

ENTERPRISE DATA DISCOVERY FAQS

How does your data discovery and classification process work from start to finish?

S3 Security begins by working with your team to define the types of sensitive, regulated, confidential, or proprietary information you want to identify and the systems, repositories, locations, and supported cloud environments that should be included in scope.

We then define the search criteria and work with your team to establish the accounts, permissions, connectivity, and scanning infrastructure required for the engagement. Depending on the environment, this may include installing scanning agents. Scanning windows are coordinated with your team to minimize operational disruption.

Once discovery is complete, our engineers review the results and eliminate as many false positives as possible before presenting findings to your team. We then work collaboratively with your stakeholders to determine which findings appear confirmed, which can be ruled out, and which may require additional investigation.

Where appropriate, we discuss remediation options and, where supported, can perform approved remediation after receiving client authorization. Final reporting documents what was identified, what was remediated, and what remains outstanding.

One distinction we would make around the term classification: our discovery process can be configured to identify specific types of sensitive information, including organization-specific or proprietary data. It should not be viewed as an automated enterprise data classification program that applies formal classification labels across the environment.

Can you effectively discover sensitive data across both on-premises and cloud environments?

Yes, across supported environments.

S3 Security can conduct discovery across a broad range of on-premises and cloud-based data sources, including servers and workstations, databases, file and network storage, email environments, Microsoft 365 and collaboration platforms, cloud storage, shared repositories, and other supported enterprise data sources. The existing service scope also identifies physical devices, databases, cloud storage, email, and SharePoint as scanning targets.

Discovery and remediation capabilities are not identical across every platform. For example, we can scan Google Drive and review and validate the findings, but remediation within that Google Cloud environment must be performed by the client. S3 Security can still reduce the client's workload by helping distinguish likely false positives from confirmed findings before remediation begins.

ENTERPRISE DATA DISCOVERY FAQS

What infrastructure, agents, or other prerequisites are required to perform scanning?

Requirements depend on the systems and environments included in scope.

During planning, S3 Security works with your team to identify the accounts, permissions, network connectivity, and scanning infrastructure required. Some on-premises environments may require scanning agents, while other targets can be accessed through different supported scanning methods.

Cloud environments generally require appropriate accounts, permissions, and connectivity so the scanning infrastructure can access the data included in scope. The existing service scope similarly identifies network/device access, agent installation assistance, firewall considerations, and access to cloud and Microsoft 365 environments among client requirements.

We also coordinate scanning windows with your team to minimize potential operational disruption. In our engineers' experience, data discovery scanning has not created significant lag or resource-consumption issues, but we still plan the scanning schedule around the client's operational needs.

How do you handle decentralized environments where data resides across multiple entities, locations, or platforms?

The core methodology does not materially change.

For decentralized environments, S3 Security replicates the discovery process across the targets, locations, or entities necessary to address the defined scope. Each applicable environment is prepared and scanned using the appropriate supported method, with findings reporting back to the central management environment for analysis.

This allows a consistent discovery methodology to be applied across multiple business units, geographic locations, platforms, repositories, or acquired organizations while providing centralized visibility into the results.

This can be particularly useful in an M&A environment, where an organization may inherit sensitive information across multiple newly acquired entities and technology environments and need to establish a clearer understanding of where that information resides.

ENTERPRISE DATA DISCOVERY FAQS

What does remediation typically entail once sensitive or regulated data is identified?

Not every confirmed finding requires remediation. Some sensitive information may be located where it belongs and protected appropriately, while other findings may represent unnecessary copies, data stored in unexpected locations, or information that no longer serves a legitimate business purpose.

S3 Security reviews confirmed findings with your team and discusses appropriate remediation options based on the data, its location, business requirements, and the capabilities of the target environment. Where supported, remediation may include actions such as deletion or encryption.

In most environments, S3 Security can remotely delete the data as determined by the client. However, remediation capabilities vary by environment. For example, S3 Security can scan Google Drive and review the resulting findings, but we cannot perform remote remediation actions within that Google Cloud environment. In those cases, our engineers can identify likely false positives and confirmed findings, helping narrow the information your team needs to investigate and remediate directly.

No remediation is performed without client authorization. Your team has the opportunity to investigate findings and determine the appropriate action before data is changed or removed.

At the conclusion of the engagement, S3 Security provides reporting documenting findings, remediation performed where applicable, and items that remain outstanding. The current service exhibit likewise identifies findings and remediation reporting as engagement deliverables.

How do you address data sovereignty and regional privacy requirements when scanning data in different countries?

This is an area we would want to evaluate carefully with your team based on the countries and regulatory requirements involved.

From a technical standpoint, the sensitive data identified during discovery is not copied back to the central management server. This helps reduce unnecessary movement of sensitive information during the discovery process.

For a multinational engagement, we would work with your team to understand the environments and locations involved and would expect applicable legal, privacy, and data residency requirements to be identified during engagement planning so they can be considered in the discovery approach.

ENTERPRISE DATA DISCOVERY FAQS

What are typical timelines for discovery, classification, and remediation activities?

Timelines vary considerably based on the size and complexity of the environment. Factors that can influence the engagement timeline include:

- Number and types of systems or repositories being scanned
- Volume of data included in scope
- Number of entities, locations, or environments involved
- Complexity of access, permissions, and deployment
- Number of potential findings requiring engineer review
- Time required for client investigation and validation
- Volume and type of remediation requested

Because the analysis and remediation portions of the engagement depend heavily on what is discovered, a meaningful timeline generally cannot be established until we understand the environment and scope.

Once we understand the systems, data volumes, locations, and information types involved, S3 Security can develop a more realistic engagement timeline.

How does your pricing model work when the volume of data and scope may vary significantly from one acquisition to another?

Because Enterprise Data Discovery engagements can vary significantly in size and complexity, pricing is based on the scope of each engagement, usually by terabytes of data.

Factors may include the number and types of systems and environments involved, data volume, deployment requirements, and the level of analysis and remediation required.

We first work with your team to understand the environment and objectives so we can develop a scope and pricing structure appropriate to the engagement.

Have more questions? Reach out to us to schedule a call with one of our data protection experts!

CONTACT US

972-378-5554

info@s3security.com
www.s3security.com

4975 Preston Park Blvd. Ste. 500
Plano, TX 75093