future design and decisions as we work towards our solution.

Notable points that will be some of our primary focus going forward are:

**Education**

In both our literature review and interview, humans were identified as the key security flaw in any business. Furthermore, the research showed that increased awareness and education has a profound effect on security measures and effectiveness in a small business. Our solution should have a large focus on educating the businesses’ owners and employees on common attacks, such as phishing, and on preventative measures one can take to prevent and diminish the effects of these attacks.

**Access control**

Following directly from the points above, limiting and controlling employees’ access to key data can diminish or completely negate the consequences of a cyber-attack. If employees cannot gain access to vital information, they cannot grant an adversary access either.

**Surveillance**

Our exploration revealed that small businesses primarily use cloud-based services. These services allow a rather precise monitoring of data access, meaning they could be used to recognize a breach whenever it happens. Ideally, our solution would work with these platforms to report breaches to the business owner and help inform how the adversary got access, leading to better security initiatives going forward.

**Certification**

While the literature showed that trust is vital in regards to a customer’s purchase decisions, our informant in the interview also highlighted that gamification could help improve engagement with our app, as employees would brag about completing courses or improving their knowledge. For our design, we will explore the possibility of making a certification tied to compliance and security that a business owner can use to advertise their data security policy, while simultaneously encouraging employees to stay on top of their security education.