GROUND LABS

FAQs/TAQs

ENTERPRISE RECON

v1.0 January 2023

This document is a repository for answers to the most frequently asked questions posed by prospects during the sales cycle and for those tough-to-answer (objection) questions that often come up. It's intended to be a living document that's updated quarterly with new questions and answers that you'd like to see addressed here.

Please submit your questions and we'll answer them and include them in the document. You can submit them to **productmarketing@groundlabs.com**

CONTENTS

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

1.0 Product

1.1 What is Enterprise Recon?

Enterprise Recon is a software solution developed, marketed and sold by Ground Labs.

It's a smart data discovery solution that enables organizations to find and secure (or remediate) payment card information, personally identifiable information (PII) and critical information across an enterprise's IT systems. It's able to scan across the broadest range of structured and unstructured data sources - whether stored on servers, desktops, file stores, email or databases, both on-prem and in the cloud.

1.2 What is data discovery?

Data discovery is a process that allows organizations to know what types of data are stored across its storage sources. It 'scans' systems and storage to detect patterns of data. From a security and privacy aspect, of most interest is the personal, sensitive, and confidential information that is found. Only when the data is 'discovered' can organizations make decisions about how it should secured and used to support business goals.

Data discovery is often a misunderstood practice. Commonly, it is seen as a technology process used in forensic and litigation proceedings. This could be a reason why important security technology is under-prioritised or ignored amongst data privacy and security professionals. However, it is vital to a healthy data management and risk management strategy.

1.3 How does Enterprise Recon address my data classification requirements?

Data classification is the process of organizing data into categories based on certain characteristics. The goal of data classification is to create a structure for data that makes it easier to understand and analyze. There are many ways to classify data, such as by type, by location, by time, or by relevance.

Data classification and data discovery can work together in several ways. For example, data classification can help to narrow down the scope of a data discovery process by providing a framework for identifying relevant data. Data discovery can also be used to identify patterns and trends in data that can be used to create new categories for data classification.

Enterprise Recon PRO provides integration with the data classification capabilities of Microsoft Purview. We are also looking at additional options for future classification capabilities within Enterprise Recon.

1.4 How does Enterprise Recon integrate with the major DLP and data classification solutions?

DLP stands for Data Loss Prevention. It is a type of security technology that is used to prevent sensitive or confidential

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

data from being leaked or exposed to unauthorized parties. DLP systems typically work by monitoring data as it is being accessed, transmitted, or stored and flagging or blocking any actions that violate the organization's security policies.

DLP systems can work alongside data discovery in several ways. For example, data discovery tools can be used to identify sensitive data that needs to be protected by DLP policies. DLP systems can then be configured to monitor and control access to this data and to alert the appropriate personnel if any unauthorized access or transmission is detected.

In addition, DLP systems can be used to monitor data as it is being accessed and analyzed during the data discovery process, to ensure that only authorized personnel have access to sensitive data, and that any data handling or analysis is done in accordance with the organization's security policies.

1.5 How many people does it take to manage Enterprise Recon in a small / medium / large enterprise, and what skill levels and training should they have?

Unlike other data management and security solutions, Enterprise Recon does not require a full-time team of people to manage its use within an enterprise – even a large enterprise. For most customers, it's a part-time capability for a single administrator in the data or security team.

Although it adds relatively little administration burden, it's increasingly important to view data discovery as part of the ongoing business-as-usual (BAU) operation. This is where automation of the discovery process is important in reducing administrative overhead.

1.6 I have no idea what our data volume requirement is, would it be permissible to license Enterprise Recon based on known entities like the number of servers or users?

Enterprise Recon licensing is based on data volume rather than number of servers or users. We can assist in estimating your data sizing requirements based on the systems, servers and users you have.

1.7 We are a channel partner and are not comfortable with your data volume licensing; none of our other vendors use this method and our customers don't like it either; how can you help us?

We can appreciate that data volume is another way vendors license in this space. We have tools that can assist you in estimation of data volume which you can use to help customers understand the data requirements for their organization or project.

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

1.8 From a licensing point of view we need to know exactly how much spend we are committing to over the next 3 years; how can we achieve this using data volume licensing, when the amount of data we will hold is unpredictable and may increase during the licence period?

Ground Labs is aware that data has many factors that can contribute to organizations' data growth and will work with our customers to help map licensing to data scanning requirements. We have also adjusted pricing to fit within various bands, so a customer has flexibility in considering the data volume needed.

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

2.0 Customer Requirements

2.1 I already have a DLP solution; why would I need your product as well?

As mentioned in question 1.4, DLP (data loss prevention) is a tool designed to block sensitive data being copied to USB sticks and other locations where it can be leaked to unauthorized locations. DLP is a useful capability but in itself, it doesn't know what information is sensitive. It's largely used as a catch-all to stop all data being leaked from the systems it's being used to 'protect'.

Data discovery is required to identify the systems that are carrying critical and sensitive data so that DLP can be targeted to protect that data. We tend to find that either there's sensitive data in more places than DLP is being used, or that DLP is being used to protect every system even those without any sensitive data and that more resources are being spent on the technology than is necessary.

Data discovery and DLP are complementary solutions that work effectively together but before DLP is put in place, you need to be confident that you've uncovered all the locations of your sensitive and critical data – that's what data discovery and specifically Enterprise Recon provide.

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

3.0 Regulation and Compliance

3.1 There is no data privacy legislation in my country; what's the point of looking at protecting PII?

More than 130 countries around the world now have data privacy legislation with more being added every year. There are several reasons why even if your country doesn't currently have its own legislation, that you should be looking at protecting your personally identifiable information (PII). These include:

- Although your country may not have legislation on the statute today, it may well be being planned. It's worth checking the timeline of any introduction and getting prepared in advance for changes to come.
- If you operate outside your borders, you need to be compliant with the privacy laws in every country in which you transact business. Countries using privacy laws have very heavy fines for those who cannot demonstrate secure handling of personal data.
- Customers expect and trust their personal data to be handled sensitively. Given a choice of vendors, they'll buy from the one that can demonstrate that they will handle their data securely. In the B2B world, this is often mandated in contractual requirements before a deal can be secured.
- Hackers and security threats don't care about borders. Not protecting PII means that the results of an attack or breach will be far more serious and costly. If sensitive data is encrypted and then stolen, it would be of little value to hackers.
- Protecting PII is the right thing to do.

3.2 Would we not be better off simply paying any fines for noncompliance rather than buying an expensive software tool?

We've seen that being done by some companies in the past. However, it's at best a temporary sticking plaster. Even for industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS) which every entity handling payment card data needs to adhere to, many of the points discussed above in 3.1 apply here too.

Most importantly, loss of customer trust may never be regained if your organization were not to treat their personal information carefully and it were to be breached. Most organizations agree that it's not a question of 'if' they'll be attacked but 'when'. At best, you're likely to lose business to a competitor seen to be more trustworthy and at worst, the threat of a serious data breach may be existential.

3.3 How does Enterprise Recon help us comply with PCI DSS 4.0?

PCI DSS 4.0 is the most significant update to the standard since the release of v2.0 back in 2010. PCI DSS v3.2.1 will stay in effect for two years as a transition period. PCI DSS v.3.2.1 will be retired on March 31 2024, after which time all entities managing payment card data will need to be assessed to v4.0 of the standard.

For the first time, v4.0 calls out data discovery specifically as a methodology that's needed to address certain require-

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

ments in the standard. These include the need to revalidate scope more frequently than before. To find out more, we have a several blog posts that can help:

https://www.groundlabs.com/blog/is-cardholder-data-discovery-a-requirement-in-pci-dss-4-0/
https://www.groundlabs.com/blog/pci-dss-4-0-myths-and-misconceptions/
https://www.groundlabs.com/blog/five-things-you-didnt-know-about-pci-dss-4-0/

https://www.groundlabs.com/blog/how-ground-labs-supports-pci-dss-compliance/

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

4.0 Competitors

4.1 What is Microsoft Purview?

Microsoft Purview is a data governance and data catalog platform that helps organizations discover, understand, and manage their data assets. It is designed to support data-driven organizations in their efforts to become more data-driven and to better understand and use their data.

Some key features of Microsoft Purview include:

- Data discovery: Purview helps organizations discover data assets across their environment, including data stored in on-premises systems, cloud services, and hybrid environments. It uses machine learning to identify and classify data, and provides a searchable catalog of data assets.
- Data lineage: Purview helps organizations understand the origin and movement of data within their environment by providing data lineage information. This includes tracking data as it is transformed, moved, or integrated with other systems.
- Data governance: Purview provides tools and features to help organizations establish and enforce data governance policies and procedures. This includes the ability to set data access controls, track data usage, and monitor data quality.
- Integration with Azure: Purview is integrated with Azure, allowing organizations to take advantage of Azure's data analytics and machine learning capabilities. This includes the ability to run data transformations and analytics on data stored in Purview using Azure services such as Azure Data Factory and Azure Synapse Analytics.

In terms of competitive analysis, Microsoft Purview is similar to other data governance and data catalog platforms, such as Alation and Collibra. It is also similar to data management platforms like Talend and Informatica. One key differentiator for Microsoft Purview is its integration with Azure, which may make it particularly appealing to organizations already using Azure for their data analytics and machine learning needs.

4.1.1 We are a 100% Microsoft shop; couldn't we just use the standard Microsoft toolset?

For some organizations that may be the right route to take. However, there are other factors that should be taken into consideration. These include:

- Can you be sure all your data is in Microsoft systems or systems covered by Microsoft security solutions? Most organizations (~70%) we speak to admit to not knowing where all their sensitive data exists. That's because users may make copies, data may exist in legacy or siloed systems and a hundred other reasons. Enterprise Recon is the most comprehensive data discovery solution which scans data stores with the widest reach to the deepest level. It has been designed to work in Microsoft, mixed and non-Microsoft environments. It's very likely we'll find sensitive data that the Microsoft solution alone will not.
- Microsoft solutions often require expensive, complex and opaque licensing schemes. They are designed to

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

upsell their server solutions which can become very expensive over time. Enterprise Recon is a best-of-breed data discovery solution that works very well in a Microsoft environment and provides deterministic pricing so you know up front exactly what it will cost for the first year and beyond.

4.2 Who is BigID?

BigID is a data discovery and data governance platform that helps organizations discover, classify, and protect their data assets. It is designed to help organizations understand and manage their data in order to comply with privacy regulations and to better utilize their data for business purposes.

Some key features of BigID include:

- Data discovery: BigID helps organizations discover data assets across their environment, including structured and unstructured data stored in on-premises systems, cloud services, and hybrid environments. It uses machine learning and natural language processing to identify and classify data and provides a searchable catalog of data assets.

  In addition to discovering structured and unstructured data, BigID also helps organizations discover "dark data" – data that is not being actively used or managed by the organization. This can include data that is no longer needed or is redundant, duplicate, or obsolete. Discovering and managing this data can help organizations reduce storage costs and improve data governance.
- Data classification: BigID helps organizations classify data according to various criteria, such as data type, sensitivity level, and business value. This allows organizations to better understand and prioritize their data assets, and to set appropriate data access controls and governance policies. This classification can be done manually or automatically using machine learning algorithms.
- Data protection: BigID provides tools and features to help organizations protect their data assets, including the ability to set data access controls, track data usage, and monitor data quality. It also helps organizations identify and address data risks and vulnerabilities, such as data leaks or unauthorized access.

  In addition to setting data access controls and tracking data usage, BigID also provides tools for data masking and data de-identification. Data masking involves replacing sensitive data with fictional or dummy data, while data de-identification involves removing or obscuring personally identifiable information from data. These techniques can help organizations protect sensitive data while still being able to use it for business purposes.

In terms of competitors, BigID is similar to other data discovery and data governance platforms such as Microsoft Purview and Alation, which also offer data discovery, classification, and protection capabilities. BigID may differentiate itself from these competitors based on its focus on "dark data" discovery, as well as its data masking and de-identification capabilities. One key differentiator for BigID is its focus on data classification and protection, which may make it particularly appealing to organizations looking to comply with privacy regulations such as GDPR or CCPA. BigID is also similar to data management platforms like Talend and Informatica, which offer data integration and transformation capabilities in addition to data discovery and governance.

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS

4.3 Who is Varonis?

Varonis is a software company that provides data security and governance solutions for businesses. Its Data Discovery and Classification platform helps organizations to understand and secure their data by identifying sensitive and risky data, detecting unusual data access, and monitoring for data breaches. Some key features of the Varonis Data Discovery and Classification platform include:

- Data discovery: Automatically discovers, classifies, and maps data across the organization, including structured and unstructured data stored on-premises and in the cloud.
- Sensitive data detection: Identifies sensitive data such as personally identifiable information (PII), financial data, and intellectual property, and alerts the organization to potential data breaches.
- Data access monitoring: Monitors and records access to data, including user activity and file access, to help organizations detect and prevent unauthorized access or data exfiltration.
- Risk assessment: Assesses the risk level of data based on a variety of factors, including data sensitivity, user activity, and access controls, and provides recommendations for improving data security.

Some potential competitors to Varonis in the data discovery and classification space include Digital Guardian, McAfee, and Symantec. These companies offer similar solutions for data discovery, sensitive data detection, and data access monitoring, but may differ in terms of specific features and pricing.

4.4 Who is Spirion?

Spirion is a leading provider of data discovery and sensitive data protection solutions for businesses and organizations. Its products are designed to help organizations locate, classify, and secure sensitive data in order to comply with regulations and protect against data breaches.

One of the key differentiators of Spirion's data discovery products is their ability to locate and classify a wide range of sensitive data types. The software is able to scan a variety of file types and locations, including desktops, servers, network shares, and cloud storage, and identify sensitive data such as credit card numbers, social security numbers, and health information. This comprehensive approach to data discovery helps organizations identify and secure all of their sensitive data, rather than just a subset of it.

In addition to its data discovery capabilities, Spirion also offers a range of tools and services to help organizations secure their sensitive data. These include data masking, which allows organizations to de-identify sensitive data while still retaining its integrity for testing and development purposes; data shredding, which securely removes sensitive data from systems; and data archiving, which helps organizations maintain records of sensitive data for compliance purposes.

One potential area of weakness for Spirion is its pricing. Its solutions may be more expensive than those offered by some of its competitors, which could be a barrier for some organizations. However, the comprehensive nature of Spirion's solutions and the wide range of data types they can locate and classify may justify the higher cost for some organizations.

Overall, Spirion is a strong player in the data discovery and protection market, with a range of comprehensive and effective solutions. Its main competitors include Symantec, McAfee, Digital Guardian, Varonis, and Proofpoint. Each of these companies offers a range of data discovery and protection solutions, but Spirion's ability to locate and classify a wide range of sensitive data types sets it apart from the competition.

CONFIDENTIAL — INTERNAL USE ONLY © 2022 GROUND LABS